BITCOIN: Cryptography, Economics, and the Future

by

Starry Peng

Advisor: Nadia Heninger

EAS499 Senior Capstone Thesis

School of Engineering and Applied Science
University of Pennsylvania

December 10, 2013

1. INTRODUCTION

In today's world, the increased connectivity provided by the Internet has changed the nature of financial transactions. With recent developments in social media, peer-to-peer software, and smartphone technology, we have seen the definition of money extend beyond the traditional, physical tender of government-backed currencies to include mobile payments, digital currencies, and virtual goods [15]. Joining this revolution of payment technologies is Bitcoin, "the world's first completely decentralized digital currency", created by an unidentified programmer named Satoshi Nakamoto in 2008 [1].

What is unique about Bitcoin is its deregulated nature—it is neither controlled nor supervised by any commercial authority, government, or financial institution. Rather, a peer-to-peer network of users controls the creation and transfer of coins. Bitcoin's independence from 3rd party intermediaries provides its users a highly desired level of privacy and convenience. Since its inception in 2008, Bitcoin has gradually gained traction around the world. While its early adopters consisted mostly of technology enthusiasts, libertarians, and cryptography experts, Bitcoin has slowly entered the mainstream consciousness. As of December 10, a single Bitcoin is worth $918 US Dollars (USD).

In this paper, we explore the Bitcoin phenomenon on several facets. Section 2 will provide a detailed overview of how Bitcoin works and its underlying cryptographic protocols. Section 3 will contextualize Bitcoin by providing a history of digital currencies as well as a holistic landscape of different types of electronic currencies. In Section 4, we delve into the economics behind Bitcoin and discuss various vulnerabilities that may cause a collapse of confidence in Bitcoin. Finally, we address the regulatory and legal aspects of Bitcoin in Section 5. To conclude, we examine the philosophical underpinnings of Bitcoin and how they apply to Bitcoin's future outlook.

2. THE TECHNOLOGY BEHIND BITCOIN

2.1. Ideal Properties of Digital Currencies

As the Internet has become an integral part of our lives, the ecommerce revolution has transformed the way in which we interact and transact online. With it came a burgeoning interest in electronic payments and digital money. The concept of digital cash, however, has been around since the 1980s and has since accumulated a rich history. In our examination of electronic currencies, we first outline the ideal properties of digital cash [133]:

1. **Secure**. Digital payments systems should use high-quality encryption techniques to ensure a high-level of security, such that transactions cannot be forged or altered.

2. **Anonymous**. Transactions should be private and accessible only to the parties involved. The untraceability of transactions is an optional but desired property.

3. **Portable**. Digital cash should be independent of any physical location, and easily transferrable through the network.

4. **Two-way**. Digital payments should be peer-to-peer and occur between users (rather than a registered entity, such as a credit card company).

5. **Offline Capable**. Payments should be processed offline without requiring 3rd party authentication. Users should be able to spend and receive money anytime.

6. **Divisible.** Digital money should be fungible and divisible into smaller units of cash.

Additionally, it would be highly desirable for digital cash to be widely accepted and to exist in a user-friendly form [133].

Most importantly, the digital transaction space is particularly vulnerable to the "double spending" problem. Because electronic files can easily be duplicated, a digital coin can simultaneously be spent and retained in one's computer files, allowing that coin to be effectively spent twice [4]. Up until now, electronic payments have required a trusted 3rd party intermediary—such as PayPal or Visa—to verify the intent and authenticity of transactions. Bitcoin is "revolutionary because for the first time the double spending problem can be solved without the need for a third party" [1]. To understand how Bitcoin accomplishes this, we must first understand aspects of public key cryptography, digital signatures, and hash functions.

2.2. Public Key Cryptography

In 1976 Diffie and Hellman introduced the concept of public key cryptography, in which a user has both a public and private key. The receiver of the message publicizes her public key, which can be used by anyone who wishes to send her a message. The sender simply uses the public key to encrypt his message into ciphertext, and the receiver uses her private key to decrypt the ciphertext into the original message. Under this scheme, the sender and receiver do not need to establish a secret communication channel in advance. "The secrecy of the encrypted message is preserved even when an attacker knows the encryption key" [3], as long as the receiver keeps her private decryption key secret. This asymmetric cryptography scheme introduced by Diffie and Hellman was especially suitable for security applications on open systems like the Internet, in which the sender and receiver may not already know each other or have had the chance to establish a private communication channel. This scheme relies on the fact that encryption is easy but reversing it via decryption is computationally infeasible for anyone other than the intended receiver. The first implementation of Diffie and Hellman's theoretic construct was the RSA public key cryptosystem, devised by Ronald Rivest et al. in 1977. For the full RSA algorithm, please refer to [119].

2.3. Digital Signatures

Encryption and decryption ensures privacy by preventing adversaries from accessing the message sent from sender to receiver. Message authentication, however, must also be used in conjunction with public key encryption. Digital signatures are a popular mechanism for message authentication, and have three desirable properties: it allows the receiver to validate that the correct sender did in fact create the message (authentication), that the sender cannot deny having sent the message (non-repudiation), and that the message was not modified in any way by an adversary (integrity) [3]. To achieve this, the sender computes a digital signature using his private key and sends his "signed" message to the receiver. As long as the receiver knows the sender's public key, she can use a verification algorithm to determine if the message was signed by the original owner and not tampered in any way. Digital signatures are widely used in electronic transactions because the authenticity of the message can be verified by anyone who has the sender's public key. Another advantage is that digital signatures are publicly verifiable—that is, if the receiver verifies a given message's signature as legitimate, then all other parties (such as a trusted 3rd party intermediary) who receive the same message should also validate it as authentic [3].

Specifically, the Bitcoin protocol uses the Elliptic Curve Digital Signature Algorithm (ECDSA), a variant of the Digital Signature Algorithm (DSA). A group is an abstract mathematical entity "consisting of a set G together with an operation * defined on pairs of elements of G" [120]. The operation * must guarantee the following four properties [120]:

1. **Closure.** $a * b \ \in G$ for all $a, b, \in G$
2. **Associativity.** $a * (b * c) = (a * b) * c$ for all $a, b, c \in G$
3. **Existence of Identity.** $e * a = a * e = a$ for all $a \in G$ where $e \in G$ is the identity
4. **Existence of Inverses.** $\forall\ a \in G,\ \exists\ b \in G$ such that $a * b = b * a = e$ and b is denoted as a^{-1}

The security of the Digital Signature Algorithm is "based on the intractability of the discrete logarithm problem in prime-order subgroups of $\mathbb{Z}_p^*$" [121]. The following problem defines the integer x as the discrete logarithm of h to base g:

> Given $g \in \mathbb{Z}_p^*$ of order n and given $h \in \mathbb{Z}_p^*$, find an integer $x,\ 0 \leq x \leq n-1$ (if it exists), such that $g^x \equiv h \pmod{p}$ [120]

This problem is extended to arbitrary groups in the DSA, in which G is a group of order n (where n is the number of elements in G). The discrete logarithm problem for G is defined as:

> Given elements $\alpha \in G$ and $\beta \in$ G, find an integer $x,\ 0 \leq x \leq n-1$ (if it exists), such that $\alpha^x \equiv \beta$ [120]

The ECDSA is the "elliptic curve analogue of the DSA", in which the subgroups of $\mathbb{Z}_p^*$ are replaced by the points on an elliptic curve $E(\mathbb{Z}_p)$ [120]. An elliptic curve E over the set of real numbers $\mathbb{Z}_p$ satisfies the following equation:

$$y^2 = x^3 + ax + b \text{ such that } x, y, a, b \in \mathbb{Z}_p \text{ and } 4a^3 + 27b^2 \neq 0 \qquad [122]$$

The set $E(\mathbb{Z}_p)$ consists of all satisfying (x, y) points as well as a special point O called the "point at infinity". An elliptic curve can generally be defined over any finite field, which consists of a finite set of elements that satisfy specific mathematical properties when combined with the binary operations of addition and multiplication [121]. The ECDSA typically uses two types of finite fields: a prime field $\mathbb{F}_p$ and a characteristic two finite field $\mathbb{F}_{2^m}$ [121]. Additionally, elliptic curve cryptography relies on the Elliptic Curve Discrete Logarithm Problem (ECDLP)—an analogue of the discrete logarithm problem seen in the DSA. Given an elliptic curve $E(\mathbb{Z}_p)$ over a specified finite field, the ECDLP can be defined as:

> Given points $P, Q \in E(\mathbb{Z}_p)$, find an integer x (if it exists) such that $Q = xP$ [123]

Point addition allows two points on the elliptic curve $E(\mathbb{Z}_p)$ to be added together to yield a third point on the curve. Scalar multiplication allows any given point P to be doubled to obtain $2P$, which also exists on the elliptic curve. The point $2P$ can then be added to the original point P to obtain $3P$, and so forth such that nP may be found on the elliptic curve. The computational intractability of the ECDLP provides the mathematical basis of security for all elliptic curve cryptography, including the ECDSA [124]. Refer to Appendices 7.1 and 7.2 for the complete ECDSA algorithm.

2.4. Hash Functions

To supplement this, the Bitcoin protocol also uses a SHA-1 cryptographic hash function. Public key cryptography and digital signature schemes typically use hash functions in their algorithms, which convert strings of arbitrary length into shorter ones of fixed-length. For example, the widely-used SHA-1 hash function produces a 160-bit hash value. Rather than encrypting the entire message, it is often more sensible to encrypt a hashed version of the message. Ideally, the hash function should be one-way: given a fixed-length binary output, it would be very difficult to find a string that hashes to the given output [125]. Additionally, the hash function should be collision-resistant—that is, it would be computationally infeasible to find two messages that share the same hash value [3]. In other words, it would be infeasible for any probabilistic polynomial algorithm to find:

$$x, y, \ x \neq y \quad \text{such that} \ H(x) = H(x') \qquad [126]$$

A one-way, collision-resistant hash function should make it impossible to forge the signature or modify the original message by attacking the hash function itself.

2.5. The Bitcoin Protocol

There are two types of objects that are broadcast to the Bitcoin network: transactions—operations that combine, divide, and remit money—and blocks, which record approved transactions [2]. Transactions and blocks are addressed by a hash of their object data. Each coin can be thought of as "a chain of digital signatures" [4] and owned by a specific Bitcoin address, which consists of a 160-bit SHA-1 "cryptographic hash of the public portion of an ECDSA key pair" [5]. The owner of the coin hashes the previous transaction, digitally signs it with her private key, and designates the recipient's public key as the next address of ownership. The recipient can then verify the coin's previous chain of ownership using the sender's public key, validating that the sender did in fact own the transferred coin at one point (see Appendix 7.3).

Additionally, Bitcoin uses a proof-of-work system based on Adam Back's Hashcash protocol. Hashcash was initially proposed as a mechanism to combat email spam, whose success is dependent on sending an enormous number of emails using a disproportionately small amount of time and CPU effort [6]. Under the Hashcash protocol, an email could only be sent if an appropriate textual stamp had been added to the email's header. To generate the stamp, the sender chooses an initial random number (a nonce) and computes a 160 bit SHA-1 hash of the header. A header is only valid if the first 20 bits of its hash is all zero. Otherwise, the sender increments the nonce and must try again. The probability of finding an acceptable header is 1 in 2^{20}, and could only be done through brute force trial-and-error [6]. The crux of this idea was that email spammers would never invest the required time and CPU power needed to generate these hashed headers. Although it is computationally difficult for the sender to generate the appropriate header, it is extremely easy for the email's recipient to verify the stamp's validity.

The ideas behind the Hashcash scheme have been applied to Bitcoin's proof-of-work protocol, "which implements a distributed timestamp service providing a full-serialized log of every Bitcoin transaction ever made" [5]. Valid transactions are added to blocks, which also include a timestamp and nonce. Transaction blocks form a hash chain, in which each block contains a hash of its preceding block. A block is added to the existing chain once its proof-of-work is solved, which involves incrementing the block's nonce until the resulting hash value has the required number of zero bits (see Appendix 7.3). Similar to Hashcash, "the average work required is exponential in the number of zero bits required and can be verified by executing a single hash" [4].

In short, the blockchain mechanism prevents double spending. The blockchain—equivalent to a public ledger of all past transactions—is distributed to all users on the Bitcoin peer-to-peer network. Each new transaction is checked against the blockchain to ensure that previously spent coins are not being reused. Once a transaction has been validated for double spending, it is added to the existing blockchain of approved transactions. The peer-to-peer network essentially acts as a trusted 3rd party, ensuring that no double spending can occur. In conjunction with this, the proof-of-work system prevents malicious users from forging or modifying transaction blocks that have already been added to the blockchain.

The Bitcoin protocol stipulates that the correct transaction history is represented by the longest blockchain in the network—that is, the chain with the most CPU power and proof-of-work effort already invested. Thus, users are always working to extend the branch with the longest blockchain currently, which is rooted in the genesis block hardcoded in the software [5]. Other shorter branches and invalid blocks are ignored by the network. This has two important implications. First, because a block contains the cryptographic hash of its predecessor, the hashed blockchain only contains backward links. Once the necessary CPU power is spent on solving a given block's proof-of-work, that block cannot be modified without redoing the proof-of-work computation for *all* descendant blocks. This substantially lowers the probability of a network attack because in order to change a previously approved transaction in the blockchain, an attacker must re-compute the proof-of-work for that specific block and *all blocks* that came after it [4]. To successfully do this and still surpass the concurrent effort of all honest users in the network is extremely unlikely. Secondly, this gives Bitcoin transactions the attractive property of being irreversible. Merchants who rely on electronic commerce are particularly susceptible to customers fraudulently using credit card chargeback. In fact, "with the possibility of reversal, the need for trust spreads. Merchants must be wary of their customers, hassling them for more information than they would otherwise need" [4]. Bitcoin addresses this issue without relying on 3rd party intermediation.

The blockchain structure has also shaped the network's economic incentives. New transactions are simultaneously broadcasted to all users, grouped into a new block. The first user to solve that block's proof-of-work puzzle appends it to the existing blockchain and earns newly minted Bitcoins as a reward. This is the only way in which new coins can be "mined" and added to the current Bitcoin monetary base. We note that coin defined here is both divisible and fungible. That is, a transaction contains multiple inputs and two outputs (one output for payment and one output to assign "change" back to the sender). If the output value exceeds that of the combined input values, the difference is paid as a transaction fee to the first network user who appends the approved transaction to the global ledger. "Transactions encapsulate the movement of Bitcoins by transferring the value received from its inputs to its output… An input identifies a previous transaction output (as the hash of the earlier transaction and an index to an output within it), and claims its full value" [2]. Thus, transaction fees and the possibility of unlocking new coins are the primary incentives for miners to contribute the needed processing power to maintain and authenticate the Bitcoin network.

Furthermore, the proof-of-work puzzle is controlled by an adaptive algorithm, which takes into account recent activity in the blockchain's history. As more people dedicate more computing power to join the mining process, the algorithm will make it increasingly harder to mine new Bitcoins in order to ensure that one new block continues to be mined every 10 minutes [5]. Miners used central processing units (CPU) to mine Bitcoins in the early days, but then transitioned to using graphical processing units (GPU), which yielded a 50x to 100x increase in mining power, and field programmable gate arrays (FPGA), which promoted power efficiency and ease of use [134]. Due to the high level of mining difficulty today, the mining game is now played almost entirely with application-specific integrated circuit (ASIC) machines. ASIC chips are designed with a specific purpose in mind—such as mining Bitcoins, and *only* mining Bitcoins. These systems are incredibly powerful and power efficient, offering a 100x increase in hashing power compared to previous technologies [134]. The endgame of Bitcoin mining is ASIC machines, which represent "the theoretical limit on the hardware capabilities of mining equipment" [135]. Today, Bitcoin mining has become a very expensive business, with ASIC mining equipment costing thousands of dollars on average.

Initially, the reward bounty for solving a block's proof-of-work was 50 new Bitcoins. This amount halves for every 210,000 block of transactions incurred until it becomes virtually impossible to mine new Bitcoins [7]. When Nakamoto designed the Bitcoin platform, he fixed the money supply at a predetermined limit of 21 million Bitcoins. The last Satoshi—or 0.00000001 of a Bitcoin—will allegedly be mined in the year 2140. After this occurs, the system will solely rely on transaction fees as an incentive to users [1]. All of this was designed to "mimic the extraction of gold or other precious metals from the earth—only a limited, known number of Bitcoins can ever be mined" [1]. This mechanism incentivizes prospective users to join the Bitcoin mining game and essentially rewards early adopters.

Perhaps the most appealing characteristic of Bitcoin as a currency is the level of anonymity it provides its users. Unlike traditional financial institutions, where information related to the transaction is limited only to the parties involved, Bitcoin transactions are made public [4]. That is, we can see the amount of Bitcoins transferred from one party to another, but the identities of the parties involved are completely hidden from the public eye (see Appendix 7.4). Derived from public keys, Bitcoin addresses are pseudonymous in that they could represent anyone on the Internet and are not linked to anyone's identity. A new public/private key pair is generated for each Bitcoin address, and any user can sign up for multiple addresses without divulging any personal information [127].

Overall, Bitcoin has several defining characteristics. Although transactions are not completely anonymous, they do offer a high level of pseudonymity. All transactions are publicly announced via the blockchain, which ensures that no double spending can occur, and are irreversible once they have been validated. Additionally, Bitcoin has low transaction costs and a finite money supply. Most importantly, Bitcoin is neither controlled nor mediated by a 3rd party institution, making it a fully deregulated and decentralized cryptocurrency.

3. CONTEXTUALIZING BITCOIN

3.1. The Cryptowars

Historically, governments have held a monopoly over cryptography, which was used mainly for diplomatic and military purposes. However, in the 1970s, the advent of the information age not only made computers more accessible to the public but changes in digital communications also increased the public's demand for encryption technologies. The government began to see cryptography as a real threat to national security. According to the FBI Director at the time, Louis Freeh, "at stake was the public's right to use strong encryption, which facilitates commerce and allows individuals to maintains their personal privacy, but which government feared would allow drug lords, spies, terrorists and even violent gangs to communicate about their crimes and their conspiracies with impunity" [102]. The increasing tension between the government's desire for surveillance and citizens' desire for privacy ultimately resulted in the Cryptowars of the 1990s.

During this decade, the US government began to treat cryptographic software as munitions [103]. In fact, the act of exporting cryptographic protocols was banned in the United States until 1999 [104]. In 1994, the Clinton administration attempted to sway the technology industry into adopting the "Clipper chip"—a new NSA encryption algorithm that included a backdoor for the government. When this failed, the administration introduced a key escrow policy, stating that "all encryption systems should leave a spare key with a 'trusted third party' that would hand the key over to the FBI on demand" [103]. This key would essentially enable the government to unlock private communications between individuals, which incited public outcry and intense opposition from the computer industry [105]. In 1994, the Communication Assistance for Law Enforcement Act (CALEA) was passed into law, mandating phone companies to install remote wiretapping ports that would allow for "point-and-click" wiretapping capabilities [104]. Similar controls to monitor citizens' digital lives were also implemented in the UK, where any provider of encryption technology must be licensed and place encryption keys in escrow with the British government [103].

The governments faced strong opposition from the Cypherpunks, a group of civil libertarians who were interested in protecting the individual's right to privacy and saw these legislative measures as a violation of democracy. These crypto-anarchists "foresaw a future world in which widely available cryptography secured personal anonymity and privacy to such an extent that it threatened the authority of the state" [106]. They believed that cryptography shifted the balance of power back into the hands of citizens, essentially acting as a check-and-balance mechanism against Big Government [102]. In this digital age, "anything that can be done cryptographically can be done without government oversight" [106]. In short, people should place their trust in cryptographic protocols, rather than a government that could abuse their civil liberties at any moment.

3.2. A Brief History of Digital Currencies

One of the most prominent figures of the Cypherpunks was David Chaum, a renowned cryptography researcher and the founding father of digital cash. The movement to digitize money began as early as 1983, when Chaum introduced the idea of using "blind signatures" in financial transactions. A blind signature scheme enables an individual to get her message signed by another party without revealing the message's content to the other person [128]. In his seminal paper "*Blind Signatures for Untraceable Payments*", Chaum implemented this idea using RSA signatures and introduced a model for an untraceable payments system [129]. The idea of blind signatures is most easily demonstrated by an example: suppose Alice would like to send Bob a message m for him to sign, without Bob actually seeing the message's content. Suppose that Bob's public key is (n, e) and his private key is (n, d). Alice sends $x = (r^e m)\ mod\ n$ to Bob where r is a random value generated to satisfy $\gcd(r, n) = 1$. The random value r essentially blinds the message m from Bob, who returns a signed value $t = x^d\ mod\ n$ to Alice. Alice can then remove the blinding factor to reveal the true signature s by computing $s = r^1 t\ mod\ n$ [128].

Building on this idea, Chaum created one of the world's first digital currencies in 1990: DigiCash. When transacting with DigiCash, a user could hide the payee's identity as well as the time and amount of payment from a 3rd party (ie. the bank). The payee's identity would only be released under exceptional circumstances, such as an audit or theft [129]. However, DigiCash was issued "only in exchange for real money deposited in the payer's bank account…and once used for payment it [was] re-deposited into the payee's bank account" [130]. Thus, DigiCash was more of an anonymous pre-paid credit card rather than a truly untraceable digital currency. The company ultimately went bankrupt eight years later due to a series of failed partnerships and poor management. Still, the principles of anonymity and privacy behind DigiCash spurred the imagination of others, while the Cypherpunks' philosophies have become the ideological pillars behind Bitcoin today. To better understand and contextualize Bitcoin, we must consider the historical evolution of other digital currencies.

3.3. Gold-Backed Currencies

Gold-backed digitized currencies are especially appealing to "gold bugs" due to their distrust of government-backed fiat currencies. These individuals believe that central banking institutions can abuse their authority of printing more money, and do so irresponsibly in a way that causes hyperinflation. This belief is particularly prevalent among those who live in volatile, underdeveloped countries such as Zimbabwe and Argentina [8]. In the subsections below, we present three comparative case studies on different gold-back currencies.

A) E-gold

In 1996, oncologist Douglas Jackson created e-gold, a new digital currency fully backed by gold stored at various safe deposit boxes around the world. Allowing transactions as small as one ten-thousandth of a gram of gold, e-gold was also the world's first micropayment system. At the peak of its success in 2008, e-gold processed over $2 billion in transactions annually and had nearly 5 million users worldwide [13]. The reasons behind e-gold's popularity also contributed to its demise: in 2007, the U.S. Department of Justice charged Jackson and his two principal directors with several counts of money laundering, conspiracy, and operating an unlicensed money transmitting business [14].

The growing success of e-gold attracted the attention of cyber-criminals, who enjoyed the anonymity provided by the currency. As the Department of Justice indictment describes:

> Persons seeking to use the e-gold payment system were only required to provide a valid email address to open an e-gold account—no other contact information was verified. Once an individual opened an e-gold account, he/she could fund the account using any number of exchangers, which converted national currency into e-gold. Once open and funded, account holders could access their accounts through the Internet and conduct anonymous transactions with other parties anywhere in the world [15].

The anonymity and global reach provided by e-gold allowed criminals to launder money easily and evade the scrutiny of law enforcement. The US federal government accused e-gold directors of knowing about the criminal activity occurring among its user base, and still allowing it to proceed. For example, criminal users carried out an investment scam by moving $146 million through the e-gold system using 10 different accounts. Because e-gold did not allow chargebacks, all payments on the system were final. Thus, consumers who were tricked into sending money to criminals could not receive refunds. Regarding payment recovery, e-gold did not provide adequate consumer protection [14].

There were several facets of e-gold's operation that made it easier for US authorities to conduct an investigation and shut it down: the company operated openly in the United States, with centralized headquarters in Florida, and at least three principal directors residing in the United [15]. Furthermore, the currency did not actually provide its users with the anonymity it had promised. Upon creation of an account, the user must deposit at least $1,000 from a traditional banking institution into the e-gold account. Thus, all e-gold accounts were traceable to real-world identities and linked to personal information recorded at these external financial institutions.

Jackson and the others charged by the Department of Justice eventually pleaded guilty to charges of "conspiracy to engage money laundering and the operation of an unlicensed money transmitting business" [16]. The company paid a $3.7 million fine and froze all accounts in the e-gold system. The only way users could access the value in their accounts and obtain a full refund was to submit additional information to e-gold, which would be reviewed by the court's Claims Administrator and the relevant authorities in the US government. Before it was shut down in 2008, e-gold was perhaps the world's most successful alternative currency. Its success subsequently inspired other gold-backed, copycat currencies.

B) <u>eBullion</u>

In 2000, Jim and Pamela Fayed launched eBullion, which allowed users to digitally transfer gold and silver between accounts. Although eBullion was incorporated in Panama, it offered a debit card service to all US customers, enabling them to convert their bullion balances into US Dollars. The company met its downfall in 2008 when Jim Fayed murdered his co-founder and wife. He was subsequently sentenced to death, and the company was investigated and prosecuted under the Patriot Act for money laundering, illegal money transmission, and other criminal activity. All client assets were seized when the company was shut down in 2008, and eBullion's one million users were never compensated for their losses [13].

C) GoldMoney

Shortly after the launch of eBullion, James Turk created GoldMoney as another competitor to e-gold and eBullion. GoldMoney branded itself as a trusted provider of digital currencies backed by gold and silver, touting its secure technology and extensive client identification strategies to deter money laundering. By 2011, GoldMoney held over $2 billion in client assets. Over time, it grew to become a savings platform for most users—demand for its currency exchange and payment services was relatively insignificant [17]. By 2012, due to increasing regulation and high costs of compliance, GoldMoney disabled the ability to make payments between user accounts [13].

Bitcoin shares several similarities with these currencies: both are digital, liquid, allows the transfer of funds between user accounts, and are relatively anonymous compared to traditional payment methods [8]. However, what makes Bitcoin a revolutionary currency are the differences. First, Bitcoin is considered fiat money and lacks backing by any physical commodity. Secondly, Bitcoin is not controlled by any governing authorities—thus, it cannot be freely minted. Finally, because Bitcoin is completely decentralized, there exists great ambiguity in terms of which regulatory jurisdiction the currency belongs to.

3.4. Online Ecommerce

The growth of the Internet has created an e-commerce boom, generating nearly ubiquitous demand for electronic payments systems. Since 2000, the percentage of retail sales through e-commerce has increased every year. The Internet has made it easier for consumers to find their desired products and also get exposure to a wider variety of goods and services [18]. Currently, online retail marketplaces earn $278.5 billion in revenues annually in the United States, and comprise one of the fastest growing markets at 11.6% CAGR [19]. Over the past decade, PayPal has become the kingpin of electronic payments in this industry.

Since the birth of online ecommerce, PayPal has dominated electronic payments in this industry. As of 2012, the service had over 117 million active users and processed $35 billion in payment volume per quarter [20]. By investing millions of dollars into anti-fraud detection technologies, PayPal is often the vendor of choice for many online merchants [8]. According to a recent report published by Javelin Strategy & Research, "91% of online consumers have used PayPal, while 24% have used Checkout by Amazon and 9% have used Google Checkout" [21]. It is unlikely that Bitcoin will gain a strong foothold in the traditional ecommerce market, especially against such powerful incumbents. Most of these consumers won't require the privacy provided by Bitcoin. Additionally, customers will likely prefer to compare prices in US Dollars or other fiat currencies, rather than Bitcoin [8].

However, Bitcoin could potentially disrupt the micropayments industry—a sector within the broader ecommerce space that has recently experienced exponential growth. While there is no standard definition of micropayments, they are generally tiny amounts of money transferred digitally and are too small to be processed by credit cards. PayPal defines micropayments as “transactions of less than $12. Innopay considers it ‘a payment of very low value, often under a euro’. Francesco Burelli, of Value Partners, defines it as ‘an online or mobile, real-time or deferred, financial transaction below €5, which initiates the instantaneous delivery of a digital good’” [22].

The demand for micropayment solutions has grown significantly due to new content offerings from online media distributors (video-on-demand, digital music downloads, and in-game purchases). While most content distributors prefer subscription-based business models that guarantee a reliable stream of revenues, many customers like having the flexibility of buying content on the spot, which can only be monetized through individual transactions of small value [23]. Presently, incumbent payment infrastructure—such as PayPal and credit cards—handle the majority of these transactions, but high transaction costs make this rather prohibitive. Merchants who rely on PayPal are required to pay a 2.9% transaction fee on the total sale amount plus a $0.30 fee per transaction. Credit card processing fees are even higher. In contrast, “transaction fees on the Bitcoin network tend to be less than 0.0005 BTC, or 1 percent of the transaction” [1].

The European micropayments market is estimated to be worth roughly €6 billion and projected to grow to more than €15 billion by 2015 [23]. This 15% CAGR is unprecedented amongst other industries, channels, and payment types. A report released by Hi-Media Group and Harris Interactive found that more than 50% of Internet users in Europe and the United States use micropayments to purchase content online [24]. Conversely, the total payment volume online from credit cards fell from 44% in 2009 to 40% in 2010, and this trend is expected to continue [21].

Despite the attractive growth seen in the micropayments space online, there has yet to be a “silver bullet” payment solution. Such a solution must deliver on low costs, high speed, and an excellent user experience [23]. Additionally, it needs to be a universal solution in that it provides the flexibility necessary for adaptation across business and distribution models. Bitcoin could potentially fill this need: because there is no 3rd party intermediary, Bitcoin is significantly cheaper and faster than traditional payment networks [1]. While a credit card transaction may take several days to receive approval, each Bitcoin transaction only requires 10 minutes to verify and authenticate. Advocates are hopeful that Bitcoin’s low transactions costs will one day transform the markets for global money transfers and remittances.

3.5. Virtual Currencies

The popularity of virtual worlds has generated huge demand for virtual goods and currencies, and their growth has resulted in increasingly complex and liquid economies of significant scale—all occurring online. The European Central Bank defines a virtual currency as a “type of unregulated, digital money, which is issued and usually controlled by its developers, and used and accepted among the members of a specific virtual community” [25]. Virtual currencies can either be purchased using “real” money at a pre-determined exchange rate or earned by users who perform certain activities in the community. It is important, however, to note the distinction between virtual currencies and electronic money. Electronic money is linked to traditional money and has a legal claim on the issuer. In contrast, it is not always possible to redeem virtual currencies at par value (since exchange rates are dictated purely by supply and demand) Furthermore, the issuing company has complete control over the virtual currency [25].

There are three primary categories of virtual currencies: closed systems, schemes with unidirectional flow, and those with bidirectional flow (see Appendix 7.5). We describe each type in the subsections below.

A) Closed Virtual Currency Schemes

These schemes are not linked to the real economy and are entirely contained within the virtual community. Users participate in the community or game by paying a subscription fee, and are not allowed to trade the currency outside of the community. Users can only earn money based on their online performance or by accomplishing certain in-game tasks. This type of scheme has been adopted by massively multiplayer online role-playing games (MMORPG), such as Blizzard Entertainment's wildly popular World of Warcraft game. The End User License Agreement mandates that it is strictly forbidden to buy and sell WoW gold in the real world. This rule, however, has not been well-enforced: a significant portion of WoW players engage in "gold farming", a process in which game players are "paid to collect gold through gameplay that can then be sold outside the game platform to other players" [15]. For many in low-income countries, gold farming has become a lucrative job option. In 2008, the gold farming economy was estimated to be $500 million in value, with gold farmers earning $145 per month on average.

B) Virtual Currency Schemes with Unidirectional Flow

Under this scheme, virtual money can be purchased using real currencies at a specified exchange rate. However, the flow is unidirectional because once the virtual money has been purchased, it cannot be traded back for the original currency [25]. We have seen this scheme adopted by gaming platforms on social networks such as Facebook. In 2009, the company introduced Facebook Credits—the currency that all players must use to purchase digital goods when playing games on Facebook's platform, such as Farmville and Mafia Wars. Facebook took 30% of all digital purchases, netting a total of $213 million in revenue in Q1 2013 [26]. In September 2013, however, Facebook Credits became obsolete after the company decided it would be simpler and more flexible for users to pay for their digital purchases using local currencies [27]. In some cases, the virtual currency is also given real purchasing power and can be exchanged for real goods and services. For example, customers can buy Microsoft Points online using a credit card. They can then use these Points to buy products in the Microsoft Store or redeem in-game purchases. Once these Points have been bought, however, they cannot be exchanged back into real money.

C) Virtual Currency Schemes with Bidirectional Flow

Virtual currencies designed under this scheme effectively operate the same as real world currencies. Users can buy and sell their virtual money at exchange rates set for traditional currencies. Linden Lab's Second Life boasts a substantial economy that uses Linden Dollars (L$). In this virtual world, users create avatars to represent their digital selves. Users can earn money in several ways: "they can sell whatever they are able to create…they can also profit from their previous investments (e.g. buying a house and then selling it at a higher price), but they can also win prizes in events" [25]. Linden Labs intends for Second Life to be a virtual replica of the real world. Accordingly, Linden Dollars and US Dollars are interchangeable at a pre-set exchange rate in the Second Life currency market. Users can purchase Linden Dollars using a credit card or PayPal account, and can sell extra Linden Dollars back for US Dollars. By the end of 2010, the money supply of Linden Dollars was worth $30 million USD [8]. Having experienced substantial growth these past few years, Second Life's "residents exchange goods and services worth about USD $600 million each year and the Second Life economy is estimated to be bigger in terms of GDP than 19 countries, including Samoa" [25].

So what is Bitcoin's role within this landscape of virtual currencies? These virtual worlds require a secure virtual currency, exchanges to facilitate the conversion of real and virtual currencies, as well as anti-fraud protection for users. Because virtual currencies are owned by the issuing company, the owner of the virtual world could issue more money at its discretion and devalue the currency without users' consent. Similarly, if the online world is hacked or compromised, users may lose all of their virtual savings. If implemented correctly with the proper anti-fraud measures, Bitcoin could become the next standard for virtual currencies due to its decentralized and independent nature.

3.6. The Bitcoin Ecosystem

Over the past few years, a small but vibrant ecosystem has developed around the Bitcoin platform. Today, few individuals carry out Bitcoin mining on their personal computers due to the increasing computational difficulty of generating new blocks—it now takes on average a year or more to mine 50 new Bitcoins [8]. As a result, most users join mining pools such as Deepbit, which distributes mining rewards to all members of the collective based on the amount of work contributed on a pro-rata basis [9]. Users can avoid the process of Bitcoin mining entirely by buying Bitcoins directly from a number of exchanges, which allow users to exchange traditional currencies—US Dollars, Japanese Yen, Euro, among others—for Bitcoins and other digital currencies [8]. For a long time, Mt. Gox was the largest and most popular Bitcoin exchange, processing "almost 90% of all exchange operations on the network" [10]. On November 4, 2013, however, Chinese-based BTC overtook Mt. Gox to become the world's largest digital currency exchange by volume.

These standard exchanges don't yet offer futures trading, but over-the-counter exchanges do exist to facilitate the exchange of Bitcoins for any service, commodity, or currency, as well as option contracts [8]. Users can either store their Bitcoins locally on their computers, or utilize one of the many 3rd party wallet services offered online and on mobile devices. Users can also use transaction services to keep, send, and receive Bitcoins without running the native Bitcoin client themselves. Both Mt. Gox and Bitcoin Mail allow users to send Bitcoins by email [8]. Users who wish to invest their Bitcoins can do so with Bitcoin-based funds and trusts, such as the Bitcoin Investment Trust. Unfortunately, due to the lack of regulation and consumer protection measures, there have been many cases of theft and fraud. For instance, Bitcoinica was shut down due to a series of thefts, and Bitcoin Savings & Trust was prosecuted by the SEC for being a Ponzi scheme [9].

As a fairly new digital currency, Bitcoin is still relatively illiquid. This begs the question, who actually uses and accepts Bitcoin? Due to its value proposition of being both pseudonymous and decentralized, Bitcoin's original user base was both small and very niche: cryptography enthusiasts, "gold-bugs" who distrusted governments and central banks, cybercriminals, and speculators [8]. As Bitcoin has slowly permeated into the public consciousness due its recent media exposure, its merchant base has gradually grown as well. There is great variety among the online vendors that currently accept Bitcoin payments: auction sites, online gambling, professional services, illicit drug marketplaces like Silk Road (recently shut down by the FBI), and even luxury goods marketplaces like Bitmit and BitPremier. Vendors that have traditionally only accepted US Dollars can now accept Bitcoins through BitPay's payment gateway, which accepts Bitcoins from buyers and pays vendors in US Dollars. In fact, as of May 2013, Wordpress, Reddit, and okCupid are some of the Internet's top merchant sites that now accept Bitcoin [11]. Notably, when Visa, Mastercard, Bank of America, and PayPal refused to process any donations to WikiLeaks, the nonprofit began accepting donations solely in Bitcoins [12].

While it appears that online vendors have embraced Bitcoins, there is little evidence that Bitcoin has gained a large footprint among brick-and-mortar retailers.

4. THE ECONOMICS OF BITCOIN

Currently, there are approximately 12 million Bitcoins in circulation. As of December 10, 2013, a single Bitcoin is worth $918 USD—which represents a stunning 6,500% appreciation in value from its market price a year ago. The entire market capitalization of all Bitcoins in circulation amount to more than $11 billion, and the network sees roughly 70,000 transactions daily (see Appendix 7.6) [53].

4.1. Economic Consensus, Incentives, and Stability

Economic incentives are embedded into the Bitcoin system by design. Transaction fees and the possibility of mining new Bitcoins incentivize miners to invest computational power and time into solving new blocks. As the Bitcoin community grows and it becomes computationally more difficult to solve the proof-of-work problems, the production rate of new Bitcoins will gradually decrease over time. These incentives favor early adopters, which has helped to accelerate Bitcoin's adoption curve [2]. The stability of Bitcoin protocols rely on players accepting and adhering to three types of consensus [5]:

1. **Consensus about Rules.** Users must agree on how to determine the validity of Bitcoin transactions, and which transactions should be added to the universal blockchain.

2. **Consensus about State**. Users must agree on the history of all approved transactions in order to prevent double spending. In distributed systems like the Bitcoin network, "each player can see part of the state and the players need to cooperate, in large numbers and across a potentially unreliable network, to achieve a consistent understanding of the global state" [5].

3. **Consensus about Value.** Users must agree that Bitcoins have value, so that they continue to accept Bitcoins as payment.

These forms of consensus are all mutually dependent upon one another—the failure of one will hurt the stability of the other two.

In the Bitcoin economy, the global equilibrium occurs when the total mining reward in dollars per second equals the total global cost of mining [5]. As long as this holds, users will continue to participate in the mining process and the Bitcoin system will remain stable. However, it is important to note that users retain the power to enforce or reject any of the rules outlined in Bitcoin's protocol. That is, a rational user will only participate in a way that maximizes his utility. Thus, Bitcoin's functionality and stability will endure so long as users *willingly* follow the rules because it makes them objectively better off [5].

One of the critical rules stipulated in the Bitcoin protocol is that miners must extend the longest branch in the blockchain. Are users properly incentivized to extend the longest chain in the network, or are they more inclined to create or sustain forks in the transaction blockchain? A fork essentially creates another version of the transaction history, leaving the system vulnerable to double spending. Applying the principal of trust assurance (the *stag hunt model*) from game theory literature, it turns out that there are only two Nash Equilibrium outcomes in the Bitcoin scheme: mutual cooperation or mutual defection [5]. If all other users cooperate by mining to extend the longest branch in the log, the player who deviates from the global strategy risks having her block rejected from the long-term consensus branch—thus lowering her expected utility.

In fact, any strategy in the Bitcoin game can achieve Nash equilibrium as long as all players adopt it, *regardless* of the strategy itself. This is an economic vulnerability in the Bitcoin scheme. In practice, users follow the rule of extending the longest branch simply because it was stipulated in Nakamoto's original paper. As new users join the network, they are incentivized to follow the strategy chosen by the majority of existing miners. Overall, the Bitcoin protocol is not self-executing. Rather, it relies on the willingness of users to adhere to consensus and the economic incentives embedded in the protocol.

4.2. The Value of Money

Critics of Bitcoin often disparage it as the next big bubble. According to Yale economist and Nobel Laureate, Robert Shiller, a speculative bubble is a social epidemic. As early investors amass great wealth due to price increases in the underlying asset, news of their success provokes the envy and curiosity of other prospective investors [28]. As more and more people are lured into investing, the asset's market valuation becomes wholly disconnected from its fundamentals [29]. Since Bitcoin is not backed by commodity or government, where does Bitcoin derive its intrinsic value and is it sustainable?

In order to answer this, we must first answer the question pondered by generations of economists: how does fiat money obtain and retain value? A professor of economics at Berkeley, Hal Varian, suggests two possible sources of value:

> Dollar bills are 'fiat' money—they are valuable because the government in power says so… A more profound, and perhaps slightly unsettling, reason that a dollar has value is simply that lots of people are willing to accept it as payment. In this view, the value of a dollar comes not so much from government mandate as from social convention [30].

In fact, Varian contends that money's value is primarily derived from social consensus. After all, there are many 'currencies' that have no government backing: cigarettes used as payments in prisons, cowrie shells, peacock feathers, and the more conventional gold and silver, among others. The Iraqi Swiss Dinar is another notable example. Backed by the Iraqi government before the 1990 Gulf War, the Swiss Dinar was disendorsed by Saddam Hussein during the war due to economic sanctions. Despite the creation of a new, official, national currency—the Saddam Dinar—the Swiss Dinar continued to circulate in the northern Kurdish regions of Iraq. Even without institutional or commodity backing, the Swiss Dinar still maintained a stable trading value [8].

While Varian contends that social convention and network effects give money intrinsic value, other economists such as Abba Lerner and G. F. Knapp believe that government decree is the key contributor. The argument is that because governments are willing to accept fiat money as payment for tax liabilities, this guarantees that there will be a last resort buyer of money should private transactions fail to provide the necessary demand for money. Similarly, in his seminal work *Common Sense of Political Economy*, P.H Wicksteed argues that "inconvertible paper money had a positive value squarely on its being made acceptable by the government for the payment of taxes" [31].

Ludwig von Mises, a prominent figure of the Austrian School of Economics, would disagree with Varian. Money is useful because it can be exchanged for other goods and services. Thus, money's sole value is derived from its purchasing power (or price)—but how is this value *initially* established? To answer this, Mises proposed the Regression Theorem [32]. He noted that today's demand for money depends on the purchasing power of money yesterday. Coupled with today's money supply, the price of money today could be established. The prior day's purchasing power of money then determines yesterday's demand for money, which subsequently sets yesterday's price of money. By applying this procedure backwards through time, the Regression Theorem states:

> We will eventually arrive at a point in time when money was just an ordinary commodity where demand and supply set its price. The commodity had an exchange value in terms of other commodities... To put it simply, on the day a commodity becomes money it *already* has an established purchasing power or price in terms of other goods. This purchasing power enables us to set up the demand for this commodity as money. This in turn, for a given supply, sets its purchasing power on the day the commodity starts to function as money. Once the price of money is fixed, it serves as input for the establishment of tomorrow's price of money [32].

This theorem essentially states that money derives its value from formerly being a commodity used in barter, before it evolves into a medium of exchange. The paper dollar was originally circulated as a convenient representation for gold. After its usage became widely adopted, paper money graduated into legal tender and by then, it had established its own purchasing power on account of being a proxy for gold for many decades [32].

In order to reconcile these opposing views, we suggest that perhaps money first establishes its value as a physical commodity used in trade and barter. If that commodity is demanded by others and once its purchasing power has been established, it becomes a medium of exchange. Money then *retains* this value through social consensus (as long as others are willing to accept it as a form of payment) and government backing (which guarantees that the demand for money will always exist). Once its purchasing power stabilizes, money can then function as a store of value and unit of account.

From this, it is clear that Bitcoin is backed by neither commodity nor government. Thus, the only value driver from the normative framework above applicable to Bitcoin would be social consensus. The initial adopters of Bitcoin consisted of a small, niche community of technology enthusiasts and cryptographers who were mainly interested in Bitcoin's security properties and innovative applications of cryptography. In the past two years, however, Bitcoin has slowly but surely diffused into various pockets of the mainstream population. Not only are more online merchants accepting Bitcoin payments, but investors and venture capitalists have also been placing major bets on the currency's future success. According to the Dow Jones Venture Source, six Bitcoin startups raised approximately $11.4 million between October 2012 and May 2013 [33]. However, Bitcoin's soaring market price could be an indicator of investors' speculative interests, rather than its acceptance as a form of payment.

The company BitPay is perhaps a better proxy for Bitcoin's market penetration. Founded in 2011, BitPay offers a payment processing service that allows customers to pay merchants using Bitcoins on an easy-to-use interface. For a small fee, merchants have the option of instantly depositing their received Bitcoins directly into their bank accounts. This feature thereby protects merchants from Bitcoin price fluctuations [34]. In September 2013, the company reportedly exceeded 10,000 Bitcoin-accepting merchants spanning 164 countries. With more than $34 million worth of Bitcoins in transaction volume so far this calendar year, BitPay and its healthy growth rate speak to the increasing adoption of Bitcoin in digital ecommerce [35].

But what happens if this social consensus disappears? If Bitcoin suddenly experiences a loss of confidence, can Bitcoin recover its intrinsic value or will this digital currency be relegated to the history books—much like its now-defunct predecessors?

4.3. The Downfall of Bitcoin: Loss of Confidence

Despite its critics, Bitcoin is currently at the height of its acceptance. As more people advocate its use, network effects will gradually shift the public perception of Bitcoin from a niche novelty to a legitimate currency. Eventually, Bitcoin will reach a point of stability when these network effects and Bitcoin's utility reinforce one another. Until then, the immature Bitcoin economy is still at risk of suffering shocks that could lead to a detrimental loss of confidence.

An event causing Bitcoin's market value to drop significantly could undermine users' incentives to mine, thereby weakening the Bitcoin network. As Kroll et. al discuss in their 2013 paper for the 12th Workshop on the Economics of Information Security:

> This leads to the possibility of a *death spiral* in which loss of confidence in Bitcoin could cause the price to go down, a falling price lowers the incentive to mine and the equilibrium mining rate, lower mining rate leads to the currency being easier to subvert, and this leads to a further loss of confidence in the currency. Such a death spiral reflects the perceived loss of consensus in the value game [5].

If Bitcoin suffers a major blow such that its price declines dramatically, the system could be stuck in a vicious cycle until all users eventually abandon the currency due to a loss of confidence. Empirically, this has not happened yet despite the numerous Bitcoin price "crashes" that have happened over the past two years (see Appendix 7.7). For instance, June 2011 saw a 68% price decline from a peak of $32, August 2012 saw a 51% decline from $15.25, and most recently, a 61% price decrease from a peak of $266 in April 2013 [36]. In any case, the currency has exhibited astounding resiliency so far, with its current price at dizzying heights.

In the next few sections, we discuss several possible events that could seriously destroy user confidence in Bitcoin, to the extent that the currency's intrinsic value derived from social consensus is completely extinguished.

4.4. Speculative Bubbles and Volatility

The impact of speculation on commodity prices is widely debated in the economics literature. Speculation is the "purchase (or sale) of an [asset] with the expectation that the price of the asset will rise (or fall) to create the opportunity for a capital gain" [39]. The price changes as a result of speculation are not tied to the underlying fundamentals. That is, price changes and volatility caused by speculators in the market are not accounted for by corresponding shifts in demand or supply. Oil price changes in particular have been dissected by economists, with some scholars contending that speculation has been the main driver of price increases in global oil prices, while others found that speculation has actually decreased or stabilized oil prices [39]. In a testimony given by the CEO of ExxonMobil, "pure speculators account for as much as 40 percent of [high oil prices]" [40]—prices that have become largely disconnected from the fundamental costs of oil extraction.

Typically price changes in commodities are driven by supply shocks or a sudden surge in demand (or both). Because the short-term supply of oil is fairly rigid, increased demand is the main driver of high oil prices, which is the case when investors flood the futures markets with speculative investments and generate artificial demand. "The proposed link between large flows of capital into commodity markets and increases in current prices appeals to common sense: speculative demand for commodity-based assets increases demand for the underlying commodity, increasing its price" [41].

How does this apply to Bitcoin? The cryptocurrency sits at the nexus of currency and commodity. In order to be a store of value and unit of account, currencies need to be relatively stable in value. Bitcoin prices, unfortunately, more closely resembles that of a highly volatile commodity. It is rather dangerous that Bitcoin's value as a currency is tied to its identity as a commodity, because commodities are especially vulnerable to price bubbles, speculative attacks, and scarcity issues. Since 2011, Bitcoin has seen five significant price adjustments, each resembling the traditional speculative bubble [1]. With the media overhyping the Bitcoin phenomenon, new investors are lured in with promises of the cryptocurrency's future growth and ensuing profits. Indeed, there is even a strong correlation between the market price of Bitcoins and the frequency of Twitter mentions (see Appendix 7.8) [42].

The same principles of speculation behind oil price increases can be applied to Bitcoin. Because the short-term supply of Bitcoins is relatively stable, investors can artificially drive up demand for the currency, such that it becomes disconnected from its fundamental value: its underlying transaction volume. A 2012 study analyzing the Bitcoin transaction graph found that 55% of all Bitcoins in circulation were dormant (inactive for the past three months) [10]. Even more surprising was the discovery that more than 97% of all accounts had fewer than 10 transactions in their lifetime. Only 80 addresses were affiliated with heavy transaction volume—a minimum of 5000 transactions—many of which were affiliated with the major Bitcoin exchanges [10].

These findings speak to the illiquidity of the Bitcoin ecosystem. Other than a few highly active stakeholders, the majority of Bitcoin users are actually not very active. Furthermore, another study found that although the remaining coins in circulation were very actively used, most of this transaction volume was attributed to the Bitcoin gambling site, Satoshi Dice [9]. This suggests that Bitcoin is presently overvalued, with a market price that does not reflect the underlying fundamentals. The only thing supporting Bitcoin's current valuation is investors hoping that the price will continue to rise. The market will eventually correct itself at some point, which could lead to a loss in confidence as Bitcoin prices tumble.

Another related issue is Bitcoin's high volatility. Volatility is the statistical measure of the dispersion of returns around the mean. A higher volatility means that there is a larger average dispersion around the mean and thus, more uncertainty about the asset's expected return [43]. Much higher than most other assets, Bitcoin's average daily change vs. USD on the Mt. Gox exchange is 0.7%, equivalent to a 136% annualized return volatility (see Appendix 7.9). Furthermore, over the past three years, if we compare Bitcoin's 30-day moving average volatility vs. the USD against the currency pair EURUSD and the S&P500 index, Bitcoin's "volatility graph looks more like the S&P500 graph than like the EURUSD graph. Therefore, in the last three years, Bitcoin prices behaved more like an asset than like a currency" [43]. In contrast, the yen and euro only fluctuate by a few basis points [44]. Economic stability is a key pillar of any currency, and it remains to be seen whether Bitcoin can satisfy this condition.

As a result of its high volatility, Bitcoin prices are extremely unpredictable. This makes it difficult for customers to hold their savings in Bitcoin, or for merchants to price their goods using a unit of account that changes drastically on a weekly basis. However, some advocates contend that volatility is a non-issue if Bitcoin is used as a medium of exchange, rather than a unit of account or a store of value. Merchants can price their goods in terms of traditional currencies, and can receive payments in the equivalent Bitcoin amount at the going market rate through services like BitPay [45]. Customers "who purchase Bitcoins to make a one-time purchase don't care about what the exchange rate will look like tomorrow; they simply care that Bitcoin can lower transaction costs in the present" [1]. The only caveat is that the Bitcoin economy must provide enough liquidity such that transactions occur quickly enough to mitigate exchange rate fluctuations. Clearly, the Bitcoin economy is not yet at that stage.

However, there is hope. Bitcoin's biggest price changes occurred primarily in 2011, and its volatility has declined over time [43]. As the size of the Bitcoin economy grows, the currency will stabilize as price shocks lessen in impact [46]. Realistically, Bitcoin is still far from attaining that scale. The total value of all Bitcoins currently in circulation is equivalent to 2000 standard gold bars, and the daily trading volume on a good day is approximately $20 million—inconsequential compared to the $4 trillion of transaction volume seen by foreign exchange markets on a daily basis [42]. "Volatility is a product of thin markets, and adding more liquidity would help regulate prices" [47]. Therefore, Bitcoin still has a long ways to go in terms of providing the liquidity and stability necessary to a currency system. With 90% of its buyers being investors, Bitcoin is currently more of a speculative investment than a medium of exchange [48]. Until Bitcoin matures and reaches an economy of scale, it remains susceptible to speculative bubbles.

4.5. Deflationary Spirals

A key component of Bitcoin's protocol is its fixed money supply: there will only ever be 21 million Bitcoins in circulation. Thus, as the Bitcoin economy expands, the only outlet for economic growth will be through the currency's appreciation in value [2]. In a mature market, where only 1% of US GDP is transacted in Bitcoins and the rest in US Dollars, Bitcoin's real purchasing power will still increase over time: each coin will capture a constant fraction of the country's growing wealth [2]. Given that the supply of Bitcoins is fixed, as the demand for Bitcoins increases, the currency becomes more valuable and goods denominated in Bitcoins will cost less—leading to deflation. Traditional economies rely on the central bank's execution of monetary policy to target a low, stable inflation rate. For example, the US Federal Reserve sets the discount window interest rate at which banks can borrow from the Fed. When the demand for US Dollars is too high, the Fed sets a higher rate to discourage borrowing. Additionally, the Fed can always print more US dollars to increase the money supply.

These levers, however, are unavailable in the Bitcoin economy. As the supply of other fiat currencies increases faster than the Bitcoin supply, Bitcoin will appreciate in value over time. This could lead to a deflationary spiral, in which prices denominated in Bitcoins fall dramatically, producers respond by lowering production, leading to lower wages, lower demand, and even lower prices. Furthermore, the appreciation of Bitcoin's value will incentivize people to hoard their coins—so they can buy more goods in the future for less money [131]. When transaction volume decreases as a result, block creation and mining becomes less profitable for users, leading to waning interest in the Bitcoin system as a whole. Ultimately, this deflationary spiral can result in a sudden loss of confidence that destroys Bitcoin value [8].

4.6. Competition from Better Alternatives

Several alternative cryptocurrencies have appeared to ride the coattails of Bitcoin's recent popularity and media attention. These alternative currencies claim to be technically superior, having been designed to improve upon Bitcoin's flaws. For example, the next largest cryptocurrency is Litecoin, which advertises better security, lower mining difficulty, and faster transaction times—authentication within 2.5 minutes on average, compared to Bitcoin's 10 minutes [37]. Another alternative, Feathercoin, is similar to Litecoin and has 16 times the size of Bitcoin's ultimate money supply [38]. Litecoin and Feathercoin both use scrypt in their proof-of-work schemes, which adds "memory-intensive algorithms" in order to remove the advantages enjoyed by GPU, FPGA, and ASIC miners over CPU miners [136].

Still, the scale of these alternative cryptocurrencies pale in comparison to Bitcoin. As of April 2013, one Litecoin was only worth $2.31 with a total market capitalization of $38 million [37]. However, aspects of Bitcoin's design could be improved upon, which may provide the perfect opportunity for a competing cryptocurrency to supplant Bitcoin's dominance. As users flee Bitcoin to use a better alternative, this could destabilize and ultimately devalue Bitcoin, resulting in the aforementioned death spiral. A more optimistic view, however, is that multiple cryptocurrencies can co-exist peacefully by serving different needs.

4.7. Structural Attacks

Technical issues and economic attacks on the Bitcoin system could also lead to a large-scale loss of confidence. We discuss these vulnerabilities in the subsections below.

A) **Technical Vulnerabilities**

An advantage Bitcoin has over credit cards is that all transactions are irreversible once they have been validated and added to the blockchain. This protects merchants from fraudulent chargebacks—a common problem with credit card payments. Because the Bitcoin protocol instructs miners to work on the longest chain with the greatest total difficulty, forks are resolved relatively quickly. In March 2013, however, a hard fork occurred in the blockchain that could not be resolved by simply using the protocol.

The Bitcoin blockchain is a public ledger containing the complete history of all valid transactions. A hard fork essentially creates "two separate histories of transactions after the forking event" [49]. In this case, the hard fork occurred due to a bug in the 0.7 version of the Bitcoin client. Miners using version 0.8 generated a large transaction block (#225430) that was technically valid but rejected by the 0.7 nodes:

> Bitcoin versions prior to 0.8 configure an insufficient number of Berkeley DB locks to process large but technically valid blocks. [These] locks have to be manually configured by API users depending on the anticipated loads… Bitcoin 0.8 does not use Berkeley DB. It uses LevelDB instead, which does not require this kind of pre-configuration. Therefore it was able to process the forking block successfully [50].

This fork couldn't be automatically resolved because the 0.7 incompatible chain commanded 60% of the network's hash power [50]. Because of this fork, miners using version 0.8 started working on a version of the blockchain with #225430 included, while miners using version 0.7 saw a different version of the transaction history (see Appendix 7.10). Following a timely detection of this hard fork, the online community of developers quickly agreed to collectively downgrade to version 0.7. Every major mining pool operator and Bitcoin developer joined the Bitcoin-dev IRC channel, and large businesses and exchanges were notified to suspend deposits [51]. The economic damage was fairly significant but relatively contained: the operators of the BTCGuild and Slush lost $26,000 USD worth of mining rewards in the 0.8 version chain that was abandoned, and the merchant OKPay suffered a $10,000 double spend [51].

Although this hard fork was resolved within 6 hours, this brings to light some of the glaring issues with Bitcoin's technical protocol. First, it is interesting to note that this technical issue relied on a purely social intervention for its resolution. Because the network is wholly decentralized, no governing body can step in to solve the problems that arise from gaps in the technical protocol. "The reason why the controlled switch to the 0.7 fork was even possible was that over 70% of Bitcoin network's hash power was controlled by a small number of mining pools and ASIC miners, and so the miners could all be individually contacted and convinced to immediately downgrade" [51]. Accordingly, mining pools hold a lot of power in the Bitcoin ecosystem—nowadays, 70% of new blocks are mined by these pools rather than by individual miners [51].

Secondly, despite the fact that Bitcoin is theoretically immune to double spending, it can in fact occur during the event of a hard fork. Fortunately, the double spend attack in this case was not executed maliciously—the user simply wanted to see if it could be done (and OKPay was eventually paid). Thirdly, the integrity of the Bitcoin system relies on the critical assumption that no adversary can obtain so much computational power such that it can falsely publish an alternative transaction history to be accepted over the actual history. If we consider Moore's law, which predicts that the computation power per unit cost doubles annually, a "history revision attack" presents very real threat [2]. This threat is further compounded by the fact that most of the network's computation power is already concentrated in a small number of mining pools. For example, in 2012 the Deepbit mining pool contributed 40% of the total computation power devoted to mining in the Bitcoin network. Thus, "merely doubling its 'market share' would make it able to revise the entire Bitcoin history in a year's time, owing to Moore's law. Botnets and governments may be there already" [2].

Nakamoto designed the original Bitcoin protocol believing that a benevolent majority of users could prevent any small number of hostile adversaries from taking over the network [4]. But what if a malevolent majority persists? Fortunately, this fear is somewhat mitigated by the reality that individuals miners can switch from one mining pool to another almost instantly. Therefore, if any one operator had malicious intentions and controlled a majority of the network's hash power, miners could easily take away this power and reset the equilibrium by leaving the pool. For example, in 2011 Deepbit reached more than 50% of the total network hash power, and its miners responded with a mass migration towards other mining collectives [51].

Additionally, other technical issues could also cause a "crisis of confidence" [8]. First, many of Bitcoin's users care deeply about the level of anonymity provided by the currency—although this may change as the user base shifts and usage becomes more mainstream. Studies have shown, however, that by using certain statistical techniques, it is possible to identify and recover real-world profiles for nearly 40% of all users [52]. This may be problematic if the pseudonymity provided by Bitcoin is misaligned with enough users' expectations of total anonymity. Secondly, Bitcoin services such as exchanges and online wallets are especially vulnerable to security breaches (hacking, theft, and fraud). Because Bitcoin transactions are irreversible, a customer cannot recover her stolen coins after the fact. We discuss this issue in greater detail in a later section.

Ultimately, hard forks, security breaches, and other technical issues can undermine the currency's "acceptance, reliability, and security", all of which are necessary to sustain user confidence in Bitcoin [49].

B) Economic Attacks

Bitcoin's stability as a decentralized payments system requires that a majority of its miners are honest users who follow the rules laid out in the Bitcoin protocol. Thus, if an attacker acquires at least 51% of the network's computing power, it can theoretically take control of the system, rewrite the rules, and reject transactions created by other users. This has become a greater cause for concern due to the "technological arms race" that has occurred in recent years, with more miners buying expensive ASIC hardware dedicated to Bitcoin mining and the formation of powerful mining pools [117]. In fact, the top two mining pools today—BTCGuild and GHash.IO—control 53% of the network's computing power [53].

The ability to double spend may be the economic motivation behind a 51% mining cartel's desire to gain control of the Bitcoin network. However, studies have shown that this type of attack yields a relatively limited payoff: the cartel may not even recover the costs needed to carry out the attack with the profits earned from double spending [8]. Another type of attack, the Goldfinger Attack, is a "51% attack that aims to destroy the Bitcoin economy in order to achieve utility *outside* the Bitcoin economy" [8]. The most probable perpetrator would be governments using a Goldfinger Attack as a law enforcement tactic. Under this type of attack, the currency can only survive if the mining reward is at least as large as the attacker's utility from destroying the system. Furthermore, the attacker doesn't necessary need to launch a full attack—it merely needs to generate enough uncertainty around the possibility of a Goldfinger attack occurring. A credible bluff could be enough to start a death spiral [8].

More recently, a study published by Cornell researchers showed that the Bitcoin mining protocol is especially vulnerable to a Selfish Mining attack by malicious mining pools. Currently, the Bitcoin protocol is assumed to be incentive-compatible: it is in the best interests of rational mining pools to be honest because a colluding minority cannot earn a disproportionally large reward by deviating from the Bitcoin protocol. Economic prospects essentially equalize across different-sized mining pools—therefore, miners cannot derive additional competitive advantages by organizing into larger pools.

The Selfish Mining strategy, however, allows a "minority pool to obtain more revenue than the pool's fair share, that is, more than its ratio of the total mining power" [54]. The key to this strategy is causing honest miners to waste computational resources by working on a "stale public branch" for no reason:

> Selfish miners achieve this goal by selectively revealing their mined blocks to invalidate the honest miners' work. Approximately speaking, the selfish mining pool keeps its mined blocks private, secretly bifurcating the blockchain and creating a private branch. Meanwhile, the honest miners continue mining on the shorter, public branch… Consequently, selfish mining judiciously reveals blocks from the private branch to the public, such that the honest miners will switch to the recently revealed blocks, abandoning the shorter public branch. This renders their previous effort spent on the shorter public branch wasted, and enables the selfish poll to collect higher revenues by incorporating a higher fraction of its blocks into the blockchain [54].

The selfish mining pool thus gains a competitive advantage. Assuming the other honest miners are rational actors, they are then incentivized to join this selfish pool, causing it to eventually grow into the majority group. According to this study, the Bitcoin economy is vulnerable against attacks launched by a selfish mining pool with more than 33% of the network's total computing power—substantially lower than the current assumption of 50%. Once the selfish miners win a majority, they become the only creator of transaction blocks, thereby controlling the entire Bitcoin network [54]. This destroys the decentralized property of Bitcoin.

Many of these economic attacks are formulated from theoretic models, and it's unclear whether and how they will manifest in practice. However, these models highlight some of the vulnerabilities inherited by the Bitcoin protocol, which could certainly contribute to a loss of confidence in the cryptocurrency. So far, our analysis of Bitcoin's economic stability has assumed that social consensus is Bitcoin's root of value. Perhaps it is worth considering that Bitcoin also derives intrinsic value from its cutting-edge cryptography. Bitcoin is not only a form of money but also a digital payments system. Surely, that quality in and of itself holds value. After all, Bitcoin is a technological innovation that has many useful properties, provides a platform for financial innovation, and could very well change our social behavior regarding financial transactions—both online and offline. Ultimately, these aspects may allow Bitcoin to transcend the classical framework of how money obtains and retains value.

5. REGULATING BITCOIN

5.1. The Case of Silk Road

On Tuesday, October 1, 2013, the FBI arrested Ross Ulbricht from the San Francisco Public Library. The 29-year-old was the alleged operator and kingpin behind Silk Road, the online black market infamous for selling drugs and other illicit goods. Known as "Dread Pirate Roberts", Ulbricht was charged with narcotics trafficking, computer hacking, and money laundering, as well as ordering 6 murder-for-hires [55]. During the site's two-year lifespan, it generated more than 9.5 million Bitcoins in sales revenue, earning more than 600,000 Bitcoins purely from sales commissions. When the criminal indictment was filed, this totaled to approximately $1.2 billion in sales revenue and $80 million in commissions [55]. Between February of 2011 and July this year, Silk Road had 957,079 users worldwide [56].

Users accessed Silk Road using the Tor network, which conceals the IP addresses of computers using its network and renders user identities anonymous [55]. Once on the site, users could purchase illegal narcotics, pirated content, forged documents, and illegal services such as computer hacking and hired assassinations. The only form of payment accepted on Silk Road was Bitcoins, and each user held one or several Bitcoin addresses associated with her Silk Road account [55].

Although Ulbricht equipped Silk Road with various encryption and security tools to protect customers and vendors, the FBI was able to track down Ulbricht due to several mistakes he made. The indictment mentioned "security mistakes, including an IP address for a VPN server used by Ulbricht listed in the code on the Silk Road, mentions of time in Dread Pirate Roberts' posts on the site that identified his time zone, and postings on the Bitcoin Talk forum under the handle 'altoid', which was tied to Ulbricht's Gmail address" [57]. In fact, Ulbricht's downfall is attributed to human error (including the seizure of nine counterfeit IDs with his photograph at the US-Canadian border), rather than technical issues with Tor and Bitcoin [58]. Within a few days, authorities in the US, Sweden, and the UK arrested eight more individuals for their drug-related involvements in Silk Road. Due to the traceable nature of Bitcoin transactions, the FBI simply followed the money trail once they gained control of Silk Road's user accounts and reviews system [59].

Since his arrest, Ulbricht's LinkedIn profile has been widely cited as an explanation for why he operated Silk Road:

> I want to use economic theory as a means to abolish the use of coercion and aggression amongst mankind… The most widespread and systemic use of force is amongst institutions and governments, so this is my current point of effort. The best way to change a government is to change the minds of the governed, however. To that end, I am creating an economic simulation to give people a first-hand experience of what it would be like to live in a world without the systemic use of force [56].

In Silk Road forums, Dread Pirate Roberts often credited Ludwig von Mises of the Austrian School of Economics for providing him the philosophical motivations behind Silk Road [61]. Evidently, Ulbricht subscribed to similar libertarian ideologies in real life.

A month after the FBI bust, Silk Road 2.0 came online with a minor improvement over its predecessor: offering users the option to now use their PGP encryption key as an extra authentication feature [62]. A new administrator is now operating under the username Dread Pirate Roberts, who posted on Twitter that "you can never kill the idea of Silk Road" [62]. While some vendors are hesitant about joining this new Silk Road, other drug marketplaces like BMR and Sheep Marketplace have risen to the challenge of serving Silk Road's former user base [63].

In addition to Ulbricht's arrest, the FBI seized 26,000 Bitcoins from Silk Road customers—valued around $3.6 million at the time [64]. A few weeks later, the FBI successfully seized 144,000 Bitcoins (worth $28.5 million) from Ulbricht's stash of 600,000 Bitcoins, then worth more than $80 million [65]. Following the news of Silk Road's demise, the market price of Bitcoin fell from around $140 to $110, which was likely caused by former Silk Road users dumping their coins [66]. However, Bitcoin's speedy recovery back to a price of $130 is perhaps suggestive of its strength apart from its Silk Road affiliation.

The high-profile bust of Silk Road has brought to light many of the regulatory issues facing Bitcoin. On one hand, this incidence refutes the claim that the survival of the Bitcoin ecosystem relies primarily on illegal transactions. By removing its association from Silk Road, Bitcoin can finally become a credible currency. The chairman of the Bitcoin Foundation's regulatory affairs committee, Marco Santori, claims that this is "a watershed moment for Bitcoin…[whose] PR problem, with which it has struggled for the last year or so, is being addressed in a very direct way" [67]. On the other hand, this case also emphasizes the difficulties faced by regulators and law enforcers when it comes to this new age of digital libertarianism. Once the public grabs ahold of an idea, although specific instantiations of said idea can be regulated and eliminated, the idea itself is nearly impossible to extinguish.

5.2. The Government's Interest in Regulating Bitcoin

Over the past year, Bitcoin has come under increasing levels of public scrutiny. While users and investors alike have become enticed by Bitcoin's potential as a currency and digital payments system, governments and regulators have grown increasingly concerned with the risks posed by the cryptocurrency. In this section, we examine why governments—particularly the US government—are interested in regulating Bitcoin: its potential for criminal use and the dangerous lack of consumer protection measures.

A) Potential for Criminal Activity

A 2012 report leaked by the FBI deemed Bitcoin to be a potential "venue for individuals to generate, transfer, launder, and steal illicit funds with some anonymity" [68]. Due to Bitcoin's decentralized and deregulated nature, as well as its pseudonymous transactions, law enforcers will have more difficulty detecting illicit activities and discovering the real identities of users. These concerns are especially top-of-mind after the US government shut down Liberty Reserve earlier this year on charges of money laundering. A centralized digital currency based out of

Costa Rica, Liberty Reserve also promised its users privacy and anonymity, which resulted in "virtually all of Liberty Reserve's business [being] derived from suspected criminal activity" [69].

In addition to money laundering, illegal commerce involving drugs, child pornography, and counterfeit goods—as we saw with Silk Road and other imitators—is another major concern. A recent paper found that the biggest driver of Bitcoin transaction volume is Satoshi Dice, an online Bitcoin gambling site of questionable legality (see Appendix 7.11)[9]. More disturbingly, the recent creation of Assassination Market—"a kind of Kickstarter for political assassinations" [70]—shows that Bitcoin not only helps facilitate illicit activities but can also promote an anti-government agenda in the spirit of radical libertarianism. In fact, Silk Road and Assassination Market can both be seen as a tribute and return to the ideologies espoused by the Cypherpunk movement of the 1990s. In fact, the creator of Assassination Market calls himself a "crypto-anarchist" and "puts his faith in the mathematical promise of cryptography to trump the government's power" [70].

While these concerns are certainly valid, it is also important to remember that Bitcoin does have legitimate uses as a currency and global payments system: "among them e-commerce, remittances, and financial empowerment for people in the Third World" [84]. Thus, it would be unfair to condemn the currency and its law-abiding users for abusive actions undertaken by a small minority. Indeed, criminals also rely on cash payments to preserve anonymity—yet it would be unfathomable to ban cash in our society. Similarly, in the early days of the Internet, many individuals were concerned that it could be used for illicit purposes. However, in the long term, we have certainly reaped many more benefits from the Internet's legitimate and useful purposes [132]. Furthermore, Bitcoin is pseudonymous as opposed to being completely anonymous—a popular misconception. All transactions are made public on the blockchain ledger and the "network doesn't actively conceal the IP addresses from which transactions were initiated" [71]. Therefore, while it may be more difficult for law enforcers to trace illicit transactions, it is not impossible to unveil user identities on the network, as several studies have already shown [9][52].

Early this November, the Senate Committee on Homeland Security and Governmental Affairs held the first congressional hearing on Bitcoin after a three month-long investigation of the cryptocurrency. The panel recognized the currency's legitimate uses and acknowledged that despite some criminal usage, Bitcoins are "not in and of themselves illegal" [72]. In fact, the government representatives were surprisingly optimistic about Bitcoin's future, and recognized the need to maintain a healthy balance between being watchful and still encouraging financial innovation. Federal Reserve Chairman Ben Bernanke also sent a letter to senators stating that virtual currencies "may hold long-term promise, particularly if the innovations promote a faster, more secure, and more efficient payment system" [73]. Additionally, the Treasury's Financial Crimes Enforcement Network (FinCEN) found that "virtual currency transactions are still relatively small in value compared with global criminal proceeds" [73]. This support bodes well for Bitcoin's future. It appears that the recent Silk Road shutdown has given federal regulators more confidence in their ability to contain and combat criminal activity.

B) **Need for Consumer Protection**

As discussed earlier, the irreversibility of Bitcoin transactions is a double-edged sword: while this feature protects merchants from false chargebacks, it leaves users vulnerable to fraud. Once a user's Bitcoins are misplaced, stolen, or deleted, it is impossible to recover said coins. Over the past few years, there have been many large-scale attacks that have depleted users of their Bitcoin wealth. In 2012, hackers stole 24,000 BTC (then worth $250,000) from the Bitfloor exchange and executed several denial-of-service attacks against Mt. Gox [1]. Due to the difficulty of tracing Bitcoin transactions, it is extremely unlikely that the perpetrators will be found. More recently in October, online wallet service Inputs.io was the victim of two separate attacks. The wallet service lost a total of 4,100 Bitcoins, then worth $1.3 million [74]. The founder, who goes by the alias TradeFortress, has since been accused of staging this heist in order to steal his customers' money [75]. Earlier this summer, the SEC charged Trendon Shavers for implementing the first Bitcoin Ponzi scheme [76]. Shavers created Bitcoin Savings and Trust, which promised 7% weekly returns to its investors, stealing approximately 500,000 Bitcoins from his investors—worth more than $5.6 million at the time [74].

Although these incidences targeted different agents of the Bitcoin ecosystem, they have one thing in common: the perpetrators took advantage of the inherent irreversibility and lack of transparency in Bitcoin transactions. What this translates to is a shocking lack of consumer protection measures. A recent study found that "18 of 40 services they studied over three years closed 'with customer account balances often wiped out'… Less popular services were more likely to just disappear than popular exchanges—but popular exchanges were more likely to suffer security breaches" [74]. This lack of security can be blamed on these 3rd party services built on top of the Bitcoin platform—the underlying protocol has proved to be relatively resilient against security risks [1].

Fundamentally, does the government have a duty to protect consumers from themselves and if so, to what extent are protective measures necessary? Because the Bitcoin system itself does not provide any protective measures for its users, it may be up to regulators to implement such measures. Protecting consumers from large-scale fraud is a necessary step towards cementing Bitcoin's mainstream status. It is critical, however, that a fair balance is maintained between protecting consumers and preserving the integrity of Bitcoin's value proposition.

5.3. Bitcoin's Legal Classification

One of the biggest questions surrounding Bitcoin is its legality. The United States government has an "exclusive right to issue currency" [8]. Not only does the Constitution give Congress the power to coin money, but the Stamp Payments Act of 1862 also limits the ability of private parties to create money. It is presently unclear whether or not Bitcoil falls under the Act's purview—it depends on legal interpretation and whether or not case law is considered (ie. *Van Auken*) [8]. However, many academics argue that because the Act has not seen an updated court interpretation since 1899, it is not applicable to the relatively new invention of digital currencies. Assuming Bitcoin is a legal entity, it must first be classified within the existing legal framework before it can be regulated. Otherwise, new legislation may be necessary. Under existing classifications, Bitcoin may be regulated as a money transmitter business, a security or investment contract, a currency, a commodity, and/or an electronic fund transfer [8].

A money transmitter is defined as a business that "transmits funds from one person to another" and must obtain an operating license in 48 states and the District of Columbia [1]. Under the Bank Secrecy Act, money transmitters must register with FinCEN, keep customer records, and report all suspicious transactions. This, in conjunction with the USA Patriot Act, serves to prevent money laundering and terrorist financing [1]. Certain participants in the Bitcoin ecosystem, such as exchanges, may be subjected to these regulations.

It is also possible to classify and regulate Bitcoin as an investment contract. The landmark *SEC v. W.J. Howey Co.* case defined an investment security as a "contract, transaction or scheme whereby a person (1) invests his money in (2) a common enterprise and (3) is led to expect profits (4) solely from the efforts of the promoter or a third party" [8]. Bitcoin advocates commonly argue that the cryptocurrency does not meet any of these requirements (known as the Howey test), while opponents contend that it fulfills all of them. The jury is still out on this classification.

The economist George Selgin classifies Bitcoin as "synthetic-commodity money"—a hybrid between a commodity and a currency [1]. As a commodity, Bitcoin would fall under the purview of the Commodity Futures Trading Commission (CFTC). The Commodity Exchange Act defines commodities as all "goods and services…and all services, rights, and interests…in which contracts for future delivery are presently or in the future dealt in" [1]. While Bitcoin certainly falls under this definition, it is worth noting that it differs from traditional commodities like oil and gold because it lacks tangible, intrinsic value and government-backing. It is more difficult, however, to classify Bitcoin as a currency under an existing legal definition. Since Bitcoin does not legally belong to any one government or state, it falls outside of the legal definition of a foreign currency. Thus, it is questionable whether or not the CFTC can regulate Bitcoin under its foreign-exchange authority. Furthermore, the Securities Acts of 1933 and 1934 states that currency is safe, liquid, does not pose an investment risk to the public, and does not resemble a security. Although Bitcoin is a currency in the literal and practical sense, it does not necessarily fit under this existing legal definition [8].

Finally, Bitcoin may be regulated under the Electronic Fund Transfer Act (EFTA) and the Federal Reserve's Regulation E [1]. Both serves to outline the rights and responsibilities of financial institutions as well as consumers involved in electronic fund transfers. An electronic fund transfer is defined as "any transfer of funds, other than a transaction originated by check, draft, or similar paper instrument, which is initiated through an electronic terminal, telephonic instrument, or computer or magnetic tape so as to order, instruct, or authorize a financial institution to debit or credit an account" [1]. The Bitcoin ecosystem itself does not qualify as a financial institution, nor does it have a central agent authorized to debit and credit user accounts. Furthermore, it is unclear what counts as an account in the Bitcoin infrastructure—an individual Bitcoin address, a collection of addresses, or an account provided by a 3rd party wallet service? Like the previous classifications considered, these existing regulatory frameworks fail to consider the nature of decentralized and deregulated virtual currencies, such as Bitcoin.

Legal jargon aside, it is clear that classifying Bitcoin under existing laws is a difficult task. There is much room for interpretation when it comes to existing regulations, most of which were created when digital currencies did not exist in the financial regulatory landscape. As of August 2013, United States Magistrate Judge Amos Mazzant of the Eastern District of Texas gave Bitcoin its first legal ruling. This US district court ruling resulted from the SEC case filed against Trendon Shavers of Bitcoin Savings & Trust (BTCST). Shavers fought against his charges by arguing that Bitcoin is not an actual currency and therefore, should not be subjected to SEC regulations [79]. However, Judge Mazzant gave the following ruling:

> It is clear that Bitcoin can be used as money. It can be used to purchase goods or services, and as Shaves stated, used to pay for individual living expenses. The only limitation of Bitcoin is that it is limited to those places that accept it as currency. However, it can also be exchanged for conventional currencies, such as the US dollar, Euro, Yen, and Yuan. Therefore, Bitcoin is a currency or form of money, and investors wishing to invest in BTCST provided an investment of money [80].

The judge further added that Bitcoin investments "meet the definition of investment contract, and as such, are securities" [80]. This landmark ruling has paved the way for potential regulation of Bitcoin as a legal entity in the United States.

5.4. The Current State of Regulation

This section will describe the current regulatory environment, as of this writing. We focus mainly on regulatory efforts undertaken by the United States, which has been central to Bitcoin's adoption and growth to date [81].

While the true drivers behind Bitcoin's underlying transaction volume remain relatively ambiguous, it certainly undisputed that the cryptocurrency has enjoyed increasing traction and widespread media hype this previous year. Indeed, businesses small and large have begun to integrate Bitcoin into their business models in order to attract attention and tech-saavy customers. This past Black Friday, more than 400 online retailers offered discounts to customers who paid with the virtual currency [82]. A Bitcoin ATM recently opened in Vancouver and exceeded more than $1 million in transactions within its first month of operation [83]. Between April and June this year, venture capitalists have invested $12 million dollars in startups innovating on the Bitcoin platform [84]. The Bitcoin craze has also reached traditionally conservative industries: a Canadian miner Alix Resources Corp paid a drilling contractor in Bitcoins [85], Shanghai-based real estate developer Shanda Group started accepting Bitcoin payments, and the University of Nicosia became the world's first accredited university to accept Bitcoins for tuition [86][87]. Furthermore, Bitcoin's early adopter base has grown beyond its niche population of technology enthusiasts, libertarians, and small businesses looking to avoid high transaction fees, to include household names like Reddit, Virgin America, and Wordpress.

Bitcoin's relatively fast adoption can be attributed to its technical features: its decentralized nature and independence from governments as well as central banks, its clever proof-of-work solution to the double spending problem, the irreversibility of transactions, and the ability to facilitate transactions across borders with minimum transactions fees and near real-time confirmation [88]. The combination of Bitcoin's acceptance into the mainstream consciousness and its potential for criminal abuse has prompted the federal government to take a long, hard look at regulating Bitcoin.

The first federal agency to issue formal guidance on Bitcoin is the Financial Crimes Enforcement Network (FinCEN) of the Treasury Department. In March 2013, FinCEN issued regulatory guidance that treats virtual currency exchanges under the same anti-money-laundering requirements as traditional money transmitters, such as Western Union [77]. More specifically, FinCEN regulation stipulates that Bitcoin exchanges and miners based in the United States "should register as Money Service Businesses and comply with anti-money laundering regulations. Ordinary Bitcoin users don't have to register just to purchase goods and services" [78]. Following this, state regulators including the California Department of Financial Institutions, the Idaho Department of Financial Services, and the New York Department of Financial Services have all followed in FinCEN's footsteps, reinterpreting their existing guidelines to include Bitcoin exchanges and service providers [88].

Earlier this summer, the New York State Department of Financial Services subpoenaed 22 major Bitcoin businesses and investors based in the US, including venture capitalists, mining equipment manufacturers, exchanges, and online wallet services [89]. With the purpose of gathering information to decide whether new regulations are necessary, the Department requested the subpoenaed parties to disclose their customer protection practices, money laundering controls, and sources of funding. According to its press release, the Department—which has the authority to create new regulations if there are no other primary regulators—believes that adding the appropriate regulatory safeguards are paramount to consumer protection, national security, and the long-term viability of virtual currencies [89]. Furthermore, the Department is currently investigating the feasibility and policy implications of BitLicenses, which would require virtual currency companies operating in New York to comply with existing requirements for consumer protection and money laundering prevention [90]. The Department of Homeland Security and the FBI have also "adopted an aggressive posture to address the emerging threat and criminal exploitation of virtual currency systems" [91].

Other federal agencies have been slower to react. The Commodity Futures Trading Commission (CFTC) is still trying to determine if Bitcoin should be regulated as a commodity [91], and the Securities and Exchange Commission (SEC) has yet to definitively issue a statement classifying Bitcoin and other digital assets [88]. Meanwhile, the IRS has not yet tailored its tax regulations specifically to virtual currencies. A recent Government Accountability Office report pushed the IRS to issue guidelines that makes it clear to citizens that they must pay taxes on their Bitcoin transactions [92]. Otherwise, virtual currencies share many of the same characteristics as desirable tax havens—this potential for tax evasion certainly adds to the government's desire to regulate the cryptocurrency [93]. The IRS can be expected to draw guidance from its existing Bartering Tax Center, whereby Bitcoins transactions would be treated as bartering [78]. Based on existing IRS rules, individuals who sell goods or provide services for Bitcoin payments have income and must therefore report it. However, capital gains tax reporting depends on the CFTC's determination of Bitcoin as a commodity or currency [78]. Finally, Bernanke has stated in a recent letter to senators that the Federal Reserve has no plans to regulate Bitcoin because "it does not necessarily have authority to directly supervise or regulate these innovations or the entities that provide them to the market" [95].

5.5. Both Sides of the Regulation Coin

The Bitcoin community is divided on whether it thinks regulation is beneficial to Bitcoin in the long-term and will help bolster the currency's legitimacy, or if it will stifle innovation and stymy user adoption. For some like Adam Levine, the editor-in-chief of *Let's Talk Bitcoin,* "it seems inevitable that regulation will be a part of mainstream legitimacy for Bitcoin. The thought is, even if it changes it for the worse a little bit, it will gain much more in legitimacy" [67]. Indeed, regulation could help put in place much-needed consumer protection measures that are inherently lacking in the technical protocol. Bobby Lee, the CEO of BTC China, says that he "and many in the industry are actually in support of government regulation in this field", and believe that governments should at least clarify what licenses are necessary to operate certain types of Bitcoin businesses [95].

Others like Jerry Brito, director of the Mercatus Center Technology Policy program, have a more cynical outlook. First, regulatory measures may be futile against Bitcoin's technical design: the decentralized nature implies that there is no central authority to subpoena, no company to sue, and no servers to shut down. In addition, the pseudonymous nature presents a very real challenge for detecting illicit activity and tracking down culprits. And "while the state may be able to uncover the identity and punish the parties to a Bitcoin transaction…it will no longer be able to prevent those transactions from happening in the first place" [91]. Finally, most of the regulations so far have only dealt with 3rd party services and businesses that operate on top of the Bitcoin platform, such as exchanges and wallet services. In the case of illicit activity, the authorities can subpoena these 3rd party services into releasing customer identification and banking information. However, it remains to be seen if and how regulators can prohibit or control private transactions that occur directly between individuals on the Bitcoin network.

Furthermore, despite initial forays into Bitcoin regulation, "no official guidance or determination exists from any US federal regulator that establishes whether Bitcoins are a currency, commodity, commodity money, or security for the purpose of determining the tax treatment of Bitcoins and whether the SEC or CFTC would have any regulatory jurisdiction over them. The uncertainty surrounding Bitcoin's legal classification for regulatory purposes could potentially retard the currency's development in the United States" [88]. The CTO of BitPay, Stephen Pair, contends that this lack of clarity has resulted in the banking industry's cautious approach to Bitcoin and skepticism towards its future adoption [47]. Moving forward, regulators must be especially cognizant of how Bitcoin interacts with the existing structure of the financial industry and how it may potentially impact the business models of incumbent banks.

Despite this, the outlook presented at the recent congressional hearings held by the Senate Committees on Homeland Security and Banking was mostly positive, suggesting that the US government does not wish to stifle Bitcoin's growth. Opponents of Bitcoin regulation were especially concerned that high levels of regulatory oversight will drive entrepreneurs and start-ups overseas to more Bitcoin-friendly jurisdictions, such as Canada and the United Kingdom. Some of these fears are already manifesting in the Bitcoin investor and start-up communities. Despite the spike in Bitcoin-related investments this past spring, deal activity has since slowed down considerably due to the rising costs of regulatory compliance and the threat of increasing government regulation [33]. Not only is it time-consuming to obtain the necessary federal and state operating licenses, it can also cost these businesses roughly $1 million to $2 million to comply with these new regulations [33]. Some states even require businesses to put up a bond for as much as several million dollars [89]. Furthermore, these compliance measures detract from Bitcoin's inherent advantages by demanding a higher level of transparency and involving a 3rd party intermediary. Stan Stalnaker, a founding member of the Digital Asset Transfer Authority (DATA), advocates that a light-handed approach will "allow the digital asset ecosystem to develop to its full potential…An enormous amount of wealth creation is possible, along with the reduction of fraud and money-laundering through digital identification related to these assets" [47].

These prohibitive costs tied to regulation may cause Bitcoin's "center of gravity" to shift to other countries. The Bitcoin Foundation has recently considered moving its US-based headquarters overseas, and other players in the ecosystem (such as the UK-based Coinfloor exchange) have even banned American customers from fear of regulatory repercussions from the United States [81]. Other countries have adopted a more laissez faire approach, and are waiting to see if Bitcoin is here to stay for the long-haul before slapping on regulations. For example, the United Kingdom's Financial Conduct Authority has no plans as of yet to regulate Bitcoin exchanges. Similarly, FINTRAC—the Canadian counterpart to FinCEN—has assured Bitcoin businesses in Canada that they will be not required to register as money transmitters. Additionally, Canada Revenue Services have already published formal guidance on how digital assets should be treated under the Canadian tax code.

Recently, Bitcoin's popularity in China has skyrocketed and the cryptocurrency is the country's newest darling. Not only has China overtaken the United States for the most number of downloads of the Bitcoin client software [81], but Chinese transactions now account for over 50% of Bitcoin's total turnover volume [99]. The dominant search engine, Baidu, has also started accepting Bitcoin payments, further compounding the currency's hot demand. Although the central government has not recognized Bitcoin as a formal medium of exchange, it has allowed people to freely participate in the ecosystem. This is a significant concession because it runs counter to a law issued by the Ministry of Commerce and Ministry of Culture in 2009, which "outlawed the use of virtual currency in the real economy, specifically the exchange of such currency for goods and services, or the exchange of it for renminbi" [99]. However, not all countries have jumped on the Bitcoin bandwagon. Earlier this summer, Thailand banned Bitcoin "due to the lack of existing applicable laws, capital controls, and the fact that Bitcoin straddles multiple financial facets" [100].

During the Senate hearings, FinCEN director Jennifer Shasky Calvery warned that Bitcoin businesses fleeing US jurisdiction in search of less stringent regulations may only find short-lived gains abroad:

> Every country has an interest in protecting its financial system from illicit actors who launder money or move it on behalf of terrorist organizations, in collecting taxes and protecting investors and protecting consumers from fraud, and ensuring a stable economy. If this virtual payment system is going to survive and be a real player in the financial system, regulation, both at home and abroad is going to catch up, because it has to [101].

So far, the US government has not yet announced new legislative measures to control Bitcoin and other virtual currencies.

5.6. Fighting the Cryptowars with PGP

Perhaps the most interesting tale of the Cryptowars occurred in 1991, when Phil Zimmerman created a high-quality encryption program for emails and files called PGP ("Pretty Good Privacy"). Designed to be easy-to-use, PGP packaged public key cryptography into a mass-market product. Zimmerman created PGP in response to the US government's Senate Bill 266:

> It is the sense of Congress that providers of electronic communications services and manufacturers of electronic communications service equipment shall ensure that communications systems permit the government to obtain the plain text contents of voice, data, and other communications when appropriately authorized by law [104].

In other words, manufacturers would be forced to insert special backdoors into their products, giving the government access to anyone's encrypted messages [104]. Before this bill was eventually defeated due to public backlash from industry groups and libertarians, Zimmerman published PGP for free in the United States—as "guerrilla freeware", in his words [108].

Following this, a group of Cypherpunk activists uploaded PGP's source code online through different bulletin boards and Internet forums, which spread the software worldwide. This caught the attention of the US Department of Justice: since PGP was a high-strength encryption protocol, it was classified as munitions under the US government's International Traffic in Arms Regulations—and therefore illegal to export [109]. In February 1993, the Justice Department opened a criminal investigation on Zimmerman for allegedly violating export restrictions on cryptography [110].

This 3-year-long case became the quintessential battlefront of the Cryptowars: thousands of netizens rallied behind Zimmerman (some even donated to his legal defense fund), and industry groups continued to lobby furiously for more lenient regulations [110]. During this time, Zimmerman became the public face for the Cypherpunk movement, and PGP became a tangible manifestation of the movement's philosophy. In an especially comical act of defiance, Zimmerman published the PGP source code in its entirety into a physical book. Books were not subjected to export restrictions and "it would be politically difficult for the Government to prohibit the export of a book that anyone may find in a public library or a bookstore" [111]. The Department of Justice eventually dropped the investigation in 1996.

In the end, the many years of public backlash and the successful deployment of PGP—despite the government's best efforts—proved to be very effective. In 1999, the US government relaxed its stringent controls and export restrictions related to cryptography. The Cryptowars were finally over.

5.7. Cryptowars 2.0?

The Cryptowars are cited as the "Internet's first major victory against government attempts to control information online" [102]. In light of the recent NSA scandal this past year, however, it appears as if a second wave of the Cryptowars may be upon us. Edward Snowden recently released top-secret documents with the disturbing revelation that the NSA and its

British counterpart, the GCHQ, have been actively pursuing the governments' agenda to harness and control the power of cryptography [112]. In fact, the agencies cite "the use of ubiquitous encryption across the Internet" as its greatest obstacle to "accessing large amounts of Internet traffic for surveillance purposes" [112].

To combat this, the NSA uses supercomputers to break encryption algorithms by brute force, controls the way that international encryption standards are set, and "actively engages US and foreign IT industries to covertly influence and/or overtly leverage their commercial products' designs" [112]. This last aspect directly contradicts the promises made by Internet companies to protect their customers' data from the prying eyes of governments and criminals. The NSA and GCHQ have defended their actions as vital in their fight against terrorism, and "the ability to defeat encryption" as crucial to foreign intelligence gathering [112]. This recent episode brings to mind the cautionary proclamations told by the Cypherpunks nearly two decades ago.

After the Watergate scandal, Senator Frank Church warned citizens that the NSA's "capability at any time could be turned around on the American people, and no American would have any privacy left, such is the capability to monitor everything: telephone conversations, telegrams, it doesn't matter . . . there would be no place to hide" [105]. Now, it appears that this warning has become reality.

5.8. Along Came Bitcoin

When Bitcoin was first introduced in late 2008, its early adopters were primarily technology enthusiasts, cryptography experts, and radical libertarians. For these people, Bitcoin appeared to be the long-awaited answer to their troubles. Their interest in Bitcoin was motivated by their fear of government surveillance, and their imaginations were reignited by Bitcoin's potential for providing privacy and security in online transactions.

Indeed, Cypherpunks like Tim May and David Chaum had already imagined online markets in which people could transact anonymously. However, there has never been a true digital cash implementation that held true to the theoretical construct—until Bitcoin came along [106]. The most revolutionary feature of Bitcoin is the fact that it had successfully solved the double spending problem without the need for a trusted 3rd party. This decentralization protects the system from government interference because intermediaries are often "the regulatory chokepoints at which government can apply pressure" [106].

The Cryptowars were essentially a long exercise in answering the question: should the government restrict strong cryptography? Furthermore, is it even possible to regulate cryptography? While it is a valid concern that the technology could be exploited at the margin by terrorists and lesser criminals, cryptography has made us better off in the long run, with its benefits outweighing the risks [113]. This line of reasoning is certainly applicable to Bitcoin as a cryptocurrency—while drug lords may use Bitcoin to hide illicit transactions, Bitcoin also has many legitimate uses. In this digital age, privacy measures like encryption techniques and cryptocurrencies are essential elements protecting our freedom of speech [58].

And indeed, digital cash and computer software should be considered speech [110]. After all, spending money "is often a matter of communicating orders to others, to transfer funds, to release funds… In fact, most financial instruments are contracts or orders. Money is increasingly just speech" [115]. So Bitcoin is a form of speech, but couldn't it also be considered an act (the transaction itself), an idea (the knowledge and ideas behind its cryptographic protocol), as well as a physical product (the source code)? The likely answer is that Bitcoin is a combination of all these things. The ambiguity surrounding Bitcoin's fundamental properties is precisely what makes it so difficult to regulate or ban.

Software is easy to implement, to use, to transfer, and to distribute. As we saw with PGP, it is nearly impossible for the government to enforce a ban or regulate software in any meaningful way. Additionally, Cypherpunks Tim May and Michael Froomkin have argued that the difficulty of distinguishing digital cash from pure speech makes this a minefield of litigation involving violated statutory rights [116]:

> Restricting digital cash may impinge on free speech, as it is generally impossible to know before looking if a message is "pure speech" (whatever that is) or has significant digital cash aspects. And note that while money laundering and tax fraud are illegal, the U.S. relies almost exclusively on detection after the crime, as opposed to inspecting private communications for evidence of criminal behavior. For U.S. authorities to begin random inspections of messages, or to ban encryption, would almost certainly mean violations of the First and Fourth and maybe other Amendments [115].

These issues are further compounded by Bitcoin's decentralized and global nature, making it even harder to regulate or ban. Simply put, the Bitcoin ecosystem does not have a Phil Zimmerman counterpart that governments can easily subpoena and put to trial. This begs the question: can a pure technology even be regulated in this digital age? Perhaps only minimally.

Judging from the recent Senate hearings, it appears that the US government has no intention of banning Bitcoin. However, suppose that governments do succeed in regulating Bitcoin. And suppose that these regulations stifle innovation and curtail mainstream adoption to the extent that it leads to Bitcoin's demise. Even then, there are already several alternative cryptocurrencies ready to take its place. The community backing Bitcoin is driven by a vision of democratic freedom aided by cryptographic protections. This community of advocates will continue to innovate and improve on Bitcoin's flaws until the perfect digital currency has been created. Bitcoin is merely the first iteration and in its youth, has already unlocked a whole platform for financial innovation.

6. CONCLUSION

The creation of true digital cash "depends upon the marriage of economics and cryptography" [133]. The ingenuity of Satoshi Nakamoto's design certainly embodies this quality. As we have seen, Bitcoin possesses many of the critical elements desired of an ideal digital currency: it is secure, pseudonymous, portable, peer-to-peer, offline capable, and divisible. However, the most revolutionary aspect of this cryptocurrency is its deregulated and decentralized nature.

Still, Bitcoin isn't without its flaws. Not only are there technical and economic vulnerabilities within the Bitcoin protocol, but it also lacks the consumer protection measures necessary for widespread adoption. Perhaps the most concerning aspect of Bitcoin is its potential for abuse at the hands of cybercriminals and terrorists. It is certainly this last reality that has caught the attention of government regulators and law enforcers. Due to the novelty of Bitcoin's design, however, there is much ambiguity around its legal classification and its suitability for regulation.

Furthermore, Bitcoin is an instantiation of a larger, more powerful idea: cryptographic protocols can provide us privacy in a world where we are always being watched by Big Government, and our basic rights are consistently challenged by a state that is supposed to protect us. And ideas are very powerful constructs—once an idea becomes accepted by the people, it takes on a life of its own. Just like how "you can never kill the idea of Silk Road", it seems highly unlikely that governments could ever kill the idea of Bitcoin.

7. APPENDIX

7.1. ECDSA Algorithm [120]

The key generation and signature generation procedures are done by entity A. To verify his signature, entity B uses the signature verification algorithm. All of the following equations are taken from Johnson and Menezes' paper on ECDSA.

Key Generation

1. Select elliptic curve $E(\mathbb{Z}_p)$. The number of points on this elliptic curve should be divisible by a large prime n.
2. Select point $P \in E(\mathbb{Z}_p)$ of order n
3. Compute $Q = dP$
4. A's public key = (E, P, n, Q)
5. A's private key = (d)

Signature Generation (to sign a message m)

1. Select an integer k in the interval [1, n-1]
2. Compute $kP = (x_1, y_1)$
3. Compute $r = x_1 \ mod \ n$ → if r = 1, return to Step 1; otherwise, proceed.
4. Compute $k^{-1} \ mod \ n$
5. Compute $s = k^{-1}[h(m) + dr]$ where h is the SHA-1 hash function → if s = 0, return to Step 1; otherwise, proceed.
6. The signature for $m = (r, s)$

Signature Verification

1. Obtain A's public key (E, P, n, Q)
2. Verify that $1 \leq \ r, s \leq n - 1$
3. Compute $w = \ s^{-1} \ mod \ n$ and $h(m)$
4. Compute $u_1 = h(m)w \ mod \ n$
5. Compute $u_2 = \ rw \ mod \ n$
6. Compute $u_1 P + \ u_2 Q = (x_0 + y_0)$
7. Compute $v = \ x_0 \ mod \ n$
8. Accept the signature as valid IFF $v = r$

7.2. ECDSA Point Addition and Multiplication [121]

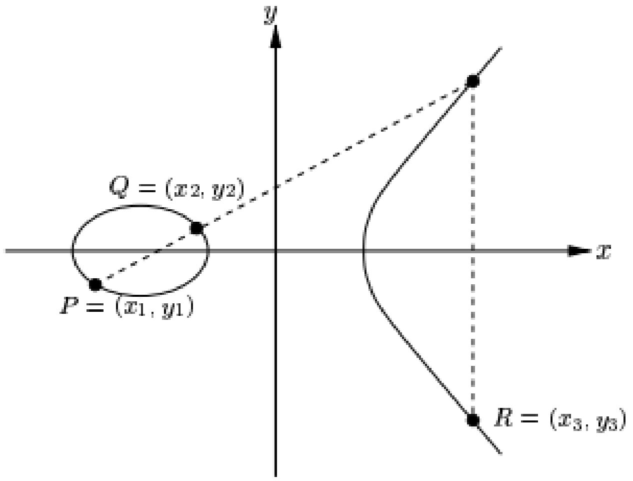


Fig. 1. Geometric description of the addition of two distinct elliptic curve points: $P + Q = R$.

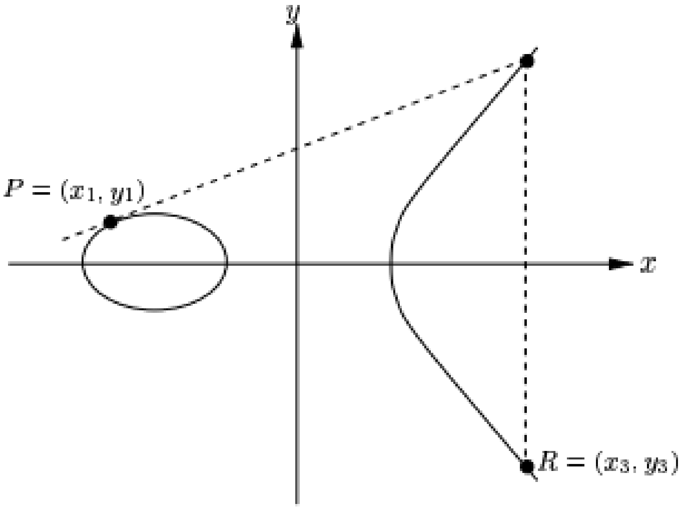
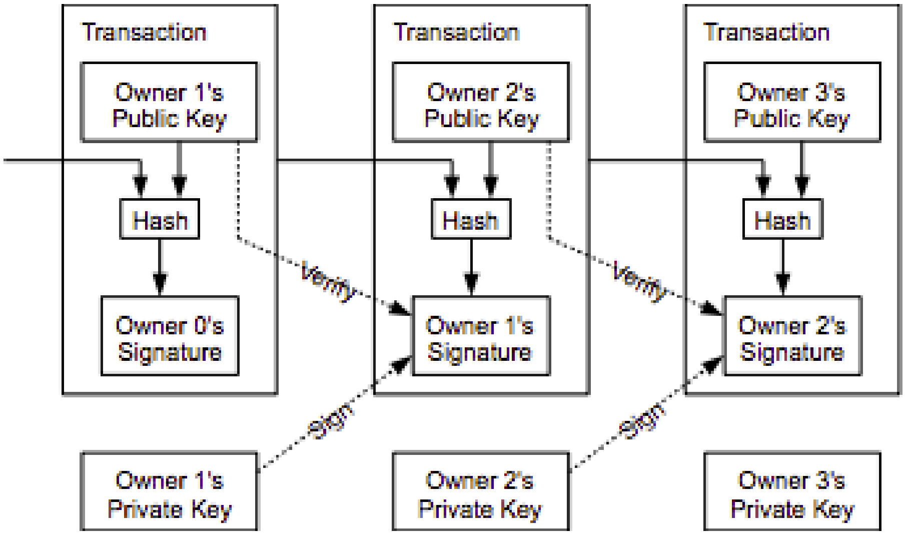
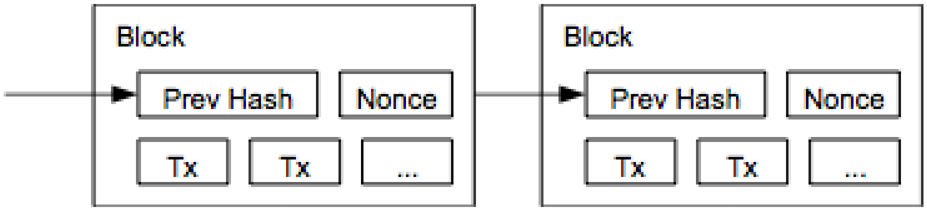


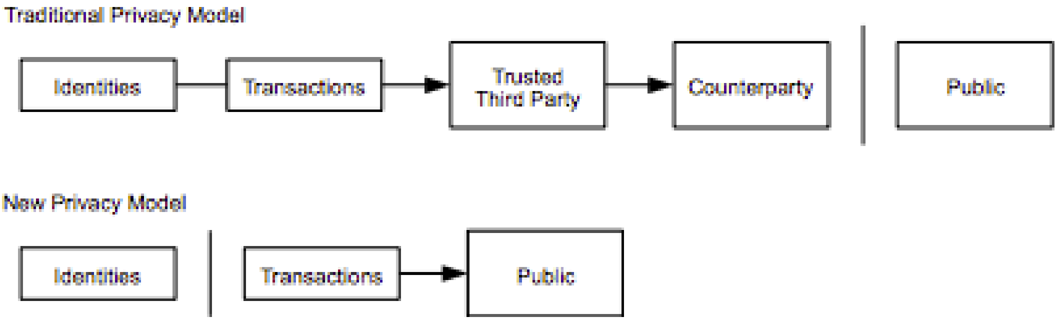
Fig. 2. Geometric description of the doubling of an elliptic curve point: $P + P = R$.

7.3 Blockchain Mechanism [4]



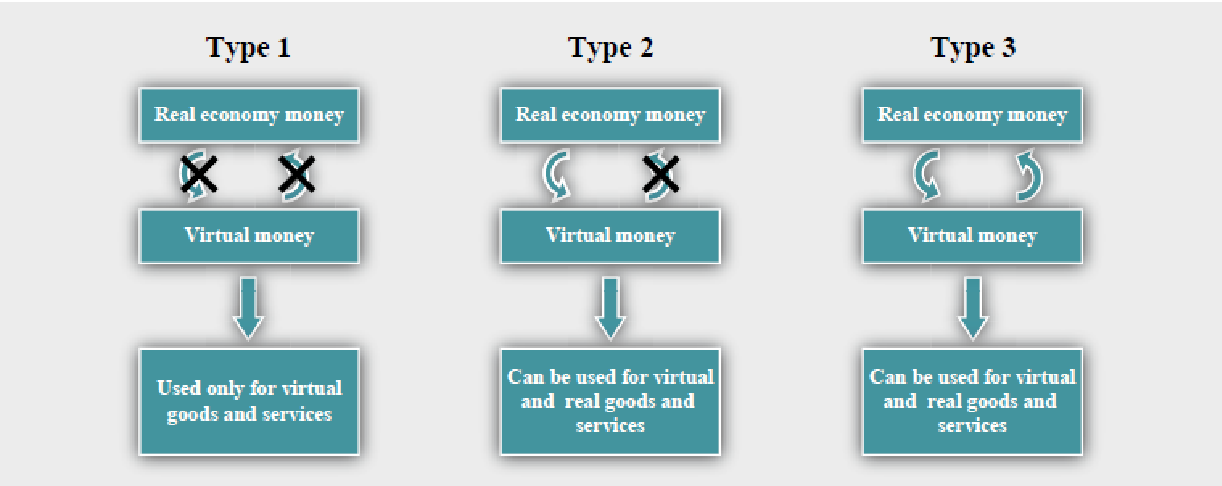


7.4. Privacy in Financial Transactions [4]



7.5. Virtual Currency Schemes [25]

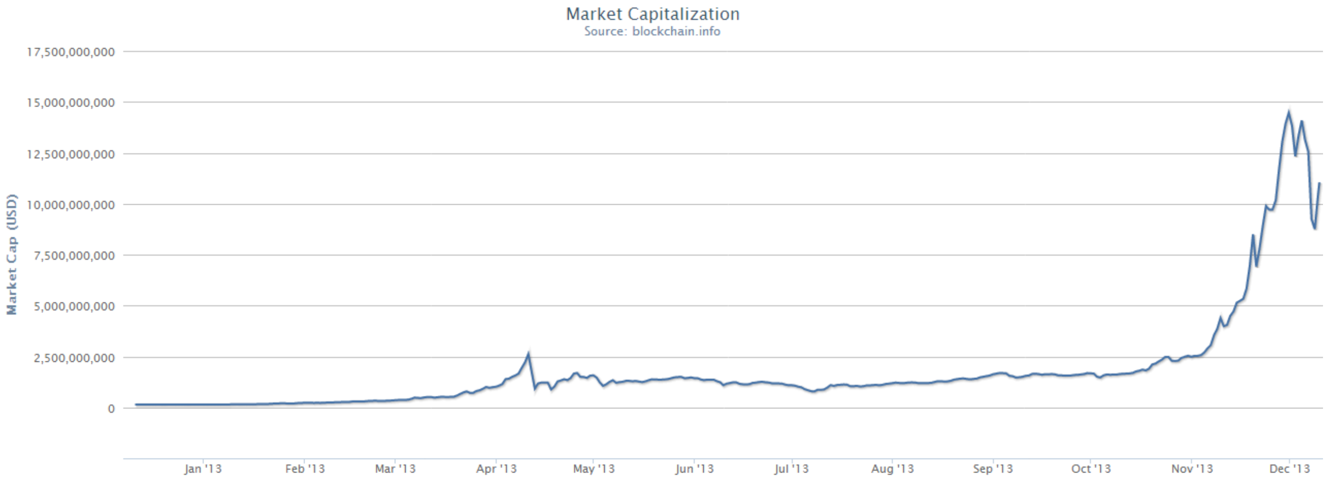
Chart 2 Types of virtual currency scheme


Type 1
Real economy money
Virtual money
Used only for virtual goods and services
Type 2
Real economy money
Virtual money
Can be used for virtual and real goods and services
Type 3
Real economy money
Virtual money
Can be used for virtual and real goods and services

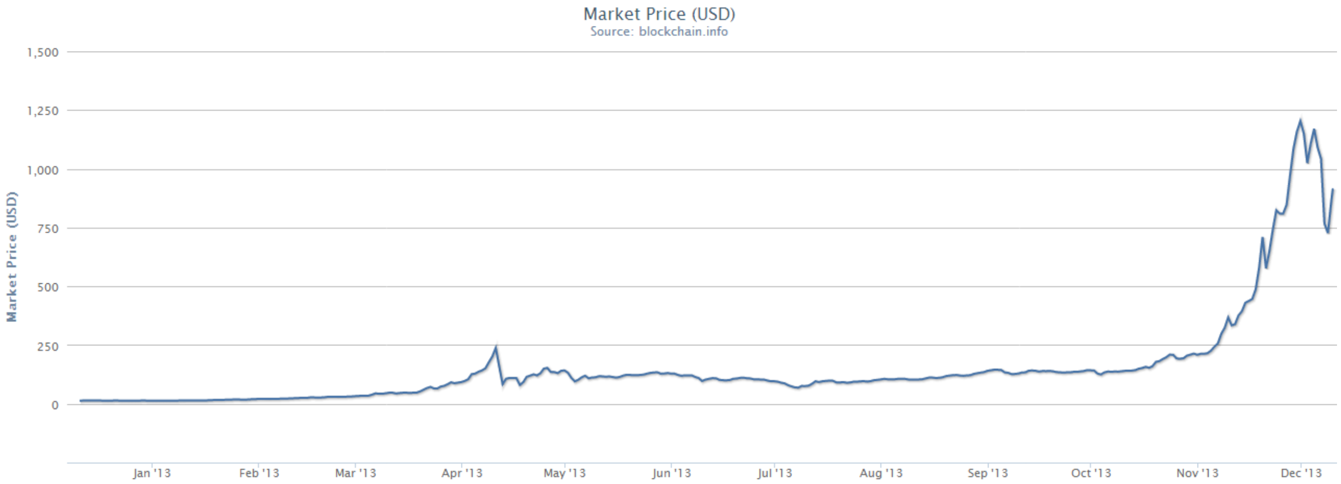
Source: ECB.
Note: A subscription fee may be required for Type 1.

7.6. Current Bitcoin Economy [53]

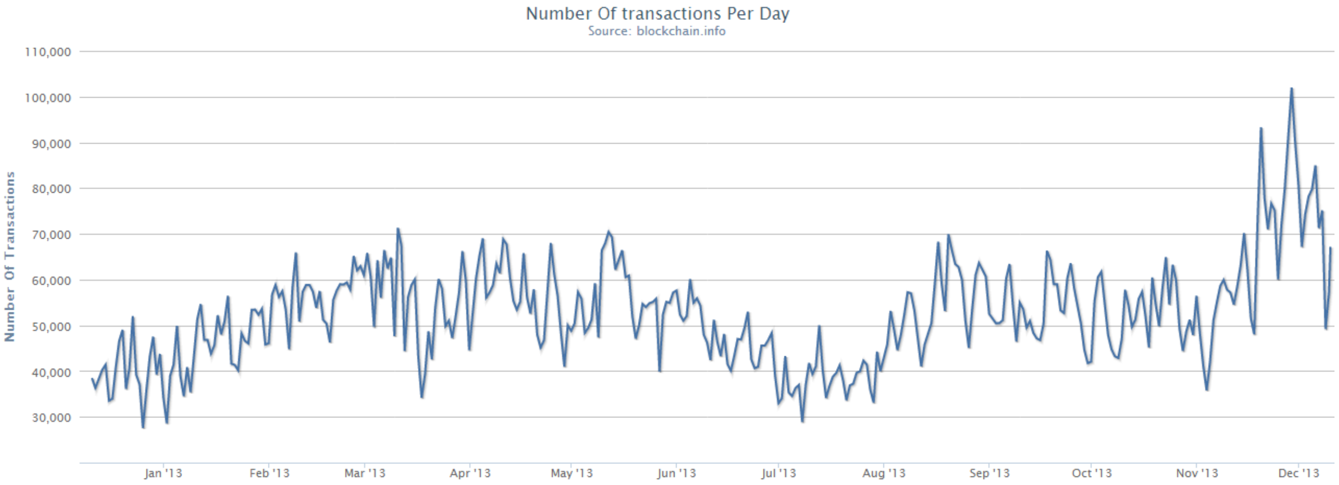
All charts are current as of Monday, December 9, 2013.


Market Capitalization

Source: blockchain.info


Market Price (USD)

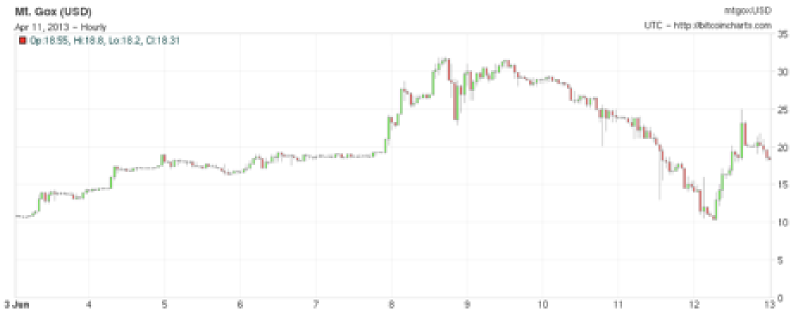
Source: blockchain.info


Number Of transactions Per Day

Source: blockchain.info

7.7. Recent History of Bitcoin Price Crashes [36]

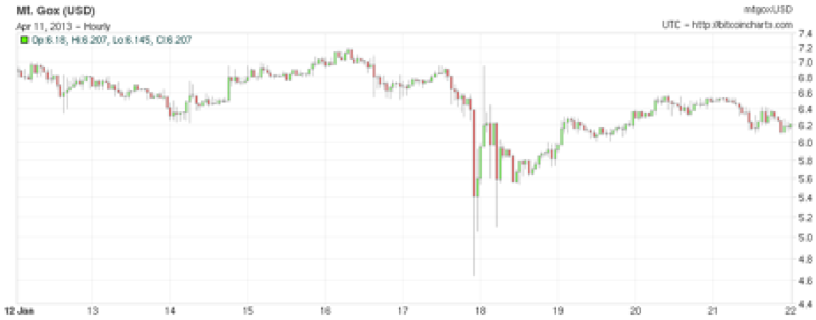
June 8-12, 2011



Peak price: $32

Price decline: 68 percent

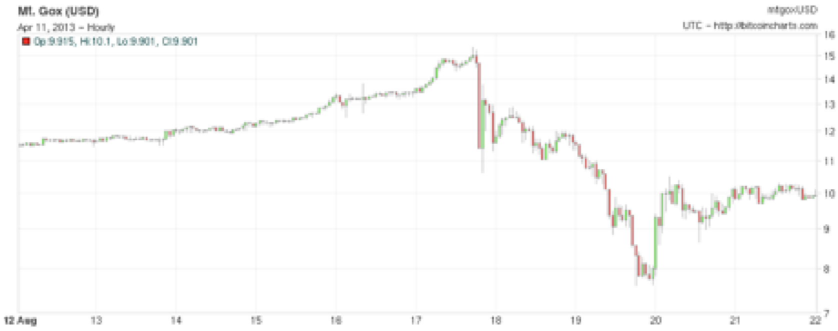
January 17, 2012



Peak price: $7.20

Price decline: 36 percent

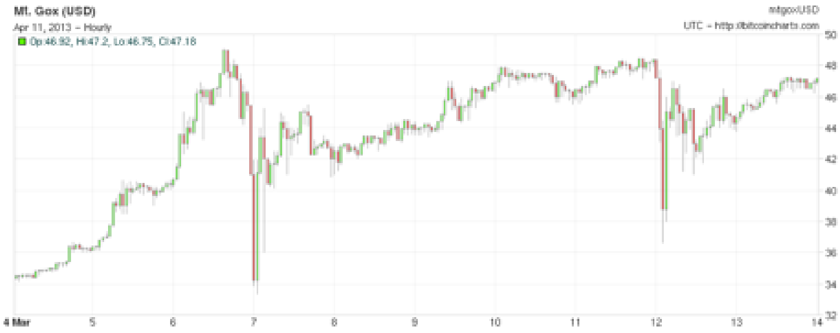
August 17-19, 2012



Peak price: $15.25

Price decline: 51 percent

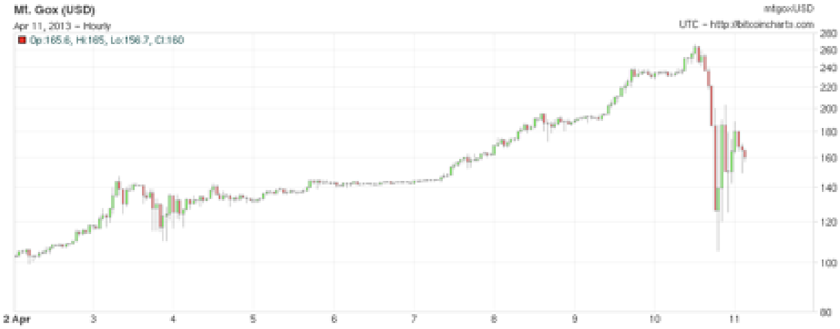
March 6 and 11, 2013



Peak price: $49

Price decline: 33 percent

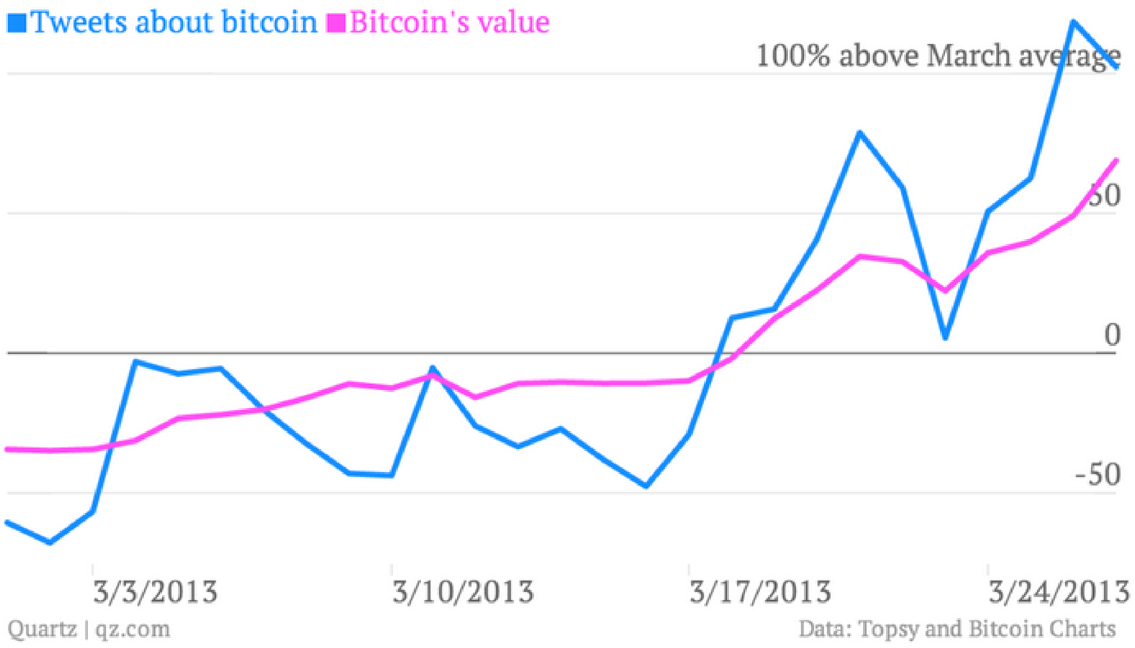
April 10, 2013



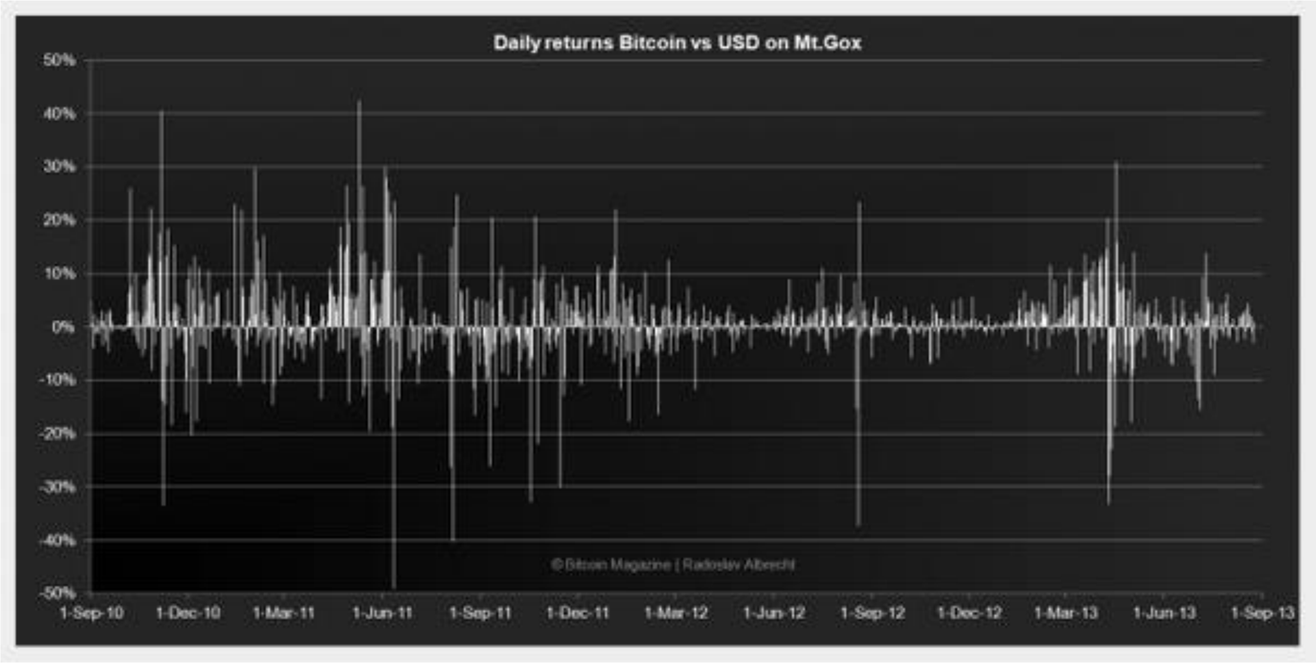
Peak price: $266

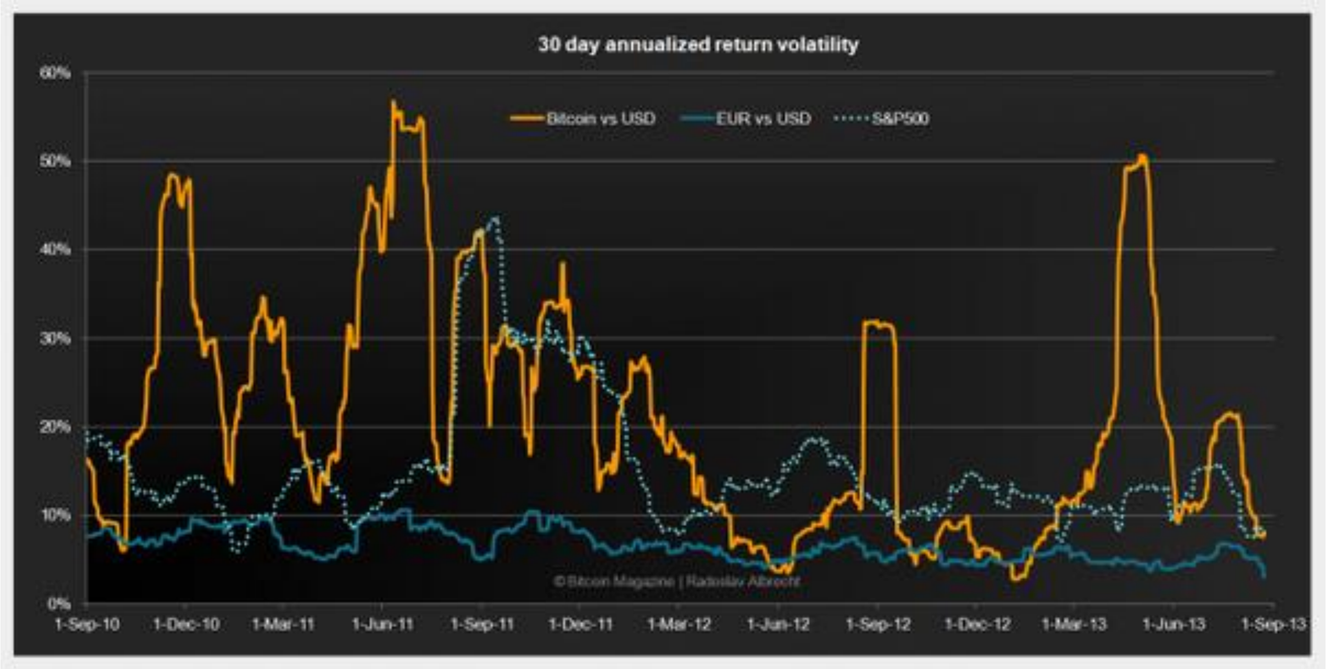
Price decline: 61 percent

7.8. Bitcoin Value vs. Twitter Mentions [42][156]

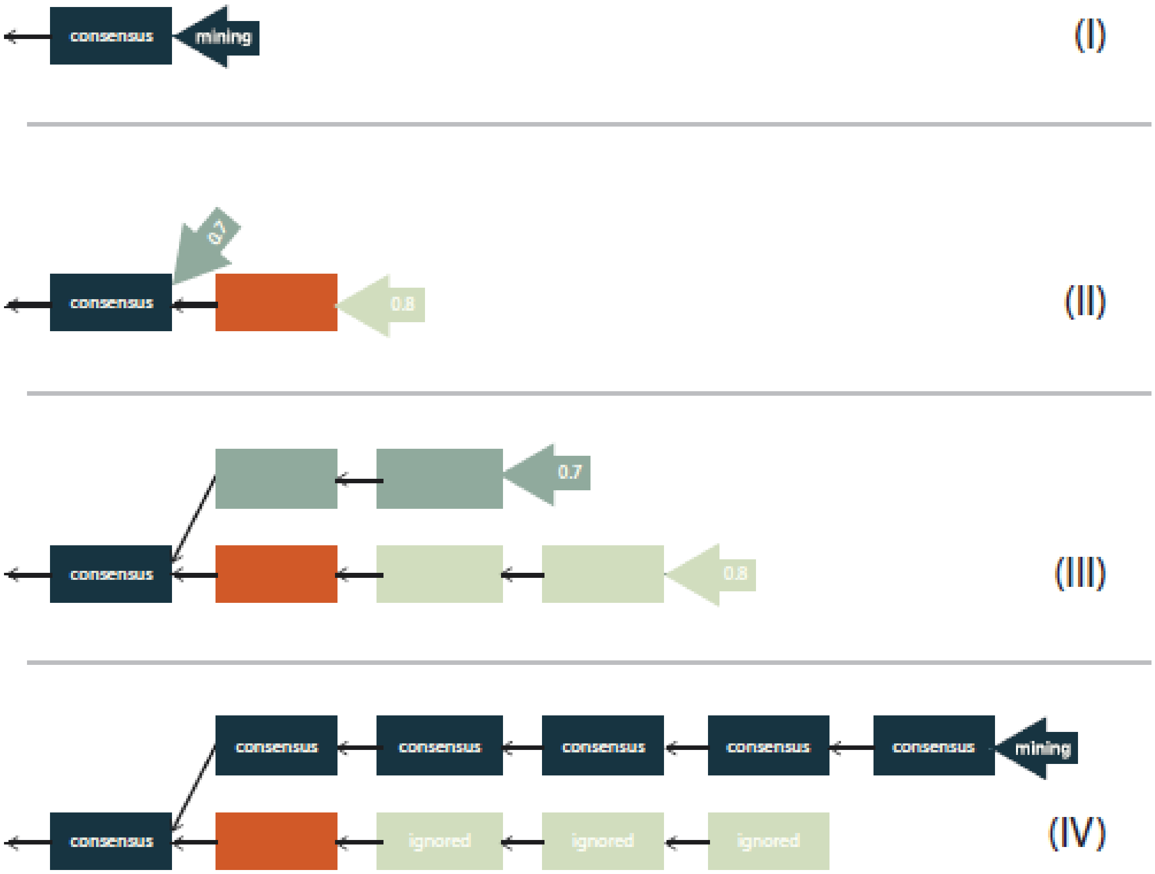


7.9. Bitcoin's Volatility [43]

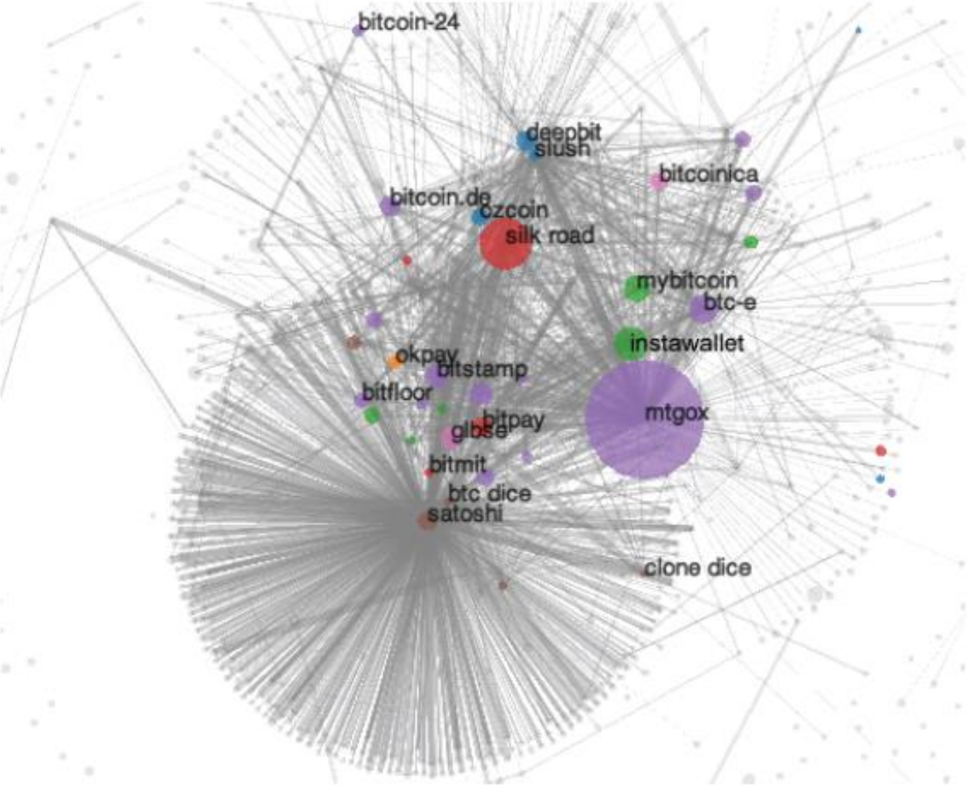


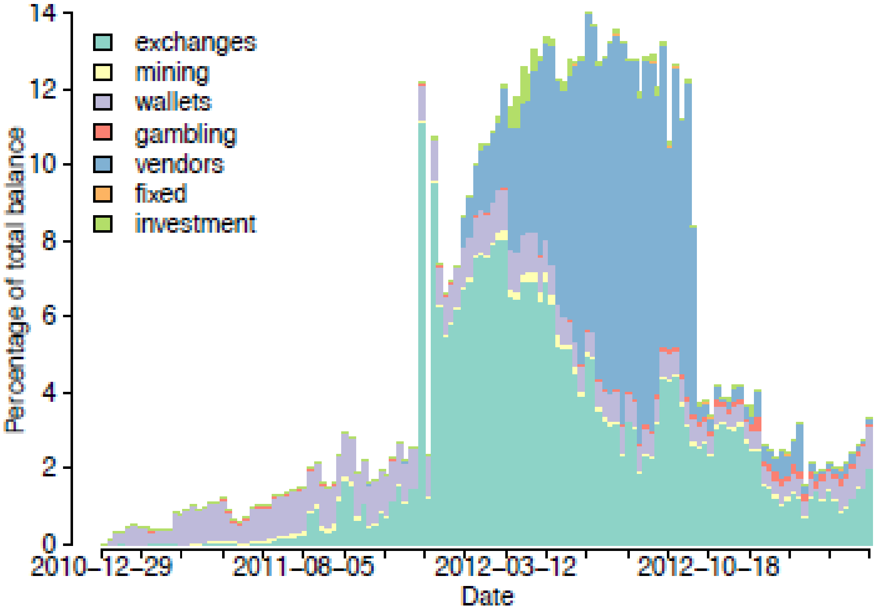


7.10. Schematic of March 2013 Hard Fork [5]



7.11. Visualization of Bitcoin's User Network [9]





Works Referenced

[1] Brito J., & Castillo, A. (2013). Bitcoin: A Primer for Policymakers.
Retrieved from http://mercatus.org/sites/default/files/Brito_BitcoinPrimer_embargoed.pdf.

[2] Barber, S., Boyen, X., Shi, E., & Uzun, E. (2012). Bitter to Better: How to Make Bitcoin a Better Currency.
In *Financial Cryptography and Data Security* (pp. 399-414). Springer Berlin Heidelberg.
Retrieved from http://crypto.stanford.edu/~xb/fc12/bitcoin.pdf.

[3] Katz, J., & Lindell, Y. (2008). *Introduction to Modern Cryptography*. CRC Press.

[4] Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system.
Retrieved from http://bitcoin.org/bitcoin.pdf.

[5] Kroll, J. A., Davey, I. C., & Felten, E. W. (2013). The Economics of Bitcoin Mining or, Bitcoin in the Presence of Adversaries. In *Proceedings of WEIS 2013*.
Retrieved from http://weis2013.econinfosec.org/papers/KrollDaveyFeltenWEIS2013.pdf.

[6] Back, A. (2002). Hashcash: a denial of service counter-measure.
Retrieved from http://www.hashcash.org/papers/hashcash.pdf.

[7] Wallace, B. (2011, November 23). The Rise and Fall of Bitcoin. *Wired.*
Retrieved from http://www.wired.com/magazine/2011/11/mf_bitcoin/.

[8] Grinberg, R. (2012). Bitcoin: an Innovative Alternative Digital Currency. *Hastings Science and Technology Law Journal*, *4*, 159. Retrieved from http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1817857.

[9] Meiklejohn, S., Pomarole, M., Jordan, G., Levchenko, K., McCoy, D., Voelker, G. M., & Savage, S. (2013, October). A fistful of bitcoins: characterizing payments among men with no names. In *Proceedings of the 2013 Internet Measurement Conference* (pp. 127-140). ACM.
Retrieved from http://cseweb.ucsd.edu/~smeiklejohn/files/imc13.pdf.

[10] Ron, D., & Shamir, A. (2012). Quantitative Analysis of the Full Bitcoin Transaction Graph. *IACR Cryptology ePrint Archive*, *2012*, 584. Retrieved from http://eprint.iacr.org/2012/584.pdf.

[11] Matonis, J. (2013, May 24). Top 10 Bitcoin Merchant Sites. *Forbes.* Retrieved from
http://www.forbes.com/sites/jonmatonis/2013/05/24/top-10-bitcoin-merchant-sites/.

[12] Greenberg, A. (2011, June 14). WikiLeaks Asks for Anonymous Bitcoin Donations. *Forbes.*
Retrieved from http://www.forbes.com/sites/andygreenberg/2011/06/14/wikileaks-asks-for-anonymous-bitcoin-donations/.

[13] Bancroft, W. (2013, October 28). Bitcoin hits $200 but where did this digital money trend really start?. *Pandodaily.* Retrieved from http://pandodaily.com/2013/10/28/bitcoin-hits-200-but-where-did-this-digital-money-trend-really-start/.

[14] Sullivan, B. (2007, May 2). Feds accuse E-Gold of helping cybercrooks. *NBC News*.
Retrieved from http://www.nbcnews.com/technology/feds-accuse-e-gold-helping-cybercrooks-6C10406525?franchiseSlug=technolog.

[15] Villasenor, J., Monk, C., & Bronk, C. (2011). Shadowy Figures: Tracking Illicit Financial Transactions in the Murky World of Digital Currencies, Peer-to-peer Networks, and Mobile Device Payments. Brookings Institution.
Retrieved from http://bakerinstitute.org/media/files/Research/d9048418/ITP-pub-FinancialTransactions-082911.pdf.

[16] Wenzel, R. (2013, April 10). Bitcoiners: Remember What Happened to eGold. *Economic Policy Journal.* Retrieved from http://www.economicpolicyjournal.com/2013/04/bitcoiners-remember-what-happened-to.html.

[17] GoldMoney is No Longer…Money. (2011, December 20). *The Bitcoin Trader.* Retrieved from http://www.thebitcointrader.com/2011/12/goldmoney-is-no-longer-money.html.

[18] IBIS*World* Business Environment Profiles. (2013, May). *E-commerce sales*. Retrieved from IBIS*World* database.

[19] IBIS*World* Industry Report 45411a. (2013, October). *E-Commerce and Online Auctions in the US.* Retrieved from IBIS*World* database.

[20] Jackson, E. M. (2012, October 27). How eBay's purchase of PayPal changed Silicon Valley. *VentureBeat.* Retrieved from http://venturebeat.com/2012/10/27/how-ebays-purchase-of-paypal-changed-silicon-valley/#8cV8y19jcBArQLfE.99.

[21] Zielke, B. (2011, March 2). Why Credit Cards Are Not the Future of Online Payment. *Mashable*. Retrieved from http://mashable.com/2011/03/02/credit-card-decline/.

[22] Mendelson, S. (2011, November). Micropayments' big future. *Financial World*. Retrieved from http://fw.ifslearning.ac.uk/archive/2011/november/features/micropaymentsbigfuturesammendelson.aspx.

[23] Value Partners. (2011, January). *Capturing the Micropayments Opportunity.* Retrieved from http://www.valuepartners.com/downloads/PDF_Comunicati/Perspective/estrattomicropayments(1).pdf.

[24] Bridges, T. (2012, July 5). Micropayments on the rise in Europe. *Rude Baguette.* Retrieved from http://www.rudebaguette.com/2012/07/05/micropayments-on-the-rise-in-europe/.

[25] European Central Bank. (2012, October). *Virtual Currency Schemes*. Retrieved from www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf.

[26] Van Grove, J. (2013, July 10). Forget Zynga: Facebook's games business stronger than ever. *CNET.* Retrieved from http://news.cnet.com/8301-1023_3-57592957-93/forget-zynga-facebooks-games-business-stronger-than-ever/.

[27] Cohen, D. (2013, September 13). Farewell, Facebook Credits. *AllFacebook*. Retrieved from http://allfacebook.com/farewell-facebook-credits_b125016.

[28] Lahart, J. (2008, May 16). Bernanke's Bubble Laboratory. *The Wall Street Journal.* Retrieved from http://online.wsj.com/news/articles/SB121089412378097011.

[29] Shiller, R. J. (2012, July 23). Bubbles without Markets. *Project Syndicate.* Retrieved from http://www.project-syndicate.org/commentary/bubbles-without-markets.

[30] Varian, H. R. (2004, January 15). Why is That Dollar Bill in Your Pocket Worth Anything?. *The New York Times*. Retrieved from http://www.nytimes.com/2004/01/15/business/15scene.html.

[31] Glasner, D. (2011, July 25). The Paradox of Fiat Money. *Uneasy Money.* Retrieved from http://uneasymoney.com/2011/07/25/the-paradox-of-fiat-money/.

[32] Shostak, F. (2004, January 20). How Does Money Acquire its Value?. *Ludwig von Mises Institute.* Retrieved from http://mises.org/daily/1430.

[33] Chernova, Y. (2013, October 23). Flurry of Bitcoin Venture Capital Deals Gives Way to Quiet. *The Wall Street Journal.* Retrieved from http://blogs.wsj.com/venturecapital/2013/10/23/flurry-of-bitcoin-venture-capital-deals-gives-way-to-quiet/.

[34] Vitalik, B. (2012, September 11). BitPay Exceeds 1,000 Merchants: An Interview with Tony Gallippi. *Bitcoin Magazine.* Retrieved from http://bitcoinmagazine.com/2298/bitpay-exceeds-1000-merchants-accepting-bitcoin/.

[35] Lomas, N. (2013, September 16). BitPay Passes 10,000 Bitcoin-Accepting Merchants On Its Payments Processing Network. *Techcrunch.* Retrieved from http://techcrunch.com/2013/09/16/bitpay-10000-merchants/.

[36] Lee, T. L. (2013, April 11). An Illustrated History of Bitcoin Crashes. *Forbes.* Retrieved from http://www.forbes.com/sites/timothylee/2013/04/11/an-illustrated-history-of-bitcoin-crashes/.

[37] Simonite, T. (2013, April 15). Bitcoin Isn't the Only Cryptocurrency in Town. *MIT Technology Review.* Retrieved from http://www.technologyreview.com/news/513661/bitcoin-isnt-the-only-cryptocurrency-in-town/.

[38] Yamada, K. (2013, August 2). 3 Bitcoin Alternatives Tested & Compared: Litecoin, Feathercoin, and Terracoin. *MakeUseOf.* Retrieved from http://www.makeuseof.com/tag/3-bitcoin-alternatives-tested-compared-litecoin-feathercoin-and-terracoin/.

[39] Knittel, C. R., & Pindyck, R. S. (2013, April). The Simple Economics of Commodity Price Speculation. *MIT CEEPR, Working Paper*. Retrieved from http://web.mit.edu/ceepr/www/publications/workingpapers/2013-006.pdf.

[40] Kennedy II, J. P. (2012, April 10). The High Cost of Gambling on Oil. *The New York Times.* Retrieved from http://www.nytimes.com/2012/04/11/opinion/ban-pure-speculators-of-oil-futures.html?_r=0.

[41] Fawley, B. W., & Juvenal, L. (2011, July). Commodity Price Gains: Speculation vs. Fundamentals. *The Regional Economist.* Retrieved from http://www.stlouisfed.org/publications/re/articles/?id=2122.

[42] Salmon, F. (2013, November 27). The Bitcoin Bubble and the Future of Currency. *Medium.* Retrieved from https://medium.com/money-banking/2b5ef79482cb.

[43] Albrecht, R. (2013, August 27). Bitcoin Volatility: The 4 Perspectives. *Bitcoin Magazine.* Retrieved from http://bitcoinmagazine.com/6543/bitcoin-volatility-analysis/.

[44] Hollander, J. (2013, November). Invest in Bitcoin: After Silk Road Bust, Canada and China Are Betting on Bitcoin. *Bustle.* Retrieved from http://www.bustle.com/articles/7898-invest-in-bitcoin-after-silk-road-bust-canada-and-china-are-betting-on-bitcoin.

[45] Brito, J. (2013, April 5). Why Bitcoin's Valuation Doesn't Really Matter. *Technology Liberation Front.* Retrieved from http://techliberation.com/2013/04/05/why-bitcoins-valuation-doesnt-really-matter/.

[46] How Volatile is Bitcoin?. (2013, August 27). *Ed and Ethan.* Retrieved from http://edandethan.com/how-volatile-is-bitcoin/.

[47] Bradbury, D. (2013, November 20). Bitcoin Faces Regulatory Push in Senate Banking Committee Hearing. *CoinDesk.* Retrieved from http://www.coindesk.com/bitcoin-regulatory-push-senate-banking-committee-hearing/.

[48] Dorrier, J. (2013, November 17). After Bubble and Crash, Volatile Virtual Currency Bitcoin Marks New High. *Singularity Hub.* Retrieved from http://singularityhub.com/2013/11/17/after-bubble-and-crash-volatile-virtual-currency-bitcoin-marks-new-highs/.

[49] Archer, P. (2013, June 6). Go Fork Yourself: Life After a Bitcoin Hard Fork. *The Genesis Block.* Retrieved from http://thegenesisblock.com/go-fork-yourself-life-after-a-bitcoin-hard-fork/.

[50] Andresen, G. (2013, March 20). Bitcoin Improvement Proposal #50. *Bitcoin Wiki.* Retrieved from https://en.bitcoin.it/wiki/BIP_50.

[51] Buterin, V. (2013, March 12). Bitcoin Network Shaken by Blockchain Fork. *Bitcoin Magazine.* Retrieved from http://bitcoinmagazine.com/3668/bitcoin-network-shaken-by-blockchain-fork/.

[52] Androulaki, E., Karame, G., Roeschlin, M., Scherer, T., & Capkun, S. (2012). Evaluating User Privacy in Bitcoin. *IACR Cryptology ePrint Archive*, *2012*, 596. Retrieved from http://eprint.iacr.org/2012/596.pdf.

[53] Charts from Blockchain.info. Retrieved from http://blockchain.info/.

[54] Eyal, I., & Sirer, E. G. (2013, November 5). Majority is not Enough: Bitcoin Mining is Vulnerable. *arXiv preprint arXiv:1311.0243*. Retrieved from http://arxiv.org/pdf/1311.0243v4.pdf.

[55] Ulbricht v. United States. (2013, September 27).
Retrieved from http://www1.icsi.berkeley.edu/~nweaver/UlbrichtCriminalComplaint.pdf.

[56] Statt, N. (2013, October 2). FBI seizes online drug marketplace Silk Road, outs owner in indictment. *CNET.* Retrieved from http://news.cnet.com/8301-1023_3-57605685-93/fbi-seizes-online-drug-marketplace-silk-road-outs-owner-in-indictment/.

[57] Greenberg, A. (2013, October 2). End of the Silk Road: FBI Says It's Busted the Web's Biggest Anonymous Drug Black Market. *Forbes.* Retrieved from http://www.forbes.com/sites/andygreenberg/2013/10/02/end-of-the-silk-road-fbi-busts-the-webs-biggest-anonymous-drug-black-market/.

[58] Higgins, P. (2013, October 6). Why You Can't Blame Bitcoin for Silk Road Shadiness. *Gizmodo.* Retrieved from http://www.gizmodo.com.au/2013/10/why-you-cant-blame-bitcoin-for-silk-road-shadiness/.

[59] Associated Press. (2013, October 8). Silk Road drug busts: 8 more arrested. *USA Today.*
Retrieved from http://www.usatoday.com/story/news/world/2013/10/08/silk-road-busts/2946925/.

[60] Estes, A. C. (2013, November 13). What Will Kill Bitcoin First?. *Gizmodo.*
Retrieved from http://gizmodo.com/what-will-kill-bitcoin-first-1463639878.

[61] Hume, T. (2013, October 5). How FBI caught Ross Ulbricht, alleged creator of criminal marketplace Silk Road. *CNN.* Retrieved from http://www.cnn.com/2013/10/04/world/americas/silk-road-ross-ulbricht/.

[62] Greenberg, A. (2013, November 6). Silk Road 2.0 Launches, Promising a Resurrected Black Market for The Dark Web. *Forbes.* Retrieved from http://www.forbes.com/sites/andygreenberg/2013/11/06/silk-road-2-0-launches-promising-a-resurrected-black-market-for-the-dark-web/.

[63] Berkman, F. (2013, October 22). Despite FBI Bust, Top Silk Road Drug Dealer Lives On. *Mashable.* Retrieved from http://mashable.com/2013/10/22/silk-road-vendor/.

[64] Greenberg, A. (2013, October 25). FBI Says It's Seized $28.5 Million in Bitcoins From Ross Ulbricht, Alleged Owner of Silk Road. *Forbes.*
Retrieved from http://www.forbes.com/sites/andygreenberg/2013/10/25/fbi-says-its-seized-20-million-in-bitcoins-from-ross-ulbricht-alleged-owner-of-silk-road/.

[65] Hern, A. (2013, October 7). FBI struggles to seize 600,000 Bitcoins from alleged Silk Road founder. *The Guardian.* Retrieved from http://www.theguardian.com/technology/2013/oct/07/fbi-bitcoin-silk-road-ross-ulbricht.

[66] Johnson, A. R. (2013, October 3). Bitcoin Rebounds After Plunge on Silk Road Charges. *The Wall Street Journal.* Retrieved from http://blogs.wsj.com/moneybeat/2013/10/03/bitcoin-rebounds-after-plunge-on-silk-road-charges/.

[67] Eha, B. P. (2013, October 5). Could the Silk Road Closure be Good for Bitcoin?. *The New Yorker.*
Retrieved from http://www.newyorker.com/online/blogs/currency/2013/10/could-the-silk-road-closure-be-good-for-bitcoin.html.

[68] FBI Directorate of Intelligence, Cyber Intelligence Section, and Criminal Intelligence Section. (2012, April 24). *Bitcoin Virtual Currency: Unique Features Present Distinct Challenges for Deterring Illicit Activity*. Retrieved from http://cryptome.org/2012/05/fbi-bitcoin.pdf.

[69] Wisniewski, C. (2013, May 30). Digital currency Liberty Reserve shut down by US government. *Naked Security.* Retrieved from http://nakedsecurity.sophos.com/2013/05/30/digital-currency-liberty-reserve-shut-down-by-us-governement/.

[70] Greenberg, A. (2013, November 18). Meet the 'Assassination Market' Creator Who's Crowdfunding Murder With Bitcoins. *Forbes.*
Retrieved from http://www.forbes.com/sites/andygreenberg/2013/11/18/meet-the-assassination-market-creator-whos-crowdfunding-murder-with-bitcoins/.

[71] Adelmann, B. (2013, August 9). Federal Court Rules That the Bitcoin is Money. *New American.*
Retrieved from http://www.thenewamerican.com/economy/markets/item/16256-federal-court-rules-that-the-bitcoin-is-money.

[72] Lee, T. B. (2013, November 18). This Senate hearing is a Bitcoin lovefest. *The Washington Post.* Retrieved from http://www.washingtonpost.com/blogs/the-switch/wp/2013/11/18/this-senate-hearing-is-a-bitcoin-lovefest/.

[73] Tracy, R. (2013, November 18). Authorities See Worth of Bitcoin. *The Wall Street Journal.* Retrieved from http://online.wsj.com/news/articles/SB10001424052702304439804579205740125297358.

[74] Peterson, A. (2013, November 26). When bitcoins go bad: 4 stories of fraud, hacking, and digital currencies. *The Washington Post.* Retrieved from http://www.washingtonpost.com/blogs/the-switch/wp/2013/11/26/when-bitcoins-go-bad-4-stories-of-fraud-and-hacking/.

[75] Franceschi-Bicchierai, L. (2013, November 8). $1.3 Million in Bitcoin Stolen in Major Online Robbery. *Mashable.* Retrieved from http://mashable.com/2013/11/08/bitcoin-theft-tradefortress/.

[76] Masnick, M. (2013, July 24). SEC Confirms that Bitcoin Savings & Trust Was a Ponzi Scheme; Files Lawsuit. *Techdirt.* Retrieved from http://www.techdirt.com/articles/20130723/16121723913/sec-confirms-that-bitcoin-savings-trust-was-ponzi-scheme-files-lawsuit.shtml.

[77] Sparshott, J. (2013, August 26). Regulator FinCEN: Virtual Currencies Must Adhere to U.S. Financial Rules. *The Wall Street Journal.* Retrieved from http://online.wsj.com/article/BT-CO-20130826-708042.html.

[78] Wood, R. W. (2013, November 18). Bitcoin Tax Tips for Congress and Everyone Else. *Forbes.* Retrieved from http://www.forbes.com/sites/robertwood/2013/11/18/bitcoin-tax-tips-for-congress-and-everyone-else/.

[79] Hill, K. (2013, August 7). Federal Judge Rules Bitcoin is Real Money. *Forbes.* Retrieved from http://www.forbes.com/sites/kashmirhill/2013/08/07/federal-judge-rules-bitcoin-is-real-money/.

[80] Court officially declares Bitcoin a real currency. (2013, August 9). *Russia Today.*
Retrieved from http://rt.com/usa/bitcoin-sec-shavers-texas-231/.

[81] Brito, J. (2013, November 18). US regulations are hampering Bitcoin's growth. *The Guardian.* Retrieved from http://www.theguardian.com/commentisfree/2013/nov/18/bitcoin-senate-hearings-regulation.

[82] Johnson, D. (2013, November 29). Black Friday: Bitcoin users get hundreds of discounts. *The Telegraph.* Retrieved from http://www.telegraph.co.uk/technology/news/10482816/Black-Friday-Bitcoin-users-get-hundreds-of-discounts.html.

[83] Soper, T. (2013, November 26). World's first Bitcoin ATM exceeds $1M in transaction volume within one month. *GeekWire.* Retrieved from http://www.geekwire.com/2013/worlds-bitcoin-atm-exceeds-1m-transaction-volume-month/.

[84] CB Insights. (2013, July 2*). Bitcoin Industry Sees More Investors than Startups*.
Retrieved from http://www.cbinsights.com/blog/trends/bitcoin-industrystartups.

[85] Hasselback, D. (2013, November 19). Governments ponder legitimacy of Bitcoins. *Financial Post.* Retrieved from http://business.financialpost.com/2013/11/19/governments-ponder-legitimacy-of-bitcoins/.

[86] Kapron, Z. (2013, November 8). Chinese can now buy real estate with Bitcoin. *Finextra.*
Retrieved from http://www.finextra.com/community/fullblog.aspx?blogid=8475.

[87] Cyprus University world first to accept Bitcoins for tuition. (2013, November 22). *Russia Today.* Retrieved from http://rt.com/business/bitcoin-nicosia-university-tuition-060/.

[88] Katten Muchin Rosenman LLP. (2013, November 28). *Current US Regulatory Developments.* Retrieved fromhttp://www.mondaq.com/unitedstates/x/277850/Financial+Services/Bitcoin+Current+US+Regulatory+Developments.

[89] Hill, K. (2013, August 12). Every Important Person in Bitcoin Just Got Subpoenaed by New York's Financial Regulator. *Forbes.* Retrieved from http://www.forbes.com/sites/kashmirhill/2013/08/12/every-important-person-in-bitcoin-just-got-subpoenaed-by-new-yorks-financial-regulator/.

[90] Hill, K. (2013, November 14). New York May Give 'BitLicenses' to Bitcoin Companies. *Forbes.*
Retrieved from http://www.forbes.com/sites/kashmirhill/2013/11/14/new-york-may-give-bitlicenses-to-virtual-currency-companies/.

[91] Adelmann, B. (2013, November 19). Government Is Taking Steps to Regulate Bitcoin. *New American.* Retrieved from http://www.thenewamerican.com/economy/sectors/item/16985-government-is-taking-steps-to-regulate-bitcoin.

[92] Wood, R. W. (2013, June 18). Bitcoin In IRS Crosshairs, Says Government Report. *Forbes.* Retrieved from http://www.forbes.com/sites/robertwood/2013/06/18/bitcoin-in-irs-crosshairs-says-government-report/.

[93] Marian, O. (2013). Are Cryptocurrencies Super Tax Havens?. *Michigan Law Review First Impressions*, *112*, 38-38. Retrieved from http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2305863.

[94] Velde, F.R. (2013). Bitcoin: a primer. *Chicago Fed Letter*, (Dec). Retrieved from http://www.chicagofed.org/digital_assets/publications/chicago_fed_letter/2013/cfldecember2013_317.pdf.

[95] Phillips, J. (2013, November 18). Bitcoin hits $750, up 107% in a week. *CNBC.*
Retrieved from http://www.cnbc.com/id/101205416.

[96] Gurri, A. (2013, May 6). Bitcoins, Free Banking, and the Optional Clause. *The Umlaut.*
Retrieved from http://theumlaut.com/2013/05/06/bitcoins-free-banking-and-the-optional-clause/.

[97] Reeves, J. (2013, November 14). Bitcoin Investing: Is the Bubble About to Burst?. *The Slant.*
Retrieved from http://slant.investorplace.com/2013/11/bitcoin-investing-bubble/.

[98] Lee, T. B. (2013, November 8). Everything you need to know about the Bitcoin 'bubble'. *The Washington Post.* Retrieved from http://www.washingtonpost.com/blogs/the-switch/wp/2013/11/08/everything-you-need-to-know-about-the-bitcoin-bubble/.

[99] Chang, G. G. (2013, November 24). A China Triangle: Bitcoin, Baidu, and Beijing. *Forbes.* Retrieved from http://www.forbes.com/sites/gordonchang/2013/11/24/a-china-triangle-bitcoin-baidu-and-beijing/.

[100] Clinch, M. (2013, July 30). Bitcoin banned in Thailand. *CNBC.*
Retrieved from http://www.cnbc.com/id/100923551.

[101] Bradbury, D. (2013, November 19). Senate Bitcoin Hearing Discusses Legitimacy and Challenges of Virtual Currencies. *Coindesk.* Retrieved from http://www.coindesk.com/senate-bitcoin-hearing-legitimacy-challenges-virtual-currencies/.

[102] Brito, J. (2013, April 10). Begun the next crypto wars have. *Technology Liberation Front.* Retrieved from http://techliberation.com/2013/04/10/begun-the-next-crypto-wars-have/.

[103] Foundation for Information Policy Research. (2005, May 25). *The Crypto Wars Are Over!* Retrieved from http://www.fipr.org/press/050525crypto.html.

[104] Zimmermann, P. (1999). Why I Wrote PGP. In *PGP User's Guide.* The MIT Press. Retrieved from http://www.philzimmermann.com/EN/essays/WhyIWrotePGP.html.

[105] Burghardt, T. (2013, November 10). The U.S. Secret State and the Internet: 'Dirty Secrets' and 'Crypto Wars' from 'Clipper Chip' and ECHELON to PRISM. *Global Research.* Retrieved from http://www.globalresearch.ca/the-u-s-secret-state-and-the-internet-dirty-secrets-and-crypto-wars-from-clipper-chip-to-prism/5357623.

[106] Brito, J. (2013, April 9). Bitcoin vs. Big Government. *Reason.* Retrieved from http://reason.com/archives/2013/04/09/bitcoin-vs-big-government.

[107] Forbes, S. (2013, April 16). Bitcoin: Whatever It Is, It's Not Money!. *Forbes.* Retrieved from http://www.forbes.com/sites/steveforbes/2013/04/16/bitcoin-whatever-it-is-its-not-money/.

[108] Levy, S. (1994, November). Pretty Good Privacy Gets Pretty Legal. *Wired.* Retrieved from http://www.wired.com/wired/archive/2.11/cypher.wars_pr.html.

[109] Gimon, C. A. (1995). Phil Zimmermann Investigation Dropped. *Info Nation.* Retrieved from http://www.skypoint.com/members/gimonca/philzim2.html.

[110] Gimon, C. A. (1995, June). The Phil Zimmermann Case. *Info Nation.* Retrieved from http://www.skypoint.com/members/gimonca/philzima.html.

[111] Zimmermann, P. (1994, November). Preface. In *PGP Source Code and Internals.* The MIT Press. Retrieved from http://www.mit.edu/~prz/EN/essays/BookPreface.html.

[112] Ball, J., Borger, J., & Greenwald, G. (2013, September 5). Revealed: how US and UK spy agencies defeat internet privacy and security. *The Guardian.* Retrieved from http://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security.

[113] Philip Zimmermann and 'Guilt' Over PGP. (2011, September 24). *Slashdot.* Retrieved from http://slashdot.org/story/01/09/24/162236/philip-zimmermann-and-guilt-over-pgp.

[114] Urken, R. K. (2013, April 4). Is Bitcoin currency safe? Maybe, but think of it as a commodity. *The Globe and Mail.* Retrieved from http://www.theglobeandmail.com/globe-investor/investor-community/trading-shots/is-bitcoin-currency-safe-maybe-but-think-of-it-as-a-commodity/article10764645/.

[115] May, T. (1997). Untraceable Digital Cash, Information Markets, and BlackNet. In *Proceedings of the Computer, Freedom & Privacy Conference*. Retrieved from http://osaka.law.miami.edu/~froomkin/articles/tcmay.htm.

[116] Froomkin, M. (1997, March). The unintended consequences of e-cash. In *Proceedings of Computers, Freedom and Privacy Conference*. Retrieved from http://osaka.law.miami.edu/~froomkin/articles/cfp97.htm.

[117] Lee, T. B. (2013, April 7). Four Reasons Bitcoin Is Worth Studying. *Forbes.* Retrieved from http://www.forbes.com/sites/timothylee/2013/04/07/four-reasons-bitcoin-is-worth-studying/.

[118] NYC Trader. (2013, November 13). Is Bitcoin for Real? Macroeconomic Considerations for an Alternative Currency. *Seeking Alpha.* Retrieved from http://seekingalpha.com/article/1836602-is-bitcoin-for-real-macroeconomic-considerations-for-an-alternative-currency.

[119] Kaliski, B. (2006). The Mathematics of the RSA Public-Key Cryptosystem. *RSA Laboratories*. Retrieved from http://www.mathaware.org/mam/06/Kaliski.pdf.

[120] Johnson, D. B., & Menezes, A. J. (1998). Elliptic curve DSA (ECDSA): an enhanced DSA. *SSYM*, *98*, 13-13. Retrieved from http://cs.ucsb.edu/~koc/ccs130h/notes/ecdsa.pdf.

[121] Johnson, D., Menezes, A., & Vanstone, S. (2001). The elliptic curve digital signature algorithm (ECDSA). *International Journal of Information Security*, *1*(1), 36-63. Retrieved from http://cs.ucsb.edu/~koc/ccs130h/notes/ecdsa-cert.pdf.

[122] Certicom. (2013). *Elliptic Curve Cryptography Tutorial.* Retrieved from http://www.certicom.com/index.php/10-introduction.

[123] Huang, M. D. A., Kueh, K. L., & Tan, K. S. (2000). Lifting elliptic curves and solving the elliptic curve discrete logarithm problem. In *Algorithmic Number Theory* (pp. 377-384). Springer Berlin Heidelberg. Retrieved from http://www-rcf.usc.edu/~mdhuang/cs599/liftants1.pdf.

[124] Menezes, A., & Teske, E. (2006). Cryptographic implications of Hess' generalized GHS attack. *Applicable algebra in Engineering, communication and computing*, *16*(6), 439-460. Retrieved from http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.58.6402&rep=rep1&type=pdf.

[125] Ius Mentis. (2005). *Crash course on cryptography: Digital signatures.* Retrieved from http://www.iusmentis.com/technology/encryption/crashcourse/digitalsignatures/.

[126] Bellovin, S. M. (2005, October 3). *Public Key Cryptography*. Lecture conducted from Columbia University, New York, NY. Retrieved from https://www.cs.columbia.edu/~smb/classes/f05/l08.pdf.

[127] Technical background of version 1 Bitcoin address. (2013, November 5). *Bitcoin Wiki.* Retrieved from https://en.bitcoin.it/wiki/Technical_background_of_version_1_Bitcoin_addresses.

[128] RSA Laboratories. (2013). *What is a Blind Signature Scheme?.* Retrieved from http://www.emc.com/emc-plus/rsa-labs/standards-initiatives/what-is-a-blind-signature-scheme.htm.

[129] Chaum, D. (1982, August). Blind Signatures for Untraceable Payments. In *Crypto* (Vol. 82, pp. 199-203). Retrieved from http://sce.uhcl.edu/yang/teaching/csci5234WebSecurityFall2011/Chaum-blind-signatures.PDF.

[130] Iwai, K. (1995, August 28). How to Really Circulate Electronic Cash on the Internet. Retrieved from http://iwai-k.com/HowToCirculateECash.pdf.

[131] Deflationary Spiral. (2013, May 18). *Bitcoin Wiki.* Retrieved from https://en.bitcoin.it/wiki/Deflationary_spiral.

[132] *Beyond Silk Road: Potential Risks, Threats, and Promises of Virtual Currencies.* (2013, November 18) (testimony of Senator Thomas Carper). Retrieved from http://www.hsgac.senate.gov/hearings/beyond-silk-road-potential-risks-threats-and-promises-of-virtual-currencies.

[133] Matonis, J. (1995, April). Digital cash and monetary freedom. *Institute for Monetary Freedom.* Retrieved from http://libertarian.co.uk/lapubs/econn/econn063.pdf.

[134] What is Bitcoin Mining?. (n.d.) *We Use Coins.* Retrieved from https://www.weusecoins.com/en/mining-guide.

[135] Liu, Alec. (2013, April). A Guide to Bitcoin Mining: Why Someone Bought a $1,500 Bitcoin Miner on eBay for $20,600. *Vice.* Retrieved from http://motherboard.vice.com/blog/a-guide-to-bitcoin-mining-why-someone-bought-a-1500-bitcoin-miner-on-ebay-for-20600.

[136] Litecoin. (2013, October 21). *Bitcoin Wiki.* Retrieved from https://en.bitcoin.it/wiki/Litecoin.

[137] Levy, S. (1994, December). E-Money (That's What I Want). *Wired.* Retrieved from http://www.wired.com/wired/archive/2.12/emoney.html.

[138] Merkle, R. C. (1980, April). Protocols for Public Key Cryptosystems. In *IEEE Symposium on Security and privacy* (Vol. 1109, pp. 122-134). Retrieved from http://www.merkle.com/papers/Protocols.pdf.

[139] Babaioff, M., Dobzinski, S., Oren, S., & Zohar, A. (2012, June). On bitcoin and red balloons. In *Proceedings of the 13th ACM Conference on Electronic Commerce* (pp. 56-73). ACM. Retrieved from http://dl.acm.org/citation.cfm?id=2229022.

[140] Spaven, E. (2013, November 4). BTC China beats Mt. Gox and Bitstamp to become the world's No. 1 bitcoin exchange. *CoinDesk.* Retrieved from http://www.coindesk.com/btc-china-beats-mt-gox-bitstamp-become-worlds-1-bitcoin-exchange/.

[141] Sorkin, A. R. (2013, November 25). Render Unto Caesar, but Who Backs Bitcoin? *Dealbook.* Retrieved from http://dealbook.nytimes.com/2013/11/25/render-unto-caesar-but-who-backs-the-bitcoin/?hpw&rref=technology&_r=2.

[142] McCullagh, D. (2001, June 14). Digging Those Digicash Blues. *Wired.* Retrieved from http://www.wired.com/techbiz/media/news/2001/06/44507?currentPage=all.

[143] Brandom, R. (2013, November 16). New York State considers licensing Bitcoin traders. *The Verge.* Retrieved from http://www.theverge.com/2013/11/16/5111546/new-york-state-weighs-bitlicense-certification-for-bitcoin-traders.

[144] Status Report on Free Market Money. (2005, January 31). *The Indomitus Report.* Retrieved from http://indomitus.net/2004status.html#ebullion.

[145] Dwyer, B. (2011, November). Average Credit Card Processing Fees. *CardFellow.* Retrieved from www.cardfellow.com/blog/average-fees-for-credit-card-processing.

[146] PayPal Corporate Website. Retrieved from https://www.paypal.com/us/webapps/mpp/paypal-fees.

[147] NewsCore. (2012, April 2). Decision Points: PayPal Versus Credit Cards. *Fox Business.* Retrieved from http://www.foxbusiness.com/personal-finance/2012/03/29/decision-points-paypal-versus-credit-cards/.

[148] Rueter, T. (2013, October 8). Amazon launches payments for other e-commerce sites. *Internet Retailer.* Retrieved from https://www.internetretailer.com/2013/10/08/amazon-launches-payments-other-e-commerce-sites.

[149] Needleman, R. (2010, December 17). Cash is dead, says Dwolla. *CNET.*
Retrieved from http://news.cnet.com/8301-19882_3-20025966-250.html.

[150] Carney, M. (2013, May 17). Bitcoin is legal, but mainstream adoption will mandate playing by the rules. *PandoDaily.* Retrieved from http://pandodaily.com/2013/05/17/bitcoin-is-legal-but-mainstream-adoption-will-mandate-playing-by-the-rules/.

[151] Buterin, V. (2013, November 4). Selfish Mining: A 25% Attack Against the Bitcoin Network. *Bitcoin Magazine.* Retrieved from http://bitcoinmagazine.com/7953/selfish-mining-a-25-attack-against-the-bitcoin-network/.

[152] Knight, W. (2013, October 14). Leading Economist Predicts a Bitcoin Backlash. *MIT Technology Review.* Retrieved from http://www.technologyreview.com/news/520296/leading-economist-predicts-a-bitcoin-backlash/.

[153] Cawrey, D. (2013, November 7). Federal Reserve economist says Bitcoin is a remarkable technical achievement. *CoinDesk.* Retrieved from http://www.coindesk.com/federal-reserve-economist-says-bitcoin-is-a-remarkable-conceptual-and-technical-achievement/.

[154] Narayanan, A. (2013, November 9). Why the Cornell paper on Bitcoin mining is important. *Freedom to Tinker.* Retrieved from https://freedom-to-tinker.com/blog/randomwalker/why-the-cornell-paper-on-bitcoin-mining-is-important/.

[155] March 2013 Chain Fork Information. (2013, May 16). *Bitcoin.org.*
Retrieved from http://bitcoin.org/en/alert/2013-03-11-chain-fork.

[156] Seward, Z. M. (2013, March 28). Bitcoin, up 152% this month, tops $1 billion in total value. *Quartz.* Retrieved from http://qz.com/68328/bitcoin-up-152-this-month-tops-1-billion-in-total-value/.