The Promise of Bitcoin and the Blockchain

BRETTON WOODS 2015

A product of

Consumers' Research
established 1929

Editor
Kyle Burgess, Consumers' Research

Primary Authors
Kyle Burgess, Consumers' Research
Joe Colangelo, Consumers' Research

Contributing Authors
Keith Ammon, NH House of Representatives
Alicia Carmona, Identity 2020
Michael J. Casey, MIT Media Lab/Digital Currency Initiative
Patrick Deegan, Open Mustard Seed & Personal BlackBox
Jinyoung Lee Englund, Digital Currency Council & FE Ventures
Juan Llanos, Blockchain Advisor and Consultant
Eric Martindale, Blockstream
Nick Szabo, Blockchain, cryptocurrency, and smart contracts pioneer
Victoria Van Eyk, ChangeTip
Jason Weinstein, Steptoe & Johnson LLP

Workshop Participants
Preeta Bansal, MIT Media Lab
Perianne Boring, Chamber of Digital Commerce
Alicia Carmona, Identity 2020
Michael J. Casey, MIT Media Lab/Digital Currency Initiative
Carol Van Cleef, Manatt, Phelps & Phillips, LLP
Patrick Deegan, Open Mustard Seed & Personal BlackBox
Jinyoung Lee Englund, Digital Currency Council & FE Ventures
Eric Martindale, Blockstream
Priya Samra, Chamber of Digital Commerce
Berin Szoka, Techfreedom
Victoria Van Eyk, ChangeTip
Michael Zeldin, BuckleySandler

Artwork
Mike Costelloe

Preface

The Mt. Washington Resort, nestled in the foothills of New Hampshire's Presidential Range, was seventy-one years earlier the site of a meeting that fundamentally changed the global monetary structure. The world was reeling from the aftermath of World War II and leaders feared that if countries failed to adopt functional monetary policies the global economy could fall into an abyss. The result was known as the Bretton Woods Accord and put the US Dollar, pegged to gold, at the center of the world's trade system, where it sits today.

One of the reasons this resort was chosen in 1944 was its remote location, which would permit delegates to break free from the distractions that may have occupied their attention in a busier setting. We chose the location for a similar reason and found that as we approached Bretton Woods, the rich, relaxing setting began to have its effect. We came as strangers, shuttling in from nearby hometowns and international airports. Libertarians carpooled with federal regulators and it was enlightening for all.

We believe that we now find ourselves in a situation not unlike that faced by our predecessors…

In discussing what we sought to secure through our work in Bretton Woods, we wanted to tackle more than we could possibly address in one workshop. We understood that, typically, those who try to make their product all things to all people end up making it nothing to any. That said, we hope this paper, as broad as it is in scope, can serve three important goals:

- Serve to inform those new to Bitcoin and blockchain technology of opportunities they may not have considered previously.
- Better inform members of the Bitcoin community of potential hurdles that may impede their ability to effect change, which they may not have realized.
- Serve as a primary document for how industry experts viewed Bitcoin and blockchain technologies in the year 2015.

A few notes on the subject of identifying opportunities for Bitcoin and the blockchain to disrupt and improve the world:

1. Goals exist both on a large, strategic scale such as human empowerment, and also on a more tactical scale, such as specific opportunities or use cases. Since many of these specific opportunities fit within multiple overarching goals, the first section will address overarching goals and tie specific opportunities to each of them.
2. The diversity of viewpoints represented by the authors of this paper means that the authors, and ultimately the signers, cannot endorse the idea that the realization of the enumerated goals are in themselves worth the cost of disruption, or that such a realization is in itself a goal worth pursuing.

At the core of Bitcoin is the ability to send money faster around the globe, improve property rights, and enable people who have never met to fully trust one another.

Joe Colangelo, Executive Director
Consumers' Research

Background

The concept of cryptographic currency is not new. Efforts to launch digital currencies began in the 1980s, with cryptocurrencies following closely behind in the 1990s. Over the years, several individuals and groups have attempted to create cryptographic currencies that can be used as a store of value, medium of exchange, and "proof of x," with "x" representing work, stake, concept, ownership, publication, or any other "provable" notion, which is independent from government issued fiat currency. What is new about today's cryptocurrencies, most notably Bitcoin and those modeled after it, is that their design is built upon an immutable distributed digital ledger with a problem-solving mechanism for mining digital "tokens" or "coins" that are fixed at a certain quantity once all tokens are mined.

Bitcoin began as a technical experiment released to a mailing list of cryptography enthusiasts in 2008 by an individual known only pseudonymously as Satoshi Nakamoto. Initially described as a "new electronic cash system that's fully peer-to-peer, with no trusted third party" (Vigna, Casey 41), Bitcoin has continuously evolved over the past seven or so years.

The idea of a universal currency without a centralized intermediary (like a bank or government) had been popular for years among diverse groups, such as cryptography experts, privacy advocates, and programmers; but it did not gain traction until a new system incorporated the additions described above. The immutable ledger – the "blockchain" – combined with incentives Nakamoto hoped would keep the system honest and protect it from hackers was what distinguished Bitcoin from its predecessors. (Vigna, Casey 43-45).

The most important aspect of Bitcoin's early growth was that to succeed, it needed to bring more people into the fold. The first adopter needs a second party to exchange bitcoin with – in the same way that anyone can create a system of exchange, but unless that currency is recognized by someone else, it is useless.

Another key facet of the system is that is has a controlled, finite supply; the release of new bitcoin tokens is slated to terminate in 2140 at 21 million tokens. This differentiates it even further from "centralized" currencies wherein issuers can merely print more money, which eventually leads to inflation.

Nakamoto's release of Bitcoin came one month after Lehman Brothers declared bankruptcy, setting the stage for the 2008 financial crisis. While it isn't clear whether this timing was intentional, it certainly came at a time when many people were losing trust in centralized currency and methods of controlling money.

Since its inception, the Bitcoin protocol has seen setbacks to its reputation such as the notorious online marketplace Silk Road, which utilized bitcoins to trade drugs, pirated material, and hacking and forging services. There has also been much debate about the protocol's ability to scale given the current "block size," which limits the quantity of transactions that can be processed at any given time. However, the community of bitcoin users – legitimate users – has also grown immensely. The community now boasts millions of users with millions of dollars' worth of bitcoins. The creator of Bitcoin, Satoshi Nakamoto, holds an estimated 1 million bitcoins, worth $430 million (as of December 31, 2015)[1]. Nakamoto largely went underground in 2010. However, as intended, the cryptocurrency's popularity as well as the range of use cases for its distributed ledger protocol have continued to grow despite the absence of its creator.

---

1. *Vigna, P., & Casey, M. (2015). The age of cryptocurrency: How bitcoin and digital money are challenging the global economic order. New York, New York: St. Martin's Press.*

Contents

Glossary

attribute authorities	authority that validates identity information and meets regulatory obligations while ensuring anonymity
bad actor	opportunistic individuals or entities lacking principle or regard for others who commit fraud, utilize unfair and deceptive trade practices, or selfishly exploit individuals, groups, or circumstances
Bitcoin	a digital asset and payment system that enables peer-to-peer transactions and relies on a network of nodes that form a distributed public ledger called the blockchain, which maintains a continuously growing record of transactions that can be verified on a decentralized and trustless basis
bitcoin	a digital token, which can be used as a digital currency, rewarded to miners for solving problems ("doing work"), the value of which incentivizes parties to devote computing power to the Bitcoin protocol
blockchain technology	a digital token, which can be used as a digital currency, rewarded to miners for solving problems ("doing work"), the value of which incentivizes parties to devote computing power to the Bitcoin protocol
block size	a limit on the maximum size of blocks in the blockchain, which limits the quantity of transactions that can be processed at any given time
cryptocurrency	a decentralized medium of exchange using cryptography to secure the currency and regulate the creation of new units on the distributed ledger
digital currency	an Internet-based medium of exchange with properties similar to those of physical currencies, but allowing for instantaneous transactions and borderless transfers
end users	clients, customers, or consumers who directly use and benefit from blockchain technologies (independent of knowledge of use)
exploration	research and development stage of a potential blockchain opportunity/use case
fritcion	a term for the transaction costs associated with making proprietary transfers in a market system
frictionless	the absence of transaction costs in a market system (frictionless market), as with direct peer-to-peer transactions
full implementation	stage where a blockchain opportunity is fully developed, active, and employed by multiple companies/organizations but without widespread use (i.e 1.0)
funders	financial backers, including donors who expect no financial return and investors who expect a financial return
goal	a long-term ambition which aims to achieve a desired result through the completion of various related shorter-term objectives
intermediaries	individuals or entities who serve as a link, guide, translator, negotiator, mediator, etc. between entities to reconcile differences or ensure mutual understanding, including: lawyers, lobbyists, and compliance officers

Glossary

initial implementation	nascent stages of executing a blockchain opportunity/use case, including smaller-scale trial implementation (i.e beta)
interchange	a term for the transactions and transfers in a market system
key players	any party with an important role in influencing an industry or determining the outcome of an activityt
legacy/incumbent services, institutions, or industries	Traditional financial establishments that conduct deposits, loans, and investments, including: commercial banks, investment banks, insurance companies, brokerages, investment companies, and non-bank financial institutions (such as credit unions, savings and loans associations, and money transmitters)
mass adoption	stage where a blockchain opportunity has achieved full implementation and widespread use on a national or international level that is more common than non-blockchain legacy counterparts (i.e. 2.0)
mesh network	a network in which each node relays data for the network through a cooperative system and self-healing algorithms that increase the reliability of data transmission
micro-loan	a very small loan, often considered far less than a loan that would be issued by a traditional financial institution
micro-payment	a payment of a very small value from one party to another, which requires frictionless transactions to be viable since any transaction fees would eliminate the value of the transaction
multi-factor authentication	an authentication procedure using multiple components (which can include a security key, password, pin, biometric, or other personalized information) in order to verify the identity of the parties in a transaction
multi-signature transaction (multi-sig)	a transaction requiring the signatures of parties involved in order to provide added security and validation prior to the transaction being broadcast onto the blockchain
opportunity	a circumstance that enhances human experience by improving upon or creating an entirely new system, structure, or process utilizing the blockchain
policy makers	legislative body enacting laws/rules regarding the employment of digital currencies and other applications of blockchain technologies
private key	a cryptographic key known only to the recipient of encrypted data that allows the recipient to decipher the data encrypted using the recipients public key
proof of “x”	concept in which “x” represents work, stake, concept, ownership, publication, or any other “provable” notion
public key	a cryptographic key that can be obtained and used by anyone to encrypt data intended for the particular individual associated with a particular key
regulators	government agency enforcing laws/rules regarding the employment of digital currencies and other applications of blockchain technologies

service providers	company or organization offering products that utilize blockchain technologies
self-sovereign	a standard that affords people control over how, with whom, and for what purpose their identity data gets shared and/or is used
service providers	company or organization offering products that utilize blockchain technologies
sidechain	a "branch" of the blockchain separate from the bitcoin blockchain, which allows users to make exchanges without the lag one experiences due to the high volume of data and exchange on the blockchain
status	phase of implementation of a use case
store of value	the measure of a commodity or asset, that has value and can be stored, retrieved, and exchanged at a later time.
traditional financial transaction	a formal institution such as a bank or credit union which deals in lending, investment and other financial services
threat	an indication of imminent harm that endangers or risks the success of an opportunity
token	a symbolic representation of an underlying asset
tokenization	the process of giving symbolic representation to an underlying asset
two-factor authentication	an authentication procedure using two components (which can include a security key, password, pin, or other personalized information) in order to verify the identity of the parties in a transaction
trust frameworks	a mechanism for achieving large-scale trust online
trusted computing	a broad term that refers to technologies and proposals for resolving computer security problems through hardware enhancements and associated software modifications
use case	
venture capitalists	individuals, companies, and foundations that drive the development of blockchain technologies through financial backing

"You never change things by fighting the existing reality. To change something, build a new model that makes the existing model obsolete."

Buckminster Fuller

I. GOALS

This paper identifies and explains the opportunities presented by blockchain technologies, the challenges faced by those opportunities, and potential ways to address those challenges. Given that there are likely countless opportunities presented by blockchain technologies, this paper focuses on the 17 most prominent, best researched, or most promising use cases of the technology. While there are a potential infinite number of discrete use cases of blockchain technologies, there is a narrower range of broader strategic goals blockchain opportunities seek to address. Many of the discrete use cases tackle similar objectives by using different tactics and therefore, can be categorized into groups based on their overarching goal. For the purposes of this paper, goal will be defined as a long-term ambition, which aims to achieve a desired result through the completion of various similar or related shorter-term objectives. This section identifies and explains the transformative goals that blockchain technology can achieve over time.

Goal Descriptions

The table below briefly describes the five overarching goals of blockchain technology use cases, as identified by the authors of this paper with consensus from numerous collaborators. They are: efficiency, consumer choice, access, privacy and protection, transparency, direct self-governance, and human empowerment.

Table 1.1 Description of Goals

Goal	*Brief Description*
I. Efficiency	Increased efficiency in systems and processes, such as administrative protocols, verification approval processes, financial transactions, and financial settlement, thereby lowering costs, saving time, reducing errors, minimizing waste, eliminating redundancies, increasing satisfaction, limiting information asymmetries, and fostering trust.
II. Consumer Choice, Access, Privacy, & Protection	Increased options and availability of goods and services to consumers who are either limited in choice or access due to preexisting barriers. Improved consumer privacy and protection.
III. Transparency	Increased and strengthened transparency in terms of the availability of information/records and the immutability of a distributed public ledger.
IV. Direct Self-Governance	Greater distribution of governance to individuals and collectives through the decentralization of authority.
V. Human Empowerment	Greater agency of individuals and collectives over their person, group, health, wealth, knowledge, property, and other factors affecting self-determination including access to information, public goods, rule of law, etc.

Goal I: Improving Efficiency

Inefficiencies exist throughout the various aspects of commerce, business, government, information sharing, resource allocation, and consumption. Some are unavoidable, such as those resulting from information asymmetries. Others can be overcome, such as outdated infrastructure, poorly trained workers, models or methods that have been outgrown, or much of the friction associated with interchange.

Goods, services, systems, processes, and technologies that increase efficiency can lower costs, save time, reduce errors, minimize waste, eliminate redundancies, increase consumer satisfaction, and help reduce information asymmetries. All of this helps to foster trust without the necessary "trusted third parties" that have traditionally been required in order to engage in trusted transactions. Lower costs resulting from improved efficiency greatly benefits consumers financially, while the remaining benefits can improve the quality of their experiences or even lives. Technology can increase the efficiency of systems and processes, such as such as financial transactions, approval processes, and administrative procedures. Blockchain technologies, specifically, can be utilized to foster these improvements in an innovative way that garners trust through transparency and decentralized record keeping.

For example, in terms of administrative procedures and approval processes, blockchain technologies could be employed to automate and distribute the execution log of a company's standard operating procedures or accounting procedures, thereby reducing inefficiencies caused by opacity, such as deficient knowledge or understanding of procedures, poor accountability, weak collaboration and distrust, and centralized management bottlenecks.

In terms of improved efficiency in financial transactions, there are already a number of companies offering services that employ blockchain technologies as a platform for transferring value/money/currency with reduced friction, such as the direct costs (i.e. fees, interest, commission, etc.) and indirect costs (i.e. opportunity cost or time value of money) of the transaction. Such technologies could ultimately supplant traditional payment mechanisms such as wire transfers (i.e. SWIFT and IBAN), automated clearing house (ACH) payments, or the various trading systems on which today's financial markets are built. This would ultimately lower the time it takes to process transactions as well as the cost associated with unnecessary, redundant, or superfluous steps and intermediaries.

Improved efficiency through blockchain technologies can have a dramatic effect on the reduction of time, energy, money, and frustration caused by waste, opacity, redundancy, poor resource allocation, and avoidable friction in transactions. Moreover, it can substantially increase the quality of work and life of those who embrace and adopt mechanisms to achieve it.

Opportunities:

- Streamlining Transactions & Improving Interchange
- Streamlining Financial Services Regulation
- Microtransactions
- Smart Contracts
- Identity Issuance
- Proof of Asset Ownership Smart Property
- Unlocking Capital through Tokenization
- Enabling Efficient, Effective, and Transparent Governance and Resource Allocation
- Efficient Provision & Management of Public Goods through Collective Action

Goal II: Expanding Consumer Choice, Access, Privacy, and Protection

Consumer choice, access, privacy, and protection are limited by existing paradigms. Current data protection and privacy systems, outdated or non-existent technological infrastructure, misaligned or lacking business incentives, or well-intentioned regulation with unintended consequences all

restrict the variety, availability, and level of security services offer to consumers. This results in lost value to consumers and businesses alike.

In terms of choice and access, a myriad of consumer choices are stifled by regulation, the prohibitive costs of offering such choices, or sometimes a combination of both. For example, financially constrained persons in the need of loans are often unable to access them, because banks are limited by the maximum interest they can charge to mitigate the higher risk associated with making such loans. These consumers are priced out of the traditional lending market and are limited to the high-interest, short-repayment-term loan options offered largely by payday or cash-for-title lenders.

In terms of privacy and consumer protection, consumers are often required to supply their personally identifiable information (PII) in order to utilize many services, even though much of the information requested is unrelated to the service itself (i.e. possibly collected for customer tracking or for sale to a third party). This leaves consumer privacy and data protection at the mercy of the security systems of service providers, opening them up to the risk of having their PII (including biometrics, such as fingerprints) hacked. Recently major companies and organizations, such as Target, JPMorgan Chase & Co., and even the U.S. Office of Personnel Management (OPM), have been hacked, exposing millions to the risk of fraud or identity theft. In other words, the current models and systems are not working.

Much value - financial as well peace of mind - can be gained by all parties (consumers, businesses, and government entities alike) through the meaningful expansion of consumer choice, access, privacy, and protection. Blockchain technologies enable the paradigm shift necessary to achieve such an expansion, by allowing for new data and privacy models that offer variety and inclusion, as well as better mechanisms for ensuring security. For example, cryptocurrencies, such as bitcoin, allow for the creation of new types of financial products, such as micro-loans, micro-payments, and multi-signature transaction (multi-sig), to foster the inclusion of the under or unbanked who wish to have greater access and options, or who are unable to safely store their wealth with formal financial institutions because of corruption or insolvency. Furthermore, blockchain-based companies have begun developing a system to establish credit scores for those previously without them (i.e. the unbanked and impoverished).

In terms of privacy, encryption services such as the tokenization of identification could be used to verify age for purchases or entry into establishments with a minimum age threshold, whereby blockchain technology serves as the verification system that validates the age of the person in question without unnecessarily granting access to a consumer's PII, instead, simply confirming that the individual is or is not of age to make the transaction or enter the establishment.

In terms of security, similar to the example above, companies are developing blockchain-based applications that enable individuals to encrypt and own their own data, allowing the tracking of unique individuals without actually identifying them. This prevents data breaches from having a significant impact on individuals by, housing their (consumer) data and PII separately and unlinked, safeguarding their identity.

Greater consumer choice, access, privacy, and protection can increase value to all parties involved. Consumers derive value from lower costs and an improved quality of life through greater access, while businesses derive value from increases in customers, sales, and market share, and governments derive value from lower threats to data security.

Opportunities:

- Streamlining Transactions & Improving Interchange
- Streamlining Financial Services Regulation
- Microtransactions

- Expanding Financial Access
- Smart Contracts
- Identity Issuance
- Unlocking Capital through Tokenization
- Enabling Efficient, Effective, and Transparent Governance and Resource Allocation
- Efficient Provision & Management of Public Goods through Collective Action

Goal III: Greater Transparency

Much of society operates in opacity, which propagates deficient understanding of rules and processes, inadequate accountability, weak or non-existent collaboration, bottlenecks of centralized management, and distrust of centralized authority. Honesty and transparency improve the visibility of errors, misappropriation, and misdirection. Corruption has fewer places to hide itself when all records are freely available for all to inspect. Increasing, strengthening, and in some cases allowing transparency in terms of availability of information, access to records, clarity of procedures and processes, etc. through distributed control or management can foster trust, efficiency, and legitimacy.

The blockchain serves as an immutable database of digital information. All data directly encoded (submitted as a valid, signed transaction and written to a confirmed block) on the blockchain is available and verifiable by any entity that has a copy of the full blockchain. The implementation of blockchain technologies allows for immutable, distributed public ledgers to instill trust, efficiency, and legitimacy. For example, in underdeveloped economies the costs of bribes, corruption, etc. are often significant, but could be reduced or eliminated by using a publicly auditable and verifiable digital currency system, providing immense gains for impoverished and disadvantaged parties. Blockchain technologies could also be employed to provide proof of reserves in banking systems, run companies on distributed ledgers, or trace government procurement flows or charitable distributions (i.e. voluntary self-reporting).

Greater transparency through blockchain technologies could increase accountability, provide more accurate monitoring and evaluation across government, non-profit, and for-profit entities while democratizing financial and service delivery systems.

Opportunities:

- Streamlining Transactions & Improving Interchange
- Streamlining Financial Services Regulation
- Smart Contracts
- Identity Issuance
- Proof of Asset Ownership Smart Property
- Unlocking Capital through Tokenization
- Enabling Efficient, Effective, and Transparent Governance and Resource Allocation
- Efficient Provision & Management of Public Goods through Collective Action

Goal IV: Greater Direct Self-Governance and Community/Peer-to-Peer Governance

Current social contracts delegate power over various aspects and forms of governance to centralized authorities, agencies, and institutions. In some cases, such as the monopoly on the legitimate use of force, relinquishing control to a centralized body may be a necessary social contract to ensure harmony and security. In other cases, such norms may have outgrown their usefulness or necessity, such as the regulation of taxicabs.

Decentralizing authority and increasing the distribution of governance to individuals and collectives, where the usefulness or necessity of centralization has been outgrown or become corrupted, enables greater direct self-governance and community or peer-to-peer governance. For example, decentralized tools like mesh networks allow communications in times of unrest, such as the use of Firechat to continue the flow of information during the 2014 Hong Kong protests. Blockchain

startups like Augur, Ombudsman, and others allow communities to crowd source information and ideas to self-govern and create tools for self-governance. Finally, with blockchain technologies, history cannot be amended any more than the public ledger can, helping to thwart censorship.

In regions where states and markets have failed or are weak, blockchain technologies provide opportunities for more direct community and self-governance, allowing communities in these regions to engage in a form of self-help in which they can create decentralized solutions to collective problems. Such decentralized local community solutions can allow these communities to leapfrog and partially bypass the development of some large, centralized institutions prevalent in regions with developed markets and states.

Where states and markets function effectively, blockchain technologies provide an alternative mode of partial social organization and governance that may be more decentralized, transparent and efficient and that may provide a source of healthy competition and innovation for big governments, financial institutions, and corporations -- thereby encouraging and showing a path toward more responsive governance by those traditional public and private institutions.

Greater self-governance through blockchain technologies can result in more amenable, efficient, equitable, and representative governance than current paradigms allow for, more effectively fostering trust and consensus among the various sectors of society.

Opportunities:

- Streamlining Transactions & Improving Interchange
- Streamlining Financial Services Regulation
- Expanding Financial Access
- Smart Contracts
- Enabling Efficient, Effective, and Transparent Governance and Resource Allocation
- Efficient Provision & Management of Public Goods through Collective Action

Goal V: Human Empowerment

Humans are often constrained by systems, processes, governance structures, financial limitations, educational barriers, inequitable resource allocation, and even distance. These constraints often appear to be out of their control, limiting their access, agency, and ability to achieve.

Human empowerment occurs when individuals and collectives are enabled to have greater agency over their person, groups, health, wealth, knowledge, identity, property, and anything else affecting their self-determination. Empowerment also includes the provision of greater access to information, rule of law, public goods (such as education, transportation, and health systems), or any other structure that increases opportunity for achievement.

There are many ways to achieve greater human empowerment. Notably, the use of technology has proven capable of doing so on an exponential scale. For example, the advent of the telephone enabled people to communicate with others vastly beyond voice and broadcast range. In a similar fashion, the mass adoption of the Internet granted people near-instant communication around the globe and across numerous platforms.

Blockchain technologies have the capability of achieving human empowerment by even greater orders of magnitude than those described above. Open and distributed ledgers can be employed to empower and connect people, including those who were previously without access, shifting power away from the center and toward the edges. The blockchain technology's unique properties of a decentralized, distributed, and transparent unit of exchange and ledger presents new opportunities for human empowerment. Unlike technologies where systems replace the need for human input or interaction, the blockchain empowers humans for the first time in history to actively participate

in enterprise-scale collective discussions and decisions through a medium that enables humans to actively withdraw consent from institutions, along with connecting people from diverse backgrounds and locations. This results in a more fluid ability for humans to communicate, collaborate and consent in a dynamic rethinking and creation of a new "social contract."

For example, in countries and cultures where there are restrictions or prohibitions to accessing the existing global financial system, such as the case of women in Afghanistan, the blockchain offers an alternative third option for receiving and sending funds. Thus increasing global financial inclusion by empowering a segment of society who was previously powerless to exercise their voice. Additionally, when applied to functions such as voting and smart contracts, a digital identity system utilizing the blockchain technology could eliminate the need for third parties and therefore presents the potential for a more efficient, trustworthy interaction.

Greater human empowerment through blockchain technologies can foster the discussion, consideration, and innovation of the social, political, and economic order and openness to reevaluate core assumptions of existing paradigms, resulting in the rethinking, readjustment, or re-ratification of social "contracts."

Opportunities:

- Streamlining Transactions & Improving Interchange
- Microtransactions
- Expanding Financial Access
- Smart Contracts
- Identity Issuance
- Proof of Asset Ownership Smart Property
- Enabling Efficient, Effective, and Transparent Governance and Resource Allocation
- Efficient Provision & Management of Public Goods through Collective Action

Opportunities

In the context of this paper, an opportunity is a circumstance that enhances human experience by improving upon or creating an entirely new system, structure, or process utilizing the blockchain, thereby championing one of the five overarching goals identified above. These opportunities are often described in terms of which stage they belong to - Blockchain 1.0, 2.0, and 3.0.

Blockchain 1.0 - Currency and Payments

Blockchain 1.0 is the first round of blockchain technology applications. It refers to the underlying technology platform (i.e. the blockchain - mining, hashing, and the public ledger), the overlying protocol (i.e. transaction enabling software), and the digital currency (i.e. bitcoin or other digital tokens/coins) which represent a store of value as well as provide value to the protocol itself. Blockchain 1.0 applications are primarily concerned with using the blockchain to conduct payment activities through software built "on top" of the blockchain (or in sidechains or independent protocols that are entirely separate from the Bitcoin blockchain) using digital tokens, coins, or currencies.

Blockchain 2.0 - Smart Contracts, Programmable Assets, Decentralized Autonomous Entities, and Proof of "X"

Blockchain 2.0 refers to the broad spectrum of economic and financial applications that exist beyond simple payments, transfers, and transactions. Such applications include traditional banking instruments such as loans and mortgages, complex financial market instruments such as stocks, bonds, futures, derivatives, as well as legal instruments such as titles, contracts, and other assets and property that can be monetized. While some of these applications are still in the nascent stages

of development, many are well on their way to becoming a reality.

Blockchain 3.0 - Non-Economic Applications

Blockchain 3.0 refers to vast array of applications that do not involve money, currency, commerce, financial markets, or other economic activity. Such applications include art, health, science, identity, governance, education, public goods, and various aspects of culture and communication. The majority, if not all of these applications are in nascent stages of development or still even in the "idea phase."

Specific opportunities presented by blockchain technologies will be covered in depth in subsequent sections of this paper; however, the infographic below is a comprehensive representation of the opportunities identified and addressed in this paper categorized by which stage they stem from.

The narrow aims these various blockchain technology use cases seek to accomplish have distinct areas of overlap, which lend themselves to clear categorization within the overarching goals outlined above. The table below groups the various opportunities presented by the blockchain by the overarching goal they help further.

Key Players

For each opportunity presented by blockchain technologies there are a relevant set of key players that either influence, or are influenced by, the execution of the opportunity. The table below lists key players as identified by the authors of this paper with consensus from numerous collaborators.

Status

While some applications or use cases of blockchain technology are partially or even fully implemented, many are in nascent stages of development. The table below lists and defines the phases of implementation, or status of the use case, as will be referenced throughout this paper.

For each opportunity, a number of factors affect expected movement - how slowly or quickly the development and adoption of the opportunities presented by these blockchain technologies will occur. Some influencing factors are drivers (internal and external forces), such as popularity of the application or VC funding, others are impediments (hindrances or obstructions), such as lack of funding or lack of clarity surrounding regulations.

Figure 1.2

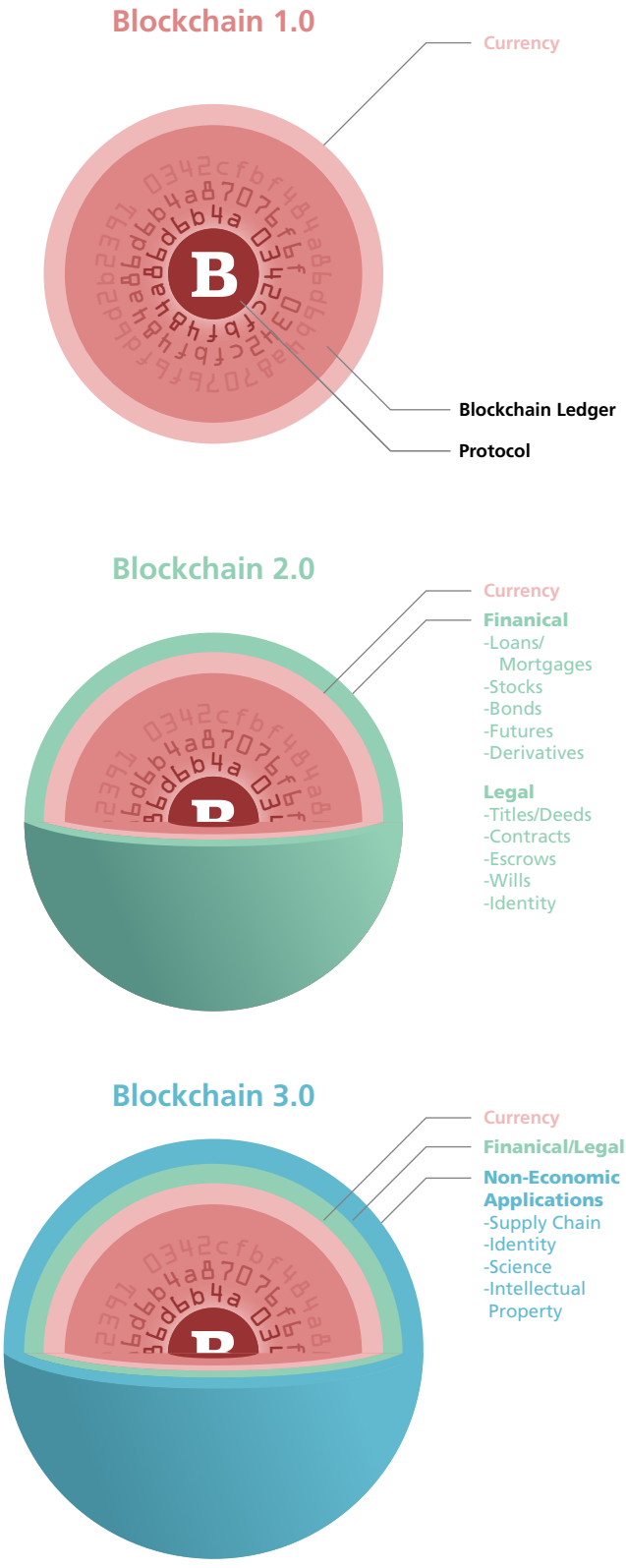

Table 1.3 Description of Key Players

Key Players	*Description*
End Users	Clients, customers, or consumers who directly use and benefit from blockchain technologies (independent of knowledge of use).
Service Providers	Companies or organizations offering products that utilize bitcoin or blockchain technologies.
Relevant regulators and policymakers	Government agencies or legislative bodies enacting or enforcing laws/rules regarding the employment of digital currencies and other applications of blockchain technologies.
Venture Capitalists (VCs)/Funders	Individuals, companies, and institutions that drive the development of blockchain technologies through financial backing.
Legacy/Incumbent Services and Institutions	Traditional financial establishments that conduct deposits, loans, and investments, including: commercial banks, investment banks, insurance companies, brokerages, investment companies, and non-bank financial institutions (such as credit unions, savings and loans associations, and money transmitters).
Bad Actors	Opportunistic individuals or entities lacking principle or regard for others who commit fraud, utilize unfair and deceptive trade practices, or selfishly exploit individuals, groups, or circumstances.
Intermediaries	Individuals or entities who serve as a link, guide, translator, negotiator, mediator, etc. between entities in order to reconcile differences or ensure mutual understanding, such as advocates, lawyers, lobbyists, compliance officers, etc.

While drivers and impediments influence the likelihood of whether an opportunity will be realized, the greatest determinant of the realization of an opportunity is its ability to overcome threats. A threat, as distinguished from an impediment, is an indication of imminent harm that endangers or risks the success of the opportunity. In the case of blockchain opportunities, some threats exist currently, whereas others may manifest in the future. The table below defines the scale of likelihood a potential threat will come to harm a blockchain opportunity.

As threats differ in their ability to impact blockchain opportunities, the table below defines the scale of severity threats pose.

Table 1.4 Status of Opportunity

Phase of Implementation	*Brief Description*
Exploration	Research and development stage of a potential blockchain opportunity/use case.
Initial implementation	Nascent stages of executing a blockchain opportunity/use case, including smaller-scale trial implementation.
Full implementation	Stage where a blockchain opportunity is fully developed, active, and employed by multiple companies/organizations but without widespread use.
Mass adoption	Stage where a blockchain opportunity has achieved full implementation and widespread use on a national or international level that is more common than non-blockchain legacy counterparts.

Recommendations

Finally, this paper identifies and explains recommendations or potential solutions for addressing these threat. Such recommendations will be given in terms of:

- Guidance to consumers, businesses, "blockchain community," core developers, and other users
- Guidance to legacy/incumbent institutions, organizations, and industries
- Guidance on regulatory compliance
- Guidance on improving current regulation or informing future policy making and regulation
- Other guidance on achieving adoption

Table 1.5 Threat Likelihood Scale

Likelihood	*Description*
Highly unlikely	Circumstances would have to change drastically in order for this threat to become a serious concern.
Somewhat likely	This threat has the potential to become a serious concern, but it remains relatively unlikely.
50/50 likelihood	This threat is just as likely to come to fruition, as it is not to come to fruition.

Table 1.5 Threat Likelihood Scale

Likelihood	*Description*
More likely than not	This threat is just as likely to come to fruition, as it is not to come to fruition.
All but certain	Circumstances would have to change drastically in order for this threat to NOT become a seriou s concern.

While drivers and impediments influence the likelihood of whether an opportunity will be realized, the greatest determinant of the realization of an opportunity is its ability to overcome threats. A threat, as distinguished from an impediment, is an indication of imminent harm that endangers or risks the success of the opportunity. In the case of blockchain opportunities, some threats exist currently, whereas others may manifest in the future. The table below defines the scale of likelihood a potential threat will come to harm a blockchain opportunity.

Table 1.6 Threat Severity Scale

Severity	*Description*
Minor	Can be overcome with minimal effort
Moderate	Could delay full implementation
Major	Could restrict broad implementation but will likely not hinder its eventual achievement if minor effort is made
Existential	Can eventually be overcome with a strong, coordinated effort over time
Insurmountable	Can likely NOT be overcome

II. OPPORTUNITIES

A. Blockchain 1.0

I. Streamlining Transactions & Improving Interchange

I. Discrete Opportunity/Use case

In this first section, we're going to talk just about the first application of the blockchain, namely the creation and use of the world's first truly virtual currency. When we talk about streamlining transactions and improving interchange, we're talking about the ability for a monetary system to become more efficient when it's run on a blockchain rather than its current logistical network.

The use of bitcoin tokens as money is currently the most prolific use of blockchain. The primary usage of the Bitcoin blockchain has been to exchange these bitcoins between users in monetary transactions.

What, if any, advantages does bitcoin hold over traditional currency and settlement methods?

Bitcoin's pseudonymous founder, Satoshi Nakamoto, described Bitcoin as "an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party." This solves a problem that is rarely on the minds of consumers or even technologists, since the problem dates to the origin of money itself. As commerce evolved from being based on barter, to minted coins to paper, it gained greater efficiency but developed a problem whereby consumers had to trust third parties for a host of services to include money creation, solvency, and accounting.

For example, when the United States was on a gold standard, users of U.S. currency trusted that the central bank had adequate reserves to redeem all treasury notes in circulation. Today, users of Federal Reserve Notes trust that the central bank won't devalue their currency through inflation. On a daily basis, consumers also trust banks to remain solvent, merchants and payment processors to keep their databases secure from attack, and credit card companies to protect them in the event of fraud.

This consumer trust has often been misplaced. Banks that established some of the greatest levels of trust among consumers failed famously in the 2008 financial crisis. Central banks the world over have diluted their currencies or, as seen most recently in Cyprus, seized depositor assets without warning. Bad actors, such as Jordan Belfort's Stratton Oakmont, have used the ways in which consumers are conditioned to trust financial institutions to perpetrate lucrative scams. The livelihood of a confidence man rests upon the ability to instill confidence in a disreputable actor.

Here is where the value of Bitcoin becomes apparent. It addresses the need to trust central banks in two ways. First, Bitcoin divulges its exact level of inflation over the next 115 years so that users and holders of Bitcoin do not have to trust policymakers to always act in consumers' best interests all of the time. Second, Bitcoin allows consumers unfettered access to their capital. A Cyprus-style deposit seizure is impossible in a Bitcoin world where consumers control their bitcoin wallets.

Bitcoin as money also has potential to solve the need to trust financial institutions to remain solvent – because Bitcoin's record of transactions is public, an institution can perform a proof-of-assets audit in open view of the public. Since MtGox famously collapsed in early 2014, several bitcoin exchanges have conducted these fully visible audits. In the future Bitcoin has the potential to enable 24/7 monitoring of the assets of an institution.

Bitcoin also promises a more secure financial transaction than can be offered by present-day clearinghouses and credit cards. The Bitcoin protocol operates on a distributed network of (currently) over 8,000 independently operated nodes. The nature of this network is such that it would be so difficult to attack that hackers will avoid doing so altogether in the absence of a critical vulnerability. The encryption behind the network, SHA-256, would take 650 million billion (6.5x1017) years for the world's fastest supercomputer to break.

This opportunity includes almost every possible financial transaction possible, including:

Consumer to Consumer transactions – Person-to-person transactions have grown in popularity in the past few years with popular platforms like Venmo, Paypal, Apple, and Google launching applications that empower consumers to send money directly to other consumers. These transactions typically originate from and end with traditional banking infrastructure. With these services a sender provides a credit card or bank account information and the recipient provides their bank account information to receive their ultimate, usable deposit. Depending on the service and the amount being transferred, these transactions take between one and four business days for the money to go from one bank account to another. With bitcoin, as soon as the transfer is confirmed, it is a liquid asset in the recipient's wallet.

Consumer to Business transactions - The low fee for sending bitcoin between wallets reduces the cost for businesses of accepting payments for goods and services by eliminating middlemen.

Coinbase, the second-largest merchant bitcoin processor, describes the advantage for merchants as the following:

> Credit card fees are a significant cost for most merchants, who typically pay processing fees between 2% and 4% of the revenue from each transaction. These fees are usually higher for online merchants because of increased fraud risk. Receiving Bitcoin payments is completely free for merchants. The customer pays a small transaction fee which is free if they're paying from their own Coinbase account. Otherwise it's the equivalent of about 1 to 5 cents.
> B2B… [1]

International remittances - The majority of international remittances are consumer-to-consumer transactions from developed to undeveloped nations. Current remittance platforms involve brick-and-mortar operations both for the sender and recipient. The costs incurred by the sender make up a significant portion of the total remittance. In a 2010 study, The Economist found that the cost for a $200 remittance between most countries averaged between $18 and $26, or between 9% and 13%. With $440 billion in remittances in 2014, that equates to a regressive tax on the world's poor of over $47 billion.

Bitcoin doesn't care about borders. It takes the same time and incurs the same fee to move from two nodes on the Bitcoin network, regardless of their geography or local currency. Bitcoin has the potential to save poor workers and their families tens of billions of dollars every year.

Streamlining transactions and improving interchange fees contributes to the following overarching goals:

- I) Efficiency: Reducing fees for all types of transactions and making money "smarter, faster, stronger" creates a more efficient world.

---

1 *https://support.coinbase.com/customer/portal/articles/1835464-why-should-i-accept-bitcoin-payments-*

- V) Human Empowerment: The ability to send, own, and receive money anywhere in the world without dealing with third parties. This is not a major change for citizens of nations with more developed banking sectors, but is a complete revolution for developing nations, billions of whom don't have access to basic banking services, much less low-fee person-to-person transactions.

- II) Consumer Protection: Consumers have the potential to benefit from assets less able to be stolen through brute force, banks that are more secure from attack, lower fees for the transfer and management of their money, and a currency that cannot be debased by a centralized authority.

Key Players

End users - Retailers, consumers, and financial institutions comprise the main group of end users whose transfer of money and value has the potential to become more efficient through the adoption of digital currency and blockchain-driven innovations.

Service providers - Examples of current service providers include companies which facilitate P2P bitcoin transactions, bitcoin transaction processing for retailers, or bitcoin remittance platforms.

- Leading companies that facilitate P2P bitcoin transactions include: Coinbase, Changetip, Circle, Xapo, and Bitcoin Core (the main software that runs the decentralized Bitcoin protocol).

- Companies that process bitcoin transactions for retailers include: Bitpay, Coinbase, and Gocoin.

- Companies that operate remittance platforms using bitcoin include: BitPesa, Hellobit, Abra, Romit, and Rebit

Relevant regulators and policymakers: We have seen a number of agencies and authorities take interest in or move to regulate the use of bitcoin, a consequence of its use as money.

- In America, a number of regulatory agencies have taken an interest in or claimed a level of jurisdiction over bitcoin. These agencies include but are not limited to the U.S. Treasury's Financial Crimes Enforcement Network (FINCEN), Department of Justice (DOJ), Securities and Exchange Commission (SEC), Consumer Financial Protection Bureau (CFPB), and Federal Reserve.

- Internationally, the nation-state governments have varied wildly in their reactions. Below are a few examples:

- It is illegal to purchase or use bitcoin in Iceland, Ecuador, and Bolivia.

- By the end of 2015 Russian legislation had planned to implement fines for users who are found to be "creating, mining, or issuing Bitcoin or other digital currencies."

- Many European countries have given bitcoin's use the same tacit green light that it has received in the United States, with varying levels of compliance requirements and taxation structures.

Venture Capitalists (VCs)/Funders:

- Some notable bitcoin investors who have invested in many bitcoin companies, including those mentioned above, include the Digital Currency Group, Pantera Capital, Winklevoss Capital, and Blockchain Capital.

- Additionally, there have been a number of legacy institutions which have invested in some of the major bitcoin companies, including Goldman Sachs, BBVA, USAA, and the New York Stock Exchange.

Legacy Services and Institutions: Legacy institutions in this space can be divided into three main categories

- Consumer to Consumer value transfer: Includes Paypal, Venmo, and banking institutions. Though not a company, cash is the ultimate P2P value transfer mechanism and can be viewed as a legacy infrastructure in this category.

- Consumer to Business value transfer: Includes credit card processing companies such as Square, Intuit, and Verisign, as well as credit card companies such as American Express, Visa, and Mastercard.

- Business to Business value transfer: Includes mostly banks that service businesses, to include all major U.S. banks and many regional ones.

Bad Actors

- These include those utilizing bitcoin for illegal or immoral activity. There was much debate in the construction of this paper as to how to define these. Often, we know them when we see them, and these parties include those selling weapons, counterfeit money, or child pornography over the Dark Web in exchange for bitcoin. Often the distinction is less clear, such as someone in Venezuela using bitcoin to purchase a commodity that's illegal to purchase in their country but legal and accepted elsewhere.

Intermediaries

Status

Bitcoin as money, with the potential to streamline transactions, is one of the applications that can be taken full advantage of with the basic core technology and a few applications for user interaction. As such, it's one of the furthest advanced of the opportunities. With over $1 billion invested in bitcoin companies so far, the applications for using bitcoin as money are numerous. Options for P2P, P2B, and international remittances are advanced and implemented. That said, the adoption of Bitcoin and blockchain technology has not yet taken off, and we don't know how long it will take (if ever) until we see the use of bitcoin as money enter its "mass adoption" phase.

Goals

Bitcoin's ability to streamline transactions and improve interchange will have a significant impact on fostering each of the overarching goals: efficiency, human empowerment, direct self-governance, transparency, and consumer choice, access, privacy and protection.

Threats

Identification of threat(s) and likelihood of occurrence as of 2015.

Threat 1: Overly burdensome regulation.

This is a multi-faced threat and will therefore be broken down into sub-threats 1a - 1d:
Financial regulation (AML/KYC):

a. Regulation to prevent Unassured safety and soundness
b. Regulation to mandate greater consumer protection
c. Regulation to protect powerful incumbents

Threat 1a: Anti-Money-Laundering (AML) and Know-Your-Customer (KYC) regulations: These regulations are designed with the end-goal of reducing the ability for criminals to access the modern international financial system to aid in the commission of crimes. On the front-end, these are designed to make it more difficult for criminals to be paid for a good or service in the first place. On the back-end, they strive to also make it more difficult for those who have received money for illicit activities to return that money to the financial system through laundering. Covered financial institutions must have AML programs. These institutions have expanded to cover more businesses over the past decade, and some bitcoin businesses might be surprised to find just how much work they should be devoting to compliance in this area.
Anti-Money-Laundering (AML) regulations require banks and money-transmitters to take steps to detect and prevent money laundering, codified by the Bank Secrecy Act of 1970. This involves filing reports of various types that constitute an alphabet soup of reporting requirements (CTR, SAR, CMIR, FBAR). Reports go directly to the Financial Crimes Enforcement Network (FINCEN), a division of the U.S. Treasury.

Know-Your-Customer (KYC) regulations attack the same problem as AML rules but from a different angle and with an arguably stronger focus on the prevention of identity theft, financial fraud, and terrorist financing. They were formally codified as a result of the USA PATRIOT Act of 2001, which outlined ways in which businesses must run their Customer Identification Programs (CIPs). These programs require that businesses (especially those that deal with large amounts of money) collect a predetermined amount of information on their customers engaging in transactions of a predetermined type or size. Companies must also file Suspicious Activity Reports (SARs) for customers whose transactions are suspicious or meet certain thresholds.

The level of detail that businesses need to retain on their customers varies according to the transaction, but generally includes basic identity information and information related to spending patterns. A component of this is the Travel Rule, which dictates that information about the sender and recipient, when it is collected, must be passed on ("travel") to another financial institution, when funds are being transferred. Traditionally, these regulations were meant solely for banks but have come to govern businesses that transact in financial equivalents, such as sellers of precious metals and other expensive items that maintain their value. It is in this category that Bitcoin companies find themselves governed by KYC requirements.

Another component of KYC regulations is that companies enforce the Office of Foreign Assets Control (OFAC) Specially Designated Nationals (SDN) list. This list is a database of personnel whose assets the U.S. government has blocked, including terrorists, narcotics traffickers, and otherwise sanctioned individuals. Companies must confirm that they are never sending these individuals any funds or acting on behalf of these individuals to help them move funds under their control.

Threat Likelihood (as of today)
All but certain: We have already seen Bitcoin and blockchain companies incur the ire of regulators for failing to comply with AML and KYC rules. Ripple, a company that runs its own digital currency and interacts with others, received a $700,000 fine from FINCEN for violations of anti-money-laundering rules.

Threat Severity
Moderate: While the threat from AML and KYC regulation can pose an existential threat to Bitcoin companies, they don't necessarily threaten the ability for Bitcoin's core technology to streamline transactions and improve interchange. One reason for this is that the Bitcoin protocol is decentralized, another is that there are enough localities around the world with non-overlapping jurisdictional authority that not everyone can enforce KYC/AML requirements. Critics of strict regulations argue that this means that the United States, with one of the most rigorous AML/KYC compliance

structures, may miss out on some of the innovations that will come from Bitcoin and blockchain technologies.

Recommendations

Recommendations or potential solution(s) for addressing threat in terms of:
Guidance to consumers, businesses, "blockchain community," core developers, and other users.

Consumers should understand the implication this regulation has for their own interests. Avoiding or trying to skirt regulations or compliance has the potential to result in negative, possibly even criminal, consequences.

Bitcoin businesses are the most important focus group for advice in navigating AML and KYC regulations. Many of these companies don't understand whether they fall under the "covered institutions" that are required to have Customer Identification Programs (CIPs). If the regulations appear unclear as to whether they cover a certain business, it is recommended to approach regulators to seek a judgement as to whether a business meets the "covered institution" threshold.

Once a business recognizes that it needs to set up a CIP, the company should aggressively invest in compliance. Unfortunately, the cost of creating and administering a CIP and a program to prevent serving those on the OFAC SDN list, is often overly-burdensome for a startup with limited resources.

Finally, for those would-be entrepreneurs, there is a grand opportunity to address the challenge of AML/KYC compliance by specializing in these attributes and providing their expertise to startups who would rather not invest in building their own compliance program from the ground-up.

Potential also exists to utilize blockchain technology to better track funds and verify user transactions in a CIP. The result is that the blockchain, rather than being at odds with AML/KYC compliance requirements, can lead to more efficient reporting than current technology. Once technological solutions are developed that overcome the issues intended to be fixed through regulations, a company should work to provide education for regulators on these solutions.

In the end, we believe that block-chain solutions will eventually make regulators' jobs easier and better – by improving the process for notice-and-comment rulemaking, for example, and providing mechanisms for more regular updates of regulatory mandates. Other uses include blockchain solutions for financial audits. These would include proof of reserves to address solvency issues, "Big Data" tools for analyzing aggregate transaction flows in identifying threats (rather than focusing on a customer-by-customer basis). Many of these will be covered in later sections.

In giving advice to regulators, we would encourage assessing the promise that Bitcoin and block-chain technologies hold for improving regulatory practices, and focusing on a method of regulating services by activity and behavior rather than technology. This is an abiding principle of regulatory design. Just as not all Internet companies are the same, not all companies that use Bitcoin and blockchain technologies should be treated the same.

We encourage focusing regulation at general purpose regulators (e.g. FTC), which are harder to capture than specialty regulators (e.g., FCC). It is important, as a general principle, to ensure that courts scrutinize regulatory decisions under a meaningful standard with rigorous analysis. It is the responsibility of regulators to subject their actions to the same scrutiny as they would expect of a court.

Many regulatory issues stem from KYC/AML/OFAC laws. The solution to the advent of Bitcoin and blockchain technology is to find points of agreement between regulators and enforcement agencies with technologists. Technology can enhance protection while allowing for innovation. It is

important to recognize the limits of regulatory power in this use-case as well. In the past, regulators could enforce rules against chartered banks and expect that it would enforce the same rules against all citizens. With Bitcoin, the use of the core protocol means that consumers can effectively transfer value outside of the banking system. The more burdensome it is for users to use bitcoin, the more will choose to do so without complying with regulations.

In the developing world it is not clear that regulatory overreach is the most immediate threat. Therefore, as with other topics where the fear of regulatory overreach or just bad regulation is a threat, education of policymakers would be part of a multi-phased solution that also includes grass roots/bottom up pressure to achieve regulatory constraint.

Threat 1b: Unassured Safety/Soundness

Threat Status

Regulations concerned with Safety and Soundness are rules, structures, and systems that are meant to prevent financial institutions or custodians from taking risks that endanger their solvency. Historically, the basis for assessing the trustworthiness of a bank has been limited to assessing the economic solvency of the bank itself. Even in this area, though, American consumers have often placed their trust in institutions unworthy of being trusted.

The most famous of these instances is the panic of 1933, when depositors rushed to remove their funds from banks. To quell the panic, FDR proclaimed a six-day bank holiday. When it was over, the country had four thousand fewer banks than it did at the beginning of 1933. This is when the government officially realized that consumers shouldn't be responsible for assessing a bank's solvency, and shouldn't lose their funds (past a certain point) if their bank fails.

The government created the Federal Deposit Insurance Company (FDIC) and has insured deposits in checking accounts ever since. This policy has boosted depositor confidence more than any other single measure. Today, consumers don't have to worry about how big a bank's footprint is, or how strong their door. They don't have to assess the bank's solvency either, so long as their deposits are below $250,000 and the banks are secured.

FDIC insurance comes at a cost, though. It comes along with a banking charter, something that is not easily earned. It also doesn't necessarily make sense for Bitcoin companies, whose assets are very different from those of traditional banks.

So the real quandary, which has been highlighted by high-profile events over the past few years, is how to protect consumers from Bitcoin companies and custodians who are potentially one security breach (or unsavory owner) away from insolvency?

So far, the industry has found itself outside a great deal of scrutiny from those who are concerned with protecting consumers from the dangers of poor safety-and-soundness. Notable solvency failures include the Japanese-based MtGox, which in February 2014 was discovered to have lost over 850,000 customer bitcoin. Due to these failures, Bitcoin has developed a poor reputation for protecting the safety and soundness of consumer funds.

Bitcoin businesses should be aware of what regulations exist in this field of consumer protection. To begin with, all companies whose business model involves acting as a fiduciary for multiple parties generally require a money transmission license. In the United States these are issued both by states as well as the federal government. Often a company classified as requiring a money-trans-

mitter license by the federal government is not classified in the same way by a state, and vice-versa. This regulatory mismatch can create difficulties for a startup trying to work in multiple states, especially with a borderless currency such as bitcoin.

While there is currently an effort being led by the Conference of State Bank Supervisors to make a "common app" for money transmission licenses, the final product is not yet available and a Bitcoin business must discover for themselves in which jurisdictions their business requires a license. With most developed countries adopting structures similar to US law on financial regulation, this is an obstacle that the Bitcoin community needs to solve if it is to become a serious player in interchanging funds.

It is clear that, so far, the stakes are not yet fully determined as to the role of safety/soundness in the cryptocurrency sector. A couple unanswered questions include:

- What is the difference between holding digital currency as a reserve, versus U.S. dollars?
- What are the reserve requirements and collateral obligations for Bitcoin companies?
- One of the primary enforcement mechanisms for money transmitter licenses is a bank inspector walking around a physical bank or business to inspect reserves, security, and processes. How is that going to work when a business deals with entirely digital currency?
- FINCEN generally does not care about the transfer of information but items of value are being consistently transmitted. That said, if a company is using dust (tiny amounts of bitcoin with data attached to them) to transfer information, does it fall under this regulatory regime?

This lack of clarity is in itself an obstacle to the development of Bitcoin businesses in the United States. Large investors are generally turned off by businesses which can be dramatically affected by an evolving regulatory environment.

Threat Likelihood (as of today)
All but certain - The United States has, as previously described, one of the most highly-regulated banking sectors in the world. To the extent that Bitcoin is exchanged through the American banking system for U.S. dollars, regulators should be able to place controls on those acting as Bitcoin fiduciaries. They have already shown the desire to do so, most notably through the New York Department of Financial Service's Bitlicense.

Threat Severity
Moderate – A case study in the dangers of burdensome regulation in this area is the effect of the New York's "Bitlicense," which has seen a number of Bitcoin businesses boycott the state. Chief among these are the institutions which are legitimately operating in the open within the United States but are not yet large enough to afford the 6-figure cost of submitting their Bitlicense application, coupled with the ongoing cost associated with maintaining compliance. This leaves New Yorkers two alternatives - large bitcoin companies that can afford such compliance costs or entirely non-compliant or "shadow" Bitcoin companies such as BTC-e, whose owners are anonymous and who attempt to operate outside of regulatory purview. While this decreases the availability and diversity of Bitcoin services available to consumers while raising the costs of compliance, it does not necessarily reduce the ability for Bitcoin and blockchain to be used to streamline transactions and improve interchange on a global level.

Recommendations
Recommendations or potential solution(s) for addressing threat in terms of:
Guidance to consumers, businesses, "blockchain community," core developers, and other users.

Bitcoin companies should work to develop technological solutions that overcome the issues intended to be fixed through regulations and provide education for regulators on these solutions.

Additionally, businesses should work to make the jobs of regulators easier and better by improving the processes they use to inform their decisions and enforce their mandates. An example of this would be developing an open-source tool that sits on the blockchain that improves upon the current system for notice-and-comment rulemaking, or provides mechanisms for more regular updates of regulatory mandates. Other uses would include blockchain solutions for financial audits such as real-time tracking of proof of reserves to address solvency issues and Big Data tools for analyzing aggregate transaction flows in identifying threats.

Implementing blockchain technology to better protect consumer funds is essential as the Bitcoin ecosystem "grows up." Bitcoin has the potential to solve the age-old reliance of consumers on third parties and completely transform the idea of consumer protection. That said, the potential for regulations made for an analog world to inhibit this "digital revolution" increases dramatically without communications with regulators. Establishing a relationship with the people (not just the agency, but the people who work there) who are in charge of regulating your business and educating them on how you operate is one of the most important proactive steps that a Bitcoin company can take to overcome this obstacle.

Guidance to legacy/incumbent institutions, organizations, and industries.
Legacy institutions are among the best-positioned to both reap the rewards of blockchain technology while complying fully with overlapping and competing regulatory frameworks. Large banks exist in a highly regulated environment and have established processes for dealing with regulators in areas whose regulations are not clear.

Guidance on improving current regulation, law enforcement efforts, or informing future policy making and regulation.
A regulator's goal with regards to this obstacle should be to fulfill their mission to protect consumers from malicious or incompetent fiduciaries without discouraging innovation.

Threat 1c: Insufficient Consumer Protection during transactions

A current threat to the streamlining of transactions and improving interchange is the absence of traditional consumer protection during transactions. This irreversibility of transactions is one of the great advantages Bitcoin holds from the point of view of merchants and at the same time is one of the greatest dangers to consumers. In traditional banking, when a customer's password is stolen or their credit card is lost the bank, credit card processors, and merchants have systems in place to ensure that it's not possible to destroy the financial life of that customer or rob them of all their money. In Bitcoin, if someone acquires the secret key to a wallet, they can instantly send all the bitcoin in that wallet to any recipient, a transaction that cannot be reversed unless the recipient willingly returns the funds.

Generally, the people who bear the risk of fraudulent/erroneous transaction is a mixture of consumer, payment provider, and retailer. Under the Fair Credit Billing Act of 1974, Congress mandated that consumers who are victims of fraudulent use of their credit card can only be held liable up to $50 of their transaction, giving them a little bit of skin in the game, but allowing them to avoid any major repercussions if a thief purchases high value items with their credit card.

Some voices in the Bitcoin community advocate for a "buyer beware" model of consumer protection. In the current state of Bitcoin, this would require every user to understand public and private

keys, PGP encryption, multi-signature wallets, and more. It's a very similar proposition to assuming in 1994 that all internet users would eventually learn how to work within their DOS prompts to utilize the hypertext transfer protocol (http) if they ever wished to access the internet.

Our current system of consumer protection is based on the assumption that the "lowest common denominator" is mostly protected from malicious actors. That translates into a consumer protection regime which does not depend on consumers reading Yelp or visiting the Better Business Bureau before making a purchase. An example of this is that even if a consumer writes down their PIN onto their ATM card, he or she is still protected from the theft of their funds.

With Bitcoin, we have seen serious breaches, thefts, and hacks which have resulted in consumer funds disappearing. In the annex is a table of all documented hacks prior to June 2015 of 400 or more bitcoin.

Threat Likelihood (as of today)
50/50 likelihood – While a portion of the market will try to figure out how to adopt consumers to an irreversible payment system, another section will build solutions that allow consumers to better guard against theft and fraud. While this is happening, though, regulators will likely be working out how to adopt existing statutes and regulations governing fraud to this new payment system.

Threat Severity
Moderate – Much in the same way that the creation of Netscape Navigator allowed consumers to access the internet without knowledge of how to use the http or ftp protocols, applications will be developed which will allow consumers (even the "lowest common denominator" ones) to utilize Bitcoin and blockchain technology easily and securely without opening themselves up to theft of their funds.

Recommendations
Recommendations or potential solution(s) for addressing threat in terms of:
Guidance to consumers, businesses, "blockchain community," core developers, and other users.

Businesses must address the threat of consumer protection head on. Best practices include using end-to-end encryption in communications will help protect customers from bad actors, including rogue employees who have access to back-end administrative tools.

This end-to-end encryption can also make platforms less susceptible to the actions of nation-states, though this presents a clear dilemma. If platforms are free from the threat of government intrusion, what incentive do they have to comply with any laws? First, we believe that consumers do not wish to become criminals in order to save a few cents on their purchases, so any company working on value-transfer in the Bitcoin world will have to convince its customers that it is operating within the letter of the law.

Second, the blockchain is (as discussed later) a terrific tool for law enforcement. The transition from cash to bitcoin for a criminal is a transition from a completely anonymous value-transfer "protocol" to a semi-trackable one. Companies that operate outside of the law can be sure that law enforcement will be tracking the movement of their funds, and will open up their executives to prosecution within whichever jurisdictions they reside.

Guidance on improving current regulation, law enforcement efforts, or informing future policy making and regulation

Regulators should be educated about the many ways that blockchain technology can enhance security and storage. Multi-sig technology creates a more secure environment than that of the existing banking system, where information is centrally held and therefore vulnerable to hacking and criminal activity.

Threat 1d: Powerful Incumbents

Part of bitcoin's promise is decentralizing services that today have gatekeepers. In the instance of streamlining transactions and improving interchange, that means disrupting every financial institution from credit unions to banks to the Federal Reserve. As we've previously identified, incumbent organizations are in the best position to drive regulation that protects their incumbent status. To the extent that this results in a higher regulatory burden, it has the potential to discourage innovation in new markets.

Parallels to this obstacle exist in every industry. The use of regulatory apparatus by incumbents has been observed recently in cities where taxi commissions have lobbied, often successfully, to ban their newest competitors, Uber and Lyft. When New Jeresey auto-dealers lobbied to prohibit Tesla Automotive from selling cars via their corporate-owned showroooms, the legislature shut down the showrooms, leaving consumers traveling to Pennsylvania or New York to purchase their Teslas. The incumbent status of banks is more powerful than the incumbent power wielded by taxi commissions by virtue of the size of the banking industry and the complex regulatory apparatus by which they are already governed.

Threat Likelihood (as of today)

Somewhat likely – The likelihood of financial companies protecting their vested interest through regulatory capture are mitigated by two caveats. First, the Federal and State regulatory apparatuses are designed to not be captured by special interests. Rather, the opposite is true, they are designed to be immune from regulatory capture. Unfortunately, the world is not ideal and these agencies have proven that they are not immune from the pressures exerted by the industries they regulate.

The more important mitigating factor is that there is scant evidence that financial institutions are threatened by a Bitcoin-version of blockchain technology. Much like the disruptions before, such as the internet and electronic trading, the establishment believes that if bitcoin ever does pose a true threat to their business model, they will be able to build or purchase the necessary infrastructure to co-opt the technology for their own use. In the meantime, it isn't to their advantage to increase regulations which may adversely affect their expansion into new services and offerings.

Threat Severity

Moderate – The obstacle is made more severe because regulators, when calculating the cost/benefit analysis of new regulations, may be skewed away from unseen benefits and tend to overemphasize the upfront adoption costs of regulation. Its severity is lowered by the ability for those who are threatened to operate in different geographies, where incumbent organizations have not captured interests and created overly-burdensome regulatory requirements.

Recommendations

Recommendations or potential solution(s) for addressing threat in terms of:
Guidance to consumers, businesses, "blockchain community," core developers, and other users

Though it hardly needs to be said, the aim of companies should be to create products so great that constituents demand access to them, overpowering the pressure from incumbents to sway lawmakers. Uber is not simply a 50% improvement on the taxicab, it is a 1000% improvement. Bitcoin companies are unlikely to find a mass audience or disrupt incumbents with a product that is simply

10% better than their competition. Bitcoin has promised a revolution; they need to deliver more than an evolution.

Products like these allow for smart regulation that serves consumers and does not inhibit innovation because consumers demand access to the product. Uber depended on the ability to rally consumers to their side in their fights against various city halls. The best way to energize those consumers was to introduce them to their product and then tell them that it was their elected officials who wanted to take it away. Unfortunately for blockchain companies, the United States has a pretty efficient financial system compared to the rest of the world. Products that offer a 10x improvement upon our current state are not as easy to develop, even with the assistance of blockchain technology. The best markets for such disruption exist in the developing world, where Bitcoin may play the role that cell phones did to land-lines, allowing consumers to skip the phase of development that relies on brick-and-mortar banks and skip ahead to digital money.

Threat 2: Insufficient Adoption, Abandonment, or Disinterest

Threat Status

Insufficient adoption, abandonment, or disinterest threatens the streamlining of transactions and improving of interchange because if consumers fail to embrace and adopt blockchain technology or Bitcoin, the currency will have no fungibility among potential enterprise clients.

A couple of contributing factors to this include that consumers may not care about adopting some use cases, such as capitalization of lower value assets. Additionally, some "unbanked" populations may not want to be banked or prefer a more decentralized option. It's possible that those who lack trust in the banking system may not choose to trust digital currencies as an alternative, especially if they think traditional system/services are in fact more trustworthy. While cryptocurrency itself may offer a more trustworthy alternative, the on and off ramps, if not appropriately regulated, may present the same issues as traditional banking institutions, which have so-far not attracted the unbanked.

The identification requirement of banking and transactions under the purview of KYC/AML may drive some consumers away if they do not want to give it up their privacy. As the anti-money laundering regimes expand and become more rigorous, better customer identification may present a big problem among illegal and undocumented immigrants.

Threat Likelihood

50/50 likelihood – There is a strong community of Bitcoin supporters and evangelists now. Despite the decline in price and stagnation in investment, more people seem to be continually attracted to the idea of Bitcoin and blockchain technologies. Without an uptick in interest, though, it's feasible that the community will fail to generate enough momentum to interest a larger population.

Threat Severity

Moderate – Even if most of the passionate Bitcoin community decides to abandon the project, the software and value-transfer aspect of the protocol will remain useful to a number of entities who are looking to streamline transactions and improve interchange. If abandoned by technologists in developed countries, it may find a home among enterprises in developing ones.

Recommendations

Guidance to legacy/incumbent institutions, organizations, and industries

Enterprise solutions and better technology will drive consumer adoption over time. If infrastructural solutions enable consumer applications, the adoption of Bitcoin technology will organically take place. Innovations in user experience and business partnerships will enable an experience signifi-

cantly better than that of any other traditional system for storage and escrow, and the natural ease of use will capture the majority of the first-time users, which will in time become the overall user base as existing participants in the ecosystem migrate to the now more widely-adopted blockchain or otherwise cryptographic solution.

Guidance on improving current regulation, law enforcement efforts, or informing future policy making and regulation

Lower costs and lower barriers to entry serve as proliferators to adoption. To ensure adoption, any proposed regulation should consider whether or not entrepreneurs building and providing these products and services face too high of a barrier for innovation – whether it is time or money. This may be an alternative for those who lack trust in the banking system and think decentralized system/services are more trustworthy.

Threat 3: Volatility

Threat Status
Unlike a fiat currency, there is a fixed amount of bitcoin (21 million BTC once all have been mined) which gives it properties similar to that of commodities such as gold. As a result, its rate of inflation cannot be managed by a government (or other governing body) to increase/decrease inflation, unemployment, or investment/economic growth like that of a fiat currency. Instead, its inherent inflation is, in a sense, built in via a mining process.

The perceived store of value of bitcoin is what fluctuates against the value of fiat currencies. In other words, bitcoin's "future usefulness" will remain highly vulnerable to speculative attacks, bad press, security breaches, loss, chance of large holders liquidating, regulation and tax treatment, etc. until Bitcoin adoption reaches a sufficiently critical mass to withstand these vulnerabilities. With a market capitalization under $10 billion and many large holders of bitcoin, the price is much more susceptible to volatility than comparable asset classes such as gold. This volatility may scare away investors who are not accustomed to less regulated markets which don't have circuit breakers to guard against large intraday price swings.

This obstacle also covers the threat of the so-called "whales" who hold extremely large amounts of bitcoin liquidating enough bitcoin that it drives down the price to a point that may threaten its existence as a store of value.

Threat Likelihood
More likely than not - Bitcoin's first 6 years as a currency/commodity have been incredibly volatile and the borderless nature of the currency means there will likely be more volatility in its future, in whichever currency it is traded.

Threat Severity
Moderate - Bitcoin's prices has managed to stay resilient despite many shocks which were thought to be existential at the time, such as Mt Gox's failure, a miner obtaining 51% of the mining pool, and double-spends. As exchanges have consolidated, many have implemented circuit breakers and all have upgraded their trading engines over the past few years to keep up with the increased volume and prospect of volatility.

Recommendations
Recommendations or potential solution(s) for addressing threat in terms of:
Guidance to consumers, businesses, "blockchain community," core developers, and other users
Exchanges should implement protections that prevent "whale" investors from manipulating the market to speculative ends: circuit-breakers, limits on margin-trading, building market-maker liquidity pools.

Consolidation among exchanges is leading to deeper order books and greater security and professional practices. The more this happens the more institutional investors will be attracted to exchanges trading bitcoin, which will further bolster liquidity and safeguard against complete collapses (or stratospheric explosions) in the price.

- Guidance to legacy/incumbent institutions, organizations, and industries
- Guidance on regulatory compliance
- Guidance on improving current regulation, law enforcement efforts, or informing future policy making and regulation
- Other guidance on achieving adoption

Increased adoption will decrease bitcoin vulnerability to shocks. When bitcoin achieves sufficient adoption its vulnerability will be comparable to that of stable fiat currencies, such as the USD. Also, time will help solve this. Bigger, deeper sources of demand and better hedging instruments will make the market more efficient, less volatile regardless of whether the price increases tenfold or stays near where it is.

The reduction in wait time for confirmations will also allow for decreased volatility as arbitrages disappear as a result of the "rails" of bitcoin-to-fiat transactions are made more robust. In other words, the shorter the wait time to confirm receipt of bitcoin, the less damage a volatile exchange rate can do.

Threat 4: Co-option by States or Incumbent Financial Institutions

Threat Status
States may develop and issue alternative centralized digital currencies. In such cases, the maintenance of the blockchain ledger may be subject to the control or manipulation of a centralized authority, annulling the benefits of decentralization offered by digital currencies such as bitcoin. Centralized control may result in burdensome regulation, fraud, corruption, or manipulation (such as the ability to invalidate legitimate transaction or validate illegal ones).

Threat Likelihood
50/50 likelihood - A state with a very strong currency has much to lose by implementing a new form of currency, but a state with a weak or nonexistent currency has much to gain and the cost is very low.

Threat Severity
Existential - Completely depending on the implementation, this has the potential to threaten the existence of bitcoin and damage the long-term open source nature of blockchain protocols. If tomorrow the United States were to implement "Treasury Coin" and issue notes on their own, closed-source blockchain, the draw to bitcoin would decrease substantially.

Recommendations
Recommendations or potential solution(s) for addressing threat in terms of:
This is rather unavoidable. The solution is to maintain innovative energy around the alternative decentralized technologies – Bitcoin and the like – and lobbying pressure to ensure that the regulatory environment is conducive to that. That will keep the competitive pressure on these incumbents

to create solutions of their own that reduce transaction costs, interchange friction and financial inclusions. These are the end goals, not that Bitcoin takes over the world per se.

Adoption by states/global corporations may have the benefit of legitimizing blockchain near term and, perhaps by inadvertence allow more opportunity for disrupters to enter the marketplace and unseat the global corporations by offering smarter/friendlier/cheaper alternatives.

Increased access to technology is a good thing – even when a ledger is state-owned and issued, the use of the blockchain to enable electronic payments is still a net-positive from governments to companies to consumers. Additionally, since this a centralized service, the ledger will be maintained by interested parties or discarded because the nation is no longer trustworthy just as in traditional fiat currencies. The individual government will not be able to influence the global Bitcoin ledger without total consensus, inhibiting and driving down corrupt bad behavior or manipulation.

Summary Paragraph(s)

The promise of Bitcoin and blockchain technology in the field of value transfer is clear – it has the potential to fundamentally transform the rails of the financial world, creating a much more efficient, egalitarian, and decentralized system.

The promise is not without obstacles, though. Some obstacles are within the Bitcoin community's ability to affect – such as conforming to existing AML and KYC regulations or implementing safeguards against volatility. Some obstacles are outside the control of the Bitcoin community, such as whether nation-states choose to adopt or prohibit bitcoin and blockchain technology. The best steps that can be taken to ensure the opportunity of streamlined transactions and improved interchange are realized is to create a motivated community of bitcoin users compliant with regulations and building useful apps atop the Bitcoin network which are of value to consumers.

II. Streamlining Financial Services Regulation

Voluntary transparency is a self-regulatory mechanism that could substantially enhance consumer protection and prudential oversight.

On a panel called 'What Keeps Regulators Up at Night' held at the November 2014 Money Transmitter Regulators Association conference in Boston, three experienced state examiners from Virginia, Wisconsin, and Texas laid out in clear terms the key issues they face when vetting money transmitters in their states. Their primary concern: the accuracy and integrity of a license holder's financial and accounting reports, which are the basis for ascertaining a company's true financial condition and for ensuring there is sufficient liquidity to meet "transmission obligations." In other words, in the second decade of the 21st century, regulators still rely on after-the-fact, paper-based reporting despite having a trove of digital technologies at their fingertips. Furthermore, regulated financial institutions seem incapable of providing unimpeachable transactional and financial reports to demonstrate their solvency definitively.

History has shown that regulation lags behind technological innovations, especially in the realm of financial service design and delivery. Focusing on bridging this gap is an (up-to-now overlooked, but critical) approach to financial oversight that could address the core purpose of prudential financial regulation.

The Current Oversight Paradigm

The main mission of a financial services prudential regulator is to ensure the safety and soundness of service providers, thus maximizing to the extent possible the protection of consumers' rights.

This includes the right to have their funds delivered to the intended beneficiary in the promised timeframe, or the right for funds to be stored safely. In other words, the primary purpose of regulatory oversight is the protection of consumer funds against loss and mismanagement by financial intermediaries. At present, the mechanism whereby regulators execute their mission is licensing, a rigorous due diligence process aimed at "credentialing" entities and individuals seeking to engage in a particular financial service activity that has been deemed risky enough to warrant this vetting process.

Licensing is an invasive and heavily front-loaded process. Depending on the state, applicants can be required to submit hundreds of page of information about business plans, service and product descriptions, actual and projected financial statements, personal financial information of officers and directors, multiple disclosures and affidavits, and, most importantly, the methodology for calculating and demonstrating that the company has sufficient liquidity to cover any "outstanding obligations"—what is known as proof of solvency, the ultimate guarantee that consumer funds are safe. In the United States, all of this is required to be done forty-eight times, one for each jurisdiction requiring licensure of non-bank financial services providers.

Apart from the cumbersome nature of this exercise, the problem with this oversight paradigm is that once this intensive review is executed, little happens throughout the rest of a company's life cycle in terms of verifying that its operations are above board. There is periodic reporting, an annual renewal of the license, which usually consists of the payment of a renewal fee, and there are examinations, which occur in approximately eighteen-month cycles, are mostly conducted on site, and are paid for by the license holder. Examiners send a laundry list of requests for disclosures and documentation ahead of time and then show up to the head offices of a license holder where they stay for about a week, in what is sometimes cynically referred to as "paid vacations for regulators," examining books and records and interviewing employees. In sum, the first problem with this paradigm is that actual, effective oversight during the ongoing operation of a company is often cursory and always after-the-fact. Months and even years may pass before a regulator finds out that a company is in dire straits.

Another problem with this oversight paradigm is that is based on mandatory or compulsory transparency: applicants are coerced into disclosing information and documentation that supervisory agencies use to determine their fitness and properness. Although compulsory transparency may seem benign, the mere existence of a rule may create the Hawthornean counter effect of a defensive attitude. As is often the case, the coercion itself may induce companies to produce and submit less than accurate reports. And if the information provided by the company is inaccurate or incomplete, regulators have no way to determine the true financial condition of a license holder and the ultimate purpose of prudential regulation -consumer protection- basically vanishes into thin air.

From Compulsory to Voluntary Transparency

Let's now consider an alternative scenario. Imagine that, instead of having to provide information and reports on an ex-post-facto basis, financial institutions openly, yet securely and in real time, published an anonymized and immutable record of all movements of incoming, transferred, and outgoing value. If companies publicly and voluntarily disclosed their database of transactions, prudential regulators would have the ability to reconstruct in real time, or at any moment in time, a company's financial statements, and thus be able to verify their integrity. The result? No more second-guessing the accuracy of coercively submitted reports.

In addition, imagine that financial institutions of any kind – not only blockchain-based ones, which are transparent by design – voluntarily published their internal ledgers, displaying their current financial obligations and side-by-side, also in real time, the liquid, real assets matching those obligations. An open and real-time mechanism like this would provide regulators and the public at large with an early-warning system that would spring into action when an asset-mismatch has occurred.

The result? Incontrovertible proof that the company is solvent enough to cover any "outstanding obligations."

Many headaches experienced by regulators and license holders would just go away if institutions embraced transparency tactics like these as a self-regulatory mechanism. It would be a win-win-win. Regulatory oversight would be less costly and more effective. The shared responsibility among regulators and transmitters to preserve safety, verify compliance, and ensure consumer protection would be dramatically improved. Moreover, consumers themselves would have the peace of mind that their funds are protected, and that the companies with which they do business and the regulators whose salaries they pay as taxpayers are really doing their jobs.

Operating in real-time is still a dream for financial services providers, even if they are introducing innovative digital platforms. For regulators, who either by choice or circumstance have historically monitored the operations of these companies on an ex-post-facto basis, it is an even remoter possibility. However, we are not too far from making real-time financial auditing possible. While these techniques will probably take some time to evolve and be adopted as industry standards, a move toward technology-enabled transparency and proof of solvency would indeed be a positive step forward.

III. Internet-Based Microtransactions

Description of Opportunity/Use Case

For decades, various parties have attempted to employ micropayments via the Internet as a way to incentivize the direct transfer of value from party to party. However, due to the nature of financial institutions and the limited technology present during the Internet's formation, the development and adoption of micropayments was stunted. Today, blockchain technology enables microtransactions down to minute fractions of pennies, thus enabling us to revisit the idea of micropayments over the Internet. Bitcoin, and other blockchain-based cryptocurrencies, open up an array of micropayment applications that were previously cost-inefficient and virtually non-existent.

In the past, low-amount transactions had been difficult to conduct due to third party fees. For example, PayPal's micropayment rate is currently 5% plus a $0.05 CAD per transaction (plus 1% for cross border transactions). Therefore, it costs $0.015 to transfer $0.30 between domestic parties, bringing the total value of the transaction to $0.365. Taking a more macro view of PayPal micropayments, this means that for 100 transactions averaging $2.00 each, the fees paid to PayPal would be roughly $15.00, or 7.5%. In terms of traditional credit card transactions, a 2-4% Visa or MasterCard fee of $0.006-$0.012 on a $0.30 transaction is too insignificant to incentivize these companies to expend resources on them, rendering the transaction unviable through such means.

With bitcoin token mining fees of roughly $0.004, micropayments can now have sufficient value for inclusion in processing. Companies, such as ChangeTip and BitMonet, offer off-chain transactions via internal ledgers where they batch transactions for entry on the blockchain. The idea behind batching is that it minimizes congestion or bloat on the blockchain and spreads the cost of mining fees over numerous microtransactions. As an alternative to off-chain batching, other companies, such as BlockCypher, employ adaptive fee calculation to conduct microtransactions directly on the blockchain. Such companies determine and attach the "most appropriate" fee needed for a miner to pick up the transaction and, once they achieve a certain level of confidence that the transaction

will be processed, guarantee the microtransaction and pay the miners' fees (for a limited number of transactions before switching to an alternative pricing structure).

Person-to-Person Transactions

Initially, the most obvious and immediate consumer use case for micropayments is peer-to-peer (P2P) transactions. One example of P2P transactions using the blockchain is the emerging concept of tipping for content. P2P microtransactions enables Internet users to send "tips" to other Internet users if they wish to support or show gratitude for content on blogs, forums, social media, or other Internet-based information sharing platforms. P2P tipping or micropayment platforms can be integrated into all manner of apps, websites, or even web browsers to enable users to seamlessly transfer the equivalent value of, say, a cookie or cup of coffee to other users, often with an accompanying image to represent what item the value is worth. One example of this type of tipping in action is Taringa!, a social network similar to Reddit geared toward Latin America. Taringa! has integrated Xapo's Bitcoin wallet service to allow users to tip other users for comments or uploaded original content such as music, writing, or art.

Micropayments can also revolutionize charitable giving over the Internet. Those who wish to make charitable contributions, but want to bypass centralized aid organizations, can use microtransactions to send value directly to the individuals or projects they wish to support. As a thought experiment, if each American Internet user transferred the equivalent of one penny each day to the same cause, America could fund 365 causes annually at roughly $2.8 million each. This kind of transfer of wealth or value at such a small scale is not possible now due to fees and third-party intermediaries; but it could be possible with batching transactions in the Bitcoin network. For example, BitPesa is successfully conducting international remittances from the U.K. to Africa and within Africa at a fraction of what traditional remittance companies charge, bringing many people access to financial services for the first time. Furthermore, if microloan entities, such as Kiva, were to integrate blockchain-based micropayment platforms into their models, they would be able to offer microloans lower than the $25.00 minimum they currently offer and they could reduce transaction fees, increasing the proportion of funds actually received by the borrower.

Alternative Models for Monetizing Content and Services

From the advent of mass media – whether considered the first government bulletins in ancient Rome and China or the emergence of the printing press – until the arrival of the Internet, content for mass communications had largely been determined for consumers, and they had few to no available alternatives. Throughout the 20th century, consumers subscribed to magazines, read local or national newspapers, listened to local or national radio programming, or watched public-access or cable television programming – all with content determined or provided by a finite number of sources. It was not until the proliferation of Internet-enabled personal computers and now smart devices (and the infinite trove of information available online) that consumers were empowered to seek out content they desired and the content paradigm began to shift. Now there is seemingly limitless content available in a myriad of formats. Just as broadcast media rocked the print media world in the mid-20th century, smart devices are disrupting all sorts of media, changing the way consumers engage with mass media and their environment.

For example, in the last few decades, consumers have transitioned away from exclusively watching television programming provided by cable companies on traditional TVs to streaming hours of video content on personal computers, mobile devices, and smart or "connected" TVs. In August 2015 Venture Beat estimated that over half of U.S. households had smart or connected TVs.

With average monthly cable subscriptions at $90 per month projected to soar to $200 per month in 2020, consumers are canceling their subscriptions and replacing them with other services, such

as Netflix, Hulu Prime, Amazon Prime, etc. Some consumers who are less willing to use paid access services resort to illegal video streaming and download sites to access content that was previously only available through purchase or rental. Furthermore, many of the major lures to paid cable, such as professional sports channels and premium programming, now offer their programming direct-to-consumer via smart or connected TVs. With these shifts in consumer behavior the major cable companies (including Comcast and Time Warner Cable) have reported significant drops in subscriptions in recent years, with a net loss of a few hundred thousand each of the last three years. While broadband subscribership for these companies is growing, it is not doing so at the same rate cable TV is shedding customers.

According to MarketWatch, a DowJones subsidiary that provides financial information coverage and analysis, the cable industry is not expected to improve. Many customers believe their cable bills are too high and there is an increasing amount of individuals opting to watch shows illegally. Furthermore, by forgoing cable TV consumers could potentially save over $1,000 per year. As cable bills continue to climb, analysts expect more consumers to drop their subscriptions and instead turn to cheaper alternatives.

Cable companies won't be the only businesses to struggle from this change in consumer behavior. With the increase in streaming traffic, Internet Service Providers (ISPs) – which are often cable television providers as well – are facing challenges to meet demand. Thus far, fixed-internet providers have been able to do so without greatly impacting profits largely by making efficiency and productivity improvements, but this likely will not hold for much longer. Furthermore, mobile traffic is growing at an unsustainable rate that cannot be easily addressed due to spectrum scarcity. Mobile providers have been able to avoid exceeding capacity, because roughly 80 percent of mobile traffic is offloaded onto fixed networks via Wi-Fi connections, putting further strain on ISPs.

A white paper, compiled by Cisco Internet Business Solutions Group, suggested that ISPs should rethink flat rate pricing for fixed-internet (broadband) services and transition to value-based pricing. Value-based pricing is built upon the concept of use-based pricing, where consumers pay based on tiers of different bandwidth and speed options, but also includes improved or premium broadband service options. Most consumers are not in favor of the tiered system, as they have grown accustomed to unlimited broadband access at fixed-fees, despite (dial-up) Internet access initially being metered and billed based on use.

In addition to cable providers and ISPs, print media and gaming companies are facing challenges due to smart devices, the increased use of mobile technology, and piracy. Consumers do not want to pay for online news, magazine articles, and games. As a result, many entities are struggling to monetize their content. It doesn't help that consumers also don't want to be bombarded with ads. Intrusive and largely privacy-imposing advertisement models to monetize user behavior online is also not an ideal way for consumers to experience the Internet, given that it involves the purchasing and selling of personal data to companies that wish to sell their products and services to the public, who may not wish to share that information.

Furthermore, advertising on mainstream news sites continues to decline and other sources of revenue remain elusive. Media companies are experimenting with paywalls (where some content is free and some is paid), traditional ads (such as banners), sponsored content (designed to be read), and "native" ads (designed to be shared/go viral); however, neither larger traditional media companies, nor small innovative startups seem to have figured out the best formula for monetizing their content. It is possible, however, that the adoption of blockchain-based micropayment platforms can address these challenges.

Blockchain technology revolutionizes the way consumers can experience the Internet, by reducing reliance on ads to monetize content, and instead allowing people to transfer small amounts of value in order to bypass annoyances (such as ads), access or unlock content (such as news articles or game features), or tip writers, creators, and musicians for their contributed value. Conversely, micropayments also enable gamification, which gives small, incentive-based rewards to users for solving problems or performing small tasks.

The opportunities microtransactions provide are virtually limitless and can dramatically change how consumers access all sorts of content and services. Microtransactions can enable consumers to pay for exactly what they use, when they use it online. For example, ISP and mobile providers could implement use-based pricing, likely lowering the strain on their networks while only charging customers for what they consume. Additionally, instead of paying a monthly access subscription fee that potentially subsidizes the consumption of other users, consumers could pay per second for video streaming, in real-time, using services similar to those offered by Streamium. Soon it could even make sense for some people to make micropayments to access Wi-Fi for brief periods, as opposed to purchasing a day pass or monthly plan for Wi-Fi access at an airport or cafe. In the services industry, consultants could potentially bill and receive their fees on a per minute basis by using services like those envisioned by Faradam. Additionally, because cryptocurrencies are infinitely divisible, miniscule transactions are now a possibility, opening the door for innovation in the product offerings of the financial services industry.

Goals

I) Efficiency

Microtransactions lower the cost of financial transfers and reduce waste by eliminating the necessity of third parties and their associated fees. They also eliminate waste by enabling consumers to pay for exactly what they consume, when they consume it, and nothing more.

II) Human Empowerment

Microtransactions can enable those with limited assets to participate in the economy through remittances, microloans, and direct (micro) charity. Moreover, microtransaction tipping can increase satisfaction between people who seek to provide gratitude for online art and creativity and people receiving said gratitude for the contributed value.

V) Consumer Choice, Access, Privacy, & Protection

Microtransactions offer for more options for transferring value, namely lower denominations at lower costs. They also reduce the necessity for online advertising as a way to monetize content, which puts less of a burden on businesses to aggregate and sell customer data, in turn improving consumers' privacy and data security.

Key Players

Consumer use and demand will drive this opportunity. If the end users of this technology adopt microtransactions to conduct P2P micropayments, other micropayment use cases will soon follow. Service providers, namely legacy institutions, will heavily influence the roll out of use-based pricing for services. Due to the regulatory compliance involved in payments, relevant regulators and policymakers will influence the burden placed on business which offer microtransactions services. If microtransactions gain traction, traditional intermediaries will be rendered unnecessary for such payments.

Status

The adoption of microtransactions as a viable payments option is still in its initial implementation phase. While the concept has gained traction in the gaming world and among those who can use it

to send remittances, only limited pockets of online communities use it for content tipping and few businesses employ it for use-based content access.

It will be a while before this opportunity reaches full implementation, as culture change is anything but rapid. Consumers and business alike will need time to come around to the idea of content tipping and use-based pricing. Some will resist change, while it will take others time to become aware of the opportunity. With the continued efforts of the companies mentioned in this section, along with new entrants and adapting legacy institutions, microtransactions will eventually gain the requisite momentum to drive popularity and mass adoption.

IV. Expanding Financial Access

Discrete Opportunity/Use case

Together, Bitcoin and the blockchain introduce a technical platform for a new global payment infrastructure, one that is distributed and consensus based, leveling the playing field for the 2.5 billion people who are unbanked or underbanked. According to a report by McKinsey titled, "Half the World is Unbanked," 2.5 billion people around the world have no credit score and don't use any type of financial services to make payments, save, borrow money, or even transfer funds. Similarly, a World Bank report in 2012 cited cost, distance to a banking facility, and bureaucratic hurdles as reasons that more than 2.5 billion of the world's poor lack a bank account. While services such as direct deposit, automated bill pay, electronic transfers, and safe storage of funds may seem standard and even expected, for those without access to financial services, they are sometimes insurmountable obstacles to overcoming poverty and building wealth.

The March 2, 2014 cover of Forbes dubbed the mobile payments industry the "15 Trillion [Dollar] Gold Rush." Staff writer Steven Bertoni reports, "Research firm Gartner estimates that mobiles payments will top $720 billion a year by 2017, up from $235 billion last year." It's no wonder that today, banking institutions and the major behemoths in payments such as Amazon, Google, Apple, PayPal, Citi, Visa, Discover, and MasterCard are setting up "innovation labs" to invent the technology to get in your wallet. The article goes on to point out that Bitcoin is that technology.

In the race to be your mobile wallet, what sets Bitcoin and the blockchain apart from the infrastructures of the aforementioned companies is its independent, distributed ledger and consensus-based model. The opportunities an open, distributed ledger provide, which a centralized organization cannot, are improved security, efficiency, affordability, privacy, transparency, and not the least of these, the ability to completely remove the middle man and be one's own bank. This "democratization of financial access" presents opportunities to people who have traditionally been oppressed, such as women at the family/community level as well as entire nation states at the global level.

For example, the World Bank Group's "Women, Business and the Law 2016" report found three potential reasons for the consistent gender gap in financial access, usage, and account ownership. The report found that due to cultures, customs, or laws, women: "face more hurdles than men in proving their identity; may have reduced physical access to financial services; and may find it more difficult to build a financial history and demonstrate creditworthiness." One such country is Afghanistan, where married women must provide additional documentation in order to obtain a national ID and are restricted from travelling outside the home. Today, nonprofit organizations like Women's Annex Foundation provide opportunities for women in Afghanistan to write blogs, develop software, create videos, and be paid for their ideas and content in bitcoin. In this digital economy, as long as a woman has access to a mobile phone and data, a woman can be empowered and have access to financial services that were traditionally prohibitive to obtain.

In another example, in the aftermath of the earthquake in Haiti, the question remains, where has all the money gone? The response of the international community from official, public and private donations exceeded an unprecedented amount of $9 billion USD, yet in an article in the Guardian by Vijaya Ramachandran and Julie Walz, there is little to no visibility on where those funds have gone. Instead, at the time of reporting, three years after the earthquake, "several hundred thousand people remain in tent camps." Imagine if every donation was made in bitcoin or if a nation state's bookkeeping was conducted on an open, distributed ledger. With multi-signature capabilities, the disbursement of any funds would have to be consensus-based and every transaction could be tracked by donors and the public at large. This unequivocal transparency of transactions could lead to greater accountability of donated or taxpayer funds leading to more responsive and responsible governance. (See the section on government efficiency and transparency for more on this topic.)

Goals

V) Human Empowerment

This opportunity will help achieve human empowerment by enabling individuals and groups to access and utilize financial services they have not had access to historically.

II) Consumer Choice, Access, Privacy, & Protection

Bitcoin removes a number of barriers that preclude consumer access to financial services. It also expands consumer choice, in that it expands access to services previously unavailable to some.

IV) Direct Self-Governance

Increased financial inclusion expands individual sense of agency and the ability to exercise that agency.

Key Players

In order for the potential for expanding financial access to be realized, the trifecta of service providers, venture capitalists and funders, as well as end users must be in play. Unlike traditional banking institutions where fees are paid by the merchant or the consumer, transactions on the blockchain are conducted by miners who are compensated a sliver of the transaction for providing the computing power needed to run the network. Without a massive and active user base, service providers will not have a sizable enough market or be able to monetize their efforts to the satisfaction of their investors. Likewise, without investors providing the necessary guidance and funding to service providers in order to scale and provide secure, reliable, and affordable services, the end users will not exist.

Status

The opportunity for expanding financial access is currently in the initial implementation stage. Since 2013, several companies and organizations emerged to provide digital wallets, international remittances, and opportunities for transparency in charitable giving. For example, to date, Coinbase (https://www.coinbase.com/) and Blockchain.info (https://blockchain.info/) are the largest digital currency wallet providers in the world. Collectively, they have over 3 million unique users. While it is possible for end users to develop their own digital wallets, it requires a level of sophistication that the average person does not have. As a result, individuals are more likely to utilize a digital wallet service provider. Much like how many of us do not develop our own email systems and instead, utilize service providers such as Gmail, Hotmail, or Microsoft Outlook.

Organizations such as Women's Annex Foundation and BitGive (http://bitgivefoundation.org/) engage end users such as women in Afghanistan and the philanthropic community. As mentioned, Women's Annex Foundation provides opportunities for women in Afghanistan to earn bitcoin for their original work through their own digital wallets and to enjoy access to financial services. BitGive organizes charitable giving opportunities where people can donate bitcoin thereby exposing a more transparent way to give to the nonprofit and philanthropic community. BitPesa (https://

www.bitpesa.co/) is successfully conducting international remittances from the U.K. to Africa and within Africa at a fraction of what conventional remittance companies charge, bringing access to financial services to many people for the first time.

Expanding financial access is a noble deed but the greater immediate reward is in streamlining existing systems for existing, trusted customers – not in providing services for those considered untested and high risk. 2015 became the "Year of the Blockchain" when legacy institutions such as banks and regulatory agencies began to understand the potential of the distributed ledger. As a result, the funding and enthusiasm has turned from new startups to well-established entities. Companies such as Citi, Visa, Discover, MasterCard, and PayPal have set up "innovation labs" to try to understand and harness the power of the blockchain to modernize their own systems. In 2016, we can expect to see a bevy of new products, services, and price points as a result.

Threats

Threat 1: Incumbent Resistance

Threat Status
Entities with entrenched financial interests that benefit from existing structures will likely resist change by inciting regulatory capture, blocking disruptive technologies, or pushing an alternative solution they can control.

Threat Likelihood
It is all but certain that incumbents will resist change.

Threat Severity
Should incumbent institutions resist the adoption or block the success of disruptive technologies, the severity of this threat is major.

Recommendations
Both the financial opportunity as well as the social impact benefits of expanding financial access should be presented to incumbents. While the transition from one established system to another may prove to be costly, in the long run, established, reputable financial institutions should take advantage of the opportunity to expand their client base while lowering overall costs.

Threat 2: Cultural Reaction

Threat Status
In some cultures, family or community structure or traditional "power" relationships may persist in undermining democratization efforts.

Threat Likelihood
There is a 50/50 likelihood that culture and traditions will have a significant impact on the achievement of this opportunity.

Threat Severity
The potential damage from this threat is moderate and will likely be short-lived once the benefits of the opportunity are realized.
Recommendations

Experts have shown that empowering women specifically drastically improves the overall condition of the family. Through community and education initiatives, women in traditionally patriarchal families or communities could obtain access to an alternative financial system.

Threat 3: Abusive Early Adopters & Criminal Exploitation of Opportunity

Threat Status

Bad actors are almost always early adopters of new technologies. The possibility of increased abuse by bad actors for nefarious purposes is virtually inevitable and is not the fault of the technology. Additionally, expanding opportunity for financial access outside the existing regulatory structures and protections may create opportunities for the criminal element to abuse the new structures for criminal gain. This would result in the creation new, more complex structures that allow for criminality. This, in turn, may result in more onerous regulations which would capitate the adoption of blockchain technology.

Threat Likelihood

It is certain that bad actors have exploited and will continue to exploit the advantages afforded by blockchain technologies (in criminal activities); however there is only somewhat likelihood that this threat will have a long-term negative impact on the adoption of the technology, given that its popularity continues to grow despite frequent press related to bad actors.

Threat Severity

Initially, this threat will (and is) having a major impact on the perception of bitcoin; however, this threat will downgrade to moderate or even minor as law enforcement and the general public see that the benefits of the technology outweigh the drawbacks.

Recommendations

Organizations working with consumers, regulators, and law enforcement should highlight that the adoption of technology by bad actors is a reflection of bad actors, not of technology. Law enforcement continues to operate to enforce the law. It's not the payment that is illegal, it is the good or service being exchanged by the bad actor that is. Moreover, as outlined in the section on law enforcement, bitcoin has been instrumental in bringing down major criminal enterprises, which should be consistently emphasized. Encouraging law enforcement to focus on stopping the bad actor takes the emphasis off fluid payment systems.

Threat 4: KYC/AML

Threat Status

While the blockchain may offer some real benefits for law enforcement, the issue of customer identification and transactional transparency remains an issue both from an AML and OFAC point of view. The possibility of increased abuse could usher in onerous regulations that could stunt the development of consumer products and services that are safe, secure, and affordable. Moreover, until law enforcement and bank regulators believe cryptocurrencies and blockchain technologies pose no greater risks, in terms of money laundering or terrorist financing, efforts may be undertaken to limit its growth or acceptance.

Threat Likelihood

More likely than not

Threat Severity

- Moderate
- Major

Recommendations

The blockchain community (or its various representatives) should work alongside regulators and law enforcement agencies to identify consumer concerns and to best protect consumers by mitigating risks while encouraging innovation (i.e.: reversibility, error resolution/finality, customer support, etc.)

Threat 5: Market Demand

Threat Status

Do the "unbanked" want to be banked? Do they prefer a more decentralized option? Or do they have no interest in any form of formalized banking? For those who lack trust in the banking system, this opportunity could be a more palatable alternative for those who believe the system/services offered by blockchain technology are more trustworthy. However, that may be insufficient for some "unbanked" persons. While the cryptocurrency itself may offer a more trustworthy alternative thank traditional banking institutions, the on and off ramps, if not appropriately regulated, may present the same issues. There may be a desire not to be tracked through the financial system because of the profile of the individual or underlying source of value. Additionally, the "unbanked" may not have sufficient identification or may not wish to share their identification information to become traditionally banked. As the anti-money laundering regimes expand and become more rigorous, better customer identification will be a big problem in the illegal immigrant community.

Threat Likelihood

It is highly unlikely that proportion of the "unbanked" that do not wish to be banked will significantly impact the success of this opportunity.

Threat Severity

If the majority of "unbanked" do not wish to be banked, this would only be a minor threat to the "unbanked" who do wish to obtain access to financial services.

Recommendations

NGOs or relevant government agencies should assess whether those lacking access to financial services desire to be "banked." Lower costs and lower barriers to entry could also serve as proliferators to adoption. To ensure this, any proposed regulation should consider whether or not entrepreneurs building and providing these products and services face too high of a barrier for innovation - be it time or money.

Summary

According to a recent industry report by Accenture, "leveraging the lower cost-to-serve capabilities enabled by the technology-driven transformation of their operating and distribution models" allows forward-looking banks to reach previously inaccessible markets, like "the hundreds of millions of people who remain outside the scope of traditional banking services."

B. Blockchain 2.0

I. Smart Contracts

Discrete Opportunity/Use case

"The formalizations of our relationships—especially contracts—provide the blueprint for ideal security."

Nick Szabo

Discrete Opportunity/Use case

The concept of contracts dates back to ancient times. Just as our Greek and Roman predecessors sought to solve trust, clarity, and enforcement issues with formalized agreements, we employ extensive legal frameworks in the hopes of achieving the same end. While we have developed our legal systems with the benefit of a millennium of philosophy, jurisprudence, case law, and legal precedents, we still face these same challenges in terms of trust, clarity, and enforcement. We must rely on third parties and the infallibility of man to enforce contractual agreements. By creating structures that do not depend on third-party intermediaries, such as self-executing, predetermined contracts, we may be able to resolve the age-old issue of trust.

While our legal frameworks are theoretically effective at rectifying the problem of trust, practice shows that this is not always true. The biggest problem is that they are not always incorruptible – conflicts of interest between judges and the parties involved in a contract dispute cannot be ruled out, for example. A judge in a court that adjudicates contract disputes is an example of one of these intermediaries, which might be circumvented or deemed unnecessary by the use of smart contracts.

Another issue with our current system of contracts is the time and complexity involved both in formulating contracts and in resolving disputes. Contracts often necessitate the involvement of expensive legal counsel in order to be binding. Resolution of disputes, meanwhile, not only requires the same experts (who are not incorruptible) as the formulation of those contracts but also involves drawn-out adjudication processes that can take years.

Smart contracts, as we will see, have the potential to make the formulation and enforcement of contracts between parties more straightforward and less corruptible.

The following excerpt, written by Nick Szabo and included with his permission, outlines what smart contracts are and how they may solve this dilemma.

The Idea of Smart Contracts

Many kinds of contractual clauses (such as collateral, bonding, delineation of property rights, etc.) can be embedded in the hardware and software we deal with, in such a way as to make breach of contract expensive (if desired, sometimes prohibitively so) for the breacher. A canonical real-life example, which we might consider to be the primitive ancestor of smart contracts, is the humble vending machine. Within a limited amount of potential loss (the amount in the till should be less than the cost of breaching the mechanism), the machine takes in coins, and via a simple mechanism, which makes a freshman computer science problem in design with finite automata, dispense change and product according to the displayed price. The vending machine is a contract with bearer: anybody with coins can participate in an exchange with the vendor. The lockbox and other security mechanisms protect the stored coins and contents from attackers, sufficiently to allow profitable deployment of vending machines in a wide variety of areas.

Smart contracts go beyond the vending machine in proposing to embed contracts in all sorts of property that is valuable and controlled by digital means. Smart contracts reference that property

in a dynamic, often proactively enforced form, and provide much better observation and verification where proactive measures must fall short.

As another example, consider a hypothetical digital security system for automobiles. The smart contract design strategy suggests that we successively refine security protocols to more fully embed in a property the contractual terms which deal with it. These protocols would give control of the cryptographic keys for operating the property to the person who rightfully owns that property, based on the terms of the contract. In the most straightforward implementation, the car can be rendered inoperable unless the proper challenge-response protocol is completed with its rightful owner, preventing theft.

If the car is being used to secure credit, strong security implemented in this traditional way would create a headache for the creditor - the repo man would no longer be able to confiscate a deadbeat's car. To redress this problem, we can create a smart lien protocol: if the owner fails to make payments, the smart contract invokes the lien protocol, which returns control of the car keys to the bank. This protocol might be much cheaper and more effective than a repo man. A further reification would provably remove the lien when the loan has been paid off, as well as account for hardship and operational exceptions. For example, it would be rude to revoke operation of the car while it's doing 75 down the freeway.

In this process of successive refinement we've gone from a crude security system to a reified contract:

1. (1) A lock to selectively let in the owner and exlude third parties;

2. (2) A back door to let in the creditor;

3. (3a) Creditor back door switched on only upon nonpayment for a certain period of time; and

4. (3b) The final electronic payment permanently switches off the back door.

Mature security systems will be undertaking different behavior for different contracts. To continue with our example, if the automobile contract were a lease, the final payment would switch off leasee access; for purchase on credit, it would switch off creditor access. A security system, by successive redesign, increasingly approaches the logic of the contract which governs the rights and obligations covering the object, information, or computation being secured. Qualitatively different contractual terms, as well as technological differences in the property, give rise to the need for different protocols.

(See "Supplement 2" in the annex to read Nick Szabo's "Smart Contracts: Building Blocks for Digital Markets" for a full conceptual breakdown of smart contracts and the concepts it opens the door for, such as verifiable identity and smart property.)

Examples of companies that are developing or have launched smart contracts platforms include: Ethereum (http://ethereum.org/), Counterparty (http://counterparty.io/), Hedgy (http://hedgy.co/), Codius (https://codius.org/), BurstCoin (http://burstcoin.info/), and BitHalo (https://bithalo.org/) and BlackHalo (http://blackhalo.info/).

Goals

The concept of smart contracts is the cornerstone on which most Blockchain 2.0 and 3.0 applications are or will be based. The adoption of smart contracts will have a significant impact on fostering

each of the overarching goals: efficiency, human empowerment, direct self-governance, transparency, and consumer choice, access, privacy and protection.

Key Players
Due to the countless potential use cases as well as implications of smart contracts, end users, service providers, relevant regulators and policymakers, venture capitalists and funders, legacy services and institutions, bad actors, and intermediaries will all play significant roles in determining the successful adoption and implementation of smart contracts.

Status
Smart contract applications are in the initial implementation phase. As listed above, a number of companies have launched smart contract services and the sector is growing. Other use cases for based off smart contract applications are in the exploration phase and will be discussed in later sections of this paper.

Threats

Threat 1: Collaboration with Authorities

Threat Status
With the possible exception of contracts with outputs that execute fully on the blockchain, enforcement of blockchain-based contracts require buy-in from enforcement authorities. For example, you may transmit a token that represents a house with delinquent tenants on the Blockchain, but you can't actually evict anyone unless you get the Sheriff involved.

Threat Likelihood
All but certain

Threat Severity
Should the issue of enforcement collaboration not be addressed properly, it will prove to be an existential threat to the adoption of smart contracts.

Recommendations
Businesses offering smart contract services should proactively collaboration with law enforcement to mitigate the creation of overly burdensome compliance requirements due to lack of cooperation. Network consensus and verification should be build into smart contract applications, so all blockchain transactions originating from stolen value would not be accepted by the network.

Threat 2: The Regulatory Burden

Threat Status
Regulation that is more harmful than helpful.
Threat Likelihood
All but certain

Threat Severity
Existential

Recommendations
Lobbying, advocacy, and education will help developers get out in front of onerous regulations. Organizations such as Consumers' Research, CoinCenter, the Digital Currency Council the Chamber

of Digital Commerce all work to address regulatory challenges and the Bitcoin community should reach out to them with their concerns.

Threat 3: Competition among Systems

Threat Status
Entrenched incumbents may be able to co-opt technology to continue using closed systems that they manage

Threat Likelihood
More likely than not

Threat Severity
Major

Recommendations
Incumbent organizations have every right to build their own networks. Multiple options should always be available and properly funded and developed. Consumers should have the right to choose and not be forced into one system or another, and there should be competition in these systems. Consumer demand should drive alternatives.

II. Identity Issuance

Discrete Opportunity/Use case
Lack of access to government-issued identity documents (such as those verifying a registered birth, civil status, or citizenship) is a crucial factor contributing to a number of important and widespread social problems. As the United Nations International Children's Emergency Fund (UNICEF) notes, documents such as a birth certificate are required to access an increasingly wide range of services, entitlements and opportunities, such as the ability to claim citizenship, to access formal financial services (i.e. savings accounts, bank loans, or the ability to send remittances through formal channels), to acquire a mobile phone contract, and to access services such as public health, education, and welfare (UNICEF 2013, 1-8). The lack of adequate identification also impacts overall personal security, especially in terms of child protection, as a link has been established between non-registration and the risk of exploitation and abuse (e.g., in cases of labor and sex trafficking, forcible conscription, and child marriage). With the acceleration of cross-border population movements worldwide (mixed migration and refugee movements), appropriate identification is often necessary to support the traceability of unaccompanied minors, the distribution of aid, and the processing of immigration status claims. Less directly, the potential data that can be collected as a result of the collection of identifiers made possible through the identity issuance process can allow countries to better plan for the provision of services, such as health and education programs, and it can provide information to track other population developments.

The scope of the problem is difficult to assess with any great precision, as the very fact of being un- and under-identified implies that a person is difficult to find, identify, or count. UNICEF estimates that approximately 230 million children under the age of five have not had their births registered. "Of these, around 85 million are in sub-Saharan Africa, 135 million in Asia (East and South Asia and the Pacific) and the remainder in the rest of the world" (UNICEF, 11). Other vulnerable populations who often lack documents have been increasing. The Office of the United Nations High Commissioner for Refugees (UNHCR) estimates that globally there are at least 10 million stateless individuals: persons without a legal nationality who, subsequently, often lack a legal identity and/or cannot obtain national identity cards or other documents needed to fully participate in society. The UNHCR also counted 19.5 million refugees in 2014, a figure that is sure to rise in the wake of the Syrian

and other refugee crises that have unfolded in 2015 (UNHCR). Refugees often flee with minimal identification from their country origin and lack the documentation required to legally enter or pursue a livelihood elsewhere. This problem is faced even within well developed economies and infrastructures, with immigrants, low income, and rural populations more likely to be un- or under-documented (e.g., they might lack national identity cards/numbers or formal credit histories that could give them access to financial services).

Given the size and severity of the problem, a number of governments and non-government organizations have attempted to deploy digital technologies to broaden registration and identity-issuance and to increase access to the rights and services often attached to possession of a verifiable identity. To date there have been a number of initiatives to increase access to verifiable digitized identities issued by a government (the Aadhaar program in India being a prime example) or, in some cases (where government action is insufficient or non-existent) by local or international development agencies such as the UNHCR (e.g., see Fall-Diaw). Other governments have attempted mobile phone- and web-based initiatives, the expansion of e-government capabilities, and other digitalized processes to increase service availability and usability, streamline processes, and improve data quality (Plan International, vi). However, none of these initiatives have utilized blockchain technology.

In the realm of identity and blockchain technology, most innovations to-date have been focused on already digitally-active consumers seeking improved security, privacy, and overall transactionality with respect to e-commerce and/or the management of their online identities. The potential is that these new online identities could both streamline the online experience (eliminating the need for multiple login passwords, for example) and make it easier for people to both share and control the proliferation of their data online (including having the ability to monetize the distribution of their own data in the future). Aside from that largely unrealized potential, the benefits of the blockchain that these innovations (apps and platforms) exploit generally center on improving trust. As shown through projects like Open Mustard Seed (Hardjono 2014), there is a growing need and opportunity to create decentralized digital institutions that provide consumers with full ownership and control over their data and most importantly their digital identities and relationships.

Shocard (http://www.shocard.com/) is an identity platform built on the blockchain that offers a mobile phone-based digital identity card protected by public and private keys, hashing, and multi-factor authentication. Onename (https://onename.com/) is another significant example that allows users to create a "blockchain ID" that can be linked to websites and social media profiles and is easily verifiable by other Onename users.

The most direct attempt to draw upon the 'promise' of the blockchain to address deep-seated global problems of identity issuance comes from a social impact systems entity. Currently in early development, Identity 2020 (www.id2020.org) aims to combine the strengths of trusted computing and blockchain technology to leverage a secure digital platform for the creation and management of "self-sovereign" digital identities: a standard that affords people control over how, with whom, and for what purpose their identity data gets shared and/or is used.

Goals

This opportunity furthers the following goals:

V) Human Empowerment
The ability to extend verifiable digital identity to millions (if not billions) of people also extends to them the security and protections affiliated with belonging to a larger organized group (whether with an NGO, local community, or state). It can allow them to be counted and to make a claim to

a wider range of privileges and public services, such as access to welfare or education systems. The capabilities interwoven in a blockchain-based system (e.g., machine learning, the use of alternative data to establish identity) can open access to financial systems and capabilities. Note that blockchain-based technology alone cannot solve the underlying issues at the heart of problems like the social inequality and poverty that feed social or financial exclusion. However, it can provide a technical tool to dismantle many of the barriers that buttress exclusion and discrimination, including cost, corruption, mistrust, and the unchallenged reliance on standards that replicate social inequalities, such as the existing criteria for meeting Know-Your-Customer (KYC) requirements.

II) Consumer Choice, Access, Privacy, & Protection

Key innovations associated with this technology include the increased security of data (via the cryptography inherent in the blockchain infrastructure), increased consumer control over how their personal data is shared (via multi-signature authorizations), and increased access to a verifiable digital identity overall. This technology could potentially be used to challenge government monopolies over who creates, verifies, and/or issues useful identifying documentation.

III) Transparency

The use of trusted computing together with the immutable public blockchain allows data entry and flow to be monitored, greatly reducing the potential for fraud and data manipulation.

Efficiency

There may be efficiency gains related to the potential for low-cost, low friction solutions to governments' identity management problems. This has advantages on an international scale. The use of this technology to create more robust and trustworthy systems in countries with poorly functioning and low-confidence identity systems (i.e., countries tagged by the Financial Action Task Force on Money Laundering, or FAFT, as having strategic deficiencies in anti-money laundering and combating the financing of terrorism) could allow more capital, in the forms of direct investment and remittances, to flow inward and help alleviate core issues, such as poverty and economic inequality, that hinder development and engender security problems.

Key Players

End users – Consumers of identification services will play a significant role in moving this opportunity forward, as they drive the demand for such services. Those with the most at stake include individuals with some minimal form of government issued identification that nevertheless fails to grant sufficient access to important services (e.g., the lack of a credit history or a credit card) as well as those whose birth was never formally registered and have no documented, government-recognized proof of existence.

Service providers – Providers of identification services including the architects/licensors of identity management platforms, the entities who license the technology (i.e., businesses, governments, aid organizations, etc.), and data providers (i.e., utility companies, mobile phone operators, etc.) are vital to ensuring that these services come to fruition.

Relevant regulators and policymakers – Government regulators will play a key role in determining whether new capabilities made available via the incorporation of blockchain technology (e.g., the collection and acceptance of alternative data criteria for fulfilling KYC requirements) can gain practical acceptance. Such bodies include the intergovernmental FATF, which sets standards for anti-money laundering and anti-terrorism financing measures, including standards for customer due diligence (i.e., identity verification).

Venture Capitalists (VCs)/Funders – VCs play a valuable role in fostering the startups seeking to commercialize opportunities around blockchain-based identity platforms, apps and other technologies.

Given that identification is an issue that crosscuts many others, investors interested in supporting innovation in financial systems, data management, and consumer Internet applications have also invested in various blockchain-oriented start-ups.

Legacy Services and Institutions – Blockchain-based identification services can be seen as playing a key role in the overall disruption of financial services reliant upon legacy identity management systems and services. It is reasonable to assume that legacy institutions will likely resist change and demand burdensome regulation on new entrants to prevent it, or they will attempt to get ahead of the identity issuance innovation curve to keep new entrants from establishing significant market share.

Status

Exploration – Entities such as Identity 2020 that seek to use blockchain technology to provide platforms for the issuance and management of identity with respect to un- and under-identifiable populations (who are often the financially excluded and socio-politically vulnerable) are still in the exploration phase. Moving these initiatives forwards depends, to a large extent, on the ability to find funding in the social impact and philanthropic realms for seed capital. Another important hurdle is the willingness of regulators, governments, local and international development organizations, and other gatekeepers to collaborate on the creation of rules and standards and to facilitate access to the populations that stand to benefit from the technology. It is worth noting the criteria laid out by the UNICEF (39) for the successful implementation of new identity registration processes:

- Universality – registration is accessible to all eligible persons regardless of their geographic location.
- Accuracy of data.
- Timeliness of registration, issuance, and management processes.
- Confidentiality.
- Cost – services should preferably be free.
- Security – with respect to data storage.
- Retrievability of data/identifiers when needed.

Initial implementation - Blockchain-based businesses primarily focused on consumers seeking improved security, privacy, control over their data, and overall transactionality with respect to their identifying information are raising seed capital and are in the initial phases of implementation (e.g., Shocard, Onename). Investment comes largely from venture capital that funds new models for managing identities and personal information online and the sectors for which identification is a core business component (e.g., financial services). It is worth speculating how the implementation of these new business models might challenge – or be challenged by – companies that outsource their identification services (e.g., logging in via Facebook or Twitter) and/or who sell that data as part of their business models.

Threats

The general risks surrounding identity issuance on the blockchain are largely associated with the origination, storage, and management of identity claims and credentials to the extent that concerns related to privacy, security, data corruption and data misuse can be mitigated. These have been summarized effectively by Plan International (2015):

- Theft of personal data.
- Violation of privacy or unauthorized (or mistakenly authorized) sharing of identifiers.
- Targeting of populations based on the ability to access personal data, a form of exploitation which could be economic, commercial (e.g., unwanted targeted advertising), or violent (e.g., persecuting ethnic or religious groups).
- Exclusion from the benefits of identity registration or issuance (i.e., if systems still cannot meet the needs of the already marginalized).

The threats that relate specifically to blockchain-based identity platforms, apps, or other technologies are specified below.

Threat 1: Private Keys are Compromised

Threat Status

Today, the exploitation of stolen private keys or cryptographically compromised infrastructure can lead to theft of personal data, violation of privacy, or unauthorized (or mistakenly authorized) transactions and/or sharing of identifiers. Looking beyond implementation risks, the successful mitigation of this threat depends on how quickly an incident is detected and how quickly control of the identity can be recovered, including any attempts to repair damages.

Threat Likelihood

Today, the prospect of having one's private keys compromised is all but certain. Yet, recent advances across many fields suggest that the next generation of decentralized identity systems (see: Rebooting the Web of Trust, http://www.weboftrust.info/) may prove to be much more resilient and may be able to address many of the remaining challenges that are presently hindering the mass adoption of blockchain technologies by the typical consumer. Moreover, deploying a ubiquitous and decentralized Public Key Infrastructure (PKI), capable of sufficiently managing private keys and the associated risks, is paramount to preserving many of the core principles demonstrated by the underlying protocols, notably "censorship resistance" and the democratization of trust.

Solutions are also needed that utilize secure hardware for the purpose of protecting private keys, transmitting verified identity information to distributed registries, establishing a root of trust (e.g., remote attestation), as well as managing authentication and authorization requests, among others. Today many private keys are stored with only software protections and are easily defeated, compared to specialized hardware devices designed for the purpose of performing specific cryptographic functions, such as generating private keys and ensuring they are never revealed or leave the device. Moreover, independent systems should be used to manage the private keys under the control of a unique physical entity (e.g., one's root id) separately from the private keys associated with various digital claims, agents, identities, profiles, personas, avatars, etc. and their transactions (e.g., one's core id).

Threat Severity

The threat of one's private key(s) being compromised is major. Without controls put in place to slow or limit the execution of transactions tied to a particular private key, damage to an entire digital identity could be instantaneous and significant.

Recommendations

Increased education around the vital importance of storing private keys is needed. Even today, many consumers are still struggling to grasp the importance of using strong passwords with their connected devices and network-connected services. Furthermore, blockchain technologies rely on private keys that are not practical to memorize and verifying ownership in the event of a compro-

mise is challenging at best. Thus, additional controls and methodologies are needed to provide a seamless experience around key management. Mitigation of this threat follows by either making it very difficult to compromise a private key or by limiting the damage that can be done with a particular private key that has been compromised.

Employing multi-factor authentication in the access control layer of hardware wallets (i.e., applications capable of signing transactions on behalf of the identity that owns or controls the wallet) should be considered. This includes combining biometric characteristics. For example, "something you are," which may include retina, thumb-scan, DNA/genomic credentials, etc. may be combined with other factors such as, "something you know" and "something you have." However, even biometric credentials can be forged, and each situation may require different combinations of characteristics in order to meet various trade-offs between criteria such as security and usability. In some cases, the disputed fourth factor of authentication might be required. This factor is loosely considered the equivalent of a trusted identity observing or vouching for some verifiable characteristic that describes another entity, such as where someone is, whether someone is known by another person or entity, etc. Utilizing multi-signature addresses and schemes, such as requiring a friend or trusted institution to provide additional verifications before executing a large financial transaction, can also reduce risk, as each additional key required to sign a transaction significantly increases the cost and complexity of mounting a successful attack (up to a point).

Hierarchically Deterministic (HD) keys can be used to make "sub-keys" that essentially serve as the commonplace key pairs (i.e., the ones in flight that could potentially be compromised) utilized for identity-related transactions. Thus, new sub-keys can be issued from the same parent key in the event that a sub-key needs to be replaced. In some cases this means that sub-keys may be used once and then thrown away. Nevertheless, the issue of securing the "root" HD key is remains paramount.

Threat 2: Privacy Concerns

Threat Status

The potential for unauthorized re-identification raises privacy concerns for consumers, from both a governmental monitoring perspective and consumer-facing businesses, where collecting and managing large datasets of personal information presents a multitude of risks.

Threat Likelihood

All but certain

Threat Severity

Major

Recommendations

This threat may be overcome through the use of multiple public keys for various purposes, e.g., interact via pseudonymous digital personas which are unlinkable yet can be trusted that they are controlled by an authenticated and re-identifiable entity. Additionally, minimizing data sharing may limit re-identification.

Threat 3: Discriminatory Conduct

Threat Status

Public logs of consumer behavior – even if not re-identified – could lead to illegal discriminatory conduct (e.g., disparate impact). For the industry verticals that adopt blockchain technologies, there is an immense opportunity to fix digital identity and rectify today's inadequate privacy standards before launching into the age of consensus-driven services. However, there remains much to be done before consumers are assured that even today's regulations can be enforced, to prevent or

identify the illegal use of the "alternative credit information" reflected on the blockchain (e.g., insurance plan providers using consumer credit history in coverage decisions).

Likewise, public logs of consumer behavior would allow businesses to bypass notification requirements relating to viewing consumer credit reports and/or regulations that would otherwise require employers to inform job applicants that they had been rejected due to their credit histories.

Threat Likelihood
Somewhat likely

Threat Severity
Moderate

Recommendations
New digital identity systems, using recent advances in trusted computing and upcoming consensus protocols should be designed, implemented, and tested to meet minimum consumer data protection standards. The application of technologies such as zero-knowledge-proofs, homomorphic encryption, digital asset escrow services, and smart contracts enable the emergence of systems that are algorithmically governed to enforce rule of law, ensuring that all transactions are trusted, yet reveal no information about the identities of any counterparties until lawfully requested.

Ownership and control of electronic records (e.g., birth certificates, citizenship, loans, title transfers, financial instruments, etc.) is also likely to be impacted. Lessons from Bitcoin, such as treating a transaction is invalid if it does not reference previously valid Bitcoin transactions as "inputs," suggests that technological solutions may even prevent the creation of incorrect records altogether.

Threat 4: Identity Fraud and Difficulty Disputing Inaccurate Information)

Threat Status
The lack of an infrastructure that links identities to blockchain transactions could make it difficult for consumers to dispute inaccurate information associated with their digital identities (e.g., if someone records that they lent identity XYZ $1 million, which was never paid back) – and likewise prevent fraudulent behavior and/or re-identify fraudulent individuals (e.g., the Sybil attack).
Threat Likelihood
All but certain

Threat Severity
The lack of trusted services to serve as "attribute authorities" that validate identity information and meet regulatory obligations while ensuring anonymity is an existential threat to blockchain adoption in identity issuance.

Recommendations
Permanent records run afoul of federal requirements (and general policy interests) that require that outdated information be deleted from consumer credit records, making it difficult for consumers to "bounce back" from financial pitfalls (i.e., under the Fair Credit Reporting Act, negative information must be deleted after seven years; bankruptcies after ten years).
While the Bitcoin blockchain is immutable and provides a permanent record of transactional history back to its first transaction, most identity related data is unlikely to be stored on the blockchain itself. Thus, "trust frameworks" for managing digital assets, in concert with blockchain technologies and consensus protocols, are needed to implement redaction, provenance, attribution, regulatory compliance, etc.

Summary Paragraph

Blockchain-based identity and related use cases are set to expand rapidly into broad applicability, in a massively disruptive and world-changing manner. Users will be able to establish a financial history, based on transactions that occur outside the formal financial system, for the purposes of evaluating creditworthiness or to fulfill KYC requirements using non-traditional criteria (thus facilitating access to services they may have been previously "excluded" from). The underlying technology will further support the generation of a transactional record for the myriad of forms of quantifiable human capital (i.e., financial, social, educational, political, etc.) and property ownership, opening up new opportunities for micro-lending and improving rights and services overall. Key to the success of this technological intervention will be the ability to work with regulators and other stakeholders (government and corporate) to negotiate the acceptance of new standards, rules, criteria, and infrastructures for the decentralized management of digital identities and the application of algorithmic governance to personal data and the resulting self-sovereign identity.

III. Proof of Asset Ownership/Smart Property

Discrete Opportunity/Use case

Peruvian economist and anti-poverty campaigner Hernando de Soto (2000) found that billions of people operating within the developing world's "informal economy" were sitting on almost $10 trillion in "dead capital" (p. 36). These people own small plots of land, dwellings, vehicles, and equipment, but they can't monetize it. The problem: a lack of formal legal title to those assets, which precludes their use as collateral. Without a recognized documentation standard validating their property rights, people can't borrow against their houses, can't insure their cars, and are put in a weak bargaining position whenever they need to sell these holdings. The causes of this failing stem from poorly resourced and often corrupt bureaucracies – neither the citizens of these countries nor the financial institutions that require reliable title documents sufficiently trust the government registrars charged with maintaining this data. So, a vicious cycle of mistrust and inaction perpetuates itself: title records are therefore, non-existent, incomplete, or prone to tampering by bribe-seeking officials. The blockchain could help break this cycle.

Key elements of property ownership could be recorded on a blockchain ledger by inserting a hash of the pertinent data into a transaction. This could be done directly onto the bitcoin blockchain by using an implementation such as colored coins or – to avoid "blockchain bloat" – by storing it in off-chain key directories that assign different controls over different components. It can also be implemented with other "permissionless" blockchain systems such as Ethereum or – in a more extreme departure from the decentralized structure of these pure cryptocurrency-financed networks – via a version of the "permissioned" systems now being developed by banks, NGOs as well as some governments.

With the data inserted into a blockchain, a de facto property title registry can be created that's recognized to be immutable (tamper-proof), universally available, trusted by all parties and interoperable across disparate, siloed databases. Additionally, because the data exists in a digital form attached to a decentralized ledger for managing digital-currency transactions, real-time transfers of ownership are possible, as are the attachment of liens and other claims on the property. Under this system, all these exchanges could in theory be managed in a frictionless, peer-to-peer manner that's validated by the network. Smart contracts and multi-signature key management systems could be written into the registry as well, to give owners sovereign control over their assets but also afford lenders and other interested parties the capacity to execute their security rights. Such a setup could enhance confidence among all users and potentially unlock financial services attached to those assets that could not be offered as collateral previously.

De Soto himself is seeking to use a blockchain registry to give, for the first time, assurances to rural villagers in Peru that they have title to their land, so they can negotiate royalty rights with large mining companies rather than engage in risky "informal mining" of their own. Meanwhile, in Honduras, the blockchain-based data management company Factom (http://factom.org/) has had discussions with the government to use the startup's time-stamping system to keep track of steps taken to survey land, validate ownership, draft title and record that information in the blockchain-based registry. Similar ideas are being considered by researchers looking at systems in Pakistan, India, and Senegal.

Yet the opportunity does not only lie in informal economies that lack titling systems. In the developed world, the creation of immutable registries and real-time, validated ownership transfers could disrupt the title insurance industry. Title insurers took in an estimated $11.3 billion in premiums in 2014 in the U.S. alone, according to the American Land Title Association (2015, March 20). With a fully validated, blockchain-based record, a buyer of a property could be assured immediately that the deed is free of liens or other encumbrances, obviating the need for time-consuming title searches and expensive insurance.

With other hardware technologies – RFID chips, for example – titling need not be limited to land. With a traceable GPS signal emitted from such chips, "movable assets" such as cars, motorbikes, machinery, street vendors' carts and sewing machines could be immutably registered on the blockchain to give lenders confidence that their loans can be properly securitized. In effect, the combination of these technologies and a blockchain ledger gives the lender the power to seize assets that were previously unattachable. As an added protection, chips could be empowered to temporarily disable a type of electronic equipment if the owner falls too far behind on loan payments. In theory, that combination of features should significantly lower the cost of financing such assets. Reliable records will also facilitate insurance of these assets – giving owners the option to insure their automobiles for damages or theft, for example, or allowing governments to viably require and monitor low-cost mandatory third-party injury insurance. In effect, it is a way to create a de facto health policy system for one source of medical costs: road accidents.

There's an opportunity here to greatly extend the definition of viable collateral for securitized finance – far beyond the typical registries of land and automobiles – thus, unleashing capital-raising powers in smaller sectors of the market previously excluded from this opportunity. Paired with the lower transaction costs that come with bitcoin and other digital currencies, making financial services at these previously prohibitively inefficient lower-funded levels viable, these innovations could conceivably lead to an explosion of microfinance.

Moreover, digital data and blockchain proof of records could also permit an extension of the definition of an asset registry to include intangible assets. A person could convert the blockchain-verified proof of their income, loan repayments, and other financial and work activities into a quantified value of economic and credit reputation that's registered as a standalone asset – intangible, yet clearly defined and viable as security for loans or insurance. Other registries of personal reputation-related data, such as transcripts of higher education could also be recorded on the blockchain so that a prospective employer or higher institution anywhere in the world could access it. Blockchain-based property title and reputation systems thus become important building blocks for financial inclusion.

There are various ways to organize blockchain-based asset registries into independent databases that boost efficiency. Within Bitcoin's blockchain, a colored coins application such as the Open Asset Protocol could create distinctly identified asset title transactions to distinguish them on the bitcoin ledger from those of pure currency transactions. Other bitcoin-focused systems have been designed to ensure that new, non-currency asset information doesn't create "blockchain bloat" and breach

the underlying protocol's current hard limit on block sizes. Factom, for one, creates a separate data layer that organizes multiple records into time-stamped sequences and then periodically records that data into the base-level bitcoin blockchain. ChainDB's data system, which forms its own chain of blocks, each of which is recorded as a hash into a single transaction on the bitcoin blockchain, similarly facilitates an "off-chain" organization of data that is nonetheless immutably tied to the decentralized Bitcoin blockchain without the need for certification by a trusted third party. Such a system could also be used to create a standalone title registry that's validated by Bitcoin's secure hashing power. Alternatively, a sidechain implementation such as the Liquid system created by Blockstream (https://blockstream.com/) could be used to run an independent property registry. This could function as a virtually independent blockchain, validated by a separate network of miners or a federation of computer owners, yet it could also be shown to be provably "trustless" because of a "lock" transaction with the main bitcoin blockchain that "pegs" the sidechain to it.

Other approaches avoid the bitcoin blockchain altogether. For example, some developers are building smart property transfer systems on top of the decentralized Ethereum system. Alternatively, some non-government organizations are exploring how consortia of NGOs, multilateral institutions, government agencies and regulated financial institutions could be formed to provide computing power under permissioned "federated blockchain" structures that are charged with validating and maintaining national or international asset title registries.

Goals

A properly implemented blockchain-based title registry would further the following goals, in order of relevance:

V) Human Empowerment

The lack of reliable property title in poor communities excludes billions from the core system of wealth creation on which western capitalism is founded. Without the ability to provably document and trade ownership rights in assets, the very opportunity of economic growth is all but denied to such people. Given that government bureaucrats have for decades failed to effectively implement analog, paper-based solutions to this problem, the blockchain's emergence offers opportunities for such places to leapfrog into similar systems of monetization as is enjoyed by Westerners. In the process, there may be a profound expansion in human empowerment.

V) Efficiency

Poor management of title registries creates enormous friction in the buying, selling and financing of properties. Even in places where they are relatively well managed, settlement of home purchases take months while agencies conduct title searches and lawyers and escrow agents rack up fees, all because there's too much uncertainty around the title and around the risk that it may carry an unforeseen lien or other encumbrance. In the West, these legal risks are covered by expensive title insurance. In the developing world it means people can lose their properties if a previously unidentified creditor to a previous owner successfully exercises their old claim. In both regions, the cost of protecting against such risks manifest in expensive legal proceedings. An immutable blockchain registry, allowing for instantaneous transfers for title and transparent, clear records, could remove a great deal of this friction and create much more efficient asset markets.

III) Transparency

It is article of faith that a blockchain ledger should be more transparent than the closed systems currently run by governments, either their digital versions or their even more outdated paper

records. What matters is how that transparency could contribute to greater confidence in governments themselves if they submit to the openness of a blockchain registry.

Key Players

There would be various beneficiaries, disrupted industries, and relevant actors involved in blockchain property title initiatives:

End users (consumers/households) – People who own homes and other assets in the developing world who have until now been unable to borrow against them or otherwise monetize their rights by using those assets as capital could now do so with the aid of a blockchain-based title or deed. They could get insurance and more easily sell their property and/or negotiate access to it with outside parties such as mining companies.

Regulators and policymakers (government registry offices) – Traditionally, governments have maintained property registries. But if such registries were transferred to a blockchain, what role would governments play in the titling process? They could still engage in endorsement, functioning as a certifying authority. They might endorse an authorized third party – an insurer, for example – to ascribe state-approved title to assets and embed that information into the blockchain.

Service providers (banks, insurance companies, and chipmakers) – Granting a vast new group of human beings with enforceable property rights should create new markets for securitized lending around the world. In this case, this technology is an opportunity for banks, not so much a disruptive threat.

For insurance companies this development is mixed. Auto and home insurance providers would likely welcome the opportunity to issue more insurance plans against assets that are immutably defined by blockchain entries. On the other hand, title insurance companies would likely go out of business or restructure to subsist on far lower fees.

In the case of movable asset registries, the prospect of using blockchain-enabled RFID chips to create a new form of securitized asset creates a market opportunity for chipmaker firms.

Status

As of the fall 2015, proof of asset ownerships and smart property projects are very much in the exploration stage. Factom's discussions with the Honduran government are nascent as are the pilot projects under consideration at the Digital Currency Initiative at the MIT Media Lab.

Within the coming year, those pilot projects will likely be launched in one or more developing countries, taking this concept to the initial implementation phase. The MIT Media Lab reports there is interest from funding institutions; multilateral agencies such as the World Bank and the International Financial Corp. and various IT firms are looking to build out such projects. Gaining government buy-in will be important for addressing some of these obstacles.

Threats

Threat 1: Attestation of land ownership inaccuracies

The blockchain seeks to prove that all information entered into a ledger has not been altered in any unauthorized way. But it can say nothing about the accuracy of that information in terms of being facts outside the blockchain. So, the first threat to progress with smart property in developing countries lies in the challenge of accurately and fairly affirming individuals' and institutions' ownership of hitherto un-titled properties. This is a current and ongoing threat to land titling

projects in particular because it is derived from political and community conditions that require institutional change or innovative tactics to get around those obstacles.

Residents of a shantytown, for example, must often depend on the local slumlord to attest to their ownership of their rudimentary homes. In many rural communities, it falls on the local village chief to make the attestation. The risks of trusting a third party can be acute in such situations.

And where the state has greater authority, the challenge for creating land title where none exists hinges on ensuring that proper procedures in terms of land surveys, claims arbitration, dispute resolution, etc. are followed. Corruption, human error and inefficiencies can subvert the process.

Threat Likelihood

The extent of this problem will vary greatly from place to place, depending on the technical aptitude and resources of government bureaucrats and how advanced the country's political institutions are. Taken in aggregate across the developing world as a whole, the existence of this threat is assessed as all but certain for land title projects, but only somewhat likely for movable assets that are registered at the point of sale.

Threat Severity

In neither case would this challenge be assessed as insurmountable or existential. It is a major threat for land title projects and a moderate one for movable assets, but in both cases innovative solutions are being developed and coordinated approaches, involving all stakeholders, can be deployed to resolve the threat.

Recommendations

For land titling, the solutions to this problem are political and strategic and will vary from place to place and culture to culture. But in general it is important to articulate incentives for local authorities to participate fairly in the attestation process. In places of weak central authority, the situation may be improved by applying creative incentives like those developed by Julius Akinyemi of the Wealth of Nations project, who has created an incentive-based reputation model for village chiefs in Senegal to attest to land ownership before the data is input into a digital registry. (In that case, it is not a blockchain registry as of now, but is likely to be upgraded to one.) Otherwise, there needs to be public awareness campaigns and lobbying efforts, much like those which Hernando de Soto is undertaking in Peru. And when it comes to state-based land registration, contemporary technology such as satellite imagery and drone-based surveys could improve the accuracy of geo-coordinates and property demarcation.

For movable assets that are titled at the point of sale by a licensed business such as a motorbike dealership or a telecommunications company, a third-party service provider could be licensed to act as authenticator on behalf of the new owner. If insurance is to be provided at the point of sale as part of this registration process, the insurer could take on this role. This would ease the process of inputting data onto the blockchain for people who are not necessarily tech savvy or familiar with private key management. However, some kind of smart contract, multi-signatory structure would also be necessary so that ultimate, self-sovereign control over the asset resides with the owner.

Threat 2: Device integrity issues

Another version of the broader problem of pre-blockchain fact accuracy relates to the integrity of the device being used to inscribe data to the blockchain. That can occur in the case of both land and movable assets and in the latter case goes beyond the computing device or smartphone used to write the initial transaction to include also the integrity of the chip and the signal that it sends to the blockchain. In all cases, the risk is that the device is somehow corrupted or hacked and so

able to send false information about the connected asset, corrupting the ledger and depriving the rightful owner of their rights.

Threat Likelihood

The likelihood that a device is not properly protected is probably more likely than not in developing world scenarios. Though the risk of there being widespread corruption of such devices might not be so high if the asset value is not especially high or if the asset is highly illiquid, like land. So, by that standard, the overall threat is only somewhat likely. A hacker has easier and bigger targets to go after than someone's motorbike in the developing world.

Threat Severity

By the same logic, the threat severity is not especially high, but will vary from place to place and from asset type to asset type. Overall, its rank is moderate.

Recommendations

There are various "trusted computing" modules being developed and a set of procedural protocols to follow, which give assurances that a device hasn't been tampered with, and thus, a user can feel more confident that what they are inputting to their device will appear in the final record. These should be followed where possible.

Threat 3: Lack of provable owner identity

Being able to accurately and reliably prove the identity of the person attesting to be the owner of a blockchain-titled piece of property is critical. And to complete the transaction that registers that title, the ID credential must be digitalized in some form. Without that, the registry can still be created but transfers of property and the addition and expiry of liens, etc., will still require the intervention of third parties, and the use of off-chain contracts.

Threat Likelihood

In the developing world, where poor asset title registries are matched with equally unreliable identity management, the threat of this posing a barrier to implementation without some kind of additional action is more likely than not to arise. The problem of "undocumented" persons is widespread.

Threat Severity

For the full implementation of a blockchain titling system, with the benefits of irrefutable, on-chain transfers of ownership, the severity of the identity threat is existential, because it can't proceed without it. However, that diminishes if the goal is simply to create a registry with third-party intervention whenever the ledger needs updating.

Recommendations

The ultimate goal should be to create digital identities that don't require state-issued ID documents, so as to bypass that failed bureaucratic function in many developing countries. This concept of identity, which draws on data analysis from people's digital economic behavior as measured by their social connections, transactions and activities in the online and mobile communications worlds, has been proven in labs to be viable with systems such as the Open Mustard Seed protocol. With privacy protection and encryption tools to give people self-sovereign control over their accumulated private data, these systems allow people to parcel out only those aspects of their identities, or attributes, that a particular service provider requires without divulging sensitive personal information. Placing this information into a blockchain setting makes it even more reliable for ID verification. These systems need to become the standard for blockchain-based property title deployments, as well as for many other blockchain 2.0 and 3.0 applications. And for that, there

needs to be a concerted effort to educate regulators and users about the benefits of these systems, so that they gain legal weight. (See the section on identity for further discussion on these kinds of identity issuance programs.)

Without developing such systems, there are other alternatives for rolling out property title in places that have more robust state-based identity issuance programs. This limits the potential market, but it's a reasonable place to start. One lies with new scanning systems developed for onboarding customers to bitcoin exchanges in compliance with know-your-customer guidelines. The information needs to be readable in such a way that it can be inserted as a hash into the metadata component of a property title transaction. Alternatively, early projects can be centered in countries that have developed national digital ID databases such as the Aadhaar system in India or that of Estonia. There are some concerns about the centralized nature of these highly sensitive databases, especially given that the Indian program allows the national government to monopolize hundreds of millions of people's biometric information – making a potentially very large cybersecurity target. However, to the extent to which they are already being used for multiple new financial services, Aadhaar and systems like it offer a useful readymade identity platform on which to trial property title registry programs with an eye to switching to digital identity solutions at a later date.

Summary

There is no doubt that the potential economic benefits of smart property and blockchain-based title registries could have a transformative impact on the global economy. Outdated and inaccurate record-keeping could be overcome, unnecessary costs could be slashed from the business of property management and asset transfers in ways that boost efficiency and, most importantly, a vast subsector of humanity could be empowered by a long overdue assertion of their property rights. Getting property title onto the blockchain could provide a building block for financial inclusion generally.

However, implementation is tricky, not least because – as with many of the non-currency applications for blockchain technology – real-world political, regulatory, and cultural factors pose barriers that must be overcome, irrespective of how well developed the technology is. Developers and other advocates for these solutions need to take a holistic approach to the undertaking, demonstrating their society-wide benefits and encouraging buy-in from governments, regulatory agencies, non-government institutions and financial institutions such as banks and insurers. Other technologies in the identity management realm, in the development of hardware such as traceable chips, drones and satellite imaging, should be incorporated into these efforts as well to overcome the many obstacles that have prevented progress in property titling for decades.

IV. Unlocking Capital through Tokenization of Unused & Underutilized Assets

Discrete Opportunity/Use case

The demand produced by an individual owner of an asset is often not sufficient to utilize the full potential of that asset. For example, over the lifetime of a vehicle, it remains parked and unoccupied in excess of 95% of its useful life – certainly not a significant amount of use by any measure. This means that unrealized value exits for underutilized assets. However, the underutilization of many resources and assets, throughout both developed and emerging economies, remains a problem relatively unaddressed by the existing centralized management structures. Very few mechanisms exist by which private assets and resources can be made available to a larger number of potential users. Moreover, the few existing mechanisms that facilitate the market for these under-utilized assets rely on profit-seeking institutions.

There exists a fundamental inefficiency in the distance between the management of an asset and the asset itself. This introduces an information deficiency, whereby no perfect model can be applied

to adequately utilize the underlying asset. However, Bitcoin offers an opportunity to ameliorate the deficiencies of the current model. For example, Bitcoin enables the tokenized representation of assets, such as the title and current responsible party for the vehicle described above, which is essential in increasing the efficiency of the shared network.

Bitcoin is the first successful digital token system. That is, it is a symbolic representation of an underlying asset—in Bitcoin's case, an amount of energy spent toward securing the system (through auditing). Though the Bitcoin protocol implements several other ideas necessary to make the system functional, the net result is a digital asset representing the provable work undertaken to generate it.

The idea of a digital token representing goods or services as divisible units introduces a number of useful optimizations not previously possible. In historical models, the tangible property of assets and services limited the scope of their use and utility. As a result of this inefficiency, new constructions, such as receipt money and securities, emerged to ease the lack of liquidity present in the transfer and securing of physical assets.

Digital tokens have no such encumbrance, and can be re-allocated at any time, without a need for transport, physical security, or jurisdictionally-defined legal enforcement. In place of legal enforcement comes mathematical enforcement, the idea that any individual token can be immediately validated against a shared ledger (i.e. the blockchain), allowing for a perfect, counterfeit-proof assertion of authenticity with minimal overhead.

As a result, these tokens introduce an entirely new class of efficiency in the transferability and subsequent trade of assets as they decrease costs by several orders of magnitude as compared to traditional physical or even legal contracts in existing markets. Since there is effectively no cost to creating a new type of token, the opportunity to represent previously unprofitable assets and services as exchangeable digital tokens is available to anyone with access to the Internet.

This introduction of a new, unparalleled capitalization opportunity grants access to a global market for the trade of those items, at nearly no cost for the holders of existing assets, ranging from time-share on vehicles to solar and wind-powered microgrids. Not only will existing assets be tokenized, but new business models and entrepreneurial opportunities will emerge as the market dynamics shift in the face of the massive influx of genuinely new capital.

Projects & Companies Related to Tokenization

There are now many players in the tokenization space, falling into two primary categories, Bitcoin Extensions and Centralized Issuers. Bitcoin Extensions attempt to build upon the existing Bitcoin protocol, minimizing the barriers to entry by focusing on technological improvements over commercial gains. Centralized issuers focus on commercial gain, and either change Bitcoin's security profile by introducing a counterparty or circumvent it entirely by operating as an authority on their corresponding tokens.

Bitcoin Extensions

Several ideas exist that extend the Bitcoin protocol without modifying or replacing it, which are the most broadly applicable technologies today. They no longer need to solve the "scale" problem to achieve sufficient security, as the production-deployed Bitcoin network has already achieved sufficient scale through its incentive mechanisms. These systems follow the decentralized security model that Bitcoin provides, with no single party responsible or able to manage their implementation or use.

Sidechains

Sidechains are a method for using bitcoin as a cryptographically-bound backing asset for the issuance of a token on a new, distinct blockchain, which may or may not share the same features as the Bitcoin blockchain. This is idea was introduced by existing Bitcoin Core developers, who in addition to developing working code to demonstrate the idea, have also recently introduced (in the form of a BIP, or Bitcoin Improvement Proposal) several "features" that were first tested on such a sidechain, including Segregated Witness and Confidential Transactions, which both measurably improve the security profile of the main Bitcoin protocol. One example of a side chain project is Liquid (https://www.blockstream.com/2015/10/12/introducing-liquid/) by Blockstream (www.blockstream.com).

Colored Coins

The idea of a "colored coin" is a simple one, where an existing token is "marked" somehow using the existing protocol. Most implementations use the existing Bitcoin protocol for the same reason as the extension protocols listed above. Two primary "colored coin" projects exist, OpenAssets (www.openassets.org) and Counterparty (http://counterparty.io). Of the two, Counterparty is the most widely used.

Centralized Issuers

Centralized issuers of tokens mirror the same model as the existing financial system, including a reliance on trust in a centralized issuer to correctly track the creation and movement of those tokens according to the rules of its construction. Existing laws, especially regarding counterparty risk (such as a centralized issuer having custody of consumer funds), apply directly to any tokenization scheme that follows this model. Many centralized token issuers are emerging, including: Chain (https://chain.com), BlockCypher (http://www.blockcypher.com), and Digital Asset Holdings (http://digitalasset.com).

Goals

This opportunity has the ability to improve consumer choice, access, privacy, and protection by reducing the startup cost of businesses and enterprises aiming to deliver competitive value to existing markets. It increases transparency by encouraging the use of blockchains to keep track of these tokens, which are by definition public and transparent. Furthermore, it improves efficiency by eliminating the expenditure resources on accounting, replacing it with an automated self-auditing system.

Key Players

Key players in the success of tokenizing underutilized assets include end users who drive demand, service providers who create uncomplicated/user-friendly platforms, relevant regulators and policymakers who determine the legal framework around which these platforms are developed, and venture capitalists who fund the development of these platforms.

Status

This opportunity is in the initial implementation stage. Colored coins are in production today and actively used commercially for a significant number of projects. Many new businesses have launched using Counterparty tokens, for example. Sidechains are also actively being commercially deployed.

Threats

Threat 1: Lack of Adoption

Threat Status

At present, people may not care about the capitalization of lower-value assets – in part, because they are unaware the opportunity to do so exists, but also because they may not see the benefits of

adopting or expending resources to develop this opportunity as too minor. Similarly, a cost-benefit analysis by regulators may skew away from the not immediately apparent benefits of this opportunity, overemphasizing upfront adoption costs.

Threat Likelihood
This threat is somewhat likely to have an impact on this opportunity; however, given the growing popularity of the sharing economy, it's more likely that people will adopt models that allow for greater employment and monetization of underutilized assets.

Threat Severity
This threat faced by this opportunity is major, if potential adopters are not apprised of the benefits of this opportunity or do not see find sufficient benefit to its development and adoption.

Recommendations
Those working on the development of tokenization technologies should partner with organizations that educate consumers as well as marketing firms to educate and provide guidance to consumers, regulators, policy-makers, and other users as to the personal and, perhaps, global benefits to adoption.

Threat 2: Inefficient Management Mechanisms

Threat Status
A blockchain that immutably stores a record of an asset's transference and custodianship offers a low-cost opportunity for recordkeeping and arbitration in the event of dispute, whether through overuse or other contractual violations. Without an efficient mechanism to manage these items, the model is reduced in its efficacy, as costs are lost over time to the overhead of the managing entity.

Threat Likelihood (as of today)
50/50 likelihood

Threat Severity
Major

Recommendations
The question remains as to which parties will undertake the initiative to start such an endeavor, especially the capital required to design and develop the initial work. VCs would stand to benefit from identifying the appropriate parties, because once such an investment is made, the system is freely utilizable by the global market, and may eventually be built in to underlying assets.

Threat 3: Regulatory Capture

Threat Status
Incumbents drive regulation that protect their incumbent status and discourage innovation in sharing of underutilized assets. For example, taxi cartels advocate for dropping the regulatory hammer on Uber or and the hotel industry does the same to AirBnb.

Threat Likelihood
50/50 likelihood

Threat Severity
Moderate

Recommendations
Community organizing is needed to build ground-up demand for these products/services so that governmental authorities cannot "ignore" constituent pressures. Regulation efforts should be focused at general purpose regulators (e.g. FTC), which are harder to capture than specialty regulators (e.g., FCC). Courts should scrutinize regulatory decisions under a meaningful standard with rigorous analysis. Products should be created in a way that constituents demand access to them, overpowering the pressure from incumbents to sway lawmakers.

Threat 4: Privacy Concerns and Risks

Threat Status
The perceived risk to privacy and security can create hesitation to share underutilized assets, such as used computing power.
Threat Likelihood
All but certain

Threat Severity
Major

Recommendations
Regulators should allow the market to develop. Supply and demand will drive participation if the underlying asset has real value. Privacy protections should be baked into the products/services as well as the language introducing these products/services into the marketplace.

C. Blockchain 3.0

I. Enabling Efficient, Effective, and Transparent Governance and Resource Allocation

Discrete Opportunity/Use case
There are a multitude of issues that prevent efficient, effective, and transparent governance and resource allocation. Censorship, corruption, redundancy, fungibility, avoidable waste, undue secrecy, overburdensome regulation, imperfect record keeping, outdated or inadequate security, etc. all hamper trust in and satisfaction with any entity that governs or allocates resources. This section primarily focuses on the opportunity presented by the blockchain to improve the inefficiencies, inadequacies, and corrupt practices of centralized governments as well as the entities granted stewardship over public resources by centralized governments.

Curtailing Corruption in Public Institutions
According to Transparency International's Corruption Perceptions Index (see Figure 2), few countries are free from concerning levels of corruption in the public sector.

"There is general agreement that the world would be a better place without corruption, but there is less general understanding of precisely what constitutes corruption" (Senior, 2006)[2]. While there is no universally accepted definition of corruption, the use of power for personal gain exists all across the globe. Corruption has many faces. Sometimes it is obvious, like the solicitation of bribes from politicians, bureaucrats, military personnel, or law enforcement agents. Other familiar and undeniable forms of corruption include: fraud, collusion, impunity, clientelism, extortion, patronage, embezzlement, tax evasion, money laundering, regulatory capture, conflicts of interest, etc.

---

2 Senior, I. (2006). *Corruption-The World's Big C. IEA Research Paper, (61).*

In other cases, however, corruption can be subtle, discreet, and can even escape the notice of those helping to carry it out, such as withholding information without due cause or the misappropriation of public funds to buy alcohol for the office holiday party of a publically funded non-profit organization (an "unallowable cost" or improper use of public funds according to the U.S. Internal Revenue Service). Nepotism and cronyism are also less conspicuous forms of corruption that pervade society, are extremely difficult to monitor or prove, and easy to overlook as being corrupt practices because they are so commonplace. Still other corrupt activities are more difficult to monitor, prove, and enforce action against, such as: transfer pricing, revolving doors, shell corporations, secrecy jurisdictions, political contributions, tax havens/offshore banking, and even lobbying if conducted in a non-transparent manner. (Transparency International has developed a thorough Anti-corruption Glossary, which defines corruption, outlines the levels of corruption, details the various types of corruption, identifies the key players involved in corruption, and explains some of the tools and frameworks available to combat corruption.)

All persons and institutions in positions of power or authority, no matter how great or small, are susceptible to the potential practice of intentional as well as inadvertent corruption; however, public institutions, foundations, non-profit and non-government organizations (NGOs), and the various other entities that subsist on public funding or tax-exempt charitable donations are accountable to a unique set of stakeholders - the public. These entities, heretofore referred to as public entities, are often (or arguably should be) subject to standards of accountability for their use of public funds and many are barred from engaging in activities that may promote special interests, such as engaging in practices that constitute lobbying or accepting gifts if holding a public office. Despite the existence of such standards, the systems employed to prevent unethical actions and abuses of power among these entities are immensely flawed, ineffective, or in some cases absent (where rule of law is tenuous). "There are many social and moral problems created by corruption, but from an economic perspective it has to be regarded as a serious impediment to the proper functioning of a market economy. It also has the effect of redistributing wealth away from the poor towards the better-off and towards employees of government" (Senior, 2006)[3]. Moreover, "Without competitive markets for public goods and services, it is difficult to ascertain the social value placed on public programs" (Hirschey, 1996)[4].

The opacity shrouding the actions and expenditures of these entities propagates inadequate accountability and distrust of centralized authority and publicly funded institutions, among other issues. Greater transparency can improve visibility and reduce or limit misappropriation, misdirection, and other illegitimate uses of power. Distributing the management of public information, such as records, procedures, processes, procurements, solicitations, awards, penalties, audits, etc. would address many issues that come into question when transparency is lacking. The blockchain serves as an immutable database of digital information that could be employed to increase transparency. All data directly encoded (i.e. submitted as a valid, signed transaction and written to a confirmed block) on the blockchain is available and verifiable by any entity that has a copy of the full blockchain.

For data that is too large to fit in a transaction or set of transactions, hash values of the data to be written to the blockchain can be created such that proof of existence and data integrity claims can be independently verified. Tokenization of the data – writing it into a digital token, such as a bitcoin – can also implement access controls such that only those with the token (e.g., an asset that has been transferred to a public key/address) can discover and/or decrypt the data. In this case, however, the data must actually be stored off chain in such a manner that it should remain available to anyone who requires access. For some data, such as media files, or content too large

3. *Senior, I. (2006). Corruption-The World's Big C. IEA Research Paper, (61).*

4. *Hirschey, M., Pappas, J. L., & Whigham, D. (1996). Managerial economics. Dryden Press.*

to be stored on the blockchain, distributed databases or other technologies may provide sufficient guarantees about discoverability and availability.

Utilizing blockchain technologies to automate processes and procedures (i.e. create executable policies/procedures on the blockchain) may ensure they are properly followed, limiting intentional or unintentional discretion in execution as well as opportunities for extortion, bribery, etc. Additionally, the Blockchain could enable real-time, irrefutable financial auditing as well as real-time "proof of reserves" in banking systems or "proof of solvency" in governments.

The implementation of blockchain technologies allows for immutable, distributed public ledgers to instill trust, efficiency, and legitimacy where previously lacking. If all records are freely available for public inspection, corruption would have fewer places to hide.

Fostering Government Accountability through Better Government Transaction Monitoring, Procurement Tracking, and Grant Flow Tracking

Distributed blockchain ledgers can be used to track government receipts and expenditures to ensure revenue is generated appropriately and that expenditures align with intended use. For example, some citizens complain that parking enforcement is used as a form of racketeering to generate revenue off motorists, while little expenditure is made to improve roads and access to public parking. A distributed public ledger housing parking enforcement revenue and government expenditures on roads and infrastructure improvements would shed some light on this concern. The blockchain can also be used to track government tendering processes and procurement flows to ensure accountability to the established procedure as well as accountability in the disbursement of funds as allocated, and to encourage civic awareness and interest in the expenditure of public funds. This would curtail issues like the Department of Defense audit report (published in 2013, released September 2015 via Freedom of Information Act request) which may have unveiled the illegal use of government funds to support lobbying efforts by defense contractors for the Department of Defense. Similarly, the blockchain can be utilized to track government grant processes and award flows to ensure accountability to the established procedure as well as accountability in the disbursement of funds as allocated, and to encourage civic awareness and interest in the expenditure of public funds to non-profit organizations, educational institutions, and other recipients of public grants. Blockchain technologies can also be employed to provide "proof of source" (i.e. supply chain transparency) in the production or acquisition of goods and services purchased with public funds.

More accurate measurement of when, where, how, and for what purpose public funds are allocated and disbursed can build confidence in publicly funded programs and institutions.

Charitable Distribution Monitoring to Foster Public Trust for Tax Breaks

Much like the government procurement and grant monitoring described above, charitable organizations that accept and disburse tax exempt donations could engage in voluntary self-reporting via the blockchain to help ensure accountability in the disbursement of funds not subject to taxation.

Precluding Censorship by Government Entities

While the U.S. government funnels international aid money and efforts toward curtailing censorship abroad, the U.S. government is not free of irreproachable when it comes to domestic censorship. In 2015 the U.S. government acknowledged in almost 1 in 3 Freedom of Information Act

(FOIA) requests the initial decision to withhold records was not legal. Additionally, in the last year, the backlog of FOIA requests has increased by 55 percent.[5]

Abroad, censorship is largely used to quash collective action. The threat of social mobilization leads some governments to take access to technology away from their citizens in order to maintain order and control over their power. Notable recent instances of this include the swath of Middle Eastern governments, such as Bahrain, Egypt, Libya, Syria, and Tunisia, Saudi Arabia, which restricted access to the Internet and social media websites and mobile apps during the Arab Spring. Other governments implement more systematic long-term censorship programs, such as China, Iran, and North Korea.

For example, the Chinese government routinely censors social media content; however,

> "Contrary to previous understandings, posts with negative, even vitriolic, criticism of the state, its leaders, and its policies are not more likely to be censored. Instead, ... the censorship program is aimed at curtailing collective action by silencing comments that represent, reinforce, or spur social mobilization, regardless of content. Censorship is oriented toward attempting to forestall collective activities that are occurring now or may occur in the future—and, as such, seem to clearly expose government intent" (King, Pan, and Roberts, 2013)[6]

This became evident during the 2014 Hong Kong protests (also referred to as the Umbrella Revolution or Umbrella Movement), when Chinese authorities filtered Internet access and censored content pertaining to mobilization.

In some cases, social movements like the 2014 Hong Kong protests have been able to circumvent government sanctioned blocks to Internet access through the use of mesh network – the use of localized technologies that do not require Internet access, but instead use peer-to-peer data and information sharing, such as Blue Tooth enable mobile phones – however, this does not necessarily prevent the censorship content which is often house on servers governments may be able to control. This is where blockchain technology becomes relevant. As stated above, the blockchain serves as an immutable database of digital information. While not all data, whether due to size or significance, can be encoded directly on the blockchain, proof of its existence can be. This means that if a government attempts to wipe content from a server or web service that has been inextricably encoded on the blockchain, its existence (i.e. logged and verifiable record of a specific file or piece of data with an exact form) cannot be erased.

Eradicating Impunity

Impunity, exemption from the reach of the law, exists in developed and developing nations alike. In developed states it often manifests as failure to hold the perpetrators of white collar or "victimless" crimes accountable for their actions. In cases where less than a handful of perpetrators are implicated, ownership of the crime is straightforward and easy to attribute. In cases where responsibility is shrouded behind complicated layers of bureaucracy and corporate hierarchical structures, culpably is markedly less simple to ascribe. Take the case of the 2014 General Motors recall. After an 18-month investigation, the U.S. Department of Justice could not clearly identify and prove the willing participation of the individual actors who chose not to disclose or act on the safety hazard posed by a faulty ignition switch, which ultimately resulted in the death and severe injury of

---

5. *http://www.huffingtonpost.com/2015/03/18/us-government-files_n_6893618.html*
6. *King, G., Pan, J., & Roberts, M. E. (2013). How censorship in China allows government criticism but silences collective expression. American Political Science Review, 107(02), 326-343.*

hundreds of people. (GM only ever claimed responsibility for 124 deaths; however, ongoing litigation against GM includes over 1,200 people. Additionally, 90 percent of the roughly 4,400 claims submitted to GM for compensation were denied.[7]) Although several employees were fired when the story broke, plausible deniability was too strong for federal prosecutors to lay charges against individuals. Examples of such impunity exist within government as well. Former President Richard Nixon, former General David H. Petraeus, and former House Speaker Dennis Hastert all committed punishable crimes they did not stand trial and serve time for, either because they were offered generous plea deals (typically not offered to those without stature) or they were never charged in the first place (again, uncommon among those without stature). Currently, it seems likely that former Secretary of State (and presidential hopeful) Hillary Clinton will circumvent charges for crimes she may have committed while Secretary of State.

If local, state, and federal law, along with internal governing procedures were codified in the blockchain as executable actions (i.e. smart contract), deviations from approved actions would not be possible without the implementation of a override, which would be recorded on the blockchain, bringing light to the discretion that gives rise to impunity, thereby diminishing its prevalence.

In developing nations, impunity often manifests as freedom from prosecution for those who have committed direct crimes against individuals and groups, such as soldiers who rape civilians under their authority or the leaders of genocide or other mass atrocity movements, such as a number of former or current leaders or military commanders in Bosnia, Rwanda, Cambodia, and the Democratic Republic of the Congo. These individuals rarely face repercussions for their actions, because the mechanisms by which they could or should be held accountable are often broken. "Where political organizations and civil society are weak or non-existent officials may wield power with impunity… and conflicts in society are less likely to remain moderate" (Johnston, 2005)[8].

Greater transparency through blockchain technologies could increase accountability, provide more accurate monitoring and evaluation across government, non-profit, and for-profit entities while democratizing financial and service delivery systems. While this opportunity is universally applicable (again, see Figure 1), it is particularly valuable in areas where the cost of corruption is significant, such as in underdeveloped economies. Reducing these costs through the implementation of a publicly auditable and verifiable digital currency system could be an immense gain for the impoverished and otherwise disadvantaged parties.

Examples

Blockchain technologies are starting to be employed in ways that monitor or facilitate government spending, which, whether intended or not, can help curtail corruption, improve transparency, and increase accountability in public entities. Three such examples include Pythia, Factom Inc., and GovCoin Systems (a blockchain-based system, not to be confused with the concept of GovCoin or #GovCoin described by the Bitcoin and blockchain community as a centralized blockchain protocol run/maintained by a centralized state authority).

The Isle of Man is considered to be the first centralized government to takes steps toward the adoption of blockchain technologies in and has done so with the assistance of the Pythia-developed and owned platform CREDITS, a "federated blockchain framework able to communicate agnostically with other chains and solely act based on information contained outside the ledger." Though only a pilot program, the Isle of Man's Department for Economic Development began storing and securing a government registry on the blockchain to serve as a "proof of stake" of cryptocurrency companies operating on the Isle of Man in May 2015. While seemingly minor, the registry is the first

---

7. http://www.wsj.com/articles/more-than-90-of-gm-ignition-suit-claims-rejected-1440453913

8. Johnston, M. (2005). Syndromes of corruption: wealth, power, and democracy. Cambridge University Press.

official government activity under development to be recorded on the blockchain with the blessing of a centralized authority. As of September 2015, the UK Government is also now exploring how to improve public registers using the blockchain.

Honduras, not far behind the Isle of Man, solicited the services of Factom, Inc., in conjunction with Epigraph, LLC, in May of 2015 to aid the country in the development of an immutable and secure land title registry using a blockchain-based platform. This step by Honduras is a significant one, considering the county's history of land seizures and other land rights abuses by its government. When completed, this registry will be a major milestone for government transparency, serving as a model for other governments to follow. Utilizing a decentralized public ledger to record property titles will combat corruption, or at the very least, bring it out in the open if government officials alter the titles in the register without regard for property rights and the rule of law. This example is explored more deeply in the section on "Proof of Asset Ownership/Smart Property."

While still in its infancy, GovCoin Systems intends to transform the way governments distribute value by leveraging blockchain technologies to reduce friction in government transactions, namely the distribution of social welfare. The obvious advantage of such a system is the reduction of transaction costs, allowing for a greater portion of the disbursement to be directly distributed to the intended recipient by cutting out the fees and the costs associated with executing and manually monitoring such a program. However, the less obvious, but far greater advantage of implementing a technology like that offered by GovCoin Systems is accountability in government spending. From the issuing agency to the supermarket purchase, tokenized disbursements can be tracked to ensure that the recipient is eligible to receive the disbursement and that the token is used for its intended purpose. This would allay taxpayers concerns about social welfare fraud. GovCoin goes so far as to tokenize social welfare beyond payments for food, but also the provision of housing and other basic needs. The company's technology relies on the development and adoption of secure and verifiable digital identity, be it on the blockchain or otherwise, in order to ensure that government disbursements are delivered to the appropriate recipients.

Goals

I) Efficiency

If adopted, efficiency will be greatly improved by this opportunity. Blockchain technologies that curtail corruption improve efficiency by enabling the reduction of friction in transactions and processes (i.e. the ability to add unauthorized costs or "take a cut" under the radar), reducing the time it takes to conduct transactions and processes, increasing awareness of redundancies, and improving the ability to act on a host of other problematic issues. Financial audits can be conducted in real-time, with less subjectivity and more complete information. The adoption of automated procedures and processes on the blockchain will reduce red tape and the time it takes bureaucratic entities to process approvals. Additionally, automated procedures and processes will expedite dispute resolution.

II) Human Empowerment

Increased transparency in governance and resource allocation, as well as greater access to information and freedom from corruption, all grant individuals and groups greater agency over their person. Improved access to information empowers people to make more informed decisions and to question whether decisions are being made in their best interest, while less corruption fosters greater financial, physical, social, and bureaucratic mobility.

III) Direct Self-Governance

While this opportunity focuses on enabling efficient, effective, and transparent centralized governance, increased direct self-governance will be a likely byproduct of automating governance systems. For example, the adoption of a blockchain-based voting system could allow for new

models of consensus, such as liquid democracy, where voters are able to vote directly on any issue, as well as consensually delegate their votes to subject matter experts as well as more traditional political representatives. While having the ability to withdraw and reassign their delegated voting privilege at any time.

IV) Transparency
This is the primary goal served by this opportunity. As stated above, the blockchain serves as an immutable database of digital information that could be employed to increase transparency. All data directly encoded (i.e. submitted as a valid, signed transaction and written to a confirmed block) on the blockchain is available and verifiable by any entity that has a copy of the full blockchain. Greater transparency can improve visibility and reduce or limit misappropriation, misdirection, and other illegitimate uses of power. Distributing the management of public information, such as records, procedures, processes, procurements, solicitations, awards, penalties, audits, etc. would address many issues that come into question when transparency is lacking. Furthermore it would help curtail corruption by limiting the ways in which it can be masked or conducted.

V) Consumer Choice, Access, Privacy, & Protection
Enabling efficient, effective, and transparent governance and resource allocation increases both consumer access, namely to information, and consumer protection, namely from corruption. Pulling backup the curtain on government services gives consumers, who are also taxpayers,

Key Players
End users - The governed, or consumers of public services, are directly, and in some cases, materially affected by government efficiency, effectiveness, and transparency, as well as corruption in the public sector. They will need to advocate for change in order to encourage and expedite the process of government adoption of blockchain technology.

Service providers - Centralized government institutions and their public servants hold a key role in this opportunity as they determine and facilitate access to government services and information. The developers of tools that enable the automation of processes on the blockchain are essential to the achievement of this objective, as they are necessary to design and execute interoperable software and databases that function on top of the blockchain.

Relevant regulators and policymakers - All policymakers and regulators are implicated in this opportunity, because all would need to prepare for the adoption of new technologies. Policy makers would mostly likely need to mandate the use of blockchain technologies in order for such a program to get funded so that regulatory bodies (and service providers) can employ them.
Venture Capitalists (VCs)/Funders - Aside from potential businesses to invest in or government contracts to win as a result of the government's adoption of blockchain technology, these actors will have a limited role in this opportunity.

Legacy Services and Institutions - These organizations may be subject to new, but potentially less burdensome regulation. Their reporting requirements will likely change, and as such, they may lobby or exercise other means to resist change (such as legal challenges).
Bad Actors - Security is paramount for the success of this opportunity and bad actors may attempt to weaken the security of government adopted technologies. Furthermore, crime tends to finds a way and bad actors may innovate new ways to commit corrupt actions through new technologies.

Intermediaries - IT security specialists and cryptographers, as well as legal and compliance experts who specialize in blockchain technologies and the related regulations, will have significant roles in helping parties who adopt blockchain technologies with ensuring they have taken all the appropriate legal and security measures for the proper adoption of the technology.

Status

Exploration Phase: This opportunity is in its infancy and likely won't gain any real traction for the foreseeable future. Change of this magnitude takes time. As demonstrated by the real-world examples above, there are some applications under development or in trial stages; however, a dramatic shift will require a level of education, consensus, and mobility not easily achieved. Policymakers, regulators, public service providers, public service users, and so on will all need to adopt and become comfortable with the technology.

Threats

Threat 1: Powerful Incumbents

Threat Status

Governments that consider adopting technologies geared toward increasing transparency will face pushback from those who exploit current systems in order to obtain benefits - financial kickbacks, elevated status, increased power, etc. Agents, fixers, introducers and other middlemen in position to extort, as well as political groups or state actors with entrenched interests will be particularly resistant to government adoption of technologies that will limit their edge or authority. At present this threat is nonexistent, as few government entities are considering adopting blockchain technologies; however, when governments move toward a meaningful policy of adoption this threat will become apparent.

Threat Likelihood

It is all but certain that those who stand to lose from the implementation of blockchain technologies to increased transparency will use whatever means they can to block the adoption of technologies that will limit income, power, or elevated status achieved through corrupt or manipulative methods.

Threat Severity

The threat of powerful incumbents blocking government adoption of blockchain technologies is existential but will eventually be overcome with a strong coordinated effort over time.

Recommendations

Consumers, businesses, core developers, the "blockchain community," and other users can encourage and foster the development of a natural market and build reward mechanisms for transparent institutions. Incumbent institutions, organizations, and industries that work with governments should proactively adopt blockchain technologies in order to stay ahead of competitors and new entrants employing blockchain technologies. Regulators and policy makers should do what is in their power to facilitate the adoption of blockchain technologies, by furthering the studies already underway of its various applications, not in the least, those which ease the burden on policy makers and regulators.

Threat 2: Ideological Pushback

Threat Status

Blockchain adoption for use in government will face ideological pushback, in part, due to some of the same reasons described above regarding entrenched interests; however, deeply ingrained notions of "this is the way government has always worked" are also difficult to combat. If the only government people have ever known is corrupt and coercive they may resist a new model, as the unfamiliar might be worse than "the devil they know."

Threat Likelihood
This threat is all but certain. People are resistant to change and governments are slow to move.

Threat Severity
Initially, this is an existential threat; however, it will likely transition to being a minor once the value of adopting blockchain technologies is recognized.

Recommendations
If entrepreneurs, businesses, core developers, and the "blockchain community" wish to see government adoption of blockchain technologies, they should first focus their efforts on non-government organizations (NGO), non-profit organizations, charities, foundations, etc. which work with government entities and government funds, but which are much more tolerant to change. As above, incumbent institutions, organizations, and industries that work with governments should proactively adopt blockchain technologies in order to stay ahead of competitors and new entrants employing blockchain technologies. Transparency will become a differentiating factor and entities that adopt it will set themselves apart from their peers, becoming more successful as a result of their decreased costs and increased efficacy of delivering funds to their intended recipients.

Regulators and policy makers should do what is in their power to facilitate the adoption of blockchain technologies, starting by furthering the studies already underway of its various applications. Hosting more frequent and broader briefings on blockchain technologies for legislative and regulatory entities will go a long way to educate those who may be hesitant to pave the way for adoption.

Threat 3: Privacy Concerns

Threat Status
The existence of a decentralized immutable record of information on government affairs and the citizens who utilize public services is both a current and future concern in terms of privacy, the perception of privacy, and the value of anonymity from the public perspective. The right to make contributions anonymously or privately, and the way this right is perceived from the public perception even if citizens are not losing this right, will be affected by the implementation of blockchain technologies in government affairs.

Threat Likelihood
Given the culture of privacy concerns that already exist within modern society, it is all but certain that consumers of government services will express concern or push back against the adoption of blockchain technologies that house records containing private or sensitive information.

Threat Severity
Initially, this is a major, but surmountable threat to the adoption of blockchain technologies in government affairs. Once people are able to trust that their privacy and anonymity can be protected, the severity of this threat will lessen.

Recommendations
To foster confidence in privacy on the blockchain, the "blockchain community" and core developers could work on developing and encouraging the adoption of zero-knowledge proof-based systems (ZKP) for individuals, and enable the transfer of assets between the privacy-focused ZKP monetary base to that of a publicly auditable institution. Examples of such solutions include "stealth addresses," Zerocash, and Zerocoin; however, these solutions in turn create their own set of issues

for regulators and law enforcement agencies working against various types of fraud as well as money laundering and terrorist financing, which such applications may enable.

Businesses and individuals creating products that address privacy concerns should bear regulatory compliance in mind as they develop. Likewise, regulators, law enforcement, and policy makers should bear in mind that individuals value their privacy and anonymity and if no government sanctioned services address their concerns, a black market may develop outside the arm of the law that would likely have far greater consequences than what could have been developed with government oversight.

Threat 4: Off-Chain Transactions

Threat Status

Currently, legal and illegal transactions can be conducted without record using cash, drugs, sex, gemstones, precious metals, valuable goods, and virtually any tradable asset. The benefits of moving government procurement and procedures/protocols onto the blockchain (using smart contracts) are based on a model of full transparency, which would theoretically flush out bribes and other illicit or coercive activity by government officials or stewards government funds. However, it is unlikely that a perfect model will develop where no off-chain transactions occur.

Threat Likelihood

The threat of off-chain transactions is all but certain, given that not all transactions can be monitored.

Threat Severity

If blockchain technologies were to be adopted and implemented on a mass scale throughout government, the threat of off-chain transactions would be moderate. That is not to say that the types of transactions occurring off-chain would not sometimes be of a serious or illicit nature, but the threat of such transactions only has moderate implications for the achievement of this opportunity. The adoption of blockchain technologies would limit the means and methods for illicit activities, likely making illicit off-chain transactions more difficult to coordinate and easier to police.

Recommendations

As with privacy concerns, overbearing regulation, law enforcement efforts, and future policy regarding blockchain technologies could drive a black market for off-chain mediums of exchange, therefore efforts in this arena should be mindful of the unintended consequences overly burdensome regulation can cause.

Threat 5: Loss of Discretion and Arbitration Challenges

Threat Status

In the future, there may be some trade-offs for the efficiencies offered by using smart contracts to execute protocols and commence transactions, including the loss of discretion and difficulties in achieving arbitration. Some argue that discretion is sometimes necessary in the application of rules and regulations and are reluctant to accept a model that does not allow for the application of discretion where appropriate. Others argue that the smart contracts employed through the blockchain pose challenges to achieving arbitration, in part again, because there is no room for discretion.

Threat Likelihood

This threat is somewhat likely to limit or preclude governments from adopting smart contract models to implement policies, procedures, protocols, rules, regulations, and laws.

Threat Severity
If there were no way to mitigate this threat, it would likely be a major roadblock to blockchain adoption by governments; however, because there are various ways to build allowances for discretion into this or any model, this threat is minor.

Recommendations
Potential changes to the Bitcoin blockchain protocol by its core developers that require all parties to an agreement to authorize or "sign" certain types of transactions could pave the way for the introduction and adoption of smart contracting, using an agreed upon third party arbitrator. Some contracts can be executed by blockchain technology, as in the moving of digital assets, but some contracts (e.g. performance-based) would still require a centralized authority for enforcement. Arbitration of this nature can be baked in to smart contract software, requiring the timing of specific keys to be signed if both parties are still in agreement to follow through. Therefore, law firms and ombudspersons can offer this arbitration as a service offering in the software.

Threat 6: Distrust of the Technology Due to Lack of Adoption

Threat Status
This opportunity may become threatened in the future if blockchain technologies never become easy enough for mainstream users to feel comfortable using it.

Threat Likelihood
This threat is highly unlikely, because, as we've seen with the penetration and adoption of the underlying protocols of the Internet, users of technologies do not need to understand or even trust the underlying protocols that drive technologies in order to find value in them or use them.

Threat Severity
The threat of this opportunity not being achieved due to a distrust of the technology is minor.

Recommendations
Entrepreneurs, businesses, developers, and the "blockchain community" need to develop (and currently are developing) better tools that are easier to use. Writers, bloggers, and technology evangelists would be valuable in helping to educate consumers and government representatives on these new tools, but ultimately the innovation in experience and simplicity needs to be driven by the desire to benefit from the model.

II. Efficient Provision & Management of Public Goods through Collective Action

Discrete Opportunity/Use case
One possible application of Blockchain 3.0 technology is the facilitation of collective action in physical or virtual common spaces, while mitigating the so-called "Tragedy of the Commons." This describes how self-interested actions by individuals and groups run contrary to the interest of a community or society as a whole by damaging, depleting, or otherwise harming a common resource or public good or space. Physical common spaces include common property having specific geographic bounds such as streets, parks, waterways, or other public property. Virtual common spaces can be described as fluid networks, not tied to fixed physical boundaries or finite resources, providing for delivery of commodities and services such as power generation, water supply, transportation logistics, broadband deployment, or small- or large-scale security or defense.

Due to its distributed, selectively transparent, and immutable nature, blockchain technology, along with cryptographic signatures, has the potential to provide proof of identity, proof of consent by a

single party, proof of joint consent (consensus) by multiple parties, proof of reputation i.e. "good actor," proof of transfer of ownership of some claim, proof of triggering preconditions, self-executing contracts, and proof of post-effects. Many of these aspects could be useful in empowering and managing the incentives of a group engaged in utilizing, consuming, sharing, and preserving a particular class of resource, while minimizing or eliminating the traditional overhead required to maintain a commons.

Elinor Ostrom, winner of the 2009 Nobel Prize in Economics for her research on commons management around the world, devised eight principles for successful management of a commons. Blockchain technology could be used to facilitate the principles outlined by Ostrom.

A special use case for blockchain technology could be to help enable free and fair voting and other alternative decision mechanisms. There have been serious questions about the integrity of proprietary, closed-source electronic voting systems, and this undermines public trust in the outcome of elections. Many municipalities resort to hand-counted paper ballots to determine the outcome of an election. This is hardly a modern day solution.

Using an open source, blockchain based system, the integrity of participation and outcome for a vote in a particular election or on a particular issue could be made secure despite the platform existing on the public Internet. Most advanced countries operate using some type of Western-style representative democracy, where the public elect representatives once every several years, and then rely on those representatives to vote in agreement with their constituents on most issues. A blockchain based voting system could lend itself to new forms of democracy, such as liquid democracy, where voters are able to vote directly on any issue. Voters could also consensually delegate their votes to subject matter experts as well as more traditional political representatives, while having the ability to withdraw and reassign their delegated voting privilege at any time.

Goals

Using blockchain technology to provision and manage public goods has the strong potential to incentivize and encourage the formation of intentional, overlapping communities, where members are able to work together with limited friction or bureaucratic overhead and are able to give and withdraw consent at any time. This would primarily further the goals of direct self-governance and human empowerment, while secondarily promoting efficiency, transparency and consumer choice.

Key Players

Key players in this process would be service or resource providers, intermediaries such as resource appropriators, relevant regulators and policymakers, software and systems developers, and end users.

Status

Any real world implementation of a system to provision and manage public goods is largely theoretical at this point. Major impediments to overcome are 1) the general public's lack of familiarity with blockchain technology and cryptographic systems, 2) the ability to tokenize and meter physical goods and services and tie them to electronic records, 3) the lack of user-friendly platforms and systems that would facilitate these processes, 4) players and institutions that have a vested interest in maintaining the status quo.

More typical voting systems will likely be developed and implemented on a wide scale before systems directly concerned with provisioning and managing public goods are developed. Examples of such voting systems currently in development include V initiative, BitCongress, and Agora Voting.

Threats

Major threats to the implementation of any such system include entrenched bureaucracies and governments as well as agencies that have been traditionally granted near-monopoly status such as power, water, and cable Internet companies. For blockchain enabled alternatives to begin and thrive, they'll likely need to exist in parallel with existing infrastructure, allowing users to adopt the new system as an alternative, similar to the way Uber and Lyft have been able to compete with and supplant taxicab monopolies in many places by gradually gaining a larger and larger voluntary user base.

In the case of voting systems, new laws and regulatory changes will need to take place so that the outcomes of such votes are granted legal status and attendant credibility.
In any case, systems will need to be designed in such a way as to be user friendly and easily adopted by the masses.

III. The Opportunities and Challenges Bitcoin and the Blockchain Pose for Law Enforcement

One of the primary potential obstacles to the growth of Bitcoin and the blockchain is a reputational issue – the misperception that bitcoin is the "currency of criminals." That perception problem can have real consequences for adoption, for investment, and for treatment by lawmakers and regulators. But it's important to keep in perspective that although the blockchain is revolutionary, it is just the most recent example in a decades-long chain of technological advances that were adopted early by criminals, forcing law enforcement to play catch-up. Law enforcement has faced this challenge time and time again – from fax machines to pagers to "push to talk" cellphones to email to Skype, law enforcement repeatedly has been forced to innovate and evolve as new technology designed for legitimate purposes is used to facilitate criminal activity. Indeed, law enforcement and other government agencies faced many of the same concerns they have about digital currencies during the early days of commercial use of the Internet itself. And while even today there is rampant criminal activity on the Internet, no one thinks of the Internet as the "network of criminals" – instead, we know it as a technological phenomenon that has transformed the way we live, communicate, socialize, learn, and do business.

So the challenge for law enforcement posed by Bitcoin and the blockchain is not unique. What is unique is that this particular technological advance can be an asset to law enforcement. The key for law enforcement is mastering the technology to unlock its potential to advance investigations. And industry and law enforcement have a shared interest in helping law enforcement advance along the learning curve as quickly as possible. After all, a stable, secure blockchain that is safe for lawful commerce is good for everyone – except criminals.

To be clear, there are certainly aspects of Bitcoin that present challenges to law enforcement. Principal among these is the problem of identifying an individual user from a bitcoin address. But this issue is in no way unique to virtual currencies but rather is part and parcel of any investigation of criminal activity facilitated using the Internet.

Indeed, the problem of attribution – often referred to as "putting fingers at the keyboard" – is perhaps the greatest challenge for any investigation of cybercrime, or any other type of crime committing using the Internet. Every day, agents and prosecutors have to figure out ways to tie a particular IP address, chat ID, MAC address, or email address to a particular human being or group of human beings. That process is made harder when the bad actor uses multiple IP addresses, or proxies, or Tor, or other anonymizing technologies. It also doesn't help law enforcement with attribution that providers maintain records for inconsistent periods of time and often have deleted those records before law enforcement has the opportunity to seek them. Nor does it help that webmail providers lack "know your customer" requirements, so they cannot verify the accuracy of user information. Of course, the same is true for cellphone companies. Indeed, if you go by sub-

scriber records, two of the most prolific drug dealers encountered by federal prosecutors in recent years were "Mickey Mouse" or "Joe Customer," based on the number of cellphones subscribed under those names. As you can imagine, subscriber records with fictional names are utterly useless and do nothing to help the process of identifying a suspect. Yet law enforcement agents work tirelessly every day to overcome those challenges, and the solution often lies in analyzing data from multiple sources to try to zero in on the particular bad actor.

Some have also expressed concern about the global nature of bitcoin, and the resulting need for law enforcement to obtain cooperation from foreign partners who may operate under different regulatory and legal regimes. That, too, is true of any investigation of Internet-based crime, as well as many investigations of crimes committed through traditional financial institutions. Indeed, because cybercrime, organized crime, financial crimes, and so many other types of crime are increasingly global, it's often difficult to investigate and prosecute cases without the cooperation of foreign counterparts – some of whom are in countries that are not so cooperative.

But Bitcoin and the blockchain provide significant advantages for law enforcement as well. The most obvious is that the blockchain allows one to trace all transactions involving a given bitcoin address, all the way back to the first transaction. That gives law enforcement the records it needs to "follow the money" in a way that would never be possible with cash or even with credit cards. That's true despite the perceived anonymity of Bitcoin – because reports of Bitcoin's anonymity are greatly exaggerated. A user's bitcoin address is essentially just an account number that stays with the user; if you can connect that address to a particular user, you can identify and trace all of the transactions in which that individual has participated using that address. Indeed, if the individual uses an exchange or wallet service as the "on ramp" to the blockchain, then the bitcoin address is essentially about as anonymous as a bank account number or credit card number, because the exchange or wallet service will maintain records linking the address to a particular identity, much like a bank or card issuer maintains records establishing the owner of each bank or card account. Even if a criminal does not use an exchange to obtain bitcoins, and even if the criminal takes advantage of existing methods for enhancing anonymity, he or she is still not truly anonymous, because there are existing techniques to help link users to their addresses. And those techniques are improving all the time.

In addition, the blockchain helps address the problem of data retention. It has been a persistent challenge for law enforcement that phone and Internet providers have inconsistent practices on retaining customer and transaction data. In cybercrime, child exploitation, and numerous other types of cases, it can take months or even years to follow the trail of a sophisticated criminal, serving process on provider after provider in different countries, until investigators finally get to the provider whose records will ultimately identify the suspect – only to find that those records no longer exist. With the blockchain, part of that problem has been eliminated; while law enforcement still must rely on the data retention practices of exchanges and wallet companies, there is no concern about retention of transaction data, because the data recorded on the blockchain isn't going anywhere.

The blockchain also does not raise "third party doctrine" issues. There is a raging debate among commentators and courts over the future of the "third party doctrine," the legal principle that says that you don't have a reasonable expectation of privacy in information you voluntarily share with a third party, such as a bank or internet service provider (ISP). The third party doctrine is essentially what makes it possible for law enforcement to obtain bank, ISP, or cellphone records with a subpoena rather than a search warrant. The viability of this doctrine has been called into question by Supreme Court justices and other judges, members of Congress, academics, and privacy advocates, and the outcome of this debate will have a profound impact on the way law enforcement operates. While the third party doctrine may impact the legal process used to obtain records from exchanges,

the blockchain itself raises no such issues. Law enforcement has the ability to access the blockchain and trace transaction histories without even a subpoena, let alone a search warrant, because it is public, and freely accessible, by design.

The borderless nature of the blockchain is another benefit to law enforcement. When evidence is within another country's borders, U.S. law enforcement must go through the cumbersome Mutual Legal Assistance Treaty (MLAT) process to seek foreign law enforcement assistance to obtain that evidence. Whether U.S. law enforcement should have to go through the MLAT process to obtain data held outside the United States by a U.S. provider is at the heart of the Department of Justice (DOJ)'s ongoing and heated litigation with Microsoft over whether the DOJ has jurisdiction to use a search warrant to get data held by Microsoft at a data center in Ireland. Microsoft and a "who's who" of other providers are arguing that the DOJ cannot use a search warrant to get data that a U.S.-based provider chooses to store overseas and instead should be required to go through the MLAT process. That issue never arises with the blockchain, which knows no borders and is available from anywhere, no MLAT required.

If nothing else, the Silk Road and Carl Force cases demonstrate that, even at this early stage, law enforcement has already developed an impressive capacity to analyze and trace transactions using the blockchain. And law enforcement is just beginning to get up the learning curve; they will get even better over time, particularly as analytics capabilities improve and new tools are developed.

Recently, a broad coalition of industry representatives led by the Chamber of Digital Commerce and Coin Center joined forces to create the "Blockchain Alliance," a public-private forum to help combat criminal activity involving bitcoin and the blockchain. The Blockchain Alliance serves as a resource for law enforcement to benefit from the expertise of some of the brightest minds in the blockchain industry for technical assistance in response to challenges faced during investigations. It also provides a resource for the blockchain community to understand the interests and concerns of law enforcement and regulators about the blockchain and its applications and serves as a mechanism for open dialogue between law enforcement and the Bitcoin community about issues of concern.

By providing this resource to law enforcement, the industry participants can help protect public safety while at the same time combating misperceptions about bitcoin and further demonstrating the industry's good-faith efforts to cooperate with investigations. Industry participants can also better understand the concerns, interests, and needs of law enforcement and regulators in this space, in order to identify the best ways to address those concerns, whether through education, information sharing, or another pathway.

Industry members include the Chamber of Digital Commerce, Coin Center, MIT Media Lab's Digital Currency Initiative and developer Gavin Andresen, BitFinex, BitFury, BitGo, Bitnet, BitPay, BitStamp, Blockchain, Bloq, Circle, CoinX, ItBit, Kraken, Netki, Noble Markets, and Xapo. The Blockchain Alliance is engaged with the Department of Justice, including the FBI and the U.S. Marshals Service, the U.S. Secret Service, Immigration and Customs Enforcement Homeland Security Investigations, IRS-Criminal Investigations, the U.S. Food and Drug Administration Office of Criminal Investigations (OCI), the U.S. Department of the Treasury's Financial Crimes Enforcement Network (FinCEN), the U.S. Commodity Futures Trading Commission (CFTC), the California Attorney General's Office, Europol and the European Cybercrime Centre (EC3), and plans to engage with other U.S. and foreign agencies as well.

There will always be people seeking to use technology to commit crimes – but that has been true for every technological advance since the telephone, if not before. Law enforcement will never drive criminals entirely off the blockchain, just like it will never eliminate crime on the Internet.

But by helping law enforcement continue to advance along its learning curve and helping address government concerns about this technology, the participants in the Bitcoin ecosystem can help make the blockchain more secure and deter its use for unlawful purposes. In doing so, the industry will foster an approach to enforcement and regulation that supports innovation and the growth of Bitcoin and the blockchain, so this transformative technology can reach its full potential.

References

American Land Title Association (2015, March 2015). "ALTA Reports $11 Billion in Title Insurance Premiums Written in 2014." Retrieved from https://www.alta.org/press/release.cfm?r=200

De Soto, H. (2000). The Mystery of Capital: Why Capitalism Triumphs in the West and Fails Everywhere Else. New York: Basic Books

Fall-Diaw, Mariama Mary. UNHCR distributes biometric ID cards to refugees in Senegal. Making a Difference, 22 October 2012. http://www.unhcr.org/508536389.html

Hirschey, M., Pappas, J. L., & Whigham, D. (1996). Managerial economics. Dryden Press.

Hardjono, Thomas, Deegan, Patrick, and Clippinger, John Henry. "Social Use Cases for the ID3 Open Mustard Seed Platform." 2014, IEEE Technology and Society Magazine. Fall. Pp. 48-54.

Johnston, M. (2005). Syndromes of corruption: wealth, power, and democracy. Cambridge University Press.

King, G., Pan, J., & Roberts, M. E. (2013). How censorship in China allows government criticism but silences collective expression. American Political Science Review, 107(02), 326-343.

Plan International. "Identifying and Addressing Risks to Children in Digitised Birth Registration Systems: A Step-by-Step Guide. 2015. pdf.

Senior, I. (2006). Corruption-The World's Big C. IEA Research Paper, (61).

UNHCR. 2015. "Worldwide displacement hits all-time high as war and persecution increase." http://www.unhcr.org/558193896.html

UNICEF. "A Passport to Protection. A Guide to Birth Registration Programming." 2013. http://www.unicef.org/protection/files/UNICEF_Birth_Registration_Handbook.pdf

Vigna, P., & Casey, M. (2015). The age of cryptocurrency: How bitcoin and digital money are challenging the global economic order. New York, New York: St. Martin's Press.

Exhibit 1

Event	Date	Amount (USD)	Bitcoins lost
Stone Man Loss	8/9/2010	$544.00	8,999.00
Bitcoin Rain	3/28/2011	$231,440.00	4,000.00
Stefan Thomas Loss	6/5/2011	$124,793.00	7,000.00
Allinvain Theft	6/13/2011	$445,688.00	25,000.01
June 2011 Mt. Gox Incident	6/19/2011	$47,123.00	2,000.00
Mass MyBitcoin Thefts	6/20/2011	$71,656.00	4,019.43
Ubitex Scam	7/1/2011	$15,515.00	1,138.98
MyBitcoin Theft	7/1/2011	$1,072,570.00	78,739.58
Bitomat.pl Loss	7/26/2011	$231,570.00	17,000.00
Mooncoin Theft	9/11/2011	$22,346.00	4,000.00
Bitcoin7 Incident	10/5/2011	$15,980.00	5,000.00
October 2011 Mt. Gox Loss	10/28/2011	$8,340.00	8,340.00
Bitcoin Savings and Trust	1/5/2012	$2,983,473.00	263,024.00
Bitscalper Scam	2/1/2012	$6,461.00	6,461.00
Andrew Nollan Scam	2/1/2012	$10,895.00	2,211.08
Linode Hacks	3/1/2012	$223,278.00	43,554.02
Betcoin Theft	4/11/2012	$15,534.00	3,171.50
Tony Silk Road Scam	4/20/2012	$146,944.00	30,000.00
May 2012 Bitcoinica Hack	5/12/2012	$191,638.00	38,527.00
Bitcoin Syndicate Theft	7/4/2012	$14,595.00	1,852.62
July 2012 Bitcoinia Theft	7/13/2012	$315,133.00	40,000.00
BTC-E Hack	7/31/2012	$35,452.00	4,500.00
Kronos Hack	8/1/2012	$42,859.00	4,000.00
Bitfloor Theft	9/4/2012	$273,209.00	24,086.17
Cdecker Theft	9/28/2012	$104,607.00	9,222.21
2012 50BTC Theft	10/13/2012	$13,437.00	1,173.52
2012 Trojan	10/18/2012	$39,146.00	3,257.00
Bit LC Theft	2/13/2013	$51,480.00	2,000.00
BTCGuild Incident	3/1/2013	$72,556.00	1,254.00
2013 Fork	3/11/2013	$55,551.00	960.1
ZigGap	4/1/2013	$195,490.00	1,708.66
Ozcoin Theft	4/19/2013	$105,600.00	922.99
Vircurex Theft	5/10/2013	$163,351.00	1,454.02
James Howells Loss	7/1/2013	$627,659.00	7,500.00
Just Dice Incident	7/15/2013	$108,807.00	1,300.16

Event	Date	Amount (USD)	Bitcoins lost
GBL Scam	8/1/2013	$3,437,446.00	22,000.00
BASIC-MINING	10/1/2013	$332,963.00	2,131.00
Silk Road Seizure	10/25/2013	$26,867,560.00	27,618.70
Inputs.io Hack	10/26/2013	$640,615.00	4,100.00
Bitcash.cz Hack	11/11/2013	$247,422.00	484.77
BIPS Hack	11/17/2013	$660,959.00	1,295.00
PicoStocks Hack	11/29/2013	$3,009,397.00	5,896.23
Sheep Marketplace Incident	12/2/2013	$4,070,923.00	5,400.00
Silk Road 2 Incident	2/13/2014	$3,624,866.00	4,400.00
2014 Mt. Gox Collapse	2/15/2014	$700,258,171.00	850,000.00
Flexcoin Theft	3/2/2014	$738,240.00	896.1
CryptoRush Theft	3/11/2014	$782,641.00	950
MintPal Incident	7/14/2014	$3,208,412.00	3,894.49
Moolah	10/23/2014	$1,500,000.00	4,087.19
Bitstamp Hack	1/4/2015	$5,000,000.00	19,000.00
Evolution	3/18/2015	$12,000,000.00	130,000.00

Exhibit 2

The following article was written by Nick Szabo and included with his permission (http://szabo.best.vwh.net/smart_contracts_2.html). For unfamiliar terms in italics used in this section, refer to the author's Glossary (http://szabo.best.vwh.net/smart_contracts_glossary.html).

Smart Contracts: Building Blocks for Digital Markets

The contract, a set of promises agreed to in a "meeting of the minds", is the traditional way to formalize a relationship. While contracts are primarily used in business relationships (the focus of this article), they can also involve personal relationships such as marriages. Contracts are also important in politics, not only because of "social contract" theories but also because contract enforcement has traditionally been considered a basic function of capitalist governments.

Whether enforced by a government, or otherwise, the contract is the basic building block of a free market economy. Over many centuries of cultural evolution has emerged both the concept of contract and principles related to it, encoded into common law. Algorithmic information theory suggests that such evolved structures are often prohibitively costly to recompute. If we started from scratch, using reason and experience, it could take many centuries to redevelop sophisticated ideas like property rights that make the modern free market work [Hayek].

The success of the common law of contracts, combined with the high cost of replacing it, makes it worthwhile to both preserve and to make use of these principles where appropriate. Yet, the digital revolution is radically changing the kinds of relationships we can have. What parts of our hard-won legal tradition will still be valuable in the cyberspace era? What is the best way to apply these common law principles to the design of our on-line relationships?

Computers make possible the running of algorithms heretofore prohibitively costly, and networks the quicker transmission of larger and more sophisticated messages. Furthermore, computer scientists and cryptographers have recently discovered many new and quite interesting algorithms. Combining these messages and algorithms makes possible a wide variety of new protocols.

New institutions, and new ways to formalize the relationships that make up these institutions, are now made possible by the digital revolution. I call these new contracts "smart", because they are far more functional than their inanimate paper-based ancestors. No use of artificial intelligence is implied. A smart contract is a set of promises, specified in digital form, including protocols within which the parties perform on these promises.

Contracts Embedded in the World

The basic idea of smart contracts is that many kinds of contractual clauses (such as liens, bonding, delineation of property rights, etc.) can be embedded in the hardware and software we deal with, in such a way as to make breach of contract expensive (if desired, sometimes prohibitively so) for the breacher. A canonical real-life example, which we might consider to be the primitive ancestor of smart contracts, is the humble vending machine. Within a limited amount of potential loss (the amount in the till should be less than the cost of breaching the mechanism), the machine takes in coins, and via a simple mechanism, which makes a beginner's level problem in design with finite automata, dispense change and product fairly. Smart contracts go beyond the vending machine in proposing to embed contracts in all sorts of property that is valuable and controlled by digital means. Smart contracts reference that property in a dynamic, proactively enforced form, and provide much better observation and verification where proactive measures must fall short. And where the vending machine, like electronic mail, implements an asynchronous protocol between

the vending company and the customer, some smart contracts entail multiple synchronous steps between two or more parties.

Other forerunners of smart contracts include POS (Point of Sale) terminals and cards, EDI (Electronic Data Interchange, used for ordering and other transactions between large corporations), and the SWIFT, ACH, and FedWire networks for transferring and clearing payments between banks. These implement commercial security models, but too often with little heed paid to the contractual needs and obligations of the parties.

Attacks against Smart Contracts

A broad statement of the key idea of smart contracts, then, is to say that contracts should be embedded in the world. The mechanisms of the world should be structured in such a way as to make the contracts

(a) robust against naive vandalism, and
(b) robust against sophisticated, incentive compatible (rational) breach

A vandal can be a strategy or sub-strategy of a game whose utility is at least partially a function of one's own negative utility; or it can be a mistake by a contracting party to the same effect. "Naive" simply refers to both lack of forethought as to the consequences of a breach, as well as the relatively low amount of resources expended to enable that breach. Naive vandalism is common enough that it must be taken into consideration. A third category, (c) sophisticated vandalism (where the vandals can and are willing to sacrifice substantial resources), for example a military attack by third parties, is of a special and difficult kind that doesn't often arise in typical contracting, so that we can place it in a separate category and ignore it here. The distinction between naive and sophisticated strategies has been computationally formalized in algorithmic information theory.

Some Basic Principals of Contract Design

The threat of physical force is an obvious way to embed a contract in the world -- have a judicial system decide what physical steps are to be taken out by an enforcement agency (including arrest, confiscation of property, etc.) in response to a breach of contract. It is what I call a reactive form of security. The need to invoke reactive security can be minimized, but not eliminated, by making contractual arrangements verifiable, for example by recording a breach on a video camera, or putting a signature on a contract, in order to prove breach claims in court. Observation of a contract in progress, in order to detect the first sign of breach and minimize losses, also is a reactive form of security. Aproactive form of security is a physical mechanism that makes breach expensive, such as a combination lock that makes access to a room containing trade secrets expensive without explicit authorization.

From common law, economic theory, and contractual conditions often found in practice, we can distill four basic objectives of contract design. The first of these isobservability, the ability of the principals to observe each others' performance of the contract, or to prove their performance to other principals. The field of accounting is, roughly speaking, primarily concerned with making contracts an organization is involved in more observable.

A second objective verifiability, the ability of a principal to prove to an arbitrator that a contract has been performed or breached, or the ability of the arbitrator to find this out by other means. The disciplines of auditing and investigation roughly correspond with verification of contract performance. Observability and verifiability can also include the ability to differentiate between intentional violations of the contract and good faith errors.

A third objective of contract design is privity, the principle that knowledge and control over the contents and performance of a contract should be distributed among parties only as much as is necessary for the performance of that contract. This is a generalization of the common law principle of contract privity, which states that third parties, other than the designated arbitrators and intermediaries, should have no say in the enforcement of a contract. Generalized privity goes beyond this to formalize the common claim, "it's none of your business". Attacks against privity are epitomized by third parties Eve the eavesdropper, a passive observer of contents or performance, and malicious Mallet, who actively interferes with performance or steals service. Under this model privacy and confidentiality, or protecting the value of information about a contract, its parties, and its performance from Eve, is subsumed under privity, as are property rights. The field of security (especially, for smart contracts, computer and network security), roughly corresponds to the goal of privity.
A fourth objective is enforceability, and at the same time minimizing the need for enforcement. Improved verifiability often also helps meet this fourth objective. Reputation, built-in incentives, "self-enforcing" protocols, and verifiability can all play a strong part in meeting the fourth objective. Computer and network security also can contribute greatly to making smart contracts self-enforcing.

Smart contracts often involve trusted third parties, exemplified by an intermediary, who is involved in the performance, and an arbitrator, who is invoked to resolve disputes arising out of performance (or lack thereof). Privity implies that we want to minimize vulnerability to third parties. Verifiability and observabiliy often require that we invoke them. A mediator must be trusted with some of the contents and/or performance of the contract. An arbitrator must be trusted with some of the contents, and some of the history of performance, and to resolve disputes and invoke penalties fairly. In smart contract design we want to get the most out of intermediaries and arbitrators, while minimizing exposure to them. One common outcome is that confidentiality is violated only in case of dispute.

In the future the size distribution of multinational companies will approach that of local business, giving rise to multinational small business . Legal barriers are the most severe cost of doing business across many jurisdictions. Smart contracts can cut through this Gordian knot of jurisdictions. Where smart contracts can increase privity, they can decrease vulnerability to capricious jurisdictions. Where smart contracts can increase observability or verifiability, they can decrease dependence on these obscure local legal codes and enforcement traditions.

The consequences of smart contract design on contract law and economics, and on strategic contract drafting, (and vice versa), have been little explored. As well, I suspect the possibilities for greatly reducing the transaction costs of executing some kinds of contracts, and the opportunities for creating new kinds of businesses and social institutions based on smart contracts, are vast but little explored. The "cypherpunks" have explored the political impact of some of the new protocol building blocks. The field of Electronic Data Interchange (EDI), in which elements of traditional business transactions (invoices, receipts, etc.) are exchanged electronically, sometimes including encryption and digital signature capabilities, can be viewed as a primitive forerunner to smart contracts. Indeed those business forms can provide good starting points and channel markers for smart contract designers.

Observability & Hidden Actions

One important task of smart contracts, that has been largely overlooked by traditional EDI, is critical to "the meeting of the minds" that is at the heart of a contract: communicating the semantics of the protocols to the parties involved. There is ample opportunity in smart contracts for "smart fine print": actions taken by the software hidden from a party to the transaction. For example, grocery store POS machines don't tell customers whether or not their names are being linked to their purchases in a database. The clerks don't even know, and they've processed thousands of such

transactions under their noses. Thus, via hidden action of the software, the customer is giving away information they might consider valuable or confidential, but the contract has been drafted, and transaction has been designed, in such a way as to hide those important parts of that transaction from the customer.

To properly communicate transaction semantics, we need good visual metaphors for the elements of the contract. These would hide the details of the protocol without surrendering control over the knowledge and execution of contract terms. A primitive but good example is provided by the SecureMosiac software from CommerceNet. Encryption is shown by putting the document in an envelope, and a digital signature by affixing a seal onto the document or envelope. On the other hand, Mosaic servers log connections, and sometimes even transactions, without warning users -- classic hidden actions.

Cryptographic Building Blocks

Protocols based on mathematics, called cryptographic protocols, are the basic building blocks that implement the improved tradeoffs between observability, verifiability, privity, and enforceability in smart contracts. Contrary to the common wisdom, obscurity is often critical to security. Cryptographic protocols are built around foci of obscurity called keys. A key's immense unknown randomness allows the rest of the system to be simple and public. The obscurity of a large random number, so vast that a lucky guess is unlikely in in, if desired, the lifetime of the universe, is the foundation upon which cryptographic protocols, and in turn smart contracts, are built.

A wide variety of new cryptographic protocols have emerged in recent years. The most traditional kind of cryptography is secret key cryptography, in which Alice and Bob (our exemplar parties to a smart contract) use a single shared, prearranged key to encrypt messages between them. A fundamental problem we will see throughout these protocols is the need to keep keys secret, and public key cryptography helps solve this. In this technique, Alice generates two keys, called the private and public keys. She keeps the private key secret and well protected, and publishes the public key. When Bob wishes to send a message to Alice, he encrypts a message with her public key, sends the encrypted message, and she decrypts the message with her private key. The private key provides a "trapdoor" that allows Alice to compute an easy inverse of the encryption function that used the public key. The public key provides no clue as to what the private key is, even though they are mathematically related. The RSA algorithm is the most widely used method of public key cryptography.

Public key cryptography also makes possible a wide variety of digital signatures. These proves that a piece of data (hereafter referred to as just an "object") was in active contact with the private key corresponding to the signature: the object was actively "signed" with that key. The digital signature probably should have been called a "digital stamp" or "digital seal" since its function resembles more those methods than an autograph. In particular, it is not biometric like an autograph, although incorporation of a typed-in password as part of the private key used to sign can sometimes substitute for an autograph. In many Asian countries, a hand-carved wooden block, called a "chop", is often used instead of autographs. Every chop is unique, and because of the unique carving and wood grain cannot be copied. A digital signature is similar to the chop, since every newly generated key is unique, but it is trivial to copy the key if obtained from the holder. A digital signature relies on the assumption that the holder will keep the private key secret.

A blind signature is a digital signature and secret-key encryption protocol that together have the mathematical property of commutativity, so that they can be stripped in reverse of the order they were applied. The effect is that Bob "signs" an object, for which he can verify its general form, but cannot see its specific content. Typically the key of the signature defines the meaning of the signed object, rather than the contents of the object signed, so that Bob doesn't sign a blank check. Blind

signatures used in digital bearer instruments, where Bob is the clearing agent, and in Chaumian credentials, where Bob is the credential issuer.

Secret sharing is a method of splitting a key (and thus control over any object encrypted with that key) into N parts, of which only M are needed to recreate the key, but less than M of the parts provide no information about the key. Secret sharing is a potent tool for distributing control over objects between principals.

The zero-knowledge interactive proof is an alternative to public key methods for challenge-response identification. Otherwise normally functioning parties who have an incentive to respond properly to the challenge, but fail to do so, do not possess the key), without revealing any information about that private key to the challenger or any eavesdroppers. ZKIPs are currently used for authentication, and in smart weapons for Identification Friend or Foe (IFF).

Information about who is talking to whom, such as can be found on telephone bills, can be quite valuable even without records of the actual content. Confidential messaging is necessary for the some of the privity features of Chaumian credentials and bearer securities to be strongly implemented on an actual network. To provide this traffic confidentiality, a digital mix can allow parties to communicate across a network without revealing their partners to network providers or the outside world. In a mix, traffic analysis by Eve is prevented by the Russian-doll encryption of the message by the sender with the public keys of each mix operator in the chain, and the mixing of messages by each operator, so that panoptic wiretapper Eve loses track of the messages. For the sender/recipient pair to remain confidential, only 1 out of N of the operators needs to be trusted with their local traffic information, although Eve can sometimes gather statistics over large numbers of messages between the same partners to eventually guess who is talking to whom. The communicating parties can also be mutually anonymous, and with normal encryption need trust no other parties with the content of messages. The "Mixmaster" software on the Internet implements most of the features of a digital mix[Mixmaster].

Protection of Keys

So far, we've assumed parties like Alice and Bob are monolithic. But in the world of smart contracts, they will use computer-based software agents and smart cards to do their electronic bidding. Keys are not necessarily tied to identities, and the task of doing such binding turns out to be more difficult than at first glance. Once keys are bound, they need to be well protected, but wide area network connections are notoriously to hacking.

If we assume that the attacker has the ability to intercept and redirect any messages in the network protocol, as is the case on wide area networks such as the Internet, then we must also assume, for practical all commercial operating systems, that they would also be able to invade client if not merchant computers and find any keys lying on the disk.

There's no completely satisfactory solution to end point operations security from network-based attacks, but here's a strategy for practically defanging this problem for public-key based systems:

All public key operations are done inside an unreadable hardware board on a machine with a very narrow serial-line connection (i.e., it carries only a simple single-use protocol with well-verified security) to a dedicated firewall. Such a board is available, for example, from Kryptor, and I believe Viacrypt may also have a PGP-compatible board. This is economical for central sites, but may be less practical for normal users. Besides better security, it has the added advantage that hardware speeds up the public key computations.

If Mallet's capability is to physically size the machine, a weaker form of key protection will suffice. The trick is to hold the keys in volatile memory. This makes the PC proof from physical attacks -- all that needed to destroy the keys is to turn off the PC. If the key backups can be hidden in a different, secure physical location, this allows the user of this PC to encrypt large amounts of data both on the PC itself and on public computer networks, without fear that physical attack against the PC will compromise that data. The data is still vulnerable to a "rubber hose attack" where the owner is coerced into revealing the hidden keys. Protection against rubber hose attacks might require some form of Shamir secret sharing which splits the keys between diverse physical sites.

The Man In the Middle & PGP's Web of Trust

How does Alice know she has Bob's key? Who, indeed, can be the parties to a smart contract? Can they be defined just by their keys? Do we need biometrics (such as autographs, typed-in passwords, retina scans, etc.)?

The public key cryptography software package "Pretty Good Privacy" (PGP) uses a model called "the web of trust". Alice chooses introducers whom she trusts to properly identify the map between other people and their public keys. PGP takes it from there, automatically validating any other keys that have been signed by Alice's designated introducers.

There are two entirely separate criteria PGP uses to judge a public key's usefulness:
1) Does the key actually belong to whom it appears to belong? In other words, has it been certified with a trusted signature?
2) Does it belong to an introducers, someone you can trust to certify other keys?

Having been told by Alice the answer to the second question, PGP can calculates the answer to the first question for the public keys Alice has collected.

Keys that have been certified by a trusted introducer are deemed valid by PGP. The keys belonging to trusted introducers must themselves be certified either by you or by other trusted introducers. This "transitivity" introduces an implicit third criterion

3) Does the key belong to someone you can trust to introduce other introducers?

PGP confuses this with criterion (2). It is not clear that any single person has enough judgment to properly undertake task (3), nor has a reasonable institution been proposed that will do so. This is one of the unsolved problems in smart contracts.

PGP also can be given trust ratings and programmed to compute a weighted score of validity-- for example, two marginally trusted signatures might be considered as credible as one fully trusted signature.

Any keys in Alice's secret key ring are "axiomatically" valid to Alice's PGP program, needing no introducer's signature. PGP also assumes that Alice ultimately trusts herself to certify other keys.

It is believed that PGP causes the emergence of a decentralized fault-tolerant web of confidence for all public keys, but a chain of introduced introducers grows weak very quickly, due to lack of transitivity.

PGP's grass-roots approach contrasts sharply with traditional public key management schemes, such as X.509 and the related Privacy Enhanced Mail (PEM). These standard schemes substitute a hierarchical system of introducers called certification authorities (CAs).

Notaries Public

Two different acts are often called "notarization". The first is simply where one swears to the truth of some affidavit before a notary or some other officer entitled to take oaths. This does not require the notary to know who the affiant is. The second act is when someone "acknowledges" before a notary that he has executed a document as ``his own act and deed." This second act requires the notary to know the person making the acknowledgment. Thus, for example, the form of an acknowledgment can go something like this:

On this ____ day of ___, 19__, personally appeared before me ____, known to me and known to me to be the person who signed the foregoing instrument, and acknowledged that he executed the same as his own act and deed.

In the first type of act of notarization, the notary merely certifies that the affiant swore the statement was true. In the second type the notary actually vouches that the person making the acknowledgment was who he claims to be.

Problems with Certification

These roles of a notary public are substantially different from the alleged role of hierarchies of "certification authorities" (CAs) in PEM/X.509, and the "web of trust" in PGP, to "prove identity". In fact the certificates generated by these systems do no such thing. Rather a certificate proves that a claim was made by a CA at some time in the past. The (implicit) claim is that a particular key belonged to a particular person at that time. That key is not biometric like an autograph, and can thus be transferred at any time. Furthermore, false claims can be made by a CA about what keys an end-user has held, and the end-user can be stuck with no evidence of CA fraud; nor does the CA have any way of proving that their claim is correct if an end-user challenges it. It is extremely difficult, on the other hand, for notary publics to forge autographs and expect to get away with it often enough to maintain their professional reputations.

Both the PGP web of trust and X.509 models suffer from more flaws. A single rooted hierarchy assumes a mythological beast called a universally trusted entity. Hierarchies in general create rigid structures that don't fit the way knowledge about keys and keyholders, and incentives to accurately reflect that knowledge, are distributed among people in the real world. In turn, while PGP distinguishes between "Alice holds a key" and "Alice can be trusted to certify a key", it does not follow that the second claim that Alice can be trusted to validate another issuer. There is little transitivity: seeing Alice's key certified by Bob, whom I know and trust, tells me little about whether Alice's certification of Charlie's key is correct. Seeing Alice certified by Bob as an introducer tells me little about whether Alice can be trusted to certify other introducers. It does tell me that I know to blame Alice if her claim turns out to be wrong; although it's far from clear that Alice has any legal liability. There is an even more severe flaw when public key is used for digital signatures. Because the claim was only made in the past, both PGP and X.509 allow the end user to plausible deny that they "signed" a document; and conversely if one's key is surreptitiously stolen, or for other reasons no revocation action is taken, there is no way to prove that one did not "sign" the document digitally "signed" with the stolen key. Finally, there is no widely accepted legal agreement on what is specifically being claimed when one "certifies" a key, nor is there any built-in or widely used mechanism for describing the actual claim one is making. Real world CAs have a nasty habit of disclaiming liability for their mistakes, or for the misunderstandings that will arise out of the often vague and sloppy, sometimes implicit claims they make. Finally, there are a wide variety of other claims one might make about a key, such as "this key belongs to an office", "this key belongs to a server", "this keyholder has a good credit rating", "use this key to decrypt your new copy of Microsquish Expel", "this key is good for 100 MB of downloads from our web server", etc. which are facilitated by neither X.509 nor the PGP web of trust.

We know too little about the best uses of public-key cryptography to establish such fixed methods with such narrow semantics. This author has suggested a mechanism, which modifies the PGP web of trust to create arbitrary certificate with a form roughly as follows:

Key about which a claim is being made type of claim, in some standard one-line format (like MIME types) Plain text description of claim Timestamp digitally "signed", Alice's key
In other words, all claims about keys should be explicit, readily known from reading the certificate itself, and no kind of claim should be arbitrarily excluded by the mechanism. The legal force of the claim can be based on the text itself, rather than overstated, obscure, and often implicit interpretations about what "certifying" is supposed to mean. Standard kinds of claims will emerge, including perhaps more transitive "good judge of judgment" certificates for which chain-following software can be written, and non-transitive "is-a-person" credentials directly "bound" to traditional notarized identification by a physical notarization protocol that includes both autographs and digital "signatures". More likely, new and more useful kinds of certificates will evolve. These standards should be allowed to emerge out of the wide varieties of possible end uses, much like case law has matured over time, rather than being dictated by our current very inexperienced understanding.

Meanwhile, there is a more practical defense against the man in the middle attack: advertise, early and often. Users of an insecure network can communicate the integrity of a key reasonably well by tying it to a persistent pattern of behavior: for example posts in a persistent style from a persistent e-mail address, persistence of a key unchallenged on a key server, etc. This is the most practical and widely used way by which PGP users gain confidence in public keys, and it does not require certification authorities or introducers. Those who advertise their keys widely, and those who are well known, are more likely to have keys bound to their person.

Virtual Personae

"Identity" is hardly the only thing we might want map to a key. After all, physical keys we use for our house, car, etc. are not necessarily tied to our identity -- we can loan them to trusted friends and relatives, make copies of them, etc. Indeed, in cyberspace we might create "virtual personae" to reflect such multi-person relationships, or in contrast to reflect different parts of our personality that we do not want others to link. Here is a possible classification scheme for virtual personae, pedagogically presented:

A nym is an identifier that links only a small amount of related information about a person, usually that information deemed by the nym holder to be relevant to a particular organization or community. Examples of nyms include electronic bulletin board nicknames, pen names, aliases, and brand names. A nym may gain reputation within its community. For example, a conglomerate may sell a wide variety of brand names, each reputable in its own market niche. With Chaumian credentials, a nym can take advantage of the positive credentials of the holder's other nyms, as provably linked by the is-a-person credential.

A true name is an identifier that links many different kinds of information about an person, such as a full birth name or social security number. As in magick, knowing a true name can confer tremendous power to one's enemies. It also can have major economic value among those who cooperate peacefully, as in the use of direct marketing to target product information to those persons most likely to be interested in those particular products.

A persona is any perstient pattern of behavior, along with consistently grouped information such as key(s), name(s), network address(es), writing style, and services provided.

A reputable name is a nym or true name that has a good reputation, usually because it carries many positive credentials, has a good credit rating, or is otherwise highly regarded. Companies strive

to carry reputable brand names, while professionals such as doctors and lawyers strive to have many good personal recommendations of their name. Reputable names can be difficult to transfer between parties, because reputation assumes persistence of behavior, but such transfer can sometimes occur (for example, the sale of brand names between companies).

Constructing Smart Contracts

Blind signatures can be used to construct digital bearer instruments, objects identified by a unique key, and issued, cleared, and redeemed by a clearing agent. When an object is transferred, the trasferee can request the clearing agent to verify that the key has never before been cleared, and issue a new key. The clearing agent prevents multiple clearing of particular objects, but can be prevented from linking particular objects one or both of the clearing nyms who transferred that object. These instruments come in an "online" variety, cleared during every transfer, and thus both verifiable and observable, and an "offline" variety, which can be transfered without being cleared, but is only verifiable when finally cleared, by revealing any the clearing nym of any intermediate holder who transfered the object multiple times (a breach of contract). Privacy from the clearing agent can take the form of transferee-unlinkability, transferer-unlinkability, or "double blinded" where both transferer and transferee are unlinkable by the clearing agent.

Digital cash the premier example of a digital bearer instrument, in which the clearing agent is a bank. Bearer instrument protocols enable online payment while honoring the characteristics desired of bearer notes, especially unforgeability (via the clearing mechanism) and transfer confidentiality (via blinding).

To implement a full transaction of payment for services, we need more than just the digital cash protocol; we need a protocol that guarantees that service will be rendered if payment is made, and vice versa. Current commercial systems use a wide variety of techniques to accomplish this, such as certified mail, face to face exchange, reliance on credit history and collection agencies to extend credit, etc. Smart contracts have the potential to greatly reduce the fraud and enforcement costs of many commercial transactions.

A credential is a claim made by one party about another. A positive credential is one the second party would prefer to reveal, such as a degree from a prestigious school, while that party would prefer not to reveal a negative credential such as a bad credit rating.

A Chaumian credential is a cryptographic protocol for proving one possesses claims made about onself by other nyms, without revealing linkages between those nyms. It's based around the is-a-person credential the true name credential, used to prove the linkage of otherwise unlinkable nyms, and to prevent the transfer of nyms between parties.

Another form of credential is bearer credential, a digital bearer instrument where the object is a credential. Here the second party in the claim refers to any bearer -- the claim is tied only to the reputable name of issuing organization, not to the nym or true name of the party holding the credential.

Smart Property

We can extend the concept of smart contracts to property. Smart property might be created by embedding smart contracts in physical objects. These embedded protocols would automatically give control of the keys for operating the property to the party who rightfully owns that property, based on the terms of the contract. For example, a car might be rendered inoperable unless the proper challenge-response protocol is completed with its rightful owner, preventing theft. If a loan was taken out to buy that car, and the owner failed to make payments, the smart contract could automatically invoke a lien, which returns control of the car keys to the bank. This "smart lien"

might be much cheaper and more effective than a repo man. Also needed is a protocol to provably remove the lien when the loan has been paid off, as well as hardship and operational exceptions. For example, it would be rude to revoke operation of the car while it's doing 75 down the freeway. Smart property is software or physical devices with the desired characteristics of ownership embedded into them; for example devices that can be rendered of far less value to parties who lack possession of a key, as demonstrated via a zero knowledge interactive proof.

One method of implementing smart property is thru operation necessary data (OND): data necessary to the operation of smart property. For example, a complex, OND can be proprietary firing sequence needed to operate a computerized engine, a CAM file needed to manufacture a specialized part, etc. To avoid theft of service, ZKIP is required to open an encrypted channel to the device. To avoid leaking the OND to Eve, tamper detection combined with a dead-man switch can be used on the device end of the channel.

We might also used and engrained immobilizing or destructive devices to foil attempts to hot-wire smart property.

A smart lien is the sharing of a smart property between parties, usually two parties called the owner and the lienholder. This property may be in the proximate possession of the owner or the lienholder, corresponding to the common-law notions of "artisan's lien" and "innkeeper's lien" respectively. Smart liens might be used to secure lines of credit, insurance policies, and many other kinds of contracts that involve smart property.

How can debts be collected? No wise bank will lend unless the lendee can either be coerced into repaying the debt, or the loan is more than covered by securely liened collateral plus some conservative function of its reputation for payment in full and on time. For all parties, both credit and liability are closely related, and limited.

The liability of a party is limited by that party's liens and by the ability to deter that party by threatening punishment for violating contracts (i.e., committing crimes as defined by the contract with the jurisdiction). The potential for other actions an party might take that cause liability, such as damage to others' persons or property, also need to be limited. More on that later.

Many parties, especially new entrants, may lack this reputation capital, and will thus need to be able to share their property with the bank via secure liens. A lien is, in a practical sense, a method of sharing a piece of property between the "owner of record" and a "lienholder", instead of the property having strictly one owner. Liens are used in many large credit transactions, such as auto loans, mortgages, farm loans, etc. They are enforced by the jurisdiction specified in the contract; usually this enforcement is done by the government and subsidized by the taxpayers rather than paid for by the contracting parties. (In fact this usually is the case with contracts and property rights in general, the enforcement clause is an implicit government subsidy). One way to implement a lien without governments is via co-signing with your privately chosen arbitrator (as long as the arbitrator has a good reputation and the contractual right to take appropriate action against you). Smart liens might greatly expand the privity and security of such arrangements.

As is the case today, credit problems will usually be solved by artfully written, menacing dunning letters and dings to one's credit rating long before the lien needs to be invoked. However, the lien needs to be enforceable to make these dunning letters credible over the long run.

What about extending the concept of contract to cover agreement to a prearranged set of tort laws? These tort laws would be defined by contracts between private arbitration and enforcement agencies, while customers would have a choice of jurisdictions in this system of free-market "gov-

ernments". If these privately practiced law organizations (PPLs for short) bear ultimate responsibility for the criminal activities of their customers, or need to insure lack of defection or future payments on the part of customers, they may in turn ask for liens against their customers, either in with contractual terms allowing arrest of customers under certain conditions (eg if they commit acts specified as criminal by the PPL contract) or (more likely for mobile world-traveling and virtual pseudonymous customers) smart liens against liquid assets such as bank accounts and investment portfolios. Smart liens over information, such as digital bearer securities, can be implemented via secret sharing (two or more keys required to unlock the encryption).

Other important areas of liability include consumer liability and property damage (including pollution). There need to mechanisms so that, for example, pollution damage to others' persons or property can be assessed, and liens should exist so that the polluter can be properly charged and the victims paid. Where pollution is quantifiable, as with SO2 emissions, markets can be set up to trade emission rights. The PPLs would have liens in place to monitor their customer's emissions and assess fees where emission rights have been exceeded.

Alas, there are some dangers where maximum damage could far surpass any liens. A good rule of thumb here is that if the risk is against a third party, and it cannot be liened or insured against, then PPLs should not allow it to be taken. PPLs that allow their customers to take such risks against non-PPL parties would ruin their credit rating. One example of such a risk is building a nuclear plant for which no insurance company is willing to submit liability coverage. If a plant is safe, presumably one should be able to convince a good insurance company to cover its potential to damage others' property.

Conclusion

Digital cash is here today, and many more smart contract mechanisms are being designed. So far the design criteria important for automating contract execution have come from disparate fields like economics and cryptography, with little cross-communication: little awareness of the technology on the one hand, and little awareness of its best business uses other. The idea of smart contracts is to recognize that these efforts are striving after common objectives, which converge on the concept of smart contracts.

Exhibit 3

Game Theory and Collaboration: A thought experiment with Decentralized Autonomous Organizations

Angus Champion de Crespigny

The Prisoners' Dilemma

Game theory is the study of strategy using mathematical or logical models of conflict and cooperation between rational decision-makers aiming to achieve optimal outcomes, and it is an interesting area of study when used to understand the collective results of individual actions around the globe. One thing game theory tells us is that, in the absence of intervention, the natural equilibrium of a number of world issues – deforestation, overfishing, pollution – leads to a race to the bottom.

What if blockchain technologies could assist in resolving these issues without the need for intervention?

To understand the causes of the race to the bottom and how these issues may be resolved, a brief overview of game theory may be beneficial. One of the most famous examples of game theory in action is the prisoners' dilemma. In this model, two prisoners, isolated for interrogation in separate rooms and unable to communicate, are told to confess to a major crime committed jointly. In prisoners' dilemma actual guilt or innocence is irrelevant.

The Prisoners' Dilemma

		Prisoner A	
		Confess/Betray	Remain Silent
Prisoner B	Confess/ Betray	5 yrs / 5 yrs	10 yrs / Set free
	Remain Silent	Set free / 10 yrs	1 yr / 1 yr

As demonstrated in the table below, if both parties remain silent, they are imprisoned for one year for a known lesser crime. If one confesses to the major crime and betrays the other party who remains silent, the incriminated prisoner is sentenced to 10 years while the confessor is set free as a reward for assisting in solving the major crime. If both confess, they are each sentenced to five years. While the best result for the pair is for both parties to maintain innocence, each prisoner in isolation is better served individually by confessing or betraying the other party. Consequently, the natural equilibrium is for each to confess and betray, leading to a negative outcome for both.

The Race to the Bottom

When such a situation is repeated many times over, in some cases this can lead to rather detrimental end states, often referred to as the race to the bottom. While it would be beneficial in the long-term for all countries to cooperate and limit pollution, in the short-term some countries may not cooperate and pollute regardless. In this case, non-polluters would consequently get the worst of both worlds – increased pollution and economic disadvantage. By polluting, countries may gain economic growth, even if the environment is damaged as a result, but in the long-term producing a worse overall result than if they had cooperated.

To solve this race to the bottom, the parties involved need to accept that the long-term benefits of collaboration are superior to the short-term benefits of cheating, and act accordingly.

Currently, actors attempt to achieve optimal outcomes through supervisory committees, organizations, or cartels, where future benefits are improved through collaboration and cheating parties are punished. These organizations however may be ineffective or non-existent for numerous reasons including corruption, insufficient incentives, short-sighted objectives, lack of trust, etc. Could an intervening body be more effective or more likely to succeed as a Decentralized Autonomous Organization (DAO)? [1]

Such an organization could automatically apply fair benefits according to a predefined set of rules, ensuring collaboration and the optimal outcome for the group. For this to work, however, two questions need to be solved, namely:

- Proof of X – how to prove beyond doubt that the activity being monitored is an accurate representation of what has been performed, and

1. *A Decentralized Autonomous Organization, or DAO, is a concept which leverages the distributed trust capabilities of digital asset protocols. A DAO would be made up of various pieces of code or small programs stored on the blockchain, which would be executed by the network of computers running the protocol. Coded correctly, such a collection of programs could run as an independent organization with no central authority controlling the code, but instead with the code stored in a distributed manner across the network.*

- Assurance of participation – how to guarantee that sufficient parties participate to ensure that no-one cheats by simply not taking part.

The following section demonstrates these issues through a real world example.

Overfishing

There is little doubt that overfishing is a chronic issue. In many parts of the world, more fish are taken from the ocean each year than can be replenished in the same time period, leading to consistently dwindling fish stocks. Despite this, a trawler that takes in fewer fish to allow for a larger population to remain, consequently allowing the population to last further into the future, also risks potential profits, as its competitor will take the fish that are left behind in addition to their own catch.

With no punishment for cheating and little way of getting caught, trawlers could continue to take each other's catch, even if it means future profits are hit – much better to have a business survive for another year than not survive beyond the next week. If, however, a "proof of catch" could be established, a DAO could be launched to oversee catches and distribute fair profits, while ensuring no participants cheat.

A "proof of catch" algorithm would need to be executed in such a way that it could not be manipulated, which is a known problem with incorporating data into a blockchain from an external source. Such an algorithm may take multiple factors and cross-compare to identify cases of cheating the algorithm, including: ship displacement, weight of fish unloaded, time spent at sea, etc. The algorithm, however, would also need to be easy and cost effective to implement in order for actors to benefit from organizing through a DAO.

Additionally, the DAO will not be successful if it cannot provide sufficient assurance of participation. That is, if participants are punished for cheating, whereas non-participant trawlers are free to overfish, there may be little incentive to participate and consequently little benefit in forming the DAO to begin with. If, however, the DAO can provide sufficient incentive to participate, assurance of participation can be met and consequently the DAO's full benefit can be realized, averting the economic race to the bottom and the need for a central authority.

Such incentive may come in a number of forms. In this case, the most basic would be a certification demonstrating a commitment to sustainability through membership of the organization, in the same way Fair Trade, Free Range, or Organic labels function. This type of certification results in value-added products that fetch premium prices, therefore incentivizing actors to participate. Another incentive may be supply chains which are fully integrated into the blockchain – if profits are distributed on the blockchain, complete end-to-end integration may be more efficient and cheaper to maintain if linked into the blockchain through the DAO from the start.

A blockchain integrated DAO would have a number of advantages. Firstly, it could significantly reduce administrative costs by automating much of the bureaucracy involved in intervention. Secondly, by publishing all activities on the blockchain, it could reduce the potential for corruption by making all activity visible to independent parties. Thirdly, as all activity would pass through a predefined set of logical rules that are immediately enforced and cannot be altered without a voting process, such infrastructure may reduce or remove the potential for cheating or rule bending by individual participants.

Realities of a DAO Migration

Assuming everything could be moved seamlessly to a DAO, there are still a number of outstanding considerations in moving any bureaucracy to such a structure.

Firstly, no DAO will be perfectly sustainably built from the start. Thus, the concept of voting for changes to the DAO has been established. Such DAOs have been upheld as the ultimate in fairness – a true democracy, free of the corruption of people in the current political environment. The question, however, is how would voting in a DAO truly differ from voting in the physical world? If a DAO is sufficiently critically important, financially powerful parties could buy votes through purchasing a larger voting stake or by lobbying individual voters, in much the same way that lobbying currently occurs. While the theory is that any users unhappy with such a situation would change DAOs, in reality this does not always happen. Despite all the recent uproar with the banks' handling of the global financial crisis and the Occupy Wall Street movement, consumers continue to open accounts and purchase products at the largest, most powerful financial institutions who many blame for the crisis. There does not appear to be a reason why such a situation would change by simply changing the platform on which voting occurs.

While a DAO may prove to be an ideal way of resolving such damaging race to the bottom situations, ultimately, such a solution may suffer at the very first step – getting off the ground. That is, how might such a DAO organically evolve, without the need for a central body mandating its creation? Blockchain technologies have plenty of potential to encourage collaboration through demonstrably fair, decentralized contracts; however such solutions will need to be created in a way that allows an organic transition from the status quo.