Protecting Consumers in the Digital Currency Economy

Bretton Woods 2016

Guiding Principles on Consumer Protection Best Practices for Businesses Working with Digital Currencies and other Blockchain-Derived Distributed Technology Assets

A product of

Consumers' Research
established 1929

in collaboration with Bretton Woods 2016 participants, product authors,
and sponsor organizations:

CoinStructive™ Microsoft bloq

Contributing Authors:

Victoria Adams, Booz Allen Hamilton
Kyle Burgess, Consumers' Reasearch
Michael Casey, MIT Media Lab, Digital Currency Initiative
Joe Colangelo, Consumers' Research
Michael Gronager, Chainalysis
Chris Groshong, CoinStructive
Andrew Hinkes, Berger Singerman LLP
Brian Knight, The Mercatus Center at George Mason University
Lance Koonce, Davis Wright Tremaine LLP
Juan Llanos, Skry
Eric Martindale, Blockstream
Jared Marx, Harris, Wiltshire & Grannis LLP
Yorke Rhodes III, Microsoft
Berin Szoka, TechFreedom
Carol Van Cleef, Manatt, Phelps & Phillips, LLP
Victoria Van Eyk, Bitcoin Strategy Group
Peter Van Valkenburgh, Coin Center
Michael Zeldin, BuckleySandler LLP

Special thanks to additional Bretton Woods 2016 workshop attendees: Keith Ammon, Natalee Binkholder, Beau Brunson, Paul Grassi, and Helen Wong

Table of Contents

Introduction

Consumers' Research[1], the nation's oldest consumer organization, hosted Bretton Woods 2016 from Sunday, July 10 – Wednesday, July 13, 2016 at the historic Omni Mount Washington Hotel in Bretton Woods, New Hampshire. This was the second annual Bretton Woods workshop held by Consumers' Research to examine bitcoin and blockchain technologies. The goal of this year's workshop was to produce guiding principles on consumer protection best practices for businesses working with digital currencies and other blockchain-derived digital assets. Workshop participants included representatives from relevant legislative and regulatory bodies, as well as a diverse array of fintech, blockchain, and traditional financial industry leaders. Together, these experts developed a list of consumer rights as well as guiding principles intended to guarantee those rights for adoption by companies working with digital currencies and distributed ledger technologies in the financial services industry.

THE STATE OF CONSUMER PROTECTION IN THE FINANCIAL SERVICES INDUSTRY

Consumer protection policy is based on two assumptions. The first is that consumers cannot effectively function in the modern economy without trusting their money and information to third parties. The second is that individual consumers are ill-equipped to assess the trustworthiness of these third parties. The result is that governments create laws and regulations to govern these third parties with the aim of ensuring that they do not mismanage the assets and information of consumers. Bitcoin and blockchain technology, however, challenge these underlying assumptions by creating the ability for consumers to carry a bank account in their pockets, or maintain unique versions of their personal information, deciding exactly who can access this data and for how long.

Distributed ledgers have the potential to impact money, trade, and access to banking more than any development in generations. However, for the technology to realize its potential, consumers need to trust it, which means knowing that their privacy is protected and their wealth is secure. The collaboration borne out of Bretton Woods 2016 has produced a model for bitcoin and blockchain-based companies that also addresses the concerns of regulatory entities.

Bretton Woods 2016 attendees included individuals affiliated with: The U.S. Federal Trade Commission (FTC), the U.S. Department of Commerce's National Institute of Standards and Technology (NIST), the U.S. House of Representatives, Microsoft, the Mercatus Center at George Mason University, Coin Center, MIT Media Lab's Digital Currency Initiative,

[1] Founded in 1929, Consumers' Research seeks to increase the knowledge and understanding of issues, policies, products, and services of concern to consumers, and to promote the freedom to act on that information.

CoinStructive, Chainalysis, and a number of other entities. (Participation in Bretton Woods 2016 does not signify an endorsement of the product.)

Consumers' Research has shared this product with representatives of regulatory bodies, industry leaders, and policy experts in a collaborative effort to build consensus around the practices recommended. After soliciting feedback from these experts, Consumers' Research is releasing the product herein for voluntary digital currency industry adoption in the hopes that proactive industry stewardship of consumer protection will stave off potentially overburdensome regulation that stifles innovation and limits consumer choice.

Relevant digital currency industry entities

- **Exchanges** - These entities have been responsible for a large percentage of the consumer protection failures in the digital currency space over the years. Whether due to fraud, theft, or mismanagement, many exchanges have failed to protect consumer information or assets (including digital currencies, tokens, virtual property or representations of value, or other blockchain-derived distributed technology digital asset). The following documents should serve as a roadmap for these exchanges to not just implement the best practices put forth by the industry, but to use the guiding principles of consumer protection to develop new and more effective best practices to serve and protect their customers. Examples of such entities include Bitfinex, Coinstamp, GDAX, and many others.
- **Hosted Wallets** - Any online service that acts as a fiduciary for digital assets faces similar consumer protection challenges as exchanges, and can glean the same value as exchanges. Examples of such entities include Blockchain.info, Airbitz, and many others.
- **Payment processors** - Payment processors that hold bitcoin for businesses or consumers, such as Bitpay or Coinbase, must take steps to protect the consumers they serve. These entities are based in the United States and are subject to U.S. regulation, which was built on assumptions about a completely different set of technology than the ones that underpin Bitcoin and blockchain-derived digital asset platforms. In 2014, FinCEN determined that bitcoin processors could be considered money transmitters subject to regulation.[2]
- **Decentralized Autonomous Organizations (DAOs)** - Decentralized or partially decentralized organizations are built by developers, and those developers may or may

[2] El-Hindi, J. (2014, October 27). Request for Administrative Ruling on the Application of FinCEN's Regulations to a Virtual Currency Payment System. FinCEN. Retrieved from https://www.fincen.gov/sites/default/files/shared/FIN-2014-R012.pdf

not already be experts in consumer protection. In the construction of a system with distributed governance or automated decision-making, adherence to the guiding principles of consumer protection in digital economies will be vital to designing systems that protect participants in these organizations.

- **Digital asset investors and traders** - Individuals and businesses that invest or trade digital assets like bitcoin or ether may or may not be experts in the technology and systems that can secure their investments. If they are not, this document will help them better understand what to demand from the services they use to trade or hold their bitcoin or other digital assets. An educated consumer is a better-protected consumer.

Relevant government and non-governmental entities

A number of federal and state agencies as well as legislative and regulatory bodies have a stake in consumer protection in the financial services industry. A number of these entities have released consumer advisories, taken enforcement actions, or developed rules/classifications regarding bitcoin and other digital currencies or the entities utilizing digital currencies and assets (described above).

Government entities

- Consumer Financial Protection Bureau (CFPB)
- Federal Trade Commission (FTC)
- Securities and Exchange Commission (SEC)
- Commodity Futures Trading Commission (CFTC)
- Federal Deposit Insurance Corporation (FDIC)
- U.S. Department of the Treasury's Financial Crimes Enforcement Network (FinCEN)
- Financial Industry Regulatory Authority (FINRA)
- National Association of Attorneys General (NAAG)
- U.S. Department of Justice (DOJ)
- U.S. Internal Revenue Service (IRS)
- Department of Homeland Security (DHS)
- U.S. Federal Reserve System
- National Credit Union Administration (NCUA)
- Federal Housing Finance Agency (FHFA)
- Consumer Product Safety Commission (CPSC)
- U.S. House of Representatives, Senate, and President
- North American of Securities Administrators Association (NASAA)
- U.S. state governments and agencies (i.e. DFSNY and CADBO), two U.S. territories
- Global governments

Non-governmental entities

- Depository Trust & Clearing Corporation (DTCC)
- Conference of State Bank Supervisors (CSBS)

See Appendix for more on relevant agencies and state and federal actions.

Consumer Bill of Rights

Security

I. Consumers have the right to secure storage of funds and data they entrust to third parties.

II. Consumers have a right to user accounts secured against intrusion and disruption by intruders.

III. Consumers have a right to user accounts secured against extensive damage in the event their accounts are compromised.

Privacy

IV. Consumers have the right to have as little data collected about them as is needed for the company to operate its *primary* business model and to meet regulatory requirements.

V. Consumers have the right to revoke the *use* and *holding* of their data where permissible by law.

VI. Consumers have a right to plain language advanced disclosures about data sharing with third parties as well as the right to "opt out" of this information sharing.

VII. Consumers have a right to strong, continuously updated data protection protocols, which ensure the data is as difficult to analyze as possible by bad actors.

Usability

VIII. Consumers have a right to user platforms with simple, well-designed user experiences and user interfaces (UX/UIs).

IX. Consumers have a right to reasonably brief and readily understandable information regarding disclosures related to platform terms and conditions, collection of PII, data sharing with third parties, and compliance with government requests information.

X. Consumers have a right to interoperability among the various platforms that operate using blockchain technology as well as essential web-based platforms.

Disclosures and Liability

XI. Consumers have a right to complete, time-stamped disclosures regarding: legal entity status, applicable legal jurisdictions, institutional solvency, asset insurance, availability of funds or assets, privacy policy, timing of payments, receipts, loan/credit terms, and fees using concise, plain language

XII. Consumers have a right to access and transfer their funds or assets at any time.

XIII. Consumers have a right to timely and unencumbered transaction processing of payments falling below certain legal requirements for reporting or monitoring.

XIV. Consumers have a right to an audit of compliance with disclosure policies.

Guiding Principles

Security

I. Protect individual user accounts, user PII, and user assets from unauthorized or fraudulent access and loss events caused by that access, including unauthorized or unlawful access by states or the financial institutions serving as fiduciaries of user assets.

II. Minimize the extent of damage users can suffer in the event their accounts are compromised.

III. Establish and maintain secure asset storage and transfer and guard against theft of consumer assets and data (such as PII) using the best available security mechanisms.

Privacy

IV. Collect and/or hold only the minimum data necessary to operate *primary* company business model and meet regulatory requirements.

V. Enable consumers to revoke the *use* and *holding* of their data where permissible by law and implement procedures to permit users to cause their data to be expunged, or abide by a published enforced destruction term (i.e. destruction at a disclosed time).

VI. Do not share data with third parties without explicit user permission obtained at the outset of the engagement or advanced disclosure that has been concisely communicated and explicitly agreed to.

VII. When writing information to a blockchain, include the minimum amount of attributable data necessary to properly record transactions and ensure the data is as difficult to analyze as possible by bad actors.

Usability

VIII. Develop platforms with a simple, intuitive, well-designed user experience and user interface (UX/UI).

IX. Provide reasonably brief and readily understandable information regarding disclosures related to platform terms and conditions, collection of PII, data sharing with third parties, and compliance with government requests information.

X. Ensure interoperability among the various platforms that operate using blockchain technology as well as essential web-based platforms.

Disclosures and Liability

XI. Disclose complete information regarding: legal entity status, applicable legal jurisdictions, institutional solvency, asset insurance, availability of funds or assets, privacy policy, timing of payments, receipts, loan/credit terms, and fees.

XII. Enable any-time access and transfer of consumer funds or assets.

XIII. Enable timely and unencumbered transaction processing of payments falling below certain legal requirements for reporting or monitoring.

XIV. Regularly conduct and disclose detailed findings of audit of compliance with disclosure policies.

Consumer Protection Challenges

This section examines the flaws, failures, and weaknesses of existing financial industry frameworks as well as newer digital currency and distributed ledger products and services. When people think about digital currency consumer protections, the theft of financial or other assets, such as Bitcoin and ether, from hosted exchanges are the first and most prominent instances that come to mind. From Mt. Gox to the recent Bitfinex hack (and a half-dozen others in between) the passive observer may believe that digital currencies are especially susceptible to being hacked or stolen.[3,4] Protecting digital currencies and other blockchain-derived distributed technology assets against theft or loss is of the utmost importance in growing and sustaining the digital economy.

1. ASSET SECURITY

Problems faced by consumers that are unique to traditional financial services, but not distributed ledger financial services:

A. The security tools utilized by traditional financial service providers are limited in scope and do not offer consumers the strongest available protection methods for securing their assets.
    a. Depending on the size of the financial institution, the security tools utilized can be quite sophisticated and may be considered the strongest available for the current technologies commonly used to conduct store value and conduct or verify transactions. However, if traditional financial institutions were open to a fundamental shift to different technologies, stronger security methods are available for them to employ.
B. When traditional security mechanisms fail, consumer assets are often guaranteed through legal or other means, regardless of whether the lost/stolen assets are recovered (through law enforcement or other means). For example, the FDIC insures consumer deposit accounts up to $250,000.
C. Perpetrators of cyber attacks and other bad actors continuously update the methods by which they cause data breaches and companies struggle to stay ahead of the curve, potentially leaving consumer assets (and data) vulnerable to exploitation, unintended

---

[3] Edwards, J. (2013, November 17). If Bitcoin Is So Secure, Why Have There Been Dozens of Bitcoin Bank Robberies And Millions In Losses? Retrieved from http://www.businessinsider.com/the-history-of-bitcoin-theft-2013-11

[4] Colangelo, J. (2016, August 2). *Consumers' Research Bitcoin Loss Calculations*. Consumers' Research. Retrieved from https://docs.google.com/spreadsheets/d/1qFSjFDqe-eQ6m9c6ima6qkrtYCfdvSr75h-hZR-rrtA/edit#gid=0

use, and further liability. According to Pew Research Center, a majority of Internet experts predict more major cyber attacks by 2025.[5]

Problems faced by consumers using traditional and distributed ledger financial services:

D. User devices and credentials may be compromised and used to obtain unauthorized access to user accounts.
E. In the event that user accounts are compromised, unauthorized parties may be able to steal the entirety of a user's financial (or other virtual) assets or claims on assets.
    a. While traditional financial institutions often enforce daily transaction limits on user accounts and digital currency wallets may have protection mechanisms such as two-factor authentication, if compromised, it is possible that some or all assets could be emptied from both types of accounts.
    b. Should a user's identity data also be compromised, they may become vulnerable or subject to further financial losses or exposure to further fraud.
F. Poorly written/designed code, smart contracts, and DAOs leave consumer assets and data (such as PII) vulnerable to exploitation and unintended use and further liability.

Problems faced by consumers that are unique to distributed ledger financial services, but not traditional financial services:

G. All things being equal, Bitcoin and blockchain companies may have a greater risk of massive and irrevocable thefts that can target the assets they secure and store for their users, as well as user data (such as personally identifiable information).
    a. Protecting digital currency assets is imperative to avoid repeats of consumer asset losses similar to Mt. Gox (2014) or Bitfinex (2016). Therefore, Bitcoin and blockchain financial service providers should implement best practices to prevent such instances to the extent possible, both to protect consumer assets, as well as reduce their own risk of dispute resolution for lost assets.
    b. Given that Bitcoin and blockchain financial services is an emerging industry, specialized best practices have not yet been fully developed, vetted, or widely adopted. If Bitcoin and blockchain companies do not implement industry best practices, they face higher risk than non-bitcoin financial service providers, due to the greater challenge of recovering the assets. Examples of such best practices include: employing effective multi-layer protocols such as full

[5] Rainie, L., Anderson, J., & Connolly, J. (2014, October 29). Cyber Attacks Likely to Increase. Per Research Center. Retrieved from http://www.pewinternet.org/2014/10/29/cyber-attacks-likely-to-increase/

encryption, (non-automated) multi-signature and multi-factor authentication and deterministically random key generation, coupled with the use of cold storage (for a majority of the assets being stored) and other security mechanisms (including federated networks, "programmable money/tokens," etc.). If Principles I & II are followed, the risk of loss described above is minimized.

c. There are currently no government-backed institutions to protect or refund custodial digital currency or other virtual assets analogous to the FDIC.

H. There are currently no government-backed institutions to protect or refund custodial digital currency or other virtual assets analogous to the FDIC.[6,7]

a. The limited access to safety nets that exists for traditional financial custodians, such as FDIC insurance, makes robust security and asset storage all the more important for digital asset and token custodians.

b. Companies can use surety bonds, private insurance, and other "guarantee" mechanisms to insure consumer assets; however, consumers are left with legal action as their primary means of recourse if the surety bond or insurance is insufficient to cover all losses. In cases such as the DAO, consensus mechanisms can be employed to "return" assets as well; however, such mechanisms should be used as a last resort, but as a best practice. In any case, in the absence of governmental intervention, market forces will slowly compel private businesses to fill the digital currency "insurance" gap; however, companies offering surety bonds, private insurance, and other "guarantee" mechanisms will likely expect strict audit rules and require that certain best practice security protocols are followed.

c. Unlike, traditional banking and financial services, the nature of digital currency transfers via blockchain technologies does not allow for "chargebacks" or the reversal of transactions, because the actual value (and therefore, ownership) is sent in the transaction, not simply a record or message that a transaction took place, which will later be subject to settlement (such as a SWIFT transaction).[8] As a resolution for consumers, legal mechanisms can be applied to hold companies accountable for the loss of assets; however, all things being equal, once transferred digital currency or other blockchain-based tokens representing

---

[6] Some custodial bitcoin providers, such as Coinbase, provide private insurance of customer assets up to a certain value. BitGo was also able to secure blanket insurance underwriting for its consumer-facing multi-signature wallet solution. These are not industry- or government-underwritten insurance programs, but they do provide some protection against lost assets for consumers. Circle offers up to $250,000.00 in FDIC insurance.

[7] Securities and Exchange Commission. (2014, May 7). Investor Alert: Bitcoin and Other Virtual Currency-Related Investments. Retrieved from https://www.sec.gov/oiea/investor-alerts-bulletins/investoralertsia_bitcoin.html.

[8] Belshe, M. (2014, December 1). CoinCenter. Are Consumer Bitcoin Balances Especially Vulnerable to Hacking? Retrieved from https://coincenter.org/entry/are-consumer-bitcoin-balances-especially-vulnerable-to-hacking

value or ownership rights are irretrievable unless there sufficient consensus is achieved to fork the digital currency and "return" the asset.[9]

d. Private insurance companies may emerge from the needs of the market that are willing to insure funds or other assets. Any such companies would be expected to have strict audit rules and to adhere to certain best practice security protocols.

I. Provide robust, user-friendly key management solution able to generate a recovery key, in case of loss or theft.

J. Provide robust mechanisms to ensure intended amount and recipient account are verified before value is transferred.

a. With digital currencies, common user errors such as entering the incorrect or unintended amount for a transfer/transaction or entering the incorrect destination account information (or public key) are irreversible, unless the recipient willingly returns the unintended transfer or portion of the transfer. In cases where an unintended recipient account is inactive, there is no way to retrieve the misdirected funds at this time.

Note: Consumer who chooses to store funds in a locally hosted wallet are responsible for the security of their personal devices.

2. DATA PRIVACY

Problems faced by consumers using traditional and distributed ledger financial services:

A. Perpetrators of cyber attacks and other bad actors continuously update the methods by which they cause data breaches and companies may struggle to stay ahead of the curve, leaving consumer data (and assets) vulnerable to exploitation, unintended use, and further liability.[10]

B. When companies collect and/or hold more data than they need to operate their ***primary*** business model and to meet regulatory requirements, the risk of fraud and theft to

---

[9] In cases where consensus drives a fork of the digital currency, assets are returned (not "refunded" per se), but some of the value may be lost (or new value may be gained) as a result of the fork. For now, Bitcoin is completely tracked, so parties have the choice to restrict or reverse certain transactions through consensus, but have chosen thus far not to on principle. These types of choices remove Bitcoin's distinction in the markets, but parties to other cryptocurrencies, such as Ethereum, have chosen to exercise this option.

[10] Rainie, L., Anderson, J., & Connolly, J. (2014, October 29). Cyber Attacks Likely to Increase. Pew Research Center. Retrieved from http://www.pewinternet.org/2014/10/29/cyber-attacks-likely-to-increase/

consumers in the case of a data breach may be much greater than it should be. In turn, this increases the liability of said companies.[11]

   a. Companies should consider pushing for the adoption of protocols or "proofs" that allow for regulatory requirements to be met without the collection and storage of data that can put consumers at risk. With blockchain-derived distributed technologies, compliance rules (such as KYC and AML requirements) are at odds with privacy and security. The collection of consumer information is not required for funds to be held and transactions to occur, however, when such information is collected and married to account data, a data breach will lead to avoidable exposure of consumer information.
   b. In the absence of "proofs" being acceptable means of regulatory compliance, collecting as little data as necessary can minimize data exploitation risk to consumers.[12]

C. Holding centralized attributable consumer data creates a target for bad actors.
   a. This problem can be likened to that faced by custodial banks, where fund aggregation leads to risk aggregation. Bad actors are more inclined to attack a single aggregator of data than a distributed network of data, because the payoff is higher (and the security is arguably easier to overcome than a distributed ledger, because it is centralized).
   b. User/self-sovereign/federated identity might be the solution to these concerns.

D. The ability of companies to *use* or *hold* consumer data indefinitely without procedures to permit users to cause their data to be expunged, or without a published, enforced destruction term (i.e. destruction at a disclosed time) prevents consumers from having

---

[11] There is some dissent among the authors on this topic. Some authors believe that consumers need to recognize that services come at a cost. If the consumer is not paying for the service, then it's likely that their information is the product being sold. Ultimately if consumers value a company's service and view the company's product as superior to other options that do not collect much data, then consumers may be willing to give up their data (e.g. Google). However, other authors point out that this does not incentivize companies to look into alternative revenue streams that aren't built off consumer data. Competitor products exist, but if more revenue can be gained from selling consumer data (via "freemium" models) than in paid services, the talent and resources go to the companies who make the most money and competitor products that don't monetize consumer data will stay at a disadvantage until alternative revenue streams are developed (which is almost a Catch-22 since companies do not need to look into alternative revenue streams). That said, in the open-source era (and in an age of digital decentralized money), an individual can code an entire service that replaces a centralized company. This individual is incentivized to do so from an expectation of donations from loyal and happy users or by providing expert support and building add-ons to that service for the service's customers. Another consideration is that "micropayments" might cause a shift in the way we consume online content and reduce/remove companies' desires to collect and sell data.

[12] Newman, N. (2014, August). How Big Data Enables Economic Harm to Consumers. Retrieved from https://www.ftc.gov/system/files/documents/public_comments/2014/08/00015-92370.pdf

ownership over their data, and as such, the ability to limit their exposure to fraud and theft.

a. It is important for consumers to understand that revoking their rights to data use or holding does not necessarily expunge the data. Revocation may create a false sense of security, as there is currently no meaningful way to prove and ensure full deletion from all sources.
b. Consumer education is a key part of ensuring that consumers understand the implications of the rights they have or agree to give up when using certain products or services.

E. The lack of plain language and brevity (i.e. simple, pertinent executive summaries) in advanced disclosures may result in consumers overlooking, misunderstanding, and ultimately consenting to terms they might otherwise give more thought to or possibly not accept.[13]

a. As above, consumer education is a key element of safeguarding consumer best interests.
b. Detailed and extensive advanced disclosures are *designed* to protect companies in the case of legal action, though they are intended to educate consumers about terms of use they are agreeing to when they register for a service. Research shows[14] that consumers do not read End User License Agreements (EULAs), terms of service, terms of use, and privacy policies, when entering agreements. Whether due to complicated legal jargon, overly lengthy terms, or other barriers, the expectation that the average American consumer is endowed with sufficient resources (such as literacy, proficiency in legal jargon, and time), to readily understand complicated and detailed advanced disclosures places an undue burden on consumers.[15,16]
c. Furthermore, the market is saturated with advanced disclosures consumers may not find palatable; yet accept due to limited or nonexistent alternatives.

---

[13] Newitz, A. (2005, February 17). Dangerous Terms: A User's Guide to EULAs. Retrieved from https://www.eff.org/wp/dangerous-terms-users-guide-eulas

[14] Bakos, Y., Marotta-Wurgler, F., & Trossen, D. R. (2014). Does anyone read the fine print? Consumer attention to standard form contracts. *Journal of Legal Studies*, 43(1), 09-40. Retrieved from: http://www.law.uchicago.edu/files/file/bakos_fineprint.pdf

[15] Cordray, R. (2016, May 5). *Prepared Remarks of CFPB Director*. Speech presented at Field Hearing on Arbitration Clauses. Retrieved from http://www.consumerfinance.gov/about-us/newsroom/prepared-remarks-cfpb-director-richard-cordray-field-hearing-arbitration-clauses/

[16] Cordray, R. (2015, December 3). *Prepared Remarks of CFPB Director*. Speech presented at Consumer Federation of America. Retrieved from http://www.consumerfinance.gov/about-us/newsroom/prepared-remarks-of-cfpb-director-richard-cordray-at-the-consumer-federation-of-america/

F. Advanced disclosures regarding data sharing with third parties address the issue of transparency regarding consumer data; however, they do not give consumers the ability to "opt out" of this information sharing. Data sharing with third parties may expose consumers to greater risk of fraud, theft, and unwanted marketing, particularly when the privacy protocols of said third parties is unknown or not disclosed to consumers. Furthermore, terms and conditions are subject to change throughout the lifetime of a relationship or agreement and consumers may no longer desire to use a product or service if new terms require third party data sharing.[17]

G. Weak data protection protocols, which do not ensure data is as difficult to analyze as possible by bad actors, may leave consumers open to greater risk of fraud and theft.

H. Information on open ledgers is public, which means that any unencrypted, attributable private information put on a blockchain is accessible to anyone who maintains, accesses, or audits that ledger.

    a. Pseudonymous information put on a blockchain may not be useful information without context or unless user pseudonyms can be identified (in that sense it is not accessible, useful data).

    b. Some open ledgers implement features, such as zero knowledge proofs, that conceal information in public transactions, while retaining their auditability using applied cryptography. These systems are not yet widely adopted, but available.[18]

I. Transactions on open and permissionless ledgers[19] are traceable, therefore privacy is limited if identity can be linked to public keys.

    a. Many tools exist to obfuscate activity, and the industry is determining which of the protocols to fold into these open networks. The traditional models of trust and knowledge are somewhat challenged when faced with ideas like selective disclosure on distributed ledgers. Networks can simultaneously be open (free to join) and private (transaction details visible only to participating parties).

    b. Bitcoin transactions are currently highly traceable, but other open and permissionless ledgers (such as Zcash), layers built on top of bitcoin (such as the Coin Shuffle protocol), or modifications to bitcoin (such as "Confidential Transactions") are not highly traceable.

---

[17] Data Risk in the Third Party Ecosystem. (2016, April) Ponemon Institute LLC. Retrieved from https://www.ponemon.org/local/upload/file/Data Risk in the Third Party Ecosystem_BuckleySandler LLP and Treliant Risk Advisors LLC Ponemon Research 2016 - FINAL2.pdf

[18] Samman, G. (2016, September 11). The Trend Towards Blockchain Privacy: Zero Knowledge Proofs. CoinDesk. Retrieved from http://www.coindesk.com/trend-towards-blockchain-privacy-zero-knowledge-proofs/

[19] … so long as he definition of "open" excludes some of the new decentralized cryptocurrency innovations, such as Z-cash, which use zero-knowledge proofs to obscure traceability back to public keys.

J. Information placed on or transactions made on blockchains are permanent, in that once the record is on a blockchain it becomes immutable and remains accessible to those who maintain, access, or audit that blockchain.[20]
    a. The immutability of a blockchain comes from the underlying trust network, not by nature of a blockchain itself. Therefore, data on a public or private blockchain can be altered with the agreement of the controlling entity or consortium (e.g. Ethereum hard fork).
K. Blockchain analysis will improve over time, which may increase the likelihood of identity linking, transaction tracing, and breaches or decryption of insufficiently protected data if sufficiently robust security or stealth protocols do not manifest.

3. USABILITY

Problems faced by consumers that are unique to traditional financial services, but not distributed ledger financial services:

A. Except where legislation requires compliance with regulation, financial services technology standards have been predominantly created by committees comprised of established stakeholders from the relevant adopting institutions, excluding or cannibalizing small but relevant players or open source development.[21,22,23,24,25]

Problems faced by consumers using traditional and distributed ledger financial services:

B. User interfaces are sometimes difficult to navigate. This can cause user confusion or limit the ability of users to execute various platform functions.

---

[20] … so long as the definition of a "blockchain" is a truly decentralized, public, permissionless censorship-resistant distributed ledger, which bitcoin more or less approximates.

[21] United States (ANSI). (n.d.). Retrieved from http://www.iso.org/iso/home/about/iso_members/iso_member_body.htm?member_id=2188

[22] About ANSI. (n.d.). Retrieved from https://www.ansi.org/about_ansi/overview/overview.aspx?menuid=1

[23] Elmore, A. (2016, April 26). Building on Blockchain Part Three: Trust, Interoperability and the Blockchain Market. Gresham. Retrieved from https://blog.c24tech.com/data-geek/building-on-blockchain-part-three-trust-interoperability-and-the-blockchain-market

[24] Financial Services Standards. (2016, November 17). Object Management Group. Retrieved from http://www.omg.org/hot-topics/finance.htm

[25] NIST is not a regulator: About NIST. (2016, August 25). Retrieved from https://www.nist.gov/about-nist

a. User experience remains one of the greatest barriers to consumer adoption of digital asset platforms.[26]
b. Engineers and computer scientists, while brilliant, are sometimes unable to recognize that their ability to navigate user interfaces far outmatches the ability of the average consumer to do so. Abilities that an engineer may take for granted, such as the ability to search a page for a phrase to find what one is looking for, are completely foreign or unknown to many potential users.[27]
c. Consumers who have access to features but cannot figure out how to easily access those features, especially around security, may as well not have access to those features at all. If the same security can be had by securely integrating with a third party at the touch of a button (like Google or Clef 2FA) it is better to go that route than asking the user to copy and paste API keys in another app.

C. The lack of plain language and brevity (i.e. simple, pertinent executive summaries) in advanced disclosures may result in consumers overlooking, misunderstanding, and ultimately consenting to terms they might otherwise give more thought to or possibly not accept. [28]
a. Detailed and extensive advanced disclosures are *designed* to protect companies in the case of legal action, though they are *intended* to educate consumers about terms of use they are agreeing to when they register for a service. Research shows[29] that consumers do not read End User License Agreements (EULAs), commonly referred to as "terms of use," when entering agreements. Whether due to complicated legal jargon, overly lengthy terms, or other barriers, the expectation that the average American consumer is endowed with sufficient resources (such as literacy, proficiency in legal jargon, and time), to understand complicated and detailed advanced disclosures places an undue burden on consumers.
b. Furthermore, the market is saturated with advanced disclosures consumers may not find palatable, yet, accept due to limited or nonexistent alternatives.

Problems faced by consumers that are unique to distributed ledger financial services, but not traditional financial services:

---

[26] Demirors, M. (2016, October 9). For Most Users, Bitcoin is Not That Great. On the Future. Retrieved from https://onthefuture.co/for-most-users-bitcoin-is-not-that-great-97b3bf4a7064#.n037afcda

[27] Krug, S. (2006). *Don't make me think!: A common sense approach to Web usability*. Retrieved from http://www.avis.it/userfiles/file/Dont_Make_Me_Think_A_Common_Sense_Approach_to_Web_Usability_2nd_Ed_2005.pdf

[28] Newitz, A. (2005, February 17). Dangerous Terms: A User's Guide to EULAs. Electronic Frontier Foundation. Retrieved from https://www.eff.org/wp/dangerous-terms-users-guide-eulas

[29] Bakos, Y., Marotta-Wurgler, F., & Trossen, D. R. (2014). Does anyone read the fine print? Consumer attention to standard form contracts. Journal of Legal Studies, 43(1), 09-40. Retrieved from: http://www.law.uchicago.edu/files/file/bakos_fineprint.pdf

D. Some Bitcoin and blockchain concepts are completely foreign to consumers, but are integral to the safe use of related products and services.
    a. The number of consumers who understand concepts such as public and private keys or who can effectively take responsibility for a randomly generated 16-digit key, represents a very select percentage of the population.[30,31]
    b. Platforms offering services that rely on complex technologies do not always account for the various scenarios ill-informed consumers may find themselves in in terms of the loss or theft of their assets or data due to a misunderstanding of how a product or service actually works.

E. Consumers cannot readily participate in data or value exchange across related platforms, because many core technical components of blockchains are not readily interoperable with their Web[32] counterparts, including:
    a. Blockchain APIs, such as JavaScript or REST APIs
    b. Blockchain primitives such as transaction initiation, key signing, and wallet management
    c. Ledger interchange formats and protocols

F. The nature of distributed ledgers and chains requires that parties adopt common formats in order for content structure innovation to progress.
    a. In the financial services sector, standards have been predominantly created by committees comprised of key players from the relevant adopting institutions, excluding or cannibalizing smaller players or open source development.[33]

G. The development of future consumer blockchain applications relies on interoperability among various systems, which are not being developed concurrently. Such applications may include:
    a. Identity systems, including privacy, security, and confidentiality factors[34]

---

[30] Pathe, S. (2014, February 5). Most Americans unfamiliar with and won't use Bitcoin. PBS Newshour. Retrieved from http://www.pbs.org/newshour/rundown/americans-unfamiliar-wont-use-bitcoin/

[31] Rizzo, P. (2015, July 29). Survey: Consumers Say Bitcoin More Inconvenient Than Checks. CoinDesk. Retrieved from http://www.coindesk.com/survey-consumers-bitcoin-inconvenient-checks/

[32] Nichol, P. B. (2016, June 29). MIT hosts the W3C blockchain interoperability workshop. CIO. Retrieved from http://www.cio.com/article/3089459/consumer-electronics/mit-hosts-the-w3c-blockchain-interoperability-workshop.html

[33] Elmore, A. (2016, April 26). Building on Blockchain Part Three: Trust, Interoperability and the Blockchain Market. Gresham. Retrieved from https://blog.c24tech.com/data-geek/building-on-blockchain-part-three-trust-interoperability-and-the-blockchain-market

[34] Prisco, G. (2016, June 03). Microsoft Building Open Blockchain-Based Identity System With Blockstack, ConsenSys. Bitcoin Magazine. Retrieved from https://bitcoinmagazine.com/articles/microsoft-building-open-blockchain-based-identity-system-with-blockstack-consensys-1464968713

b. Rights expression and licensing systems
c. Decentralized processing, computing, and storage infrastructure

4. DISCLOSURE AND LIABILITY

Problems faced by consumers that are unique to traditional financial services, but not distributed ledger financial services:

A. Consumers can incur fees and encounter other problems when their funds or other assets are not readily available, either due to limited banking hours or other barriers to access.
    a. In today's high-tech world, there is no reason consumers should not be able to access or transfer their assets at any time of day or night. With traditional banking, limitations on when consumers can access their assets are based on preferences that benefit financial institutions, and are not what is in the best interest of consumers.
    b. 24-hour access to funds promotes commerce and is not only good for consumers, but the financial institutions that serve them, so long as those institutions are equipped to manage client needs at all hours.
B. Consumer funds or other assets are subject to a greater risk of fraud or double-spend when payments are not fully processed (i.e. completed) or available for use in a timely and unencumbered manner.

Problems faced by consumers using traditional and distributed ledger financial services:

C. Some legal jurisdictions have greater consumer protections than others.[35] Not knowing the legal jurisdiction of an entity could result in avoidable theft, loss, civil/criminal forfeiture, or appropriation of consumer assets.
D. When consumers entrust third parties with their assets they run the risk of theft or loss, including bank failures.
    a. A bank failure occurs when a bank becomes insolvent or too illiquid to meet its obligations to its depositors or other creditors. Bank runs, which occur when depositors all demand their money at once, can cause or expedite bank failure.
    b. Deposit insurance in the U.S. came about as a result of the 1933 Banking Act; this was passed in response to the turmoil created by the Wall Street Crash of 1929, after which one-third of banks failed.

---

[35] The State of Consumer Protection Around the World. (2013, April). Consumers International. Retrieved from http://www.consumersinternational.org/media/1139641/english_full_report_april.pdf

c. The deposit insurance offered by the FDIC and other policies or instruments, such as surety bonds, lessen the uncertainty that consumers feel in times of economic crisis. Such instruments assure consumers that their cash assets will be protected up to a certain point. This encourages consumer spending in good times, and also serves as a hedge against people making a run on the banks in bad times.

E. Consumers may be susceptible to "pretexting" (the practice of obtaining personal information through false pretenses) by banks, credit card companies, and other financial institutions that may exploit their information for uses other than its intended purposes.
    a. Private information such bank balances and account numbers can be bought and sold by banks, credit card companies, and other financial institutions. Due to information sharing among separate divisions within companies offering multiple services (i.e. banking, investment, insurance, etc.) as well as with third parties, these entities have the ability to engage in pretexting. Consumers must trust that these actors will safeguard their information and only use it for its intended purposes.

F. When the timing of payments is inconsistent or unclear, consumers face challenges regarding budgeting and availability uncertainty. These challenges can result in otherwise avoidable and burdensome overdraft fees, late payment fees, credit score penalties, etc.[36]

G. Without proof of payment or proof of transaction (including trade and investment activity), consumers are often unable to take legal action regarding goods/services purchased or trades and investments made.

H. When consumers may be ill-informed about the lending terms of loans and consumer credit, they are susceptible to poor/unfavorable and arguably abusive loan terms as well as credit billing and credit card practices.
    a. In 1968, Congress passed The Truth in Lending Act (TILA) under the auspices of promoting the informed use of consumer credit. The law requires disclosures about the terms of consumer credit as well as the way in which costs associated with borrowing are calculated and disclosed.
    b. The Mortgage Reform and Anti-Predatory Lending Act (part of the Dodd-Frank Act), amended the Truth in Lending Act of 1968, because Congress felt that lending institutions had been taking advantage of lower-income borrowers. The "Know Before You Owe" rule, instituted as part of Dodd-Frank, increased the required disclosures for mortgages.

---

[36] See-To, E. (2006). *When do you pay? The business impact of payment time perception* (Working paper). Lancaster University Management School. Retrieved from http://eprints.lancs.ac.uk/48864/1/Document.pdf

I. Lack of knowledge regarding how fees can be incurred can leave consumers vulnerable to racking up fees, which can have materially damaging effects on the financial health of certain consumers.

J. The lack of plain language and brevity (i.e. simple, pertinent executive summaries) in advanced disclosures may result in consumers overlooking, misunderstanding, and ultimately consenting to terms they might otherwise give more thought to or possibly not accept.

    a. Detailed and extensive advanced disclosures are *designed* to protect companies in the case of legal action, though they are intended to educate consumers about terms of use they are agreeing to when they register for a service. Research shows[37] that consumers do not read End User License Agreements (EULAs), commonly referred to as "terms of use," when entering agreements. Whether due to complicated legal jargon, overly lengthy terms, or other barriers, the expectation that the average American consumer is endowed with sufficient resources (such as literacy, proficiency in legal jargon, and time), to understand complicated and detailed advanced disclosures places an undue burden on consumers.

Problems faced by consumers that are unique to distributed ledger financial services, but not traditional financial services:

K. Given the rapid evolution of technology, consumers may not understand the legal incorporation status or type of entity they are engaging with. Such misunderstandings could materially harm consumers who believe they are guaranteed certain protections, when they actually aren't, due to liability restrictions associated with certain types of entities.

    a. For example, distributed autonomous organizations (DAOs) may be subject to different liability structures than the legal entities consumers are familiar with, such as limited liability corporations or S corporations and C corporations.[38]

---

[37] Bakos, Y., Marotta-Wurgler, F., & Trossen, D. R. (2014). Does anyone read the fine print? Consumer attention to standard form contracts. Journal of Legal Studies, 43(1), 09-40. Retrieved from: http://www.law.uchicago.edu/files/file/bakos_fineprint.pdf

[38] Hinkes, D. (2016, June 21). A Legal Analysis of the DAO Exploit and Possible Investor Rights. Bitcoin Magazine. Retrieved from https://bitcoinmagazine.com/articles/a-legal-analysis-of-the-dao-exploit-and-possible-investor-rights-1466524659

Recommended Solutions

1. ASSET SECURITY

Consumer Rights

Companies using blockchain-derived distributed technologies to run digital currency exchanges, hosted wallets, payment processors, DAOs, and digital asset investments/trades should bestow the following rights on consumers using their products:

I. Consumers have the right to secure storage of funds and data they entrust to third parties.
II. Consumers have a right to user accounts secured against intrusion and disruption by intruders.
III. Consumers have a right to user accounts secured against extensive damage in the event their accounts are compromised.

Consumer Protection Guiding Principles

Companies using blockchain-derived distributed technologies to run digital currency exchanges, hosted wallets, payment processors, DAOs, and digital asset investments/trades should employ the following guiding principles to ensure the above enumerated consumer rights:

I. Protect individual user accounts, user PII, and user assets from unauthorized or fraudulent access and loss events caused by that access, including unauthorized or unlawful access by states or the financial institutions serving as fiduciaries of user assets. This addresses the following consumer protection challenges:
    a. User devices and credentials may be compromised and used to obtain unauthorized access to user accounts.
II. Minimize the extent of damage users can suffer in the event their accounts are compromised. This addresses the following consumer protection challenges:
    b. In the event that user accounts are compromised, unauthorized parties may be able to steal the entirety of a user's funds.
III. Establish and maintain secure asset storage and transfer and guard against theft of consumer assets and data (such as personally identifiable information) using the best available security mechanisms. This addresses the following consumer protection challenges:
    c. Bitcoin and blockchain companies have a greater risk of massive and irrevocable thefts that can target the funds they secure and store for their users.

d. There are currently no institutions to protect or refund custodial cryptocurrency analogous to the FDIC.

Additional resource on security:
Higgins, S. (2015, February 18). Security Standard Proposed for Bitcoin Exchanges and Wallets. CoinDesk. Retrieved from http://www.coindesk.com/security-standard-proposed-bitcoin-exchanges-wallets/

2. DATA PRIVACY

Consumer Rights

Companies using blockchain-derived distributed technologies to run digital currency exchanges, hosted wallets, payment processors, DAOs, and digital asset investments/trades should bestow the following rights on consumers using their products:

IV. Consumers have the right to have as little data collected about them as is needed for the company to operate its *primary* business model and to meet regulatory requirements.
V. Consumers have the right to revoke the *use* and *holding* of their data where permissible by law.
VI. Consumers have a right to plain language advanced disclosures about data sharing with third parties as well as the right to "opt out" of this information sharing.
VII. Consumers have a right to strong, continuously updated data protection protocols, which ensure the data is as difficult to analyze as possible by bad actors.

Consumer Protection Guiding Principles [39]

Companies using blockchain-derived distributed technologies to run digital currency exchanges, hosted wallets, payment processors, DAOs, and digital asset investors/traders, companies should employ the following guiding principles to ensure the above enumerated consumer rights:

IV. Collect and/or hold only the minimum data necessary to operate *primary* company business model and meet regulatory requirements. This addresses the following problems:

[39] Authors repeatedly recommended the use of federated identity services to resolve data privacy issues; however, such services are not yet sufficiently operable, nor do they meet regulatory compliance requirements at this time.

a. When companies collect more data than they need to operate their *primary* business model and to meet regulatory requirements, the risk of fraud and theft to consumers in the case of a data breach is much greater than it should be. In turn, this increases the liability of said companies.
    1. Companies may make some allowances for collection of specifically enumerated data for R&D purposes, provided that there is appropriate affirmative opt-in consent given by users.
    2. Should companies choose to collect and monetize additional consumer data to subsidize the cost of the service to the end user, they should secure that data using the best mechanisms available, as well as fully disclose what information has been collected and for what purpose(s).
b. Holding centralized attributable consumer data creates a target for bad actors.

V. Enable consumers to revoke the *use* and *holding* of their data where permissible by law and implement procedures to permit users to cause their data to be expunged, or abide by a published enforced destruction term (i.e. destruction at a disclosed time).[40][41] This addresses the following consumer protection challenges:
    c. The ability of companies to *use* or *hold* consumer data indefinitely prevents consumers from having ownership over their data, and as such, the ability to limit their exposure to fraud and theft.

VI. Do not share data with third parties without explicit user permission obtained at the outset of the engagement or advanced disclosure that has been concisely communicated and explicitly agreed to. This addresses the following consumer protection challenges:
    d. The lack of plain language and brevity (i.e. simple, pertinent executive summaries) in advanced disclosures may result in consumers overlooking, misunderstanding, and ultimately consenting to terms they might otherwise give more thought to or possibly not accept.[42]
    e. Advanced disclosures regarding data sharing with third parties address the issue of transparency regarding consumer data; however, they do not give consumers the ability to "opt out" of this information sharing. Data sharing with third parties may open consumers to greater risk of fraud, theft, and

---

[40] Some authors question the possibility of "revoking use" of data or "owning" data. "Data ownership" is a very difficult concept. Data really cannot be owned, because it can be so easily duplicated. Additionally, no laws are currently in place to create or enforce any such a property right (unless it is copyrightable). Nor is achieving robust "data ownership" through law necessarily a desirable policy goal (see the problems that aggressive copyright enforcement generate for Internet companies).

[41] There was dissent among the authors regarding the following recommended addition: Companies can obtain a contractual interest in consumer data, which should be honored as a form of payment for service, provided the terms were clearly disclosed ahead of time.

[42] Newitz, A. (2005, February 17). Dangerous Terms: A User's Guide to EULAs. Electronic Frontier Foundation. Retrieved from https://www.eff.org/wp/dangerous-terms-users-guide-eulas

unwanted marketing, particularly when the privacy protocols of said third parties is unknown or not disclosed to consumers.

VII. When writing information to a blockchain, include the minimum amount of attributable data necessary to properly record transactions and ensure the data is as difficult to analyze as possible by bad actors.[43] This addresses the following consumer protection challenges:

   f. Weak data protection protocols, which do not ensure data is as difficult to analyze as possible by bad actors, may leave consumers open to greater risk of fraud and theft.
   g. Information on open ledgers is public, which means that any private information put on a blockchain is accessible to anyone who maintains, accesses, or audits that ledger.
   h. Transactions on open and permissionless ledgers are traceable, therefore privacy is limited if identity can be linked to public keys.
   i. Information placed on or transactions made on blockchains are permanent, in that once the record is on a blockchain it becomes immutable and remains accessible to those who maintain, access, or audit that blockchain.
   j. Blockchain analysis will improve over time, increasing the likelihood of breaches or decryption of insufficiently protected data.

Additional resource on privacy: IDEF Core Documents. (2015, October 15). Retrieved from https://www.idesg.org/The-ID-Ecosystem/Identity-Ecosystem-Framework/IDEF-Core-Documents

3. USABILITY

Consumer Rights

Companies using blockchain-derived distributed technologies to run digital currency exchanges, hosted wallets, payment processors, DAOs, and digital asset investments or trades should bestow the following rights on consumers using their products:

VIII. Consumers have a right to user platforms with simple, well-designed user experiences and user interfaces (UX/UIs).

IX. Consumers have a right to reasonably brief and readily understandable information regarding disclosures related to platform terms and conditions, collection of PII, data sharing with third parties, and compliance with government requests information.

---

[43] There was some dissent among the authors on this principle regarding transparency, being a primary tenet of blockchain technologies.

X. Consumers have a right to interoperability among the various platforms that operate using blockchain technology as well as essential web-based platforms.

Consumer Protection Guiding Principles

Companies using blockchain-derived distributed technologies to run digital currency exchanges, hosted wallets, payment processors, DAOs, and digital asset investments or trades should employ the following guiding principles to ensure the above enumerated consumer rights:

VIII. Develop platforms with a simple, intuitive, well-designed user experience and user interface (UX/UI). This addresses the following consumer protection challenges:
   a. User interfaces are sometimes difficult to navigate. This can cause user confusion or limit the ability of users to execute various platform functions.
   b. Some Bitcoin and blockchain concepts are completely foreign to consumers, but are integral to the safe use of related products and services.

IX. Provide reasonably brief and readily understandable information regarding disclosures related to platform terms and conditions, collection of personally identifiable information, data sharing with third parties, and compliance with government requests information. This addresses the following consumer protection challenges:
   c. The lack of plain language and brevity (i.e. simple, pertinent executive summaries) in advanced disclosures may result in consumers overlooking, misunderstanding, and ultimately consenting to terms they might otherwise give more thought to or possibly not accept.[44]

X. Ensure interoperability among the various platforms that operate using blockchain technology as well as essential web-based platforms. This addresses the following consumer protection challenges:
   d. At the moment, consumers cannot readily participate in data or value exchange across related platforms, because many core technical components of blockchains are not readily interoperable with their Web counterparts, [45] including:
   e. The nature of distributed ledgers and chains requires that parties adopt common transaction and cryptographic formats in order for content structure innovation to progress.

---

[44] Newitz, A. (2005, February 17). Dangerous Terms: A User's Guide to EULAs. Electronic Frontier Foundation. Retrieved from https://www.eff.org/wp/dangerous-terms-users-guide-eulas

[45] Nichol, P. B. (2016, June 29). MIT hosts the W3C blockchain interoperability workshop. Retrieved from http://www.cio.com/article/3089459/consumer-electronics/mit-hosts-the-w3c-blockchain-interoperability-workshop.html

f. The development of future consumer blockchain applications may rely on interoperability among various systems, which are not being developed concurrently.

4. DISCLOSURE AND LIABILITY [46]

Consumer Rights

Companies using blockchain-derived distributed technologies to run digital currency exchanges, hosted wallets, payment processors, DAOs, and digital asset investments/trades should bestow the following rights on consumers using their products:

XI. Consumers have a right to complete, time-stamped disclosures regarding: legal entity status, applicable legal jurisdictions, institutional solvency, asset insurance, availability of funds or assets, privacy policy, timing of payments, receipts, loan/credit terms, and fees using concise, plain language
XII. Consumers have a right to access and transfer their funds or assets at any time.
XIII. Consumers have a right to timely and unencumbered transaction processing of payments falling below certain legal requirements for reporting or monitoring.
XIV. Consumers have a right to an audit of compliance with disclosure policies.

Consumer Protection Guiding Principles

Companies using blockchain-derived distributed technologies to run digital currency exchanges, hosted wallets, payment processors, DAOs, and digital asset investments/trades should employ the following best practices to execute the above enumerated consumer protection guiding principles.

XV. Disclose and maintain complete, time-stamped information regarding: legal entity status, applicable legal jurisdictions, institutional solvency, asset insurance, availability of funds or assets, privacy policy, timing of payments, receipts, loan/credit terms, and fees using concise, plain language. This addresses the following consumer protection challenges:
    a. **Legal entity status:** Given the rapid evolution of technology, consumers may not understand the legal incorporation status or type of entity they are engaging with. Such misunderstandings could materially harm consumers who

[46] Liability and protection might depend on the class of user:
A. Consumers: Sophisticated consumers vs. laypeople, "Average Joe" consumers
B. Investors: Accredited investors vs. institutional investors

believe they are guaranteed certain protections, when they actually aren't, due to liability restrictions associated with certain types of entities.

b. **Applicable legal jurisdiction:** Some legal jurisdictions have greater consumer protections than others.[47] Not knowing the legal jurisdiction of an entity could result in avoidable theft, loss, civil/criminal forfeiture, or other appropriation of consumer assets.
c. Institutional Solvency: When consumer entrust third parties with their assets they run the risk of theft or loss, including bank failures.
d. **Privacy Policy:** [48] Consumers may be susceptible to "pretexting" (the practice of obtaining personal information through false pretenses) by banks, credit card companies, and other financial institutions that may exploit their information for uses other than its intended purposes.
e. **Timing of Payments:** When the timing of payments is inconsistent or unclear, consumers face challenges regarding budgeting and availability uncertainty. These challenges can result in otherwise avoidable and burdensome overdraft fees, late payment fees, credit score penalties, etc.[49]
f. **Receipts (pre-payment disclosure, post-payment disclosure):** Without proof of payment or proof of transaction (including trade and investment activity), consumers are often unable to take legal action regarding goods and services purchased or trades and investments made.
g. **Loan/credit terms:** When consumers may be ill-informed about the lending terms of loans and consumer credit, they are susceptible to poor/unfavorable and sometimes exploitative loan terms as well as credit billing and credit card practices.
h. **Fees (ATM/Yearly/etc.):** Lack of knowledge regarding how fees can be incurred can leave consumers vulnerable to racking up fees, which can have materially damaging effects on the financial health of certain consumers.

XVI. Enable any-time access and transfer of consumer funds or assets, while taking care not to disable protections against fraud (such as withdrawal limit protections), within the boundaries of existing regulation. This addresses the following consumer protection challenges:
    i. Consumers can incur fees and encounter other problems when their funds or assets are not readily available, either due to limited banking hours or other barriers to access.

---

[47] The State of Consumer Protection Around the World. (2013, April). Consumers International. Retrieved from http://www.consumersinternational.org/media/1139641/english_full_report_april.pdf

[48] The Gramm-Leach-Bliley Act. (n.d.). Retrieved from https://epic.org/privacy/glba/

[49] See-To, E. (2006). *When do you pay? The business impact of payment time perception* (Working paper). Lancaster University Management School. Retrieved from http://eprints.lancs.ac.uk/48864/1/Document.pdf

XIII. Enable timely and unencumbered transaction processing of payments falling below certain legal requirements for reporting or monitoring. This addresses the following consumer protection challenges:

   j. Consumer funds are subject to a greater risk of fraud or double-spend when payments are not fully processed (i.e. completed) or available for use in a timely and unencumbered manner.

XIV. Regularly conduct and disclose detailed findings of audit of compliance with disclosure policies. This addresses the following consumer protection challenges:

   k. The lack of plain language and brevity (i.e. simple, pertinent executive summaries) in advanced disclosures may result in consumers overlooking, misunderstanding, and ultimately consenting to terms they might otherwise give more thought to or possibly not accept.

Appendix

RELEVANT STATE AND FEDERAL ACTIONS REGARDING DIGITAL CURRENCIES

Digital Currency Federal Advisories

CFPB	Risks to consumers posed by virtual currencies
CSBS	Model State Consumer and Investor Guidance on Virtual Currency
FTC	Consumer Information: Before paying with bitcoins...
North American Securities Administrators Association	Informed Investor Advisory: Virtual Currency
SEC	Investor Alert: Bitcoin and other Virtual-Currency Related Investments
SEC	Ponzi Schemes Using virtual Currencies
FINRA	Investor Alert: Bitcoin: More than a Bit Risky
Federal Reserve	Remarks on The Use of Distributed Ledger Technologies in Payment, Clearing, and Settlement

Digital Currency State Advisories

Alabama	Investor Alert - Use of Bitcoins are HIGH RISK with Minimal Protection for Consumers
California	What You Should Know About Virtual Currencies
Maryland	Virtual Currencies: Risks for buying, selling, transacting, and investing
Massachusetts	Consumer Alert: Buy Bitcoins at Your Own Risk
Michigan	Consumer advisory alleging virtual currency was "real-life risk" to investors
Texas	Texas Securities Commissioner Warns about Risks Associated with Investments Tied to Digital Currencies
Washington	Consumer/investor advisory on Bitcoin

Applicable Federal Consumer Protection Regulations

- Federal Trade Commission Act[50] – created the Federal Trade Commission (FTC) to prevent unfair competition, deceptive acts, regulate trade, etc.
- The Banking Secrecy Act (BSA)
- The Dodd-Frank Act[51] and the Commodities Exchange Act[52] (CEA)
- International Swaps and Derivatives Association (ISDA)
- Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies
- Title 17 of the Code of Federal Regulations[53]
- Commodity Futures Trading Commission (CFTC) rulings
- SEC Rulings
- Regulation 1.31 for recordkeeping rules
- Fair Credit Reporting Act (FCRA) – regulates the collection, dissemination, and use of consumer credit information[54]
- Fair Debt Collection Practices Act (FDCPA) – eliminates abusive consumer practices, ensure fairness, etc.[55]
- Truth in Lending Act (TILA) – requires clear disclosure of key terms of the lending arrangement and all costs.[56]

Applicable Non-federal Consumer Protection Regulations

Relevant section of the NY BitLicense[57]

- Disclosure of material risks
- Disclosure of general terms and conditions
- Disclosures of the terms of transactions
- Acknowledgement of disclosures
- Receipts
- Prevention of fraud

---

[50] Federal Trade Commission Act. Retrieved from https://www.ftc.gov/enforcement/statutes/federal-trade-commission-act

[51] H.R.4173 - 111th Congress (2009-2010): Dodd-Frank Wall Street Reform and Consumer Protection Act. Retrieved from https://www.congress.gov/bill/111th-congress/house-bill/4173

[52] Commodity Exchange Act. Retrieved from http://www.cftc.gov/LawRegulation/CommodityExchangeAct/index.htm

[53] 17 CFR - Commodity and Securities Exchanges. Retrieved from https://www.law.cornell.edu/cfr/text/17

[54] H.R. 15073. Retrieved from https://www.govtrack.us/congress/bills/91/hr15073/text

[55] Fair Debt Collection Practices Act. Retrieved from https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/fair-debt-collection-practices-act-text

[56] CFPB Laws and Regulations: Truth in Lending Act. Retrieved from http://files.consumerfinance.gov/f/201503_cfpb_truth-in-lending-act.pdf

[57] Final NYDFS BitLicense Regulations. Retrieved from http://www.dfs.ny.gov/legal/regulations/adoptions/dfsp200t.pdf

CSBS Model Framework[58]

- Required consumer protection policies and documentation of such policies
- Holding an actual amount of virtual currency in trust for customers and ensuring that amount is identifiable separately from any other customer or virtual currency business entity holdings
- Required policies and documentation of complaints and error resolution
- Required receipt to consumers with disclosures regarding exchange rates
- Required disclosures to consumers about risks that are particular to virtual currency
- Required disclosure of virtual currency insurance coverage, which at a minimum includes notice that virtual currency is not insured or otherwise guaranteed against loss by any governmental agency
- Public disclosure of licensing information and agency contact information

[58] Model Regulatory Framework . (2015, September 15). Retrieved from https://www.csbs.org/regulatory/ep/Pages/framework.aspx