Bitcoin: Our Best Tool for Privacy and Identity on the Internet

Peter Van Valkenburgh
March 3, 2015

Coin Center Report

COIN CENTER
coincenter.org

Peter Van Valkenburgh, *Bitcoin: Our Best Tool for Privacy and Identity on the Internet*, Coin Center Report, March 3, 2015, available at http://coincenter.org/2015/03/bitcoin-our-best-tool-for-privacy-and-identity.

Abstract

Financial privacy is an umbrella term for both data security and privacy. We can think of security as the ability to hide information from all comers and privacy, following Nissenbaum's concept of *contextual integrity,* as the ability to shape how we selectively reveal information and how it is used after revelation. Poor security and poor privacy have costs: identity theft, merchant compliance costs, chilling effects on speech, and cloaking costs from user self-help. Cryptocurrencies, such as Bitcoin, can be used to improve security and grant users more granular control over when and how they choose to identify themselves. We outline these potential benefits and describe how they can be achieved without hamstringing the investigatory powers of law enforcement or the goals of financial regulators.

Author

Peter Van Valkenburgh
Director of Research
Coin Center
peter@coincenter.org

About Coin Center

Coin Center is a non-profit research and advocacy center focused on the public policy issues facing cryptocurrency technologies such as Bitcoin. Our mission is to build a better understanding of these technologies and to promote a regulatory climate that preserves the freedom to innovate using blockchain technologies. We do this by producing and publishing policy research from respected academics and experts, educating policymakers and the media about blockchain technology, and by engaging in advocacy for sound public policy.

Bitcoin: Our Best Tool for Privacy and Identity on the Internet

Peter Van Valkenburgh

I. Introduction: Financial Privacy, Data Security, and Contextual Integrity

The umbrella term *financial privacy* can describe two related but distinct sub-topics that should be treated separately. The first is *data security* and the second is *privacy*. Data security, in the context of financial privacy, means ensuring that an individual maintains principal authority over the credentials that enable her to engage in financial activities. She may choose to share or store these credentials with her agents so that they can safeguard them or use them on her behalf and in her best interests. She should, however, always maintain the ultimate authority over these credentials and their use.

The second topic, privacy, is altogether more complex. It is best described by Helen Nissenbaum's concept of *contextual integrity*.[1] Contextual integrity refers to the ability of an individual to control what information is released and what information is kept private depending on the context of a given social interaction.

[1] Nissenbaum, Helen. "Privacy as contextual integrity." Wash. L. Rev. 79 (2004): 119. *Available at:* http://www.kentlaw.edu/faculty/rwarner/classes/internetlaw/2011/materials/nissenbaum_norms.pdf

Compare, for example, the information we'd want released to our dentist in advance of an appointment with the information we'd want released to our spouse in advance of a night out. These interactions have different contexts: medical and commercial vs. romantic and personal. Therefore, we cannot equate privacy with mere data security. Security simply means withholding some secret. Privacy means controlling to whom and in which situations we choose to reveal those secrets.

Without data security we would be unable to have privacy, no secret could be maintained regardless of context; security is necessary yet not sufficient to give us privacy. For that we need more nuanced control of the flow of information, and we need to understand the social context of particular interactions and the related institutions that govern those contexts.

To simplify, we can think of security as the ability to hide information from all comers and privacy as the ability to shape how we selectively reveal information and how it is used after revelation.

Cryptocurrencies, such as Bitcoin, are technologies that can strengthen both the security and privacy of its users relative to the users of traditional financial tools such as credit cards or bank accounts. Regulation is another tool for strengthening (and in some cases weakening) the security and privacy of individuals. Technology and regulation may work in tandem to create robust data security and privacy or they may work at cross purposes, such as when regulation generates unintended consequences that hamper the development of new privacy- and security-strengthening technologies, or when some other governmental goal, say crime prevention or *national* security, is privileged over an individual's privacy or security.

This report highlights the costs of poor security and poor privacy, and identifies how cryptocurrencies can strengthen financial data security and privacy as well as why regulations should be tailored to preserve the benefits of the technology.

II. Poor Data Security: Identity Theft and Fraud

As discussed in the introduction, financial data security is the ability of individuals to maintain principal control over the credentials that enable them to engage in financial activities. The technological breakthroughs of the 20th Century, particularly credit card networks, have eroded security in the name of countervailing virtues: speed, interoperability, universality, and ease-of-use. When security is the goal, by contrast, an ancient technology, cash, is king.

A simple way to conceptualize how cash is different than credit is to think *push* versus *pull*.[2] When a customer hands her grocer cash she is *pushing* value. When a customer hands her grocer a credit card, even if it feels just about the same, she is, instead, asking the grocer to *pull* value from her accounts. This pull is the beginning of a complicated, underappreciated

[2] *See See* Richard Gendal Brown, *How Are Payments with Bitcoin Different than Credit Cards? A Backgrounder for Policymakers*, Coin Center (Jan. 2015) *available at* http://coincenter.org/2015/01/payment-security/.

payment ballet, comprising many dancers and several acts. The grocer is pulling from a *merchant acquirer* (e.g. Bank of America Merchant Services), who is pulling from a *card network* (e.g. Visa), who, in turn, pulls from the *card issuer* (e.g. Bank of America), whose monthly bills ultimately pull value from the hungry customer in the grocery. Each pull is initiated by sharing the individual's credentials with the next party in the chain.

Each link in that chain will hold and often retain some of the customer's credential data, inflating the circle of trust and making her security increasingly porous. With cash, security is maintained by possession. Only the individual with possession of the bill has the ability to spend it. With credit, security is maintained by safeguarding the customer's credential data, which will necessarily pass through the hands of all parties to the pull transaction.

Should any of those parties, including the merchant and the merchant's employees and subcontractors, fail to maintain good cyber-hygiene, the customer could find that her private information now extends to a seedy black market, or even the entire public at large. From a purely technical standpoint, paying with a credit card is the same as handing your online banking password to a chain of four or more strangers, each of whom passes it along to the last link who logs-in to your account and transfers the funds. Security, therefore, demands trust in each of these agents to only pull as much of your balance as you've authorized and to keep the credential out of the hands of criminals and others who you've not authorized.

Recent data breaches at Target,[3] Home Depot,[4] and JP Morgan[5] exemplify the innate vulnerabilities of *pull*-based payment technology. At Target, consumer credit card credentials were stored on an internal server, but hackers did not initially infiltrate this server. Instead, they targeted a vulnerable server controlled by a heating and cooling company that Target used as a facilities services vendor. By granting some network access to this vendor, Target unknowingly and unintentionally extended the network of trust to which its customers belonged. Once the heating and cooling company was compromised, so was Target and so were all of their customers. With enough new and variable links in a chain, one is likely to be weak enough to unravel the whole.

The Target scandal has been costly. Target's own estimate is $148 million lost from this single breach.[6] Across the entire American economy, the losses from similar security breaches are profound. The Bureau of Justice Statistics estimates that identity theft cost Americans over $24.7 billion in 2012.[7] That's $10 billion more in losses than all other

[3] *See* Brian Krebs, "Target Hackers Broke in Via HVAC Company," *KrebsonSecurity* (Feb. 2015) http://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company/.
[4] *See* Robin Sidel, "Home Depot's 56 Million Card Breach Bigger Than Target's," *Wall Street Journal* (Sep. 2014) http://online.wsj.com/articles/home-depot-breach-bigger-than-targets-1411073571.
[5] *See* Elizabeth Weise, "Citi, E*Trade attacked by JPMorgan hackers, reports say," *USA Today* (Oct. 2014) http://www.usatoday.com/story/tech/2014/10/08/citigroup-etrade-jpmorgan-hackers/16923659/.
[6] http://www.nytimes.com/2014/08/06/business/target-puts-data-breach-costs-at-148-million.html
[7] *See* Bureau of Justice Statistics, *Data Collection: National Crime Victimization Survey (NCVS)* (2012) *available at* http://www.bjs.gov/index.cfm?ty=dcdetail&iid=245.

property crimes combined.[8] Eighty five percent of thefts involved the unauthorized use of existing financial accounts — a direct consequence of poor credential security. That year alone, 7.7 million people experienced the fraudulent use of a credit card and 7.5 million more experienced the fraudulent use of a debit card.[9] Some 34.2 million individuals, over 14% of the adult U.S. population, reported having suffered one or more incidents of identity theft in the past.[10]

Many incidents of fraud are cleared up relatively quickly by canceling the card, issuing a new card, and initiating a chargeback to return lost funds to the consumer. These chargebacks, however, leave merchants without payment for fraudulently purchased goods that have already been shipped and delivered; a careful con-artist will escape the ordeal wealthier and scot-free.

For some unlucky customers, identity theft can drag on. Once a consumer's credentials have fallen into the wrong hands, many fraudulent accounts can be created in her name. The result may be years of ruined credit ratings, financial losses, and—in roughly half of all cases extending beyond six months—severe emotional distress.[11]

A. Cryptocurrency Provides Improved Payment Security for Consumers

A cryptocurrency like Bitcoin provides a consumer the means to reliably and provably pay without the use of intermediaries. Recall that credit card payments necessarily involve sharing the payment credential with at least four other parties: the merchant, the merchant's card processor (merchant acquirer), the card network (e.g. Visa or Mastercard), and the card issuer (usually the customer's bank). With a Bitcoin payment, by contrast, none of these parties get access to the credential; the entire transaction can take place without the customer sharing her payment credential with anyone.

There is no credential-holding card issuer involved because the funds are controlled by a user's bitcoin wallet. This wallet is merely a piece of software, like a web browser, that runs on the user's phone or computer. It enables Bitcoin users to connect to the network and move their funds. Funds are "stored" as credits to one or more pseudonymous addresses on a public ledger, called the block chain, and the credential necessary to move funds out of those addresses, called a private key, is stored on the individual's smartphone, computer, or even a secret scrap of paper. At no point need a third party be trusted with custody of funds or the credentials necessary to access and spend those funds.

[8] *Id.*
[9] *Id.*
[10] *Id.*
[11] *Id.* (Severe emotional distress reported by 47% of victims who spent 6 months or more resolving financial and credit problems.)

There is no credential-holding credit card network because fund transfers, say from a customer's pseudonymous address to the merchant's pseudonymous address, are validated by the peer-to-peer Bitcoin network using cryptography. The customer can sign a transaction request with her credential, proving that she has authority to send the funds credited to her addresses, and she can do this without revealing the credential to the network. Think of it like owning a special rubber stamp to sign documents. Anyone can see that a stamp on a document is from you, but they cannot recreate the stamping tool in order to forge documents in your name. This technology is not new or unique to cryptocurrency, digital signatures form the basis of all trusted communication on the Internet.

There is no credential-holding merchant acquirer in the Bitcoin ecosystem because merchants can receive bitcoins simply by requesting that transfers be sent to a public address for which they hold the private key. There are companies, like Bitpay, that make it easier for a technologically unsophisticated merchant to accept cryptocurrency as payment.[12] These intermediaries, however, unlike merchant acquirers in the credit card space, do not need to take or retain any customer data that could be used by hackers or mischievous employees; they merely help the merchant set up their own Bitcoin addresses and wallets, and/or offer to automatically exchange customer Bitcoin payments into dollars.

The cryptocurrency user can, therefore, exercise greater control over her data security than she could with previous payment systems. Cryptocurrency eliminates the risk posed by entrusting intermediaries with sensitive financial information. With cryptocurrency the user's security does not depend on the robustness of anti-malware software on some remote server located on the property of a retailer she visited once long ago, or on the trustworthiness of the waiter who takes a her credit card out of sight to pay the tab.

Cryptocurrency is not, however, without its own security risks. The user herself and the user's own devices and online accounts can be compromised and stored cryptocurrency can be stolen.[13] This possibility creates some new dangers not present in previous payment systems. A credit card company would potentially refund amounts lost by the fraudulent charges of a hacker, but cryptocurrency is like cash in this regard: it will not be easily returned once stolen from a wallet.

There are two factors that mitigate this risk of loss. First, the user may choose only to hold and use small amounts of cryptocurrency at any time, much the way a cash user only keeps so many dollars in her wallet, while keeping the bulk of her holdings entrusted to a bank, which can insure her against loss.

Secondly, the risk of loss can be mitigated by employing security technologies native to cryptocurrency protocols. One of these technologies is called "multi-signature transactions" or multi-sig for short. Using multi-sig, a cryptocurrency user's wallet could place funds in a

[12] *See e.g.*, Bitpay, "Features," https://bitpay.com/features (last accessed Oct. 15, 2014).
[13] It's important to note that this is not a new vulnerability; online and mobile banking apps made end-user devices attractive targets for hackers long ago.

public address that has three controlling keys (hence multiple signatures) to enable transfer. The funds could be locked in that address until two of the three keys are turned.[14]

The user could retain two of these keys—one that she stores on her phone and another that she writes on a piece of paper and keeps in a safety deposit box—and the third key can be held by a trusted third party. This could be a loved one, or a private company that specializes in monitoring its customers' cryptocurrency accounts, ensuring that privately held bitcoins do not get hacked and fraudulently spent.

Whenever the user's phone initiates a transaction, the third-party can sign-off so long as it doesn't look fraudulent. If the phone initiated a transfer of all of the user's funds out of her wallet to an unknown account, however, this third party could decide to not sign off without some further contact with the user, or some good reason to believe that the phone had not been stolen or the user not manipulated into paying a known scammer.

The user, meanwhile, retains a backup key (possibly in a bank safe deposit box), in case the trusted third party ever disappears and stops signing-off on *any* transactions. At this point, the user could dig up her third key and move funds again, perhaps to a new multi-sig wallet with a better third party watchdog.

This tripartite security can be had without giving any custodial control of funds to the third party. Unlike existing escrow solutions, at no point in the transaction can the fraud protection service make-off with the funds; it has only one of three keys and at least two are required to request a transfer. The worst the service can do is disappear, at which point the user is forced to move her funds using the back-up key in addition to the key on her phone.

This solution combines the consumer protection benefits of legacy credit card payment systems the added security of cryptocurrencies. As with credit cards, there is fraud protection apart from user-self help, and transactions are easy to initiate, requiring only the single user credential stored on the phone. Unlike credit cards, however, security is vastly improved because at no point do third parties have access to financial credentials. Without sufficient keys to effect a transfer, the third parties' servers never become an attractive target for hackers seeking to steal bitcoins .

B. Cost from Poor Security: Compliance Costs for Merchants and Processors

Credit card technology was not set up from the start to preserve robust financial privacy in a global and interconnected world, so merchants and payment providers must spend time and resources ensuring that systems remain secure.

Firms may assume this obligation because consumers expect it, because private contract or government regulation require it, or because, as with chargebacks, the merchant will bear

[14] *See* Ben Davenport, *What is Multi-Sig, and What Can It Do? A Backgrounder for Policymakers*, Coin Center (Jan. 2015) *available at* http://coincenter.org/2015/01/payment-security/

much of the costs from a breach. Two quick examples from current financial industry practice illustrate these compliance costs:

First, chip and pin technology is being incorporated into the point of sale systems of many American retailers. Installation of these systems is costly—one hundred million dollars for Target stores alone.[15] Yet chip and pin systems would likely not have prevented the sort of financial privacy breaches suffered at Target or Home Depot[16] nor do these systems stop fraud and identity theft online.[17]

Second, as rates of online fraud surged in the 2000s, Visa and Mastercard began developing a technological anti-fraud solution for ecommerce known as the 3-D Secure protocol.[18] 3-D secure has been in development for years but many claim that it has yet to make any meaningful improvements to financial security for online purchases.[19]

It is surprising that in 2014 we still have no viable improvement to credit card payment systems developed in the 1960s, despite losing $30 billion to fraud in 2012 alone, and spending an unknown amount of capital year-after-year investing in security systems that have failed to bear fruit. Banks and credit card networks developed their infrastructure well before modern advances in communications, notably personal computing and the Internet. These early systems could be designed to place trust in many parties, and even to leak a tolerable amount of sensitive information, all without suffering large-scale costs from fraud or theft, because information was, on the whole, stickier and more difficult to share, send, or hack-into. Personal data would be stored on cards in locked cabinets, on computers that did not connect to a global network, or not stored at all because of the cost. Today, this sensitive data can be costlessly reproduced, shared, and spread. Every computer is networked and every device a potential target for cybercriminals at home or abroad. Unsurprisingly, attempts to protect sensitive data across so many trusted parties and without altering the underlying infrastructure have proven costly and ineffective.

C. Cryptocurrency Reduces Compliance Costs for Merchants

Cryptocurrency has the potential to slash the compliance costs of securing customer data by fundamentally changing the infrastructure. As discussed, cryptocurrency payments do not necessitate the storage, even temporary storage, of personal data on the servers of a merchant. This enables merchants to focus on providing valuable products rather than accumulating and securing a vulnerable database against hackers—an endless arms race.

---

[15] *See* Brian Krebs, "The Target Breach, By the Numbers," *KrebsonSecurity* (May 6, 2014) https://krebsonsecurity.com/2014/05/the-target-breach-by-the-numbers/.
[16] *Id.*
[17] Like CVV2 numbers, chip and pin systems are only an additional barrier to fraud when the cards are used in person—so that the physical "chip" can be scanned and its number checked against the consumer's memorized pin.
[18] *See* Steven J. Murdoch and Ross Anderson, "Verified by Visa and MasterCard SecureCode: or, How Not to Design Authentication", 6052 *Lecture Notes in Computer Science* 336 (Jan. 2010).
[19] *Id.*

A merchant accepting Bitcoin need only receive and keep coins sent by customers or have access to a service, such as BitPay, that will rapidly and automatically exchange payment in cryptocurrency for the local fiat currency. This allows payment networks to be global and interoperable without requiring any shared global database of user account information and private financial histories, beyond a pseudonymous ledger. In many ways it is the same as using cash.

Additionally, like cash, cryptocurrency payments can be irreversible. Once a merchant sees that cryptocurrency has been moved into her wallet, she can be assured that there will not be a subsequent chargeback due to fraud after her products have been shipped or handed over.

III. Poor Financial Privacy: Breaches of Contextual Integrity

Privacy cannot be defined simply as the retention of personal or intimate facts. There are many facts that we consider private that are not intimate per se, for example our bank balances or social security numbers. There are also many intimate facts that we are happy to reveal so long as the listener is someone we trust and the mood is right.

Helen Nissenbaum's concept of contextual integrity is a flexible definition of privacy. Defined as contextual integrity, privacy is not secrecy. It is control over the flow of information, control that can be fine-tuned based on the circumstances of a given interaction. This control has intuitive appeal; we frequently choose to withhold or reveal information about ourselves based on our moment to moment context. I would not casually tell my dentist the entirety of my web-browsing or video-rental history but I would give them my dental records. Nor would I hand my employer my medical history but they will need my social security number for tax purposes.[20]

This notion of privacy, however, is not well served by our existing financial or identification infrastructure. Unless we want to pay with cash, which necessarily precludes any purchase not made in person, we are required to offer our name, home address, credit card number, expiration date, and secret code (CVV2 number). Accordingly, the databases of our chosen merchants and financial services providers are comprehensive lists of our habits and routines. This despite the fact that all a retailer like Amazon really needs to know in order to sell me an e-book is that I have enough money to pay.

Ignoring context and assembling comprehensive databases of financial data has costs: individuals may forgo transactions (chilling effects) or take costly measures to obscure their identity (cloaking costs) in an effort to maintain contextual integrity, i.e. to avoid sharing all of their personal information indiscriminately. Additionally, the aggregation of information

[20] David Birch has worked diligently to articulate this gripe in the context of transactions. As Birch frames it: "What is needed to enable transactions is not identity per se but the associated entitlements." Not, "*I am John Doe"* but instead *"I am old enough to order this beer."* Birch calls this form of identification "pseudonyms with credentials." David Birch, *Identity is the New Money* (2014).

into centralized databases creates a "honeypot" that incentivizes criminals with the promise of a large reward (many IDs that can be sold together on a black market) from a single hack.

A. Chilling Effects

Privacy is fundamental to free speech, diversity, creativity, and democratic self-governance. [21] Intuitively, we modify our behavior whenever we know or fear that we are being observed. We abstain from some activities in which we'd otherwise engage or conform to modes of acting we'd otherwise eschew. Simply put, when we are observed we become culturally and intellectually homogenized; we go mainstream. This phenomena has been intuited by scholars and writers for centuries.[22] More recently—chilling effects have been observed empirically.[23]

Chilling effects are by no means benign or marginal. We lose more than a vibrant counterculture when a lack of privacy causes citizens to avoid associations or transactions that are not mainstream. Homogenization means less technological innovation, less scientific discovery, and fewer diverse voices in politics.

Nor does the law historically take a blind eye to these threats. As Supreme Court Justice William Douglas wrote:

> Where fundamental personal rights are involved—as is true when as here the Government gets large access to one's beliefs, ideas, politics, religion, cultural concerns, and the like—the Act should be 'narrowly drawn' to meet the precise evil.[24]

And the threat is particularly grave when financial privacy, specifically, is violated. Justice Douglas continues:

> In a sense a person is defined by the checks he writes. By examining them the agents get to know his doctors, lawyers, creditors, political allies, social connections, religious affiliation, educational interests, the papers and magazines he reads, and so on ad infinitum. . . . Bank accounts at times harbor criminal plans. . . . I am not yet ready to agree that America is so possessed with evil that we must level all constitutional barriers to give our civil authorities the tools to catch criminals.[25]

Privacy violations, in this context are, as suggested by Justice Douglas, not merely a matter of Fourth Amendment or Fifth Amendment constitutional concern; they also implicate our First Amendment rights to assemble and speak. Merchant data breaches may not threaten to

---

[21] *See* Neil M. Richards, "The Dangers of Surveillance," 126 Harv. L. Rev. 1934 (2013).
[22] *See e.g.*, Jeremy Bentham, *Panopticon* (1787); George Orwell, *Nineteen Eighty-Four* (1949).
[23] See Alex Marthews and Catherine Tucker, "Government Surveillance and Internet Search Behavior" (August 28, 2014) available at SSRN: http://ssrn.com/abstract=2412564; See generally Anthony Giddens, The Nation-State and Violence (1985).
[24] California Bankers Association v. Scultz, 416 U.S. 21 (1974) (Douglas, J., dissenting)(Citing Cantwell v. Connecticut, 310 U.S. 296, 307, 60 S.Ct. 900, 905, 84 L.Ed. 1213)
[25] *Id.*

reveal a full pattern of personal data; however, breaches at banks—as has recently occurred at JP Morgan Chase[26]—and state surveillance do put such intimate knowledge at risk.

B. Cloaking Costs

When a consumer is concerned with the visibility of her purchasing behavior or the security of her financial credentials, she may abstain from certain choices—chilling—or she may choose to cloak, rather than forgo, certain purchases. Cloaking may mean taking a cab across town to buy products in person from a physical merchant with cash, rather than over the Internet with credit. Such cloaking may also involve more sophisticated efforts; either way, it is a wasteful, non-productive exercise necessitated only by the poor default-state of financial privacy today.

Cloaking can be effectuated through the use of several exotic technological tools. Online product browsing can take place through encrypted browsers and routers—the TOR project.[27] Encrypted email or messaging tools—PGP—can be used to schedule in-person meetings between merchants and customers.[28] The final transaction can be made in person with untraceable cash or with barter. These arrangements are already available with existing open source tools and, notably, without cryptocurrency.

Law enforcement should not seek to quell these innovations. Cryptographic tools are tremendously valuable to an individual who fears ridicule, prejudice, or illegitimate persecution on the basis of the books she buys, newspapers she reads, or politicians she supports. Encryption is particularly indispensable to those living in repressive, totalitarian states, and such tools are a tremendous reason for hope that such coercive and intrusive regimes might one day be untenable.

Moreover, battling emergent, user-driven technologies is costly, ineffective, and likely to harm bystanders or legitimate users while leaving sophisticated criminals unscathed. These pitfalls are exemplified by recent attempts to stymie digital copyright piracy. Piracy was only made more appealing to users given industry resistance to legitimate markets for digital music files and streaming platforms. Similarly, regulations that hamstring and weaken the

---

[26] The JP Morgan breach is still being investigated, but it is already larger in terms of the number of customers exposed: 76 million households and seven million small-business accounts. Thus far it appears that the breach has resulted in some personally identifiable information being released: names, phone numbers, and addresses. *See* Elizabeth Weise, "Citi, E*Trade attacked by JPMorgan hackers, reports say," *USA Today* (Oct. 2014) http://www.usatoday.com/story/tech/2014/10/08/citigroup-etrade-jpmorgan-hackers/16923659/. The more frightening scenario is a breach at a bank that reveals customer social security numbers and complete transaction histories, records of every purchase made and every transfer sent by the consumer for the life of the account. This can be a deeply personal history, recounting legal relationships, medical expenses, reading habits, and other legal but sensitive activities.

[27] *See* The Tor Project, "Tor: Overview," https://www.torproject.org/about/overview.html.en (last accessed Oct. 15, 2014).

[28] *See* Philip Zimmermann, "Why I wrote PGP" https://www.philzimmermann.com/EN/essays/WhyIWrotePGP.html (last accessed Oct. 15, 2014)

privacy of mainstream financial tools may simply push more individuals into using exotic cloaking technologies. This is counter-productive for regulators, making it *more* difficult to identify suspicious behavior because even non-criminal users will have taken extreme steps to remain private.

This is also a bad outcome for law-abiding individuals: cloaking tools add a costly layer of complicated software and hardware to otherwise simple interactions. Ideally, regulators should seek to encourage the development of technological tools that robustly guard user privacy all the way up to the point when criminal investigations coupled with due process rightfully demand the revelation of private facts. The rule of law and privacy need not be irreconcilable.

C. Cryptocurrency Reduces Chilling Effects and Cloaking Costs

With cryptocurrency, there is no centralized institution that records every transaction under the name of a real person and address. Therefore, no single entity has the depth and fidelity of information regarding an individual's purchasing habits that an institution such as JP Morgan currently has regarding its customers. Already this shows great promise for mitigating chilling and cloaking costs. The user of a cryptocurrency can take technological steps to be sure that there is no single vulnerable database out in the financial cloud that could reveal a sensitive, personal medical condition, an embarrassing but legal habit, or support for a controversial political candidate.

While no single institution records all of the transactions of a cryptocurrency user under a real name, many cryptocurrencies, such as Bitcoin, are not entirely anonymous. Rather, they are *pseudonymous*: All of the transactions of a particular public address—a random string of numbers and letters—are visibly recorded on a public ledger.[29] The name or names of the people controlling that address are, however, unlisted. This provides law enforcement with a unique opportunity. For once, a set of transactions belonging to some discrete individual or group can be observed to be benign even without knowledge of or direct personal investigation of those persons. The full blockchain, a complete and public record of all cryptocurrency transactions, can be scoured by law enforcement technologists in order to flag only those transactions that appear suspicious because of their size, frequency, or interaction with known suspicious addresses. At that point, a warrant can be sought permitting the investigator to use tools that could de-anonymize only those public addresses involved in suspicious transactions.[30]

---

[29] Bitcoin transactions and the public addresses involved can all be viewed in real time at websites such as BlockChain.info, https://blockchain.info/.

[30] De-anonymizing Bitcoin transactions has proven easier than many initially expected. *See* Alex Biryukov, et al. "Deanonymisation of clients in Bitcoin P2P network," *eprint arXiv:1405.7418* (May 2014) *available at* http://arxiv.org/pdf/1405.7418v3.pdf; Elli Androulaki, et al. "Evaluating User Privacy in Bitcoin," 7859 *Financial Cryptography and Data Security Lecture Notes in Computer Science* 34 (2013); Philip Koshy, et al. An "Analysis of Anonymity in Bitcoin Using P2P Network Traffic" (Doctoral dissertation, Pennsylvania State

By automatically eliminating benign transactions from regulatory scrutiny *before* any costly attempt at de-anonymization, law enforcement can reduce its own enforcement costs by narrowing the field of suspect addresses in advance of real investigation. This will help law enforcement focus limited taxpayer resources on real threats. Simultaneously, innocent parties can be assured that their privacy is not being violated while their pseudonymous account's good name is cleared. This also stands in stark and beneficial contrast to the current financial ecosystem, where transaction visibility for law enforcement only comes at the expense of (a) an invasion into the privacy of many innocents and (b) the cybersecurity liability inherent in storing a wealth of personal data across many intermediary servers.

The usefulness of this public record to law enforcement may be why Bitcoin has proven less attractive to criminals than *centralized* digital currencies, which have closed books, such as the now defunct Liberty Reserve.[31] Edward Lowery, Special Agent for the United States Secret Service, testified before the Senate Committee on Homeland Security and Governmental Affairs Committee that "within what we see in our investigations, the online cybercriminals, the high-level international cybercriminals we are talking about, have not, by and large, gravitated towards the peer-to-peer crypto-currencies such as Bitcoin."[32]

At present there is reason to believe that the public ledger underlying Bitcoin transactions is, in fact, too prone to revealing the true identities of its pseudonymous users. The transaction graph can be observed and addresses that feed into and out of each other can be identified as all belonging to a single user. Should any of the inputs or outputs of those addresses be traced to a known identity—either an IP address, or a credit card used to purchase the coins on an exchange—the entire crypto-denominated financial history of the individual might be obtained.

One potential solution to this privacy vulnerability is the use of services that shuffle coins between many users, making it difficult or impossible to trace the coin to a prior address. These services pose obvious difficulties for law enforcement in situations where money laundering or other illegal activities are suspected. Some coin mixing services, however, should be tolerated. A cryptocurrency start-up might, for example, advertise itself as a legally-compliant anonymization service. Users will be told that their coins will be mixed, effectively granting them anonymity on the public block chain but that, additionally, a

---

University) (2013) *available at* http://ifca.ai/fc14/papers/fc14_submission_71.pdf; Sarah Meiklejohn, et al., A Fistful of Bitcoins: Characterizing Payments Among Men with No Names," *Proceedings of the 2013 conference on Internet measurement conference* (ACM, 2013) *available at* http://cseweb.ucsd.edu/~smeiklejohn/files/imc13.pdf.

[31] *See, e.g.*, Indictment of Arthur Budovsky, U.S. v. Liberty Reserve et al. *available at* http://www.justice.gov/usao/nys/pressreleases/September14/MaximChukharevPleaPR/Liberty%20Reserve,%20et%20al.%20Indictment%20-%20Redacted.pdf.

[32] Edward Lowery III, Testimony before the U.S. Senate Committee on Homeland Security & Governmental Affairs (November 18, 2013) *available at* http://www.hsgac.senate.gov/hearings/beyond-silk-road-potential-risks-threats-and-promises-of-virtual-currencies (Quote comes from question and answer session and was not, therefore in written testimony submitted by Lowery. The quote can be found in the video at 1:07:15).

confidential record will be kept that identifies their name and the input and output addresses from the mixing. The user and the service can contract to keep this record confidential except when presented with a valid warrant from law enforcement.

Law enforcement, in turn, can identify suspicious transactions, check whether these transactions involved addresses utilized in the legally-compliant mixing service, and, if so, seek a warrant and identification. Coin mixing services can compete to gain the trust of customers who fear privacy abuse from warrantless surveillance by publicly disclosing their responses to law enforcement requests, much as Google has sought to do with government requests for user-data.[33]

This is the sort of compromise that may inevitably leave both law enforcement and civil libertarians with a bad taste. With such a young and promising technology, however, it seems imprudent to insist that one extreme ideological perspective or the other—full anonymity or full surveillance—should dictate its development. Neither is likely attainable.

IV. Cryptocurrency, Contextual Integrity, and Identity

The most promising uses of cryptocurrency and block chain technology to enhance our privacy may be yet to come. The ideal of contextual integrity is a world where individuals can tailor what information they choose to share with which specific merchants or individuals. This necessarily entails *owning* one's information, a difficult proposition when data can be so easily reproduced even without authorization. Intellectual property law is, indeed, a poor solution to this problem of data ownership. The costs of a lawsuit against any and every infringing party often vastly outweigh the benefits to be gained from exclusive possession of data. Moreover, the sort of data we are discussing has less to do with artistic creativity, or a scientific invention and more to do with the mere certification of a certain right, entitlement, or identity.

A person seeking to drink at a bar need only prove that she is over 21 years of age, she shouldn't need to share her name, drivers license number, and home address to do so. A person seeking a credit card need only prove she has a positive credit rating from a reputable credit monitoring agency, she shouldn't need to give her social security number and birthdate to a stranger to do so. A person seeking to transfer large sums of money to an overseas address shouldn't need to share her intimate personal details, even if there is a slight risk that such a transaction might be financing terrorism, she should only need to show that she and the recipient have a clean criminal record and are upstanding citizens of some country or another.

[33] Craig Timberg and Cecilia Kang, "Google challenges U.S. gag order, citing First Amendment" *Washington Post* (June 18, 2013) http://www.washingtonpost.com/business/technology/google-challenges-us-gag-order-citing-first-amendment/2013/06/18/96835c72-d832-11e2-a9f2-42ee3912ae0e_story.html

At present each of these proofs of identity or proofs of entitlement is performed using a bevy of personal information that, especially when aggregated, can reveal any and all personal details. Even if this data is used for and only for the intended purpose, that information may be stored, sold, leaked, aggregated, misplaced, or hacked. Cryptocurrency and blockchain technology provides an alternative.

Individuals seeking to prove certain facts for the purposes of an entitlement can be granted a special form of digital property, a token of certification from a reputable third party. Control of these tokens is limited, using public key cryptography, to the holder of a secret key. By way of example, the token (when signed with the privacy key) could verifiably announce: *I am over 21, therefore I can legally drink*; *I have an 800+ credit score, therefore I am worthy of a line of credit*; *I am an American Citizen with a clean criminal record and so is my globetrotting cousin, therefore I should be able to send him money in Afghanistan with minimal scrutiny*.

Experian or Transunion can attest to your credit score and grant you a token that proves it. The Department of Motor Vehicles can give you a token that proves your age, and another that proves you've passed a driving test. The local police or even the FBI can give you a token that proves you've no criminal record. And the hospital where you were born can give you a token that proves your age, place of birth, and citizenship. These tokens can be digital assets assigned to a pseudonymous addresses on a public ledger (e.g. Bitcoin's block chain) and under the exclusive control of the individual who controls the private key linked to that public address. The holder of that key can be given software (effectively an advanced Bitcoin wallet) that would share any requested credential but withhold other personal identifiable information. Each use of the token can be visible to the party demanding it as a time-limited verification of the attested identity or entitlement, but also appear otherwise unique so as to avoid leaving a trail of activity that could be linked to the individual's name. The issuers of these certificates can put a name to a certificate that they have issued but they can also agree, under contract, to only do so if faced with a proper legal request for de-anonymization. Finally, if a certifying company's customer improperly lends her token to another individual (enabling this individual to make transactions for which she is not authorized), then the company can cancel the certificate and reveal their customer's identity to law enforcement.

Accordingly, an individual can present the bartender with a token proving she's old enough to legally drink but revealing no name or address. An individual using an online cryptocurrency bank to transfer a large sum of money to a foreign address can present her own citizenship token and the token of the recipient, as issued by their birth hospitals or by the U.S. Citizenship and Immigration Service, as well as the cryptographic coins she'd like sent. The service can record those certificates and send the funds forward. Should the FBI have probable cause to believe that the pseudonymous transaction they've just observed is linked to money laundering or the financing of terrorism they can seek a warrant from a judge. The warrant can be sent to the certificate issuer and if it checks out they can provide the name and address of the individuals involved in the transfer. Unless law enforcement has probable cause, however, this individual can have efficiently transacted anonymously in a

manner that should raise no eyebrows: someone with US citizenship sent money overseas to another citizen, we don't know who but that's none of our business anyway.

This may all sound like science fiction but the technologies capable of implementing such a system are already in development.[34] One way to look at Bitcoin is as a system that allows an otherwise anonymous individual to prove that they have a certain amount of funds without revealing any other personal details about themselves. The same technology could be leveraged to prove all sorts of attributes.

V. Conclusion

Policymakers should be aware that cryptocurrencies and block chain technology have this great potential to promote both security, privacy, and the rule of law. These tools already provide enhanced security for simple payment applications and they may, one day soon, offer robust privacy for the law abiding citizens without facilitating illegal activity amongst the less virtuous.

[34] This system is possible even with existing cryptocurrency infrastructure using the Bitcoin blockchain. A certifying company can create a Bitcoin address on behalf of a customer and sign an initial transaction with that addresses. The transaction could include an OP_RETURN value (an optional component to any Bitcoin transaction message) that interacts with wallet software that the certifying company provides the user. The OP_RETURN value could tell the customer's wallet what Identity values the wallet can sign-for with the FI as certificate validator.

For example, imagine a fictional company, Bitcoin ID Services (BIS). Alice hires BIS as her certifier. BIS creates a new Bitcoin address for alice, signs the initial transaction, and the OP_RETURN value could say (after decompression and translation so the text is human readable) "Alice's wallet is allowed to use this address to sign messages saying she is any of the following: *An american citizen*, *A bank customer in good standing*, *Over 21*, *Licensed to Drive*, *Has no criminal record*, *Has an american passport*, etc." Then when one of the people Alice transacts with needs ID for a given transaction, say a bartender, this merchant can ask Alice to use her certifying wallet to send an *IamOver21* certificate. The bartender can rely on the certificate or it can, recognizing the certifier, query BIS as to the certificate's continued authenticity or, in the case of serious and valuable transactions, demand some second identification factor like a biometrics test. Throughout this process, robust identification takes place—a person under 21 would not be able to sign—but Alice's privacy is protected—the bartender still does not know her name or where she lives.