



## Comments to the Consumer Financial Protection Bureau on Proposed Rules Relating to Prepaid Accounts

---

**Peter Van Valkenburgh**

**Submitted March 23, 2015**

In December, the Consumer Financial Protection Bureau published a proposed rulemaking relating to prepaid products that briefly noted that some of its requirements may apply to virtual currency products. This comment letter is focused on the proposed rule's potential applicability to virtual currencies. We thank the Bureau for considering it.

Coin Center is an independent 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.

We are not a trade association nor an industry group, and the comments that follow do not represent the views of any particular affected party. Our interest is helping the Bureau meet its public interest goals while ensuring that its policies do not inadvertently hamper the potential of blockchain innovation. We hope you find this submission useful.

### **Introduction**

In its recent Notice of Proposed Rulemaking, the Consumer Financial Protection Bureau ("the Bureau"), briefly suggested that the proposed expansion of the definition for "prepaid accounts" would potentially subject virtual currency products to regulation under the Electronic Fund Transfer Act (Regulation E).<sup>1</sup> While we do not disagree that meaningful steps can be taken to protect virtual currency consumers, we believe that the choice to regulate virtual currency firms as providers of prepaid accounts is premature. In Part 1 of this comment, we respectfully argue that the Bureau has yet to collect the data necessary to

---

<sup>1</sup> Consumer Financial Protection Bureau, CFPB Notice of Proposed Rulemaking, *Prepaid Accounts Under the Electronic Fund Transfer Act (Regulation E) and the Truth in Lending Act (Regulation Z)*, (December 23, 2015) available at <https://www.federalregister.gov/articles/2014/12/23/2014-27286/prepaid-accounts-under-the-electronic-fund-transfer-act-regulation-e-and-the-truth-in-lending-act>.

properly judge the costs and benefits of such a regulatory plan when it comes to virtual currency. In Part 2, we suggest that the nascent state of the virtual currency industry and a lack of widespread consumer adoption affords the Bureau time to conduct such a study. In Part 3, we suggest what particular aspects of the industry require study, owing to the unique risks and compliance costs associated with the technology. Finally, we conclude by suggesting that the Bureau adopt a formal exception from coverage in the proposed rulemaking, at least until further study of the industry and its underlying technologies has been made.

## **I. Procedural fairness in this rulemaking suggests that virtual currency products and services be studied further**

The Bureau has wisely taken a slow and methodical approach to the process of extending Regulations E and Z to prepaid products. This process has, in the Bureau's own words, "determine[d] current industry practices in a number of areas to inform [the Bureau's] understanding of the potential costs and benefits of extending various Regulation E provisions to prepaid accounts."<sup>2</sup> Respectfully, we argue that the Bureau has not, thus far, taken this same cautious and calculated approach in extending Regulation E to virtual currency products.

With respect to traditional prepaid products, the Bureau has made an Advanced Notice of Proposed Rulemaking, and solicited comments from the public or industry in relation to that proposal.<sup>3</sup> Nowhere in that advanced notice were virtual currencies or virtual currency businesses mentioned by name or by description of their general technology.

Similarly, the Bureau conducted an extensive study of the specific products it contemplated regulating under the proposed rulemaking, "in order to better understand existing compliance with Regulation E and other features and protections currently offered by prepaid products."<sup>4</sup> The Bureau looked at "publicly-available account agreements for prepaid products that appear to meet the Bureau's proposed definition of the term 'prepaid account.'"<sup>5</sup> This study looked at account agreements from 325 different prepaid programs including general purposes reloadable accounts, payroll cards, government benefit cards, "1 emergency relief card, 1 non-reloadable non-gift card, 1 government tax refund card, 1 student refund card, 2 insurance cards, 3 student financial aid disbursement cards, 5 prison release cards, 7 P2P programs, and 7 cards similarly used for other specific purposes." Not one of these diverse card programs utilized a virtual currency, and not one of these

---

<sup>2</sup> CFPB *supra* note 1, (Section III. Overview of Outreach and Related Industry and Consumer Research) available at <http://www.federalregister.gov/a/2014-27286/p-318>.

<sup>3</sup> Consumer Financial Protection Bureau, CFPB Advance Notice of Proposed Rulemaking, *Electronic Fund Transfers (Regulation E)*, (May 2012) available at [http://files.consumerfinance.gov/f/201205\\_cfpb\\_GPRcards\\_ANPR.pdf](http://files.consumerfinance.gov/f/201205_cfpb_GPRcards_ANPR.pdf).

<sup>4</sup> Consumer Financial Protection Bureau, *Study of prepaid account agreements*, (Nov 2012) available at [http://files.consumerfinance.gov/f/201411\\_cfpb\\_study-of-prepaid-account-agreements.pdf](http://files.consumerfinance.gov/f/201411_cfpb_study-of-prepaid-account-agreements.pdf).

<sup>5</sup> *Id.*

businesses would be understood to be a virtual currency business. Because of this omission it seems reasonable to conclude:

- A. that the Bureau has not formally collected data on user agreements in the virtual currency space despite the longstanding public availability of these agreements,<sup>6</sup> and
- B. that a virtual currency business would not have reason to be on notice of their potential involvement in the rulemaking because neither the ANPR nor the study of “prepaid products that appear to meet the Bureau's proposed definition of the term ‘prepaid account’”<sup>7</sup> made any mention of their businesses or products.

The Bureau has not collected the data necessary to judge the costs and benefits of regulating virtual currency as prepaid products. The Bureau also did not place virtual currency companies or the public on notice or seek their comments until its most recent Notice of Proposed Rulemaking, which was released a full two years into the ongoing process. We respectfully urge the Bureau to offer the virtual currency industry the same careful study and measured process that it offered the traditional prepaid industry.

The extension of the definition of prepaid products is likely to catch some innovative product developers off-guard. The Bureau has countenanced this fact with respect to some new technologies other than virtual currencies. It initiated a Call for Information regarding “mobile financial services” defined to include “mobile banking services” and “mobile financial management services.”<sup>7</sup> Again, no mention of virtual currencies was made in this call.

While it is true that some virtual currency products are available as mobile applications, no mention was made of these products in the call. Several virtual currency businesses offer no mobile product, choosing instead to offer desktop software or hardware. It is easy to imagine that had these companies been aware of the call, they would have believed it to be unrelated their sector of the industry. Moreover, while those virtual currency companies offering mobile products may have been remiss in failing to answer the call, it is perhaps forgivable given the reasonable presumption among industry participants that regulations would be developed specifically for virtual currencies rather than as part of a larger effort to regulate prepaid products. Regardless, this call did not generate for the Bureau any useful information regarding the impact that compliance with Regulation E would have on virtual currency businesses, nor did it put these businesses on notice of the rulemaking, as it did for producers of innovative mobile technologies.

At the conclusion of these many information gathering activities, the Bureau concluded “that objections about the burden of including various types of products within the ambit of this

---

<sup>6</sup> See e.g. Coinbase, *Coinbase User Agreement*, [https://www.coinbase.com/legal/user\\_agreement](https://www.coinbase.com/legal/user_agreement).

<sup>7</sup> Consumer Financial Protection Bureau, CFPB Notice and Request for Information, *Regarding the Use of Mobile Financial Services by Consumers and Its Potential for Improving the Financial Lives of Economically Vulnerable Consumers*, (Jun 2014) available at [http://files.consumerfinance.gov/f/201406\\_cfpb\\_request-for-information\\_mobile.pdf](http://files.consumerfinance.gov/f/201406_cfpb_request-for-information_mobile.pdf).

proposed rule are largely negated by the fact that a significant majority of these products are already substantially in compliance with existing Regulation E provisions.”<sup>8</sup> That conclusion, while surely reasonable with regard to the studied products, is premature with respect to virtual currency. That data hasn’t been solicited or collected. Therefore, objections from virtual currency businesses based on the burden of Regulation E compliance are not “negated,” and should not be dismissed out of hand.

The Bureau has announced that it is aware of this state of affairs, specifying that its “analysis of mobile financial products and services, as well as virtual currencies and related products and services, including the applicability of existing regulations and this proposed regulation to such products and services, is ongoing.”<sup>9</sup> However, the Bureau may be relying on the current proposal’s presumed non-application to these products as a cushion for these transitional industries: “the Bureau anticipates that this proposal, if effective today, would apply to relatively few mobile banking products (see, e.g., proposed comments 2(b)(3)(i)-4 and 2(b)(3)(i)-5 [referencing virtual currencies].”<sup>10</sup> We do not believe this general non-application can be reasonably anticipated from the words of the regulation. We therefore respectfully ask that the Bureau formally announce that the current proposal shall not be binding on virtual currency businesses until the Bureau’s “ongoing” analysis of virtual currency is complete.

## **II. The Bureau has ample time to study virtual currencies**

The traditional prepaid industry is massive and growing. Experts at Mastercard estimate that the market for prepaid will expand to \$822 Billion by 2017. The market for virtual currency products, on the other hand, is small. Bitcoin is, by an order of magnitude, the largest virtual currency in circulation, and yet, presently, the scale of the Bitcoin economy is miniscule by global standards. As of January 2015, Bitcoin’s total market capitalization is around \$2.5 Billion, less than the price tag of Santiago Calatrava’s new train station in Manhattan,<sup>11</sup> or a bit more than total US spending on cat litter in 2013.<sup>12</sup> Similarly, while Visa’s card network is designed to handle peak volumes of 47,000 transactions per second, Bitcoin’s design currently limits transaction volume to seven transactions per second. Our own survey of the

---

<sup>8</sup> CFPB *supra* note 1, (Section V. Section-by-Section Analysis of the Proposed Rule) *available at* <http://www.federalregister.gov/a/2014-27286/p-368>.

<sup>9</sup> CFPB *supra* note 1, (Section II. Background, Sub-section E. Other Payments-Related Bureau Actions) *available at* <http://www.federalregister.gov/a/2014-27286/p-316>.

<sup>10</sup> CFPB *supra* note 1, (Section V. Section-by-Section Analysis of the Proposed Rule, Scope of Proposed Definition and Application to Virtual Wallets and Virtual Currency Products) *available at* <http://www.federalregister.gov/a/2014-27286/p-431>.

<sup>11</sup> David Dunlap, *How Cost of Train Station at World Trade Center Swelled to \$4 Billion*, N.Y. Times (Dec. 2, 2014) *available at* <http://www.nytimes.com/2014/12/03/nyregion/the-4-billion-train-station-at-the-world-trade-center.html>.

<sup>12</sup> Euromonitor International, *Pet Care Market Place Update* (Sep. 2013) *available at* <http://www.pijaccanada.com/en/CommonDocs/Resources/Euromonitor%20Pet%20Care%2020>.

general American population reveals that over 65% of Americans have no idea what Bitcoin is, and that only 4.7% have ever tried using it.<sup>13</sup>

The Bureau has rightly decided to extend regulation E protections to the traditional prepaid space given consumer dependence on these products. As the Bureau reports, “[c]onsumers use prepaid cards for a variety of purposes, including making purchases, paying bills, and receiving payments. For those consumers without other transaction accounts, they may depend entirely on their prepaid cards to meet their payment account needs.”<sup>14</sup> This is in no way the case with virtual currencies at present. Indeed the only individuals depending entirely on Bitcoin are a handful of attention seeking journalists, and the results of these experiments in living on Bitcoin are unlikely to appeal to the typical consumer.<sup>15</sup>

Similarly, the Bureau is right to regulate traditional prepaid products given the risk of consumer confusion. As other commenters have pointed out, “consumers do not know that debit cards may have protections that prepaid products lack.”<sup>16</sup> This is particularly alarming given that, as the Bureau has said, “prepaid cards can be so similar to credit and debit cards (which are protected under Regulations Z and E).”<sup>17</sup>

The risk of similar consumer confusion with regard to virtual currencies is low. To date, there are no virtual currency plastic cards available in the US. Bitcoin products have, until very recently, been highly technical, and extremely difficult for the average customer to use. And more recently, user-friendly products have been careful to differentiate themselves from traditional products in the eyes of consumers. This is all in stark contrast to traditional prepaid services that bear the same labeling and form factor as a credit or debit product, and whose products can be a means of payment wherever Visa or Mastercard are accepted. Brick and mortar merchants accepting Bitcoin, on the otherhand, are still difficult to find even in cosmopolitan cities.<sup>18</sup> Online, there are more options, primarily thanks to Overstock.com and Dell Computer’s decision to take Bitcoin. These companies, however, remain outliers.

The Bureau has wisely chosen to adjust its regulations based on the risk of consumer confusion. Gift cards that enable purchases only with some group of affiliated merchants are exempted under the current rule because, “[w]hile consumers may mistakenly assume that protections that apply to debit cards also apply to general-use prepaid cards, they are

---

<sup>13</sup> Coin Center, *Coin Center Public Sentiment Survey*, (Feb 2015), available at <http://coincenter.org/survey/>.

<sup>14</sup> CFPB *supra* note 1, (Section V. Section-by-Section Analysis of the Proposed Rule) available at <http://www.federalregister.gov/a/2014-27286/p-376>.

<sup>15</sup> See e.g. Kashmir Hill, *Living On Bitcoin A Year Later: Will It Be Easier?*, Forbes (May 6, 2014) available at <http://www.forbes.com/sites/kashmirhill/2014/05/06/living-on-bitcoin-a-year-later-will-it-be-easier/> (“I lost 5 pounds and had to move out of my house, but I survived.”).

<sup>16</sup> CFPB *supra* note 1, (Section V. Section-by-Section Analysis of the Proposed Rule) available at <http://www.federalregister.gov/a/2014-27286/p-367>.

<sup>17</sup> *Id.*

<sup>18</sup> The directory site [coinmap.org](http://coinmap.org) lists only 14 businesses in Washington, DC, however even this number seems inflated given that it includes the IRS and business to business companies such as “Bitcoin Solutions LLC.” <http://coinmap.org/>.

unlikely to be similarly confused with respect to closed loop gift cards.”<sup>19</sup> We ask that a similar exemption be granted to virtual currency products at least until these products begin to gain the sort of mainstream adoption that could reasonably lead to consumer confusion.

### **III. Without more data it is unclear whether virtual currency would be best regulated under Regulation E**

The CFPB should be lauded for its data-driven approach to regulation. As described in the previous sections, the Bureau has shown abundant caution and care with respect to the consumer products it seeks to safeguard. With respect to virtual currency regulation, however, the data necessary to effectively regulate simply doesn’t yet exist.

#### **Classifying Virtual Currencies by Underlying Technologies and Risks**

The blanket phrase “virtual currency” can be taken to encompass a variety of distinct sub-group technologies, each with inherent and heterogeneous risk-profiles. It is as of yet unclear, however, whether any systematic attempt has been made by the Bureau to study the relative prevalence of consumer products in one sub-group or another. Nor is there available data on the inherent risks of one sub-group versus another. Nor has the Bureau sought to tailor regulations to aggressively protect against harms stemming from inherently risky sub-groups while avoiding the unnecessary application of compliance costs on inherently benign sub-groups. To illustrate this data-gap, one particular distinction—centralized virtual currency versus decentralized- or crypto-currencies—will be quickly investigated below.

#### **Centralized Virtual Currency versus Cryptocurrency**

Centralized virtual currencies are created and controlled by a singular authority, usually a business. For example, Amazon.com has created Amazon Coin to allow its users to buy digital content on its sites.<sup>20</sup> Such a business can create digital tokens and distribute or sell them to customers. They can peg the value of the currency by promising to redeem those tokens for a fixed amount of fiat currency or some item of value, or they can allow the value to float according to market supply and demand. As the Financial Action Task Force (FATF) has explained, “the vast majority of virtual currency payments transactions involve centralised virtual currencies. Examples [include] E-gold (defunct); Liberty Reserve dollars/euros (defunct); Second Life “Linden dollars”; PerfectMoney; WebMoney ‘WM units’; and World of Warcraft gold.”<sup>21</sup>

---

<sup>19</sup> CFPB *supra* note 1, (Section V. Section-by-Section Analysis of the Proposed Rule) *available at* <http://www.federalregister.gov/a/2014-27286/p-411>.

<sup>20</sup> See Amazon Inc., *Amazon Coins*, <http://www.amazon.com/gp/feature.html?docId=1001166401>; see also Wikipedia, *Amazon Coin*, [http://en.wikipedia.org/wiki/Amazon\\_Coin](http://en.wikipedia.org/wiki/Amazon_Coin).

<sup>21</sup> Financial Action Task Force, *Virtual Currencies: Key Definitions and Potential AML/CFT Risks*, (June 2014) *available at*

Decentralized currencies, by contrast, are created and maintained by an open community of interested participants using open source software. These participants run the software, or a compatible modification of the software, on Internet-connected computers that, together, form an open peer-to-peer network. Decentralized virtual currencies are also known as cryptocurrencies because all decentralized currencies, to date, have utilized theories and functions from the science of cryptography in order to guarantee both (A) that network participants cannot spend the currency held by other participants and (B) that the money supply grows at a predictable rate. Bitcoin, launched in 2009,<sup>22</sup> was the first cryptocurrency, and, as of 2015, it remains the largest by market capitalization.<sup>23</sup>

Even though cryptocurrency software is released and updated by an individual or group of individuals, e.g. Bitcoin's "Core Devs,"<sup>24</sup> these individuals cannot unilaterally change how the currency functions. To make any change to the currency, the updated software must be adopted by a majority of the peer-to-peer network. This network, composed as it will be of technologically sophisticated users, will audit the new code and likely reject any code that attempts to inject risk or fraud into the system.

The consumer protection implications of this distinction are not trivial: a business utilizing a centralized virtual currency can unilaterally decide to devalue consumer balances by issuing more currency, similar to how a normal financial service could choose to take on more debt. A cryptocurrency business is not at such liberty; it cannot unilaterally create more tokens because monetary supply is governed by an open, collaborative protocol of which they are only a small part.

A centralized virtual currency business can rearrange consumer balances, or refuse to honor a consumer credit, and it, ultimately, is the sole fiduciary of the currency's accounting records. A cryptocurrency business, even if it rearranges consumer balances once deposited, can only receive and dispense funds to a consumer by writing to an indelible and public accounting record, the public ledger or blockchain of the cryptocurrency. This ledger, unlike the closed, internal ledger of a centralized virtual currency business (or, for that matter, a traditional financial services business) can be publicly audited in real time to guarantee the solvency of the firm.

A centralized virtual currency business can operate using closed source software, meaning the underlying scarcity or safety of the currency cannot be easily audited by outside technologists. A cryptocurrency is open-source by default and the underlying fundamentals of that technology are scrutinized by a bevy of third-party validators.

---

<http://www.fatf-gafi.org/media/fatf/documents/reports/virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf>.

<sup>22</sup> See Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, (May 2009) available at <https://bitcoin.org/bitcoin.pdf>.

<sup>23</sup> See Market capitalization of top cryptocurrencies available at <http://coinmarketcap.com/>.

<sup>24</sup> See List of Bitcoin Core Developers available at <https://bitcoin.org/en/development>.

In short, even with only this first possible distinction—centralized versus decentralized—in mind, we can see that the consumer protection risks endemic to any particular virtual currency business can vary profoundly.

Regulations will affect how the virtual currency industry develops. Given that decentralized virtual currencies have some inbuilt consumer protections—owing to their open-source, decentralized, and transparent nature—it would be unfortunate if premature and indiscriminate regulatory action stifled the development of these technologies. To avoid this outcome, and to be certain that consumers are protected against technologies lacking in-built protections, the Bureau should take time to formally study the emerging virtual currency industry, its sub-groups, and the unique consumer risks of each sub-group.

### **Understanding the Unique Costs of Regulations for Virtual Currency Firms**

Aside from mere classification of risks, more data must be collected with regard to how the costs of compliance with Regulation E would affect virtual currency businesses. As a first cut, some aspects of the proposed rulemaking would have highly disparate effects on cryptocurrency firms as compared with traditional financial services providers or centralized virtual currency businesses.

For example, the proposal seeks to limit consumer liability for lost or stolen cards. While this is, no doubt, an important protection, it is harder to achieve for a cryptocurrency company. A traditional card company can often reverse fraudulent charges, i.e. initiate a chargeback. This arrangement forces the merchant who allowed a fraudulent card-swipe to bear some of the risk from fraud. A Bitcoin business, however, has no way to chargeback a merchant who has accepted the stolen bitcoins of one of its customers. Bitcoin transactions are not reversible by design. Once funds are moved into an account on the Bitcoin public ledger, only the holder of a private cryptographic key is allowed, by the protocol, to sign for transactions using funds assigned to that address. Therefore, the only way to recover lost or stolen funds is to find the private key of the Bitcoin address where the stolen funds now reside, effectively like trying to guess the password of a stranger.

A smart thief will have secured that key with the same precautions that a legitimate holder of the currency may take. The key could be on a scrap of paper in a safe-deposit box under the name of a friend. The key could be on a thumb-drive in a sock-drawer in Kyrgyzstan. Moreover, the thief may be moving the stolen funds across many addresses each with its own key that must be obtained in order to recover the loot. This transaction irreversibility means that a Bitcoin business will need to bear the risk of loss exclusively. While that outcome may be, in the eyes of the Bureau, desirable, the industry deserves an opportunity to explain how it would be affected by such costs.

Moreover, cryptocurrency technology may allow for alternative systems that could be implemented to prevent consumer losses altogether. These systems could prove superior to existing regulatory tools, such as those contemplated in this proposed rulemaking, and they could be mandated by regulators in the alternative to legacy regulatory approaches. So-called

multi-signature wallets or real time proof of reserves, discussed in the next two subsections, may enable these protections.

## Multi-Signature Wallets

Multi-signature wallets assign bitcoins to public addresses that are linked to multiple private keys, each separately stored, some majority of which are needed to effectuate any transfer. Think of it like the keys to a hypothetical safe deposit box at a bank: You have one key, your banker has the other, and both are required to open the box. Bitcoin addresses can be mathematically linked so that some number ( $M$ ) of the total linked keys ( $N$ ) are required to move funds out of an address. This is what is referred to as  $M$ -of- $N$  transactions<sup>25</sup> or, more simply, Multi-sig.

Using Multi-sig, control of consumer funds can be divided between many entities or end-user devices. For example keys can be divided between the consumer's mobile device, a fraud monitoring company, and a backup or insurance key-holder to hedge against the loss of the phone or the bankruptcy of the monitoring company. A majority of these companies or devices would need to sign off on any transaction made, putatively, on the consumer's behalf. Normally, the consumer signs for a transaction with the phone, and the fraud monitoring company, if the transaction looks normal, signs as well. With two of three parties agreeing, the transaction goes forward unimpeded. But if one key is compromised, either because the consumer's mobile phone has been stolen or hacked, or because the fraud-prevention service is no longer trustworthy, then that key alone is not sufficient to move funds.

One service that has already begun offering multi-sig wallets and transaction monitoring is BitGo. BitGo was recently chosen by the bitcoin exchange Bitstamp to help secure customer funds in light of a January 2015 hack.<sup>26</sup> BitGo's co-founder and Chief Product Officer describes how his company monitors a multi-sig wallet that they have created for a client and what motivates their decision to sign-off or refuse to sign-off on a requested transfer:

Before deciding to co-sign, BitGo applies security policy checks on the wallet, such as enforcing velocity limits, address target whitelists, IP restrictions, and so on. If the transaction passes the security checks, BitGo issues the second signature on the transaction using its key, and submits it to the network. If not, then BitGo may either reject the transaction, or hold it for additional approval from another administrator on the wallet. The final (backup) key does not come into play during normal operation. It is a cold-storage key which is for disaster recovery, and also allows the customer to retain ultimate custody of the bitcoin.<sup>27</sup>

---

<sup>25</sup> See Gavin Andresen, *BIP 0011*, (Oct. 2011)

<https://github.com/bitcoin/bips/blob/master/bip-0011.mediawiki>.

<sup>26</sup> See Bitstamp, *Bitstamp is open for business - Better than ever!*, (Jan. 2015)

<https://www.bitstamp.net/article/bitstamp-is-open-for-business-better-than-ever/>.

<sup>27</sup> Ben Davenport, *No Sleep till Multi-Sig*, Medium.com (Jan. 2015) available at

These technical aspects of the Bitcoin protocol may offer protections substantially more effective than those available to a holder of large sums of legacy cash or credit: multi-sig bitcoin holdings can't be spent unless an external security firm signs off or seeks additional confirmation from a customer. Rather than merely ensuring the customer against loss and leaving either the merchant or the financial intermediary liable for the theft. A multi-sig wallet could prevent many losses to fraud before they even happen.

### **Real-time Proof of Reserves**

Similarly, Bitcoin and cryptocurrency technologies can offer superior proof that intermediaries are solvent, that consumer funds are protected against loss, mismanagement, or the excessive fees of financial intermediaries. All cryptocurrency transactions take place on a public ledger, called the blockchain. A company could voluntarily, or if required by a regulator, provide real time records of consumer funds as they travel through the intermediary. These records could indicate, authoritatively, whether funds are remaining within the organization's publicly announced customer addresses on the public ledger and whether any fees are being deducted from those addresses.

Some virtual currency companies are already offering this form of real-time disclosure and proof of solvency. Bitreserve, for example, has developed an automated system of transparency that it hopes could even help stem future financial crises:

Bitreserve is the first financial service in the world to publish a real-time, verifiable, proof of solvency. Anyone at any time can confirm that the aggregate amount of value in our members' wallets is matched with assets in our full reserve.

Built for a post-trust world, Bitreserve's real-time transparency system eliminates the opportunities for fraud and destructive risk-taking that have caused the collapse of banks and other financial institutions throughout history.

We're setting this new standard of transparency, accountability and consumer protection with two features called the Reservechain™ and the Reservedledger™. The Reservechain enables anyone to trace a transaction all the way back to the point where it entered our network. The Reservedledger is a real-time publication of every change in our obligations to our members and every change in assets held in our reserve.<sup>28</sup>

The technology described by Bitreserve is not unique to this one company. Programmatic money that exists on a public ledger, as enabled by cryptocurrency generally, holds great promise in automating regulatory compliance. The Bureau's forward-thinking approach, and

---

<https://medium.com/@bendavenport/no-sleep-till-multi-sig-7db367998bc7>.

<sup>28</sup> Bitreserve HQ Inc., *Transparency*, <https://bitreserve.org/en/transparency>.

it's remit to guard against future financial crises, makes it the ideal regulator to seize and benefit from these new tools.

### **Gathering Information on these Regulatory Alternatives**

After the collection of data relevant to consumer protection in the virtual currency industry, the Bureau may find that some combination of mandated technological protections, such as multi-sig wallets or real-time proof of solvency, and existing protections, such as insurance, would better achieve the goal of consumer protection than can current approaches. We do not mean to suggest that all current Bitcoin businesses already use these consumer protective technologies. There is, undeniably, much fraud and crime. However, we want to stress that the Bureau has, at this moment, an opportunity to prevent consumer harms by *utilizing the novel options presented by the technology, rather than stymying their development*, but this can only happen if further study of the technology and communication with the industry takes place.

We respectfully ask that the Bureau take time to investigate these options for the good of both consumers and innovative virtual currency companies. Companies such as Bitgo and BitReserve, amongst a host of others, would surely relish the opportunity to work alongside the Bureau in a careful and deliberate regulatory process that seeks to utilize new tools and efficiencies. This course, we believe, would be preferable to a costly rush to regulate such promising technology with legacy tools and approaches.

### **Conclusion: We respectfully suggest an exception from this rulemaking for virtual currency products**

Given a need for procedural fairness to virtual currency companies, the need for meaningful and perhaps novel consumer protection strategies with regards to virtual currency technology, and the relatively slow rate of virtual currency adoption, we respectfully suggest that the Bureau formally exempt virtual currencies from the present rulemaking.

We recognize that the Bureau is concerned that “to try to carve out very specific types of products ... is complicated and could result in consumer confusion as to what protections might apply to otherwise indistinguishable products.”<sup>29</sup> However, as discussed, we do not believe that virtual currency products are marketed in a manner or at a scale that is likely to generate such consumer confusion. As public surveys have revealed, few Americans even know what Bitcoin is, let alone mistake it for a debit or credit card.

---

<sup>29</sup> CFPB *supra* note 1, (Section V. Section-by-Section Analysis of the Proposed Rule) *available at* <http://www.federalregister.gov/a/2014-27286/p-376>.