Profit-Driven Abuses of Virtual Currencies

Danny Yuxing Huang

Department of Computer Science and Engineering
University of California, San Diego
dhuang@cs.ucsd.edu

ABSTRACT

This paper traces the rise of virtual currencies and surveys their more popular incarnations, such Liberty Reserve and Bitcoin. Using cash and conventional electronic payment networks (e.g. Visa and PayPal) as a reference point, we delineate the evolution of financial abuses in the face of virtual currencies. In particular, we describe the properties of virtual currencies that make them susceptible to abuses. We also discuss how criminals can exploit virtual currencies for profit, and how these malicious activities can be countered. We find that the very benefits which have made virtual currencies popular are also facilitating crimes.

1. INTRODUCTION

Business transactions are increasingly carried out online. This renders hard cash almost obsolete and gives rise to electronic payment systems such as Visa and PayPal. Such payment networks provide a more efficient medium for the flow of money between merchants and buyers. Fundamentally, however, the money is still denominated in national currencies that are subject to government regulations. In war-torn regions or countries with incompetent governments, rampant inflation or fluctuations in exchange rates are a common sight. They disrupt both cash-based and electronic transactions. Furthermore, payment networks like Visa and PayPal may have to disclose transaction records under certain government regulations, thus compromising clients' privacy.

Given these problems, recent years have seen a growth of virtual currencies. In contrast to conventional e-payment networks, virtual currencies are decoupled from existing financial institutions. Still, virtual currencies often fit into economists' definition of money; they serve as "a medium of exchange," "a unit of account," and "a store of value" [26]. Issued by private entities, they often lack government regulations and claim to promote a greater level of privacy. In many ways, this facilitates everyday transactions. For instance, payments may be processed faster even across borders. Transaction fees may also be lower as the payment system is more efficient. These benefits, at the same time, encourage illicit activities—ranging from money laundering to selling contraband items—which are otherwise more difficult to accomplish in traditional payment networks.

In the short run, more people are likely to adopt virtual currencies for legitimate businesses. This paper, on the other hand, focuses on the other side of the story. We are interested in ways where miscreants can abuse virtual currencies for profit. Some of the attack models will be familiar to us, such as money laundering and theft. A virtual currency, after all, is money, which, no matter in what form, could be laundered or stolen. Using cash and conventional payment systems (e.g. Visa and PayPal) as a reference point, we describe how financial crimes have evolved vis-à-vis the rise of virtual currencies. In addition, virtual currencies present new paradigms for how transactions and businesses may be operated. These paradigms present attack models that are unique to the world of virtual currencies.

What is it special about virtual currencies—particularly in terms of technical aspects—that may be conducive to abuses? Will such malicious activities undermine the development of virtual currencies? Or will they be outweighed by the benefits that virtual currencies provide? What is the future for virtual currencies?

While this paper cannot provide a clear answer, we present evidence, based on existing literature and our own work, that addresses each of the question. In Section 2, we first trace the rise of virtual currencies. By surveying a list of popular virtual currencies, we hope to provide the reader with relevant background information for later discussions. Subsequently, we will describe how miscreants can abuse virtual currencies. We start with familiar attacks models in Section 3, while in Section 4 we describe exploitations that are unique to virtual currencies. Given these abuses, we discuss how they may be mitigated in Section 5.

This paper distinguishes the following terms:

- ❖ **Money**. We adhere to an abstract definition that economists generally agree upon: It is "a medium of exchange," "a unit of account," and "a store of value" [26, 11]. Examples range from bank notes (fiat currency), gold coins, cigarettes that were used to pay for services in prisons [23] (commodity currency), to Bitcoin [1] (virtual or digital currency).

[1]Following online conventions, we use "Bitcoin" to label the protocol and the currency, and "bitcoin" to describe the currency unit.

- ❖ **Cash**. This refers to physical bank notes traditionally issued by central banks.
- ❖ **Traditional e-payment networks**. These offer a digital medium that facilitates the flow of money—denominated in national currencies such as US Dollars—from one party to another. Examples include Visa, MasterCard, and PayPal.
- ❖ **Virtual currencies**. These are digital currencies issued and regulated by private entities. Governments or central banks are not involved. Virtual currencies have their own units of account or denominations (e.g. point systems). Transactions are usually conducted over the Internet—for instance, on websites or through peer-to-peer networks.

When we use the term "virtual currency", we refer to it as both a form of money and a digital payment system. In contrast to traditional e-payment networks, a virtual currency typically uses its own denominations, primarily operates online, and is more decoupled from financial institutions. We admit that this distinction can be blurry in many cases, and we will explore in greater detail in the next section.

Also, we use the term "crime" in the strictest sense; by definition, a crime is an illegal activity. However, virtual currencies are a relatively new phenomenon. Some malicious activities may be in legal gray areas, even though their intent is clearly to cause harm to others, or to exploit the system for personal gains. In this case, we refer to them as "exploitations" or "abuses." People behind such attacks are "miscreants," rather than "criminals."

2. BACKGROUND ON VIRTUAL CURRENCIES

This section provides an overview on virtual currencies. First, we start off from a historical perspective in Section 2.1, in which we propose possible causes for the rise of virtual currencies. Then we describe the main virtual currencies, which, depending on how the currency is operated, can be broken down into two categories: centralized and decentralized virtual currencies (Sections 2.2 and 2.3).

2.1 Rise of virtual currencies

Money has taken many forms. From barters to gold coins to banknotes, each new form is an innovation that attempted to address issues in the previous incarnation. People embraced conventional e-payment systems because physical cash was simply not conducive to the flow of money in an increasingly interconnected world. Similarly, the rise of virtual currencies can be largely attributed to problems with conventional e-payment networks, as listed below:

Distrust in financial institutions. Conventional e-payment networks essentially carry national currencies in digital forms. These currencies are regulated by central banks, whose ability to manipulate the monetary supply raises the eyebrows of many libertarians.[2] Some governments are unstable, corrupt or incapable, causing inflation to skyrocket particularly in war-torn regions. The recent financial crisis in Cyprus further fueled the people's distrust in traditional financial institutions.

Need for privacy. Conventional e-payment networks are often operated by a small number of large corporations, which have a global view of every single transaction. A government may examine private transaction records [7]. It may even bar e-payment networks from processing payments for certain political organizations. A recent example is WikiLeaks, a whistle-blower website against the US government. Following orders by the government, Visa and PayPal stopped processing donations to the non-profit organization [15]. To some people, the e-payment networks have made it easy for governments to spy on its citizens and infringe upon their civil rights, prompting many to switch to virtual currencies to avoid government tracking.

Similarly, conventional e-payment systems present a single choke point for criminal activities. Recent years have seen a surge in cyber crimes that are increasingly sophisticated. Examples include click fraud, spamming, and online pharmacies. Their operations involve highly specialized affiliates that span a number of countries. For years, they have been relying the conventional e-payment networks such as Visa to pay each other and to receive payments from buyers. Recent studies [25, 27, 18] have shown that, by informing Visa of such crimes, Visa can stop processing payments for these affiliate programs, effectively cutting their source of income and terminating their operations. In response, several criminal organizations, notably some online market place for illegal drugs, have switched to virtual currencies to avoid crackdowns [1, 2, 9].

2.2 Centralized currencies

Domain-specific currencies. Examples include in-game currencies like Linden Dollars for Second Life [11], and QQ Coins for the popular Chinese instant messenger QQ [14]. These currencies were designed mostly to facilitate the flow of wealth between accounts, circumventing transaction fees that are otherwise necessary in traditional e-payment networks. They are mostly restricted to trading virtual goods within the respective system. Their use outside of the virtual economy is limited.

Liberty Reserve. Operated by a company based in Costa Rica, Liberty Reserve was a virtual currency known for its anonymity. To register an account, a user needed to provide basic information such as his name and date of birth. These data were not verified against official identification documents or existing bank accounts. Liberty Reserve relied on third-party exchanges to facilitate the de-

[2]Most countries are off the gold standard these days. Their central banks can arbitrarily change the monetary supply based on practical needs. After all, these are fiat currencies, which are not backed by any commodities.

posit and withdrawal of money. These exchanges themselves were account-holders at Liberty Reserve. A typical depositor would give, say, US dollars to one such exchange. After deducting the transaction fees, the exchange would credit the appropriate amount, in Liberty Reserve currency units known as the LR, into the user's account. In this way, the user could trade with merchants, who would also accept LRs. Merchants who wished to withdraw LRs as US dollars would contact exchanges and follow a similar process. In May 2013, US federal prosecutors shut down Liberty Reserve [1].

WebMoney. Operated by a Russia-based company, WebMoney follows an operational model that is similar to Liberty Reserve. Money is stored as WebMoney Units. To deposit or withdraw money, a user goes through third-party exchanges known as Guarantors, who facilitate the conversion between WebMoney units and various national currencies. No bank accounts or credit cards are needed. Unlike Liberty Reserve, WebMoney does verify identification documents.[3]

2.3 Decentralized currencies

Centralized currencies have a major weakness: Users have to trust the operators. First, a single-entity operator has a relatively small attack surface. Any compromise to the system may jeopardize the entire payment network. A police takedown, for instance, would invalidate the wealth of all the users. Second, the operator himself may misbehave—for example running away with the money. To this end, another class of virtual currencies come into popularity. They do not depend on a central authority for operations. Instead, they rely on cryptographic primitives to establish trust across the peer-to-peer networks.

2.3.1 Bitcoin

First proposed by Satoshi Nakamoto in 2008, Bitcoin is a virtual currency whose value has increased by more than 200 times during the past five years. Its use ranges from coffee shops in San Francisco to Silk Road, formerly a online market place for illegal drugs. At its core, Bitcoin is a peer-to-peer network; each node, which runs the *bitcoind* client, is responsible for keeping track of transactions, issuing the currency, and regulating the money supply [30].

Transactions. Suppose Adam owns a bitcoin (denoted as 1 BTC) and he wants to send it to Betty. Also suppose Betty is new to Bitcoin. Like any other participants in the Bitcoin economy, Betty first needs to join the Bitcoin peer-to-peer network. Next, she generates a public-private key pair. Her public key, also known as her *wallet address*, will be used to send or receive bitcoins. To send his bitcoin, Adam first creates a transaction that is signed with his private key. This transaction authorizes a change in ownership of Adam's existing 1 BTC to Betty's public key. Adam's node subsequently broadcasts this transaction, so that the entire bitcoin network can learn that Betty is the new owner. Using her private key, Betty can now send her newly received 1 BTC to others and participate in the Bitcoin economy. Transactions are irreversible; Adam cannot revoke the 1 BTC that he has just sent to Alice.

The Bitcoin network records all transactions in an append-only ledger known as the *block chain*. It is a singly linked list of *blocks*, each of which contains a set of transactions. Once created, a block cannot be modified; all transactions contains are said to be *confirmed*. As new transactions are constantly broadcast across the network, new blocks have to be created, one after another, to keep track of these pending transactions. A new block always contains a reference to the previously created block—hence forming the block *chain*.

Given that the state of all transactions is distributed in a peer-to-peer network, the block chain must be secure and consistent. Malicious nodes cannot tamper with the transactions, and the entire network must agree on exactly one block chain. To meet both of these constraints, Bitcoin uses the proof-of-work mechanism. When a node is creating a block, it must also compute a double SHA-256 hash based on three values: the pending transactions, the previous block's hash, and a nonce value.[4] The result of this hash, a 256-bit integer known as the *block hash*, must be less than some integer T, also known as the *target*; otherwise, the node must choose a different nonce and repeat the entire process in a brute-force manner. Since SHA-256 basically returns a random integer, the probability of finding the solution is $\frac{T}{2^{256}}$.

A block is successfully created when a node finds the right nonce. Let it be the Nth block in the chain. Immediately, the node announces Block N to the Bitcoin network. Other nodes may also have been looking for the correct nonces for Block N. Upon hearing the block announcement, however, they stop the search because someone else has already found the solution. Every node subsequently append this newly broadcast block to their block chain, before starting another round of the block creation process for Block $N + 1$.

This proof-of-work mechanism offers security and consistency. The network sets T such that it takes, on average, ten minutes for somebody to find the nonce. A malicious node which hopes to tamper with the latest block must undo these ten-minutes of brute-force search, but even it were to do so, the other nodes would have found new blocks in the mean time. For a miscreants to succeed, he must muster more than 50% of the network's entire computational power. This, however, defeats the very purpose of cheating. The miscreant, with the majority of the computational power, would be more incentivized to abide by the protocol and generate more profit. As such, the security of the transaction record is guaranteed. Furthermore, this process allows the the entire network to reach a global consensus on the content of

[3] `http://www.wmtransfer.com/eng/about/index.shtml`

[4] Technically, miners need to find a 32-bit nonce value. Given today's computational power, the nonce space is rather small and quickly exhausted. An additional nonce, known as the *coinbase*, is used, which can have arbitrary length.

the block chain. Despite being on a peer-to-peer network, participants in the Bitcoin economy can trust the integrity of the system.

Issuance. The proof-of-work process is computationally intensive; it requires time and energy. Individual nodes are still incentivized to do so, because finding the right nonce results in a reward of 25 BTC. This reward is created out of thin air; it is how Bitcoin increases the money supply. The node which found the nonce is said to have *mined* 25 bitcoins or *mined* a block. Nodes that actively brute-force through the nonce space are known as *miners*.

Monetary policies. Bitcoin has a fixed money supply of 21 million bitcoins. At the time of writing, more than half of the total amount has been mined. When the network reaches the limit, miners are incentivized through transaction fees. Each transaction should include a small fee, or else they would risk not being confirmed into blocks. These fees will collectively go into the rewards for successful miners.

In a typical economy, an increase in money supply results in inflation. To avoid this problem, Bitcoin practices controlled deflation. Firstly, T is gradually lowered, as the total computational power (or *hash rate*) of the network increases. Even though mining hardware becomes more sophisticated and more people participate in mining, the net effect is that it still takes an average of ten minutes to mine a block. Secondly, the reward for mining halves for every 210,000 blocks. In about three years, only 12.5 BTC will be rewarded per block. In this way, the overall money supply in the Bitcoin economy slowly decreases over time.

2.3.2 Ripple

Like Bitcoin, Ripple is a cryptocurrency that is distributed across a peer-to-peer network. Transactions are irreversible, anyone can be a peer, and the global ledger is maintained across the peers.

Transactions are conducted through IOUs, which one can think of as the basic unit for transactions. An IOU can be in any national currencies or even in Ripple's internal currency. It is sent over trusted paths in the network. For example, Alice trusts Bob, and Bob trusts Carol. Suppose Alice owes Carol $1. There is no edge between Alice and Carol in the Ripple social graph, since they do not trust each other. Instead, Bob can act as the intermediary. Alice signs and sends a $1 IOU to Bob, who in turn signs and sends another $1 IOU to Carol. The total debt for Bob remains constant, while he is able to facilitate a transaction between Alice and Carol. In general, the Ripple network automatically finds a trusted path between any two individuals who wish to engage in transactions. If the IOUs involve the conversion of currencies, the Ripple network needs to find intermediaries who are willing to do the conversions—possibly through more intermediate currencies—at the lowest fees.[5]

Each new transaction, or issuance of IOUs, results in a change in the local ledger. Eventually, these changes must be committed to the global ledger, which is distributed across the Ripple peers. Consensus is reached through an iterative voting process. For instance, Carol's node proposes that an IOU of $1 to Carol be added to the global ledger. This proposition is broadcast to the network, and all the peers vote. This process is repeated until the number of votes for Carol reaches some dynamic threshold; it typically takes less than ten seconds. At this point, everyone includes the transaction into their ledgers, and the global state is consistent across the network.[6]

2.3.3 Chaum's Currency

Long pre-dating Bitcoin and Ripple, David Chaum, a cryptographer, created a theoretical currency[7] in 1982 for which transactions are untraceable [8]. Under this scheme, anyone can create a unit of the currency, which we shall call a Coin for the purpose of this discussion. Before it can be used in transactions, a Coin has to be signed by a trusted party. These trusted parties, which we shall call exchanges, maintain the ledger, but they have no knowledge how the Coin is spent or obtained.

Suppose that Alice is about to pay Bob a Coin, which is worth $1. First, Alice generates a Coin and encrypts it with her private encryption function. She takes the encrypted Coin to an exchange, which signs the encrypted Coin with its private key, returns it to Alice, and takes a $1 bill from Alice's wallet. Alice verifies the signed encrypted Coin with the exchange's public key. Satisfied, she strips away the encryption with her private decryption function. The Coin is now unencrypted but signed by the exchange. She pays Bob with the signed Coin. After verifying it, he takes the signed Coin to the original exchange. The exchange checks the signature, gives Bob a $1 bill, and marks the Coin as being spent in its internal ledger. Throughout this process, the exchange does not know where Alice spent her Coin, or where Bob obtained his Coin from.

2.4 Properties of virtual currencies

We summarize the properties of virtual currencies in Table 1. Virtual currencies are different from traditional e-payment networks in three main areas.

(a) **Relation with government**. Virtual currencies are mostly independent of conventional financial institutions. One does not need a proper bank account to register with WebMoney, Liberty Reserve or Bitcoin, for instance. Transactions are denominated in the currency's own unit of account. In particular, Bitcoin is not pegged to any national currencies. The value of a bitcoin floats against the US Dollar depending on the supply and demand. By contrast, traditional e-payment systems process transactions denominated in national currencies, whose values may vary significantly in an unstable economy.

[5] `https://ripple.com/ripple_primer.pdf`

[6] `https://ripple.com/wiki/Consensus`

[7] Based on the idea, Chaum later founded DigiCash, an electronic money company, in 1990, which went bankrupt eight years later.

Properties	*Traditional e-payments*	*Centralized VCs*	*Decentralized VCs*
Relation with government:			
❖ Decoupled from financial institutions	No	Yes	Yes
❖ Government-regulated	Yes	Maybe	Not yet
Properties of transactions:			
❖ Public	No	No	Yes
❖ Anonymous	No	Maybe	Likely
❖ Reversible	Yes	Likely	No
Properties of payment system			
❖ Logically centralized ledger	Yes	Yes	No
❖ Independent units of account	Unlikely	Likely	Likely

Table 1: Various properties of traditional e-payment systems, in comparison with centralized and decentralized virtual currencies.

As a mature industry, traditional e-payment systems are typically operated under strict government regulations. For large payment systems like Visa and PayPal, their offices are located in multiple countries. Should suspicious transactions occur in one country, another country may be able to intervene. Likewise, centralized virtual currencies are run by companies that are subject to the law, yet the level of enforcement remains questionable. For example, Liberty Reserve was operated by a shell company in Costa Rica, effectively evading government regulations [1]. WebMoney is operated in Russia, a country whose corruption ranking is amongst the highest in the world.[8] There were known cases of Russian cyber-criminals transferring funds with WebMoney, while the Russia authorities did not take actions. Eventually, the US government had to lure the criminals to the US for indictment [2].

By contrast, decentralized virtual currencies do not have an operator for whom to hold accountable. In the US, they mostly fall under legal gray areas, although the government is in the process of drafting relevant regulations [17].

(b) **Transactions**. In a decentralized currency, all the peers collectively maintain the global ledger that is distributed over the network. Every transaction is visible to every peer. Despite the transparency, linking transactions with specific users is difficult; a Bitcoin user, for instance, can create as many wallets as she wants at no additional cost. As such, transactions can remain mostly anonymous. By contrast, traditional e-payment systems and centralized virtual currencies store transaction records in logically centralized ledgers. Only the operator has a global view of all the transactions. An operator may compromise the privacy of sensitive transactions, especially when co-operation with law enforcement agencies is requested. An exception is Liberty Reserve. It does not store information about its users, whose authenticity is also questionable [1].

Disputable transactions can be revoked on traditional e-payment networks and for centralized currencies. Typically, there is a holding period after a purchase; for example, PayPal holds payments for up to 21 days in case of disputes.[9] The merchant receives the payment if the buyer is satisfied after some number of days. For a decentralized currency, reversible transactions are more difficult to implement. The protocol must take into account dishonest peers who may unilaterally roll back a transaction and carry out a double-spending attack. Moreover, even if a consensus algorithm for transaction revocation exists, transactions may be disputed due to subjective reasons. This often requires human intervention by a trusted authority, which is hard to find in a peer-to-peer network.

(c) **Payment system**. Both traditional e-payments and centralized virtual currencies require a central service that manages all transactions. On the other hand, users of decentralized virtual currencies process transactions on a peer-to-peer network, where the ledger is distributed.

Both centralized and decentralized virtual currencies typically hold money in their own accounting units. As in the case of Bitcoin and Liberty Reserve, a user needs to go through a third-party exchange to convert between the virtual currency and national currencies. For WebMoney and Ripple, the currency units mainly serve as a bridge between multiple national currencies. A user can easily convert the units into, say, US dollars and vice versa, directly within the virtual currency system itself. By contrast, traditional e-payment networks represent money in national currencies.

What, then, makes a virtual currency a *currency*, rather than a mere payment system? While the distinction can be murky at times, we propose two possible reasons. First, a virtual currency typically has few ties with governments or financial institutions. Second, such a libertarian impression is further reinforced by the use of a separate unit of account—Bitcoin, WebMoney Units, and LR, to name a few. These accounting units could be pegged to national currencies; a WMZ-type WebMoney unit, for instance, is equivalent to a

[8] `http://cpi.transparency.org/cpi2012/results/`

[9] `https://www.paypal.com/us/webapps/mpp/security/paypal-funds-availability`

US dollar.[10] Also, these accounting units could float freely depending on the market; the price of a bitcoin skyrocketed from $20 in February to more than $1,000 in November 2013.[11] Regardless, virtual currencies project a different image from conventional e-payment systems. They provide benefits in areas where traditional e-payments fall short. This gives rise to the increasing popularity of virtual currencies we see today.

3. CONVENTIONAL EXPLOITATIONS

Whether it is in the form of gold coins or bank notes, money is deeply ingrained in human society. Where there is money, there is greed; where there is greed, there are crimes. Virtual currencies, as a form of money, have not failed to breed malicious activities. A lot of such misdeeds are not new. Money laundering, for example, can be achieved via cash, conventional e-payment networks, as well as Liberty Reserve. The question is, however, whether virtual currencies have made such abuses easier to carry out and harder to catch. As we will discuss later in this section, the answer is not straightforward and very often depends upon the form of virtual currency used.

This section lists several malicious activities. For each, we present how they can be achieved in different virtual currencies, and whether the difficulty would change without virtual currencies.

3.1 Theft

Theft happens when the ownership is changed without consent. Depending on whether a currency is centralized or decentralized, we can broadly group money stealing into two categories.

For centralized currencies, a thief typically has to hack into the owner's account and transfer the money away. This approach works for the theft of QQ Coins and game currencies alike, where malware was implanted to compromise the victim's account [37, 20]. Similar malware can also be deployed to steal credentials of conventional e-payment accounts like PayPal.

Decentralized currencies, by comparison, lack the concept of centrally managed accounts, but there must be a mechanism that certifies ownership. For Bitcoin, the private key is required to send money. It is, by default, stored as an unencrypted "wallet file" on disk. Cyber-thieves have developed malware that scans for such files and emails them back [32, 13]. Once the ownership is changed to the public key of the thief, there is no way for the original owner to recover the money. One could opt for cloud-based wallets that store private keys in a purportedly safer manner, except that these services could either be hacked or could vanish with the money [3, 34].

The irreversible nature of transactions encourages the theft of decentralized currencies. By comparison, traditional e-payments and centralize virtual currencies impose holding periods for transactions. Any suspicious funds could be promptly returned to the original owner after an investigation by the central authority, as discussed in Section 2.4. This is simply not possible for Bitcoin or Ripple.

Fundamentally, the attack model is not new. Digital assets, no matter how secure in the back end, still need to be accessible to users that may not be as tech-savvy. Traditional authentication techniques—ones that are based on passwords or public-private keys—form the weakest link. Over the years, miscreants have developed a wide range of experience exploiting such authentication mechanisms. A centralized payment system operated by large companies has the financial and logistical means to secure their system, for instance, through phone verifications.[12] For a decentralized currency like Bitcoin, users may have to rely on their own judgment to protect themselves against thieves.

3.2 Money laundering

Conventional electronic transactions are traceable. Should suspicion arise, law enforcement agents may be able to examine one's bank account where the law applies. To wipe their digital trail of shady transactions—e.g. income from drug trafficking or payments to hitmen—criminals engage in money laundering. Typically, trusted intermediaries, known as mules, would withdraw cash from one bank account. This cash may end up in another bank or in a different account after possibly a few more intermediate steps [10]. Such complexities are needed, as banks are legally bound to cooperate with law enforcement agencies. Furthermore, banks are in full knowledge of one's transaction history. This leaves criminals very little room for privacy.

Virtual currencies offer a relatively safe haven for money launderers. For instance, Liberty Reserve does not even check the identities of account holders. Its exchanges are usually unlicensed money transmitting businesses in countries like Russia and Nigeria. These countries are typically corrupt,[13] or laws are not strongly enforced [2]. Moreover, a US-based company may not have any leverage in cases against these virtual currencies, who do not have an international presence [2]. As such, the currency is popular among cyber-criminals who engage in credit card thefts, underground gambling, drug-dealing, and so forth [1]. In a similar way, WebMoney is exploited for its privacy. Online counterfeit pharmaceuticals pay their advertisers in WebMoney [27]. One can also buy fake identification documents

[10] http://wiki.wmtransfer.com/projects/webmoney/wiki/WMZ

[11] https://blockchain.info/charts/market-price

[12] PayPal allows its users to authenticate using a physical security device, or through text messages. See https://www.paypal.com/us/cgi-bin?cmd=xpt/Marketing_CommandDriven/securitycenter/PayPalSecurityKey-outside&bn_r=o

[13] http://cpi.transparency.org/cpi2012/results/

using WebMoney [21]. To a large degree, both the buyers and the merchants are protected from police inquiries.

With the crackdown on Liberty Reserve, Bitcoin could become a popular option for dirty money [13]. The most notably example is Silk Road, an online market place for contraband items such as drugs and guns [9]. All transactions are in Bitcoin. Transactions go through a long chain of intermediate wallets—known as "tumblers" or "mixers"—that make them difficult to trace. However, such mixing services require Silk Road to temporarily hold funds. When FBI took down Silk Road, all such funds were confiscated, suffering the same fate as Liberty Reserve.

Virtual currencies are popular with dirty money because, unlike traditional e-payment systems, they are lightly regulated. Centralized currencies like WebMoney and Liberty Reserve can protect their clients, largely thanks to legal loopholes in the host country. Bitcoin, to some extent, masks user identities with disposable wallets. Anonymity is further enhanced by large mixing services. These services, however, can easily fall prey to government raids; like centralized currencies, Bitcoin mixers present a single choke point that may result in the loss of deposits. In brief, virtual currencies have made hiding money significantly easier than the money-mule days, but the risks are still considerable.

3.3 Market disruption

In a modern capitalist market, prices automatically adjust based on the supply and demand of goods. This "invisible hand" of market forces allows resources to be allocated efficiently. However, monopoly may disrupt such equilibrium and could cause prices to soar. To avoid such scenarios, many countries impose anti-trust laws that attempt to prevent big conglomerates from getting too powerful. In a similar way, trades are highly regulated in conventional money markets, leaving little room for individuals to disrupt the market.

Consensus in Bitcoin. In the absence of a centralized authority, peer-to-peer virtual currencies rely on consensus protocols to enforce fairness. For example, Bitcoin uses the proof-of-work puzzles. For a block chain that has $N-1$ existing blocks, the first node which finds a suitable nonce value decides the contents of Block N: what transactions to include, and what the previous block is. Everyone else must discard their own progress and instead accept the new Block N. In this way, as the announcement of Block N spreads across the peer-to-peer network, every node will eventually have a consistent view of the block chain.

Occasionally, the block chain could be *forked*. This could happen when two nodes have mined the Nth block a few seconds apart. Both blocks are unlikely to be the same, as the nonce value and the included transactions will be different between the two nodes. However, they share the same parent: Block $N-1$. Instead of being a linked list, the block chain now becomes a tree. This is undesirable, as a tree structure cannot impose a strict ordering for the transactions. To resolve this problem, the network randomly picks either block version. When a node mines Block $N+1$, it appends the block to whichever block chain it currently has, thereby forming the longer chain. Those that have a different version of Block N will switch to the longer chain instead, effectively discarding the transactions in their original Block N. The entire network finally agrees on a single block chain.

This example shows that consensus is achieved through the majority of the hashing power. Fast nodes get to decide the contents of the next block, or which branch of the block chain to switch to. This approach is more secure than majority-based consensus. Identities on the network can be easily created to become the majority, but there is no cheap way of generating massive computational power that can dominate the network and influence the decision-making process.

Pooled mining. Bitcoin's consensus protocol is on shakier grounds with the rise of *pooled mining*. In conventional bitcoin mining, each miner solves the proof-of-work puzzle on his own. If he finds a suitable nonce, he is rewarded with 25 BTC. In reality, however, either somebody else would find the nonce in the mean time, thus rendering the miner's effort useless, or it would take a long time—months or even years—to stumble upon the right nonce. Solo mining is thus a risky business. By contrast, pooled mining spreads out the risk and reduces the uncertainty of rewards.

Under this scheme, a mining pool combines the hashing power of a large number of member workers. The pool carves up the nonce space. Each worker effectively works on a small piece of the overall proof-of-work puzzle. With many workers solving the puzzle in parallel, finding the right nonce is significantly faster. When a pool mines a block, it divides the 25 BTC of reward among its members in proportion to the respective computational power. At the same time, the pool takes a small cut as the operation fee. Even if another mining pool has found the solution first, this mining pool still pays its participants. As a result, a worker's income remains relatively steady despite the uncertain nature of mining.

As more miners are incentivized to join mining pools, the burgeoning size of mining pools may pose threats to consensus on Bitcoin. At the time of writing, the entire Bitcoin network is solving 5×10^{15} hashes a second.[14] BTCGuild and 50BTC, two of the biggest mining pools, each contribute to more than a fifth of the total computational power.[15] If these conglomerates grow too big or too dishonest, the decision-making process of Bitcoin may be undermined.

51% attacks. Consensus, especially in the face of forking, is achieved through the majority of hashing capabilities. The protocol assumes that no single entities would possess half of the network's computational resources, yet this assumption may break as pools grow. A mining pool may have amassed more than 50% of the total hashing power, or a few large pools may collude to become the dominant

[14] `https://blockchain.info/stats`

[15] `http://btcguild.com` and `http://50btc.com`

player. When this happens, a cartel forms, which can make unilateral decisions only favorable to itself.

Such a cartel can give preference over a particular branch if the block chain is forked, forcing the other branch to be discarded. This is useful to the cartel, especially if the discarded branch contains transactions from rival merchants. This form of censorship will delay payment processing times for the affected merchants and even reduce their transaction volumes. The cartel can also favor a branch with higher transaction fees. Moreover, the discarded chain may contain double-spending transactions (See Section 4.1), either carried out by the cartel or its allies. The cartel's ability to dictate forked branches puts honest miners and merchants at an absolute disadvantage [22].

Selfish mining. A pool can inflict significant damage on the others even without becoming a cartel. It can adopt the *selfish mining* strategy [12], in which the malicious pool deliberately forks the block chain. Under normal circumstances, an honest pool would immediately announce any blocks it has mined. A selfish mining pool, by contrast, keeps the new block private. Effectively, the selfish pool has constructed a private block chain that is one block longer than the public chain. As it continues mining, any new block created will be appended to the private chain.

Meanwhile, the honest miners are also busy solving the proof-of-work puzzles. Suppose they mine a block, while the selfish miner is two blocks ahead. In this case, the selfish miner announces its private chain to the Bitcoin network. As it is the longer chain, the network has to accept it. The honest miners' chain is discarded. Having wasted their effort, the honest miners have lost one block worth of revenue.

Obviously, the selfish miner may not always be two blocks ahead, but it adheres to this general mining strategy. In the short run, it may lose money, especially when the private chain has the same length as the public chain, but the network picks the public chain. In the long run, however, the selfish pool can cause some serious financial damage to large pools, prompting their workers to switch over to the selfish pool. Eventually, the selfish pool may grow to a sufficient size for a 51% attack.

Summary. In practice, many of the attacks outlined above may have limited effects. The key assumption so far is that people are rational and will try their best to maximize their profit. This may not hold in the Bitcoin economy, where many participants are libertarians who champion a truly democratic currency. Cartels are fundamentally against such ideological principles. Miners may leave mining pools that are growing too big, even though these pools may promise higher mining revenue.

How effectively can ideologies protect Bitcoin remains questionable. For centralized payment systems like Visa or WebMoney, a central authority maintains the ledger and decides on the regulations. Bitcoin, by comparison, champions decentralization. As consistency is hard to achieve in a distributed system, Bitcoin achieves consensus by the majority of hashing powers. There would be no need to trust the government or any big corporations. The responsibility is collectively shouldered by the numerous miners, some of whom may be altruistic, and some of whom may be rational. In the long run, this could create uncertainty in the market.

4. UNCONVENTIONAL EXPLOITATIONS

As shown in the previous section, virtual currencies can breed malicious activities similar to what cash and traditional e-payment systems are capable of, albeit to varying degrees. This section, in contrast, focuses on abuses that are unique to virtual currencies. Certain benefits, such as the absence of a centralized authority, are what makes virtual currencies stand out from cash and traditional e-payments. However, these very qualities are attractive to miscreants and may undermine the virtual currencies. By describing two attack models, this section presents a cost-benefit analysis on virtual currencies. The bigger questions remain: Would the benefits of virtual currencies outweigh their potentials for exploitations? What is the future of virtual currencies?

4.1 Double spending

We all know that a dollar spent is a dollar gone. As the physical bank note leaves our wallet, there is no way for us to reuse it. With traditional e-payment networks, double-spending is equally hard, if not impossible. Every transaction is recorded at a centralized authority, which imposes strict consistency on the state of the transactions. In order words, the order of transactions as recorded in the database is exactly the order in which they occurred. No transactions can happen at the same time. This property can prevent any double-spending attacks.

Centralized virtual currencies, such as WebMoney, follow a similar consistency model. They are also immune to double-spending attacks. By comparison, decentralized currencies like Bitcoin distribute state across a peer-to-peer network. Although this has the benefit of increased privacy, the relatively weak consistency model facilitates double-spending attacks.

Recall, from Section 2.3.1, that a transaction can be thought of as an ownership transfer of bitcoins.[16] Before Adam can transfer 1 BTC to Betty, there must exist a block, somewhere in the block chain, confirming that Adam owns the 1 BTC, either because someone had transferred it to Adam, or because the bitcoin was created from mining. Suppose Adam creates a transaction, instructing the ownership be changed to Betty, who runs an online bookstore. This transaction remains pending until it is included—i.e. confirmed—in a block. At this point, Betty is confident that the 1 BTC belongs to her, since it is recorded in the block chain. Betty delivers the book to Adam.

Forked-chain attack. Occasionally, however, the block chain could be forked (Section 3.3). Adam's transfer, though

[16]This is a simplified view of how transactions work in Bitcoin. It is sufficient for our purpose in this paper. For details, see [30].

confirmed, may end up in a block that eventually gets discarded. The transfer to Betty is invalidated from the block chain, and Adam can legitimately spend the 1 BTC again, even though he has already received the book. This is the simplest kind of double-spending attack, but its success is contingent on the appearance of forked chains. It rarely happens. Even if it does, there is a 50% chance that the initial spending would be discarded by the block chain and could be subsequently reused. The opportunity costs to Adam would be too high.

To prevent this rare form of double-spending, Betty can wait for the transaction to be confirmed by more subsequent blocks [30]. If Adam's payment occurs in Block N, she will not deliver the book until the creation of Block $N + 2$ and possibly Block $N + 3$. Since each block takes an average of ten minutes to be created, Betty would have to wait more than 20 minutes. If the item is expensive, it is worth the wait given the risk. Most e-books are cheap, so Betty is more incentivized to offer fast payment processing without waiting for any confirmations.

Fast payment attack. Even in the absence of forking in the block chain, double-spending attacks are still possible if Betty offers fast payment processing [19]. Suppose Adam wishes to double-spend his 1 BTC, which he obtained by normal means. He creates two transactions: T_{AB}, which transfers the bitcoin from Adam to Betty, and T_{AE}, which transfers the *same* bitcoin from Adam to Eve, a co-conspirator. First, he initiates T_{AB} at time t_0. Adam's node broadcasts the transaction, and when Betty's node receives it, Betty thinks she is the new owner of the bitcoin. Because she does not wait for any confirmations, she delivers the goods to Adam. Next, at time $t_0 + \Delta t$, Adam initiates T_{AE}, which is also announced on the Bitcoin network.[17] If the attack is successful, only T_{AE} will be confirmed into a block, making Eve the legitimate owner instead of Betty. Eve can send the 1 BTC back to Adam, so he has effectively purchased the item for free.

For the attack to work, Adam must ensure that only T_{AE} gets confirmed. Right now, Betty's node broadcasts T_{AB} and Eve's node broadcasts T_{AE}. Half the network will receive either transaction, so only half of the time will the attack succeed. To increase the success probability, Adam employs *helper nodes*. These nodes are directly connected to Adam, but they are more than one hop away from Betty. The purpose of the helper nodes is to spread T_{AE} to a more diverse set of peers than Betty does, so that the majority of the network will hear about T_{AE}, thus increasing its likelihood of being confirmed by the next block.

The improved attack model works as follows. At t_0, Adam directly sends—rather than broadcasts—T_{AB} to Betty, who, in turn, broadcasts the transaction. The announcement of T_{AB} is thus limited to nodes that are reachable from Betty (except Adam). At $t_0 + \Delta t$, Adam directly sends T_{AE} to the helper nodes, which spread the announcement to their neighbors and beyond. When Δt is sufficiently small (e.g. no more than 1 second) and the number of helpers is sufficiently large (e.g. more than two), the attack is almost guaranteed to be a success [19].

Summary. Consistency and privacy are at a constant tug-of-war. Both are desirable qualities a payment system should have, but neither can co-exist. At one end of the spectrum, we have centralized systems, ranging from traditional e-payment networks such as Visa and PayPal to centralized currencies like WebMoney. A logically centralized database oversees all transactions and imposes strict orderings on them, making double-spending attacks almost impossible. Some users, however, may be uncomfortable with their accounts being run by such Big-Brother authorities. Governments may intervene, in the case of Visa and PayPal, or operators of WebMoney may run away with the money.

At the other end of the spectrum, we have peer-to-peer currencies like Bitcoin. Without any central authorities, the currency relies of proof-of-work puzzles to reach consensus across the network. Before a transaction is confirmed, Bitcoin does not guarantee its ordering. Exploiting this vulnerability, attackers can generate two concurrent transactions from the same bitcoin, tricking the victim of believing in one ordering, while notifying the network of the other ordering. The lack of a strict consistency model before transaction confirmations improves the performance of the peer-to-peer network, but it also facilitates double-spending attacks. Even after a block is confirmed, the global consensus will be disrupted if the block chain forks, giving another opportunity for double-spenders to strike. To this end, merchants will have to wait more than 10 minutes to process transactions. This ensures safety but introduces inconveniences that users of Visa or WebMoney would not otherwise experience.

4.2 Stealing computational power

In addition to stealing, criminals can typically acquire more cash through counterfeiting—or, literally, printing fake money. In the context of conventional e-payment networks, criminals could hack into the central databases and simply increase their balance. Given the high level of security these days, such acts are extremely difficult. For decentralized currencies like Bitcoin, everyone can print the currency out of nothing—i.e. mining—but he must invest significant energy and time to solve the proof-of-work puzzles. Arguably, a miscreant could simply counterfeit a bitcoin by making a fake transaction to himself. Without the proof-of-work, the transaction is bound to break the cryptographic constraints and be useless. Thus, it is impossible to counterfeit a bitcoin.

It is possible, however, for a miscreant to generate bitcoins without doing the proof-of-work himself: He can have an unsuspecting victim do it on his behalf. To achieve this goal, the miscreant can compromise a victim's computer and install a piece of mining software. The mining software connects to a mining pool using the miscreant's credentials. As

[17] Betty's node will also receive T_{AE}. Since the transaction comes after T_{AB}, Betty will consider T_{AE} as invalid and ignore it.

the software silently solves the proof-of-work puzzles in the background, the mining pool credits the miscreants for the work. Meanwhile, the victim suffers. As most of the CPU or GPU is constantly calculating the hashes, the victim host's productivity decreases, while the energy bill increases.

Effectively, the miscreant is stealing computational power for direct profit. This class of abuse is unique to Bitcoin or any crypto-currencies that rely on proof-of-work puzzles. While the proof-of-work paradigm brings integrity and consistency to the peer-to-peer payment system, it overlooks the *intent* of mining. Bitcoin assumes that the computers solving the puzzles belong to the wallet address that receives the well-deserved reward; in most cases, this is true. There is no mechanism in place that establishes intent—that the mining infrastructure is indeed willing to do the hard work for the given wallet address, and that the identity behind the wallet address is the same as (or related to) the one operating the mining hardware. Such a mechanism could be difficult to design and implement. It may present significant overhead to the Bitcoin network, making Bitcoin hard to deploy and manage. Furthermore, it may sacrifice anonymity, a central tenet of the currency. For simplicity and privacy reasons, Bitcoin does not associate mining hardware with recipient wallet addresses.

The trade-off is that Bitcoin is vulnerable to botnets. They already have a large number of compromised hosts at their disposal. When infected with bitcoin-mining malware, these hosts embody a massive profitability potential thanks to their collective computational powers. Because Bitcoin does not check the intent, these earnings are recognized as a part of Bitcoin economy [16].

Operation. For a botnet to start mining bitcoins, first it infects its hosts with bitcoin-mining software. These applications themselves are not malicious; they are mostly off-the-shelf mining software that honest miners use. Since the intent is to generate profit for the botnet at the cost of the victim, these applications are considered malware. Typically, each of the malware is configured to mine bitcoins for as long as the victim host is running. In order to receive steady payouts, the malware would do pooled-mining. The botnet would embed its credentials and the URL of the pool; the pool, in turn, would credit the botnet for the work done on the compromised computers.

Bitcoin-mining malware can connect to either a public or private mining pool. Examples of public mining pools include 50BTC and Eligius, where anyone could register an account and get paid in proportion to their hashing power. Mining on public pools is easiest to set up, but it is risky. If the malware is exposed, the botnet's credentials, along with the URL of the mining pool, may be made public. The pool operators *may* blacklist the botnet's account and invalidate any unpaid rewards.[18] To this end, botnets can set up their own private mining pools, where only botnets can participate in the pool mining. The risk of exposure is put to the minimum, yet botnets need to invest infrastructure that runs the mining pool servers, which should be capable of handling tens of thousands of connections. A middle-ground approach is for botnets to run light-weight proxies. Mining malware connects to the proxies, which in turn connect to public mining pools. This method reduces the cost of investment, while protecting the privacy of the operation.

Earnings. Our study has found at least nine bitcoin-mining botnets, which have earned more than 4,000 BTC to date [16]. This would amount to at least 1 million US dollars if the botnets were to cash out the bitcoins at the time of writing.

An example of such a botnet is ZeroAccess. Well-known for its large population, the botnet reportedly had at least a million hosts, according to Sohpos and Symantec [36, 31]. We have found close to 1,000 samples of bitcoin-mining malware that belongs to the botnet. The malware first connected to mining pool proxies and later to Eligius, a public mining pool that publishes all statistics about it workers. Using this data, we estimate that the botnet has received more than 450 BTC from malware mining.

The biggest earner in our study is the BMControl botnet. Its malware also connects Eligius, and their mining payouts are estimated to be more than 800 BTC. Interestingly, each malware binary does not contain the botnet's credentials. Instead, it visits a URL on PasteBin, a cloud-based file hosting service, and extracts the credentials from the encrypted page. This makes it hard to expose the mining credentials. It also facilitates the update of these credentials, should one of them become blacklisted.

Summary. Both examples illustrate the profitability of bitcoin-mining on botnets. Botnets are willing to go to great lengths and make their systems ever more sophisticated to avoid detection. In contrast to honest miners who invest heavily in hardware and electricity, the unit costs of botnet mining are low: for example, acquiring compromised machines, deploying the mining software and running mining pools. In this way, they were able to generate large numbers of bitcoins within only a few months. This abuse is made easy because Bitcoin champions anonymity; it does not link the identity of the miner with the identity of the recipient wallet, and it does not establish intent between the two. In many ways, the very property that helps the rise of Bitcoin is also undermining Bitcoin.

5. MITIGATION

The past two sections presented ways miscreants can abuse virtual currencies. To this end, this section discusses how they can be countered, from the perspectives of law enforcement agencies (Section 5.1) and of the virtual currency system itself (Section 5.2). Both approaches, in general, ap-

[18]Even if a pool is in clear knowledge of botnet mining activities, it may choose to ignore the botnet. First, the pool makes a cut from any form of mining. Second, we have evidence that botnets launched distributed denial-of-service attacks against pools that had blacklisted them.

ply to any financial crime, but we focus on how they are relevant within the context of virtual currencies, and whether there are particular challenges.

Furthermore, we argue that some virtual currency abuses may automatically die out. As discussed in Section 5.3, unfavorable economic conditions, led by the invisible hand of market forces, may raise the cost of abuse. The same conditions may result in the demise of the virtual currency. This may ultimately deter any long-term investment in malicious activities.

5.1 Legal

Abuses of virtual currencies often fall into legal gray areas; these make evidence gathering and formal indictment difficult. While it is beyond the scope of this paper to deliberate over various legal nuances (e.g. whether Bitcoin exchanges should be labeled as money transmitters), we stress the importance of de-anonymizing transactions as a tool for intelligence collection.

Anonymity is one of the reasons that miscreants have switched to virtual currencies, instead of traditional e-payment networks. De-anonymization is thus the key to curbing abuses. For Bitcoin, it is difficult, but feasible. Even though wallets are not explicitly linked to the identity of the owners, the currency is at best pseudo-anonymous. One way to identify wallets is to examine the transaction graph. A transaction may involve multiple source wallets and destination wallets.[19] For a transaction to be valid, the sender must have the private keys to all the source wallets. It follows that these source wallets are linked to the same person [33]. We group them in a single cluster.

By transitivity, if some of the wallets from this cluster appear as the source of another transaction, we can add the new source wallets to the same cluster. Instead of individual wallets, we now see bitcoins as moving from one cluster to another. Even if one wallet in a cluster is identified, we can identity all the wallets in a cluster.

To identify wallets, an undercover law enforcement agent must participate in transactions with the miscreants. He can, for instance, make purchases from Silk Road to identify a subset of the wallets used by the service. Similarly, the agent can cash out his bitcoins to label wallets of an exchange [28]. In this way, the agent can potentially trace how Silk Road sends its income to an exchange.

In response, miscreants have incentives to adopt more anonymous virtual currencies, including the recently proposed ZeroCoin [29]. Although it remains as a research project, this Bitcoin-based virtual currency may make it more difficult, if not impossible, to trace transactions and identify miscreants. Essentially, ZeroCoin implements a mixing service within Bitcoin. First, a user mints a ZeroCoin by paying for it with a bitcoin. The ZeroCoin contains a secret number, x, that only the user knows. To redeem it, the user creates a transaction with x, along with a zero-knowledge proof, stating that the user had previously posted a ZeroCoin with the secret number x. Because it is a zero-knowledge proof, anyone on the network can verify that the user did mint a ZeroCoin with x, and that the coin has not been spent. Nobody, however, knows exactly which ZeroCoin the user refers to. This allows the user's spending transactions to remain untraceable to anyone—including law enforcement officials.

[19] They are technically known as the input and output wallets respectively.

5.2 Securing the protocol

In a decentralized currency like Bitcoin, the security of the payment system depends on the developers, the buyers and the merchants. For instance, when a popular Bitcoin client update was released, a bug in the implementation caused new clients to mine on one block chain, and legacy clients to mine on the other. Effectively, the block chain was forked, presenting serious risks for double-spending attacks. As everyone scrambled to revert back to the legacy client, the development team quickly released a newer update the resolved the issue [5].

Double spending attacks can be reduced if merchants are willing to add observers in the network [19].[20] These nodes are distributed in different parts of the network and they notify the merchant of discrepancies in transactions. Instead of delivering the goods immediately upon hearing a payment transaction on its node, the merchant waits, usually for a few seconds, until all its observers agree upon the transaction. Although the merchant must invest in the observer infrastructure, this additional cost reduces the risk of fast payment processing.

Individual users who are afraid of wallet thefts can split their private keys using threshold cryptography techniques. These parts can be distributed on multiple locations, such as on smart phones, desktop computers, and even as print-outs to be stored in a safe.[21] An attacker needs to obtain some minimum threshold of the parts to succeed. This greatly reduces the risks of malware attacks [3].

5.3 Laissez-faire

In the end, Adam Smith may probably argue that any interventions would not be effective, and that we ought to let the "invisible hand" take its course. For some abuses of Bitcoin, such a laissez-faire approach may offer the ideal counter-measure.

5.3.1 Loss in profitability

Bitcoin-mining malware was a serious problem particularly in late 2012 and early 2013. Since, they have been on the wane. The most likely reason is that the profit margin is declining; it is getting exponentially more difficult to gener-

[20] The original authors used version 0.5.2 of the Bitcoin client. Some online forum posts claim that newer versions of the client have fixed the problem.

[21] `https://bitcoinarmory.com/about`

ate bitcoins. Using our own mining hardware, for example, we were able to generate 0.01 BTC every day in September 2013. Two months later, we could only mine the same amount every five days.

Such a drastic increase in difficulty is a result of the rising computational power of the network. Recall the Bitcoin target T from Section 2.3.1. It is an integer that Bitcoin automatically adjusts, so that on average it takes about ten minutes to generate a block, regardless of the network hash rate. As the number of miners increases and the mining hardware gets faster, the total computational power goes up. In response, T goes down, along with the probability of mining a block (i.e. $\frac{T}{2^{256}}$).

The increase in total hashing capability is chiefly attributed to more sophisticated mining hardware. Back in 2011 and 2012, people mostly mined on CPUs and GPUs. These devices were capable of computing 10 to 500 megahashes per second (MH/s). To stay ahead of the game, a few individuals developed custom FPGA boards that pushed the computation power into the giga-hash era. This was soon followed by the introduction of custom ASIC devices that could each do more than 100 GH/s [35]. Early adopters of new generations of mining hardware had to invest a hefty sum, but the investment quickly paid off as their hashing rates were disproportionately higher than the average miner. As the network as a whole caught up with the newer technology, everyone was on a level playing field again—until faster mining devices were released. Between March and November 2013, the total hashing rate increased by 150 times, from 30 TH/s to more than 4,000 TH/s.[22]

With the money supply staying relatively constant, an increase in network hashing rate means that the mining reward per unit hash rate diminishes. This puts bitcoin-mining botnets at a disadvantage. Suppose that a compromised PC (e.g. in Asia) costs 0.5 to 1 cent [6]. Further suppose that the victim PC has a relatively recent CPU model that can mine at 10 MH/s. At today's exchange rate, it is able to generate 0.5 cents per day, if the computer is powered on for 12 hours daily.[23] The malware binary has to remain undetected for at least a day for the botnet to make money. In reality, however, the average lifetime of such malware binaries is about 3 days, according to our experience. The hash rate can fluctuate wildly depending on the user's activity and the model of the compromised host. The prospects of earning a profit is slim, especially when the difficulty of mining a block exponentially increases.

As a result, mining botnets that were active in late 2012 and early 2013 are relatively dormant at the time of writing [16]. Based on the current trend, it is likely that bitcoin-mining on botnets will disappear in a few months. Even though the absence of identity checks had made malware mining easy at first, the lack of profitability will eventually put an end to these malicious activities.

[22] `https://blockchain.info/charts/hash-rate`

[23] We have found clear diurnal patterns for the hashing rates of botnets. This indicate that most of the compromised hosts are mining at most half of the time.

5.3.2 Deflationary spiral

Miscreants abuse Bitcoin only if it is profitable. With their dishonest bitcoins earned, the miscreants can either exchange them into a national currency, or invest the money within the Bitcoin economy—provided that the bitcoins remain valuable. Given the fixed money supply, it is possible that Bitcoin will go into a deflationary spiral, thus causing the value of the currency to plummet.

In the case of a national currency, the central bank can manipulate the money supply in response to economic conditions [4]. By contrast, the total number of bitcoins in circulation is capped at 21 million. As the Bitcoin economy booms, the value of the currency rises, creating greater incentives to horde rather to spend. This results in a vicious cycle, in which the amount of currency in circulation further decreases, prompting more people to save than to spend. With fewer purchases, prices of goods and services in the economy fall, leading to lower wages and further price decreases. The overall productivity of the Bitcoin economy decreases [15, 3].

Still, the possibility of a deflationary spiral remains debatable (e.g. [24]). With such a gloomy prospect looming ahead, a potential abuser may think twice before committing to any long-term investment in malicious activities. The independence from central banks and the deflationary monetary policies are what makes Bitcoin attractive in the first place. The same qualities, ironically, may curb exploitations in the economy and even lead to the demise of the currency.

6. CONCLUSION

This paper traces the rise of virtual currencies and discusses how they can be used for malicious activities. As with any technological innovations, virtual currencies are a double-edged sword. Oftentimes, the very qualities that made the virtual currency a success in the first place are exploited by miscreants. Given the benefits, virtual currencies will still be increasingly embraced, at least in the short-run. As virtual currencies continue to evolve, incentives will change. Some abuses may abate, while others may surge. The future of virtual currencies hinges on how the community can learn the problems of today and combat the challenges of tomorrow.

7. ACKNOWLEDGMENTS

This author wishes to thank Dr. Alex Snoeren and Dr. Kirill Levchenko for offering valuable suggestions at the beginning of the research exam. Their insight helped to shape the main arguments of this paper. This author is also grateful for their editorial advice as this paper was being written.

8. REFERENCES

[1] U.S. v. Liberty Reserve, et al. Indictment - Redacted. US Department of Justice, http://www.justice.gov/usao/nys/pressreleases/May13/LibertyReserveetalDocuments.php, May 2013.

[2] Andrew E. Kramer. In russia, hackers appear to be untouchable, *The New York Times*. http://query.nytimes.com/gst/fullpage.html?res=9803EFDB1439F937A1575BC0A9669D8B63, August 2010.

[3] Simon Barber, Xavier Boyen, Elaine Shi, and Ersin Uzun. *Financial Cryptography and Data Security, Lecture Notes in Computer Science Volume 7397*, chapter Bitter to Better — How to Make Bitcoin a Better Currency, pages 399–414. Springer, 2012.

[4] Board of Governors of the Federal Reserve System. What is the money supply? Is it important? http://www.federalreserve.gov/faqs/money_12845.htm, September 2013.

[5] Vitalik Buterin. Bitcoin network shaken by blockchain fork. *The Bitcoin Magazine*, http://bitcoinmagazine.com/3668/bitcoin-network-shaken-by-blockchain-fork/, March 2013.

[6] Juan Caballero, Chris Grier, Christian Kreibich, and Vern Paxson. Measuring pay-per-install: the commoditization of malware distribution. In *Proceedings of the 20th USENIX conference on Security*, SEC'11, pages 13–13, Berkeley, CA, USA, 2011. USENIX Association.

[7] Charlie Savage and Mark Mazzetti. C.I.A. collects global data on transfers of money, *The New York Times*, November 2013.

[8] David Chaum. Blind signatures for untraceable payments. In *Advances in Cryptology: Proceedings of CRYPTO '82*, pages 199–203. Plenum, 1982.

[9] Nicolas Christin. Traveling the Silk Road: a measurement analysis of a large anonymous online marketplace. In *Proceedings of the 22nd international conference on World Wide Web*, WWW '13, pages 213–224, Republic and Canton of Geneva, Switzerland, 2013. International World Wide Web Conferences Steering Committee.

[10] Matthew DeSantis, Chad Dougherty, and Mindi McDowell. Understanding and protecting yourself against money mule schemes. United States Computer Emergency Readiness Team, https://www.us-cert.gov/sites/default/files/publications/money_mules.pdf, 2011.

[11] European Central Bank. Virtual currency schemes. http://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf, October 2012.

[12] I. Eyal and E. G. Sirer. Majority is not Enough: Bitcoin Mining is Vulnerable. *ArXiv e-prints*, November 2013.

[13] FBI. Bitcoin virtual currency: Unique features present distinct challenges for deterring illicit activity, April 2012.

[14] Geoffrey A. Fowler and Juying Qin. QQ: China's New Coin of the Realm? *The Wall Street Journal*, http://online.wsj.com/news/articles/SB117519670114653518, March 2007.

[15] Reuben Grinberg. Bitcoin: An innovative alternative digital currency. Social Science Research Network, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1817857, December 2011.

[16] Danny Yuxing Huang, Hitesh Dharmdasani, Sarah Meiklejohn, Vacha Dave, Chris Grier, Damon McCoy, Stefan Savage, Alex C. Snoeren, Nicholas Weaver, and Kirill Levchenko. Botcoin: Monetizing stolen cycles. In *Proceedings of the Network and Distributed System Security Symposium (NDSS)*, 2014.

[17] Jeff Sommer. A bitcoin puzzle: Heads, it's excitement. tails, it's anxiety., *The New York Times*, November 2013.

[18] Chris Kanich, Nicholas Weavery, Damon McCoy, Tristan Halvorson, Christian Kreibichy, Kirill Levchenko, Vern Paxson, Geoffrey M. Voelker, and Stefan Savage. Show me the money: characterizing spam-advertised revenue. In *Proceedings of the 20th USENIX conference on Security*, SEC'11, Berkeley, CA, USA, 2011. USENIX Association.

[19] Ghassan O. Karame, Elli Androulaki, and Srdjan Capkun. Double-spending fast payments in bitcoin. In *Proceedings of the 2012 ACM conference on Computer and communications security*, CCS '12, pages 906–917, New York, NY, USA, 2012. ACM.

[20] Kaspersky Lab. "Winnti": More than just a game. http://www.securelist.com/en/downloads/vlpdfs/winnti-more-than-just-a-game-130410.pdf, April 2013.

[21] Brian Krebs. Reintroducing scanlab (a.k.a scamlab). http://krebsonsecurity.com/2010/12/reintroducing-scanlab-a-k-a-scamlab/, December 2010.

[22] Joshua A. Kroll, Ian C. Davey, and Edward W. Felten. The economics of bitcoin mining, or bitcoin in the presence of adversaries. In *The Twelfth Workshop on the Economics of Information Security*, 2013.

[23] S.E Lankenau. Smoke 'Em If You Got 'Em: Cigarette Black Markets in U.S. Prisons and Jails. In *The Prison Journal*, pages 142–161, 2001.

[24] Timothy B. Lee. Everything you need to know about the Bitcoin "bubble". The Washington Post, http://www.washingtonpost.com/blogs/the-switch/wp/2013/11/08/everything-

you-need-to-know-about-the-bitcoin-bubble/, November 2013.

[25] Kirill Levchenko, Andreas Pitsillidis, Neha Chachra, Brandon Enright, Tristan Halvorson, Chris Kanich, Christian Kreibich, He Liu, Damon McCoy, Nicholas Weaver, Vern Paxson, Geoffrey M. Voelker, and Stefan Savage. Click trajectories: End-to-end analysis of the spam value chain. In *IN PROC. IEEE SYMP. SECURITY and PRIVACY*, pages 431–446, 2011.

[26] N. Greogry Mankiw. *Macroeconomics (6th ed.)*, pages 22–32. New York: Worth Publishers, 2007.

[27] Damon McCoy, Andreas Pitsillidis, Grant Jordan, Nicholas Weaver, Christian Kreibich, Brian Krebs, Geoffrey M. Voelker, Stefan Savage, and Kirill Levchenko. Pharmaleaks: understanding the business of online pharmaceutical affiliate programs. In *Proceedings of the 21st USENIX conference on Security symposium*, Security'12, Berkeley, CA, USA, 2012. USENIX Association.

[28] Sarah Meiklejohn, Marjori Pomarole, Grant Jordan, Kirill Levchenko, Damon McCoy, Geoffrey M. Voelker, and Stefan Savage. A fistful of bitcoins: characterizing payments among men with no names. In *Proceedings of the 2013 conference on Internet measurement conference*, IMC '13, pages 127–140, New York, NY, USA, 2013. ACM.

[29] Ian Miers, Christina Garman, Matthew Green, and Aviel D. Rubin. Zerocoin: Anonymous distributed e-cash from bitcoin. In *Proceedings of the 2013 IEEE Symposium on Security and Privacy*, SP '13, pages 397–411, Washington, DC, USA, 2013. IEEE Computer Society.

[30] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system. May 2009.

[31] Alan Neville and Ross Gibb. Zeroaccess in depth. Technical report, Symantec, 2013.

[32] Kevin Poulsen. New malware steals your bitcoin. The Wired Magazine, http://www.wired.com/threatlevel/2011/06/bitcoin-malware/, June 2011.

[33] Fergal Reid and Martin Harrigan. *Security and Privacy in Social Networks*, chapter An Analysis of Anonymity in the Bitcoin System, pages 197–223. Springer, 2013.

[34] Kadhim Shubber. $4.1m goes missing as Chinese bitcoin trading platform GBL vanishes. Coindesk, http://www.coindesk.com/4-1m-goes-missing-chinese-bitcoin-trading-platform-gbl-vanishes/, November 2013.

[35] Michael Bedford Taylor. Bitcoin and the age of bespoke silicon. In *International Conference on Compilers, Architecture and Synthesis for Embedded Systems (CASES)*, 2013.

[36] James Wyke. The ZeroAccess Botnet - Mining and Fraud for Massive Financial Gain. Technical report, SophosLabs, 2012.

[37] Jianwei Zhuge, Thorsten Holz, Chengyu Song, Jinpeng Guo, Xinhui Han, and Wei Zou. *Managing Information Risk and the Economics of Security*, chapter Studying Malicious Websites and the Underground Economy on the Chinese Web, pages 225–244. Springer, 2009.