S.J. QUINNEY COLLEGE OF LAW

LEGAL STUDIES RESEARCH PAPER SERIES

New Kids on the Blockchain: How Bitcoin's Technology Could Reinvent the Stock Market

Larissa Lee

S.J. Quinney College of Law research paper No.138

S.J. Quinney College of Law
University of Utah
Salt Lake City, UT 84112

NEW KIDS ON THE BLOCKCHAIN: HOW BITCOIN'S TECHNOLOGY COULD REINVENT THE STOCK MARKET

Larissa Lee

ABSTRACT

Bitcoin is the first and most successful digital currency in the world. It is polarized in the news almost daily, with either glowing reviews of the many benefits of an alternative and international currency, or doomsday predictions of anarchy, deflation, and another tulip bubble.

This article focuses on the truly innovative aspect of Bitcoin—and that which has gone mostly unnoticed since its inception—the technological platform used to transfer Bitcoin from one party to another. This technology is called the Blockchain. The Blockchain eschews a bank or other middleman and allows parties to transfer funds directly to one another, using a peer-to-peer system. This disruptive technology has done for money transfers what email did for sending mail—by removing the need for a trusted third party just as email removed the need for using the post office to send mail.

If this technology can be used for peer-to-peer money transfers, why not extend the technology to accomplish other forms of transfers? Imagine selling a house or buying a car peer-to-peer. What about using the Blockchain technology to buy and sell stocks? Stocks exchanged completely peer-to-peer could resolve many of the issues facing the stock market today, including high frequency trading and short sales. This article develops a peer-to-peer stock market system, the legal implications of such a system, and how this system will fit in with current legislation and regulation.

TABLE OF CONTENTS

INTRODUCTION

What do Lamborghinis, drug dealers, pirates, hackers, the Winklevoss twins, the FBI, and Congress have in common? Each has involved itself in some way in the phenomenon that is Bitcoin in the past few years. With a market capitalization of almost $5 billion,[1] Bitcoin has garnered much attention, and not all of it is positive. Several countries have banned Bitcoin transfers altogether, while others—including the United States—have tried to place limits or restrictions on transfers by taxing those transfers. The European Union officially recognizes Bitcoin as a currency, but several other countries are grappling at how to classify it. Is it money? Property? A security? Hundreds of other digital currencies ("cryptocurrencies") have since popped up and it is still unclear what effect these will have on the global economy.

However, the truly innovative aspect of Bitcoin—and that which has gone mostly unnoticed since its inception—is the technological platform used to transfer Bitcoin from one party to another. This technology is called the Blockchain. The Blockchain eschews a bank or other middleman and allows parties to transfer funds directly to one another, using a peer-to-peer system. This disruptive technology has done for money transfers what email did for sending mail—by removing the need for a trusted third party just as email removed the need for using the post office to send mail.

What about other practical implications of the Blockchain? Could this technology be extended beyond money transfers to accomplish other forms of transfers? Imagine selling a house or buying a car peer-to-peer. What about using the Blockchain technology to buy and sell

[1] CRYPTO-CURRENCY MARKET CAPITALIZATIONS, http://coinmarketcap.com (last visited Nov. 1, 2015).

stocks?[2] Stocks exchanged completely peer-to-peer ("cryptosecurities") could resolve many of the issues facing the stock market today, including high frequency trading and short sales.

This article seeks to develop and analyze these claims and examine other potential benefits and disadvantages of a peer-to-peer stock market system. Considering all of these factors, the article then looks at the legal implications of a cryptosecurities market and whether this market could fit within the existing legal regime, or whether Congress and the SEC would need to change the laws to fit the new system. This cryptosecurities market would be an alternative trading market, not a replacement for the current stock market regime.

The article proceeds in five parts. Part I examines what exactly is a Bitcoin and its role in today's society. Part II delves into the Blockchain, focusing on how this Bitcoin technology actually works and the process behind each Bitcoin transfer. Part III examines the problems facing the current stock market regime and explores how a cryptosecurities market could correct these problems. Part IV looks at the benefits and disadvantages of a peer-to-peer stock exchange. Finally, Part V determines whether this new system of cryptosecurities could fit within existing laws and regulations, or whether new laws and regulations would need to be developed around this new technology.

I. WHAT IS BITCOIN?

The Bitcoin concept first emerged in October 2008 when Satoshi Nakamoto—a

[2] This idea was initially proposed in 2014 by Patrick Byrne, Chief Executive Officer of Overstock. Cade Metz, *Overstock's Radical Plan to Reinvent the Stock Market with Bitcoin*, WIRED (July 30, 2014, 6:30 AM), http://www.wired.com/2014/07/overstock-and-cryptocurrency/. Overstock tested this concept out with a $25 million private corporate "cryptobond" in June 2015. Josh Beckerman, *Overstock Launches Corporate Bond Billed as World's First Cryptocurrency*, WALL STREET JOURNAL (June 5, 2015, 8:03 PM), http://www.wsj.com/articles/overstock-launches-corporate-bond-billed-as-worlds-first-cryptosecurity-1433549038. In August 2015, Overstock announced the arrival of t0 (pronounced tee-zero), the world's first "Blockchain-based private and public equities trading platform." Pete Rizzo, *Overstock Unveils Blockchain Trading Platform at Nasdaq Event* (Aug. 5, 2015 2:19 AM), http://www.coindesk.com/overstock-unveils-blockchain-trading-platform-to/.

pseudonym for a person or possibly a group of people—published a whitepaper outlining the idea.[3] This paper envisioned a "purely peer-to-peer version of electronic cash" that would allow "online payments to be sent directly from one party to another without going through a financial institution."[4] Since this time, almost 700 other digital currencies have appeared with varying levels of success.[5] Although the focus of this article will be on Bitcoin's underlying technology and not Bitcoin itself, it is helpful to understand Bitcoin's impact on society, the government's attempt to classify what exactly a Bitcoin is, and how Bitcoin gets its value.

A. Bitcoin's Impact on Society

For the first few years of its existence, Bitcoin yearned for legitimacy but tended to be used mainly for black market goods and illegal drugs sold over the internet.[6] Silk Road, the now-defunct illegal drug website ran by a man calling himself The Dread Pirate Roberts, required users to buy and sell exclusively in Bitcoin in order to evade government authorities.[7] The site also used an eBay style escrow system that "consisted of an internal Bitcoin 'bank,' where every Silk Road user had to hold an account maintained by Silk Road, pending completion of the transaction."[8] It was not until late 2013 that the FBI finally shut down the online drug marketplace and began prosecuting Ross Ulbricht, who in February 2015 was convicted of

[3] Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System* (Oct. 2008), http://bitcoin.org/bitcoin.pdf.
[4] Id.
[5] CRYPTO-CURRENCY MARKET CAPITALIZATIONS, http://coinmarketcap.com (last visited Nov. 1, 2015).
[6] *An Abridged History of Bitcoin*, THE NEW YORK TIMES, http://www.nytimes.com/interactive/technology/bitcoin-timeline.html?_r=0#/#time284_8158 (last updated Nov. 19, 2013).
[7] "The Dread Pirate Roberts isn't shy about naming Silk Road's active ingredient: The cryptographic digital currency known as Bitcoin. 'We've won the State's War on Drugs because of Bitcoin,' [Roberts] writes." Andy Greenberg, *Meet The Dread Pirate Roberts, The Man Behind Booming Black Market Drug Website Silk Road*, FORBES (August 14, 2013, 11:31 AM), http://www.forbes.com/sites/andygreenberg/2013/08/14/meet-the-dread-pirate-roberts-the-man-behind-booming-black-market-drug-website-silk-road/.
[8] Press Release, Manhattan U.S. Attorney Announces Seizure of Additional $28 Million Worth of Bitcoins Belonging to Ross William Ulbricht, Alleged Owner and Operator of Silk Road Website (Oct. 25, 2013), http://www.justice.gov/usao/nys/pressreleases/October13/SilkRoadSeizurePR.php?print=1.

narcotics and money laundering conspiracies using the alias The Dread Pirate Roberts.[9]

On November 18, 2013, the Senate held a hearing during the aftermath of the Silk Road shut down.[10] While regulators acknowledged that Bitcoins may be used for illicit purposes, they argued that Bitcoins are also "an innovative way of driving legitimate operations."[11] Overall, the tone of the hearing was optimistic. "The Senate hearing is the clearest indication yet of the government's desire to grapple with the consequences of [Bitcoin's] growth, and the recognition that Bitcoin and other similar networks could become more lasting and significant parts of the financial landscape."[12]

Today Bitcoins have been used to purchase a Lamborghini[13] and pay college tuition.[14] Bitcoin ATMs are currently popping up all around the globe.[15] Over 80,000 merchants currently accept Bitcoin payments.[16] Some of the major retailers that accept Bitcoin payments include Amazon, Microsoft, Home Depot, Target, Time, Inc., and—not surprisingly—Overstock.[17] Bitcoins have been pooled into investment trusts by online platforms such as SecondMarket where investors are able to "buy a stake in the Bitcoin market without directly purchasing the

---

[9] Robert McMillan, *Who Owns the World's Biggest Bitcoin Wallet? The FBI*, WIRED (Dec. 18, 2013, 6:30 AM), http://www.wired.com/wiredenterprise/2013/12/fbi_wallet/; http://www.wired.com/2015/02/silk-road-ross-ulbricht-verdict/.

[10] Cade Metz, *The Magic Number: Bitcoin Prices Top $1,000*, WIRED (Nov. 27, 2013, 10:59 AM), http://www.wired.com/business/2013/11/bitcoin-one-thousand/?cid=15030794.

[11] *Id.*

[12] *An Abridged History of Bitcoin*, *supra* n.6.

[13] Craig Trudell, *Bitcoin Meets Tesla with Lamborghini Dealership's Model S Sale*, BLOOMBERG TECH. (Dec. 6, 2013, 10:00 PM), http://www.bloomberg.com/news/2013-12-06/bitcoin-meets-tesla-in-california-dealership-model-s-transaction.html.

[14] Not only can you pay college tuition, but at a university in Cyprus, you can also get a masters degree in Digital Currency. Panos Mourdoukoutas, *Bitcoin Gets an Endorsement for College Tuition Payments and a MOOC*, FORBES (November 21, 2013, 1:58 PM), http://www.forbes.com/sites/panosmourdoukoutas/2013/11/21/bitcoin-gets-an-endorsement-for-college-tuition-payments-and-a-mooc/.

[15] *Bitcoin ATMs are Spreading Across the World*, REUTERS (Dec. 30, 2013, 5:20 PM), http://www.reuters.com/article/2013/12/30/idUS104162105820131230.

[16] Greg Bensinger, *First U.S. Bitcoin Exchange Set to Open*, WALL STREET JOURNAL (Jan. 25, 2015), http://www.wsj.com/articles/first-u-s-bitcoin-exchange-set-to-open-1422221641.

[17] Jonas Chokun, *Who Accepts Bitcoins as Payment? List of Companies, Stores, Shops*, BITCOIN VALUES, http://www.bitcoinvalues.net/who-accepts-bitcoins-payment-companies-stores-take-bitcoins.html (last visited May 24, 2015).

currency themselves."[18] Even the Winklevoss twins[19] have purchased a stake worth almost $11 million in Bitcoins and have filed paperwork with the Securities and Exchange Commission to create an exchange-traded fund, using only Bitcoins.[20] A federal district court in Texas declared these types of Bitcoin investments to be securities governed by SEC regulations.[21]

Some countries have formally recognized Bitcoin as a legitimate currency, while others have banned Bitcoin entirely.[22] Several countries have not banned Bitcoins but have issued clear warnings about the risks of Bitcoin use.[23] Not only is the enormous amount of volatility a big risk, but hacking into online Bitcoin wallets can also be a serious risk. For example, in October 2013, hackers stole $1.2 million from a company storing Bitcoins online.[24]

Many Bitcoin critics and those wishing to regulate or abolish Bitcoin point out its propensity to be used in facilitating illegal transactions. Bitcoin transfers are completely

---

[18] Brian P. Eha, *SecondMarket Establishes New Bitcoin Trust for Accredited Investors*, ENTREPRENEUR (Sept. 26, 2013), http://www.entrepreneur.com/article/228597.

[19] Tyler and Cameron Winklevoss—most known for their legal battle with Mark Zuckerberg over the ownership of Facebook—launched Gemini in January 2015, the second U.S.-based Bitcoin exchange. Nathaniel Popper & Peter Lattman, *Never Mind Facebook; Winklevoss Twins Rule in Digital Money*, N.Y. TIMES (Apr. 11, 2013, 3:11 PM), http://dealbook.nytimes.com/2013/04/11/as-big-investors-emerge-bitcoin-gets-ready-for-its-close-up/?_r=0; Joanna Campione, *Bitcoin Comes to America: Now, with Regulated Exchange*, YAHOO FINANCE (May 7, 2015, 12:21 PM), http://finance.yahoo.com/news/first-bitcoin-exchange-gets-approval-from-new-york-state-regulators-022427666.html.

[20] *An Abridged History of Bitcoin*, *supra* n.6.

[21] Securities and Exchange Commission v. Shavers, No. 4:13-CV-416**,** 2013 WL 4028182 (E.D. Texas, Aug. 6, 2013).

[22] Germany and Canada both recognize Bitcoin as legal tender. Matt Clinch, *Bitcoin Recognized by Germany as 'Private Money'*, CNBC (Aug. 19, 2013, 10:25 AM), http://www.cnbc.com/id/100971898; Drew Hasselback, *Governments Ponder Legitimacy of Bitcoins*, FINANCIAL POST (Nov. 19, 2013, 4:52 PM), http://business.financialpost.com/2013/11/19/governments-ponder-legitimacy-of-bitcoins/. Countries banning Bitcoin include Thailand and China. Matt Clinch, *Bitcoin Banned in Thailand*, CNBC (Jul. 30, 2013, 6:20 AM), http://www.cnbc.com/id/100923551; Andrew Mouton, *What a Bitcoin is Really Worth in India and China*, MARKET WATCH (Jan. 1, 2014, 7:02 AM), http://www.marketwatch.com/story/what-a-bitcoin-is-really-worth-in-india-and-china-2014-01-01.

[23] While India has not banned Bitcoins outright, it has issued a warning on the dangers of Bitcoin use. Andrew Mouton, *What a Bitcoin is Really Worth in India and China*, MARKET WATCH (Jan. 1, 2014, 7:02 AM), http://www.marketwatch.com/story/what-a-bitcoin-is-really-worth-in-india-and-china-2014-01-01. France has issued similar warnings. Robin Sidel, et al., *Central Banks Warn of Bitcoin Risks*, THE WALL STREET JOURNAL (Dec. 5, 2013, 11:23 PM), http://online.wsj.com/news/articles/SB10001424052702303497804579239451297424842.

[24] Robert McMillan, *$1.2M Hack Shows Why You Should Never Store Bitcoins on the Internet*, WIRED (Nov. 7, 2013, 3:49 PM), http://www.wired.com/wiredenterprise/2013/11/inputs/.

anonymous, and extremely difficult to trace. However, almost all of these issues also happen when parties to a transaction use cash. Cash is extremely difficult to trace, and most transactions are anonymous. The one distinguishable difference is that Bitcoin can be used to make payments online whereas cash cannot be used online. This enables more illicit uses of the currency because even the parties buying and selling can remain anonymous with almost no information about each other.[25] When exchanging cash, the parties must at least determine how and where to exchange the cash for the illicit goods.

B. What is a Bitcoin—Currency, Property, or Security?

Although Satoshi Nakamoto referred to Bitcoin as "electronic cash," no one is really sure yet what Bitcoins are. Bitcoins do not have a physical form, and although there are several options of novelty coins one can purchase, the actual Bitcoin itself is just a unique string of numbers that only the holder of the Bitcoin has access to. Additionally, Bitcoin is not considered legal tender in any country, nor is any other digital currency.

By 2014, with millions of dollars in Bitcoin being exchanged every hour tax-free, the Internal Revenue Service (IRS) classified Bitcoin and all other digital currencies as property for tax purposes, and not as a foreign currency.[26] This decision encourages the investment of Bitcoin while discouraging users to trade in Bitcoin because they must calculate gain or loss and report it like they would any other property for tax purposes. However, stocks and bonds are also classified as property for tax purposes and therefore if Bitcoins are more like a security and less like a currency then it makes sense to classify them as property.

---

[25] Although transactions are completed anonymously, it might be possible to track a user's identity by following the Bitcoin through the Blockchain and to a Bitcoin exchange, and then subpoenaing the exchange. Tom Simonite, *Mapping the Bitcoin Economy Could Reveal Users' Identities*, MIT TECH. REVIEW (Sept. 5, 2013), http://www.technologyreview.com/news/518816/mapping-the-bitcoin-economy-could-reveal-users-identities/.

[26] Josh Ungerman, *IRS Approach to Taxation of Bitcoin*, FORBES (Dec. 4, 2014, 1:02 AM), http://www.forbes.com/sites/irswatch/2014/12/04/irs-approach-to-taxation-of-bitcoin/.

In the Securities Act of 1933, Congress defined a "security" as:

> any note, stock, treasury stock, security future, security-based swap, bond, debenture, evidence of indebtedness, certificate of interest or participation in any profit-sharing agreement, collateral-trust certificate, preorganization certificate or subscription, transferable share, investment contract, voting-trust certificate, certificate of deposit for a security, factional undivided interest in oil, gas, or other mineral rights, and put, call, straddle, option, or privilege on any security, certificate of deposit, or group or index of securities (including any interest therein or based on the value thereof), or any put, call, straddle, option, or privilege entered into on a national securities exchange relating to foreign currency, or, in general, any interest or instrument commonly known as a "security", or any certificate of interest or participation in, temporary or interim certificate for, receipt for, guarantee of, or warrant or right to subscribe to or purchase, any of the foregoing.[27]

The U.S. Supreme Court in *Marine Bank v. Weaver*[28] said that the definition of security is meant to be broad and includes not only stocks and bonds but also the "countless and variable schemes devised by those who seek the use of the money of others on the promise of profits."[29] It is unlikely that Bitcoin, unattached to any investment trust or other scheme, falls into this definition.

First, cryptocurrencies—or any currencies for that matter— are not explicitly listed in the statute. Second, Bitcoin does not pass the investment contract test the U.S. Supreme Court developed in *SEC v. W.J. Howey Co*.[30] (the "*Howey* test"). For an investment to constitute a security under the *Howey* test, it must involve the investment of money—or any valuable consideration—in a common enterprise with a reasonable expectation of profits derived primarily from the efforts of a promoter or third party.[31]

The first issue is that there is no common enterprise. Unless attached to an investment

---

[27] 15 U.S.C. § 77(b)(a)(1) (2012).
[28] 455 U.S. 551 (1982).
[29] *Id.* at 555.
[30] 328 U.S. 293 (1946).
[31] *Id. Howey* originally said *solely* from the efforts of others instead of primarily, but the courts have since modified this test.

trust, Bitcoins are not being pooled into groups. No one enterprise is in charge of Bitcoin, seeking to take people's money with the promise of profits. Bitcoin is purely autonomous and has no central authority. Secondly, "primarily from the efforts of another" prong is not satisfied in the case of Bitcoin because whether the value of Bitcoin rises or falls is not dependent on anyone's efforts—the change in price is based on fluctuations in value tied to market conditions. Additionally, Bitcoin on its own does not pay out dividends, and voting rights are not in proportion to the number of Bitcoins owned, but rather the amount of computational power a user devotes to the system.[32]

The other issue with declaring all Bitcoins to be securities is that there is no issuer—just users trading amongst themselves. "The fundamental principle underlying the 1933 Act is that all offers and sales of securities require . . . [issuer] registration unless an exemption is available."[33] Because there is no issuer and it would be impossible to register Bitcoin as a security, it is unlikely it could be classified as a security, outside of being pooled into an investment trust of some kind. Although the jury is still out on what a Bitcoin is, for purposes of this article I will refer to it as a digital currency.[34]

C. How Do Bitcoins Get Their Value?

Many wonder how Bitcoin and other alternative currencies get their value. It is difficult to imagine how a single Bitcoin could be worth hundreds or even thousands of U.S. Dollars.

---

[32] For Bitcoin, "voting rights" are essentially given to the Bitcoin miners. This concept is explored more in the following section.

[33] James M. Bartos, United States Securities Law: A Practical Guide, 8 (2006) (emphasis omitted).

[34] Notably, the European Union recently declared Bitcoin a "currency" and not "property" for tax purposes, meaning transfers of Bitcoin in the EU will not be considered a taxable event. *See* Sam Schechner, *EU Rules Bitcoin is a Currency, Not a Commodity—Virtually*, WALL STREET JOURNAL (Oct. 22, 2015 6:15 AM), http://blogs.wsj.com/digits/2015/10/22/eu-rules-bitcoin-is-a-currency-not-a-commodity-virtually/.

Many have claimed that Bitcoin is no more than a Ponzi scheme,[35] or have worried that it represents the next tulip disaster waiting to happen.[36] However, most of the same arguments could be made about the U.S. Dollar. For most of the greenback's history, the value of the dollar was tied to the government's guarantee that you could trade in your dollars at any time for gold or silver.[37] In 1971, the U.S. abandoned the gold standard and now its value is backed solely by the Federal Reserve and the confidence of the American people.[38]

Bitcoin, too, is backed by the confidence of its users. Bitcoin users prefer Bitcoin to traditional currency for several reasons. In describing its purpose, a digital currency called Bitshares posted the following to its website:

> Today many people have lost faith in the financial institutions we've trusted for centuries. Some of our largest banks have failed and no longer exist. Those that survived needed massive bailouts. Citizens in some countries have lost their life savings to pay for failed government decisions. And for those who do find safety, the value of their savings is being drained by the constant drip of inflation. Our financial system is overdue for a reset.[39]

As you may have surmised from the above quote, the number one reason why users are attracted to Bitcoin is mistrust of the government and its centralized federal reserve. Many

---

[35] Eric Posner, *Fool's Gold: Bitcoin is a Ponzi Scheme—the Internet's Favorite Currency will Collapse*, SLATE (April 11, 2013, 11:11 AM), www.slate.com/articles/news_and_politics/view_from_chicago/2013/04/bitcoin_is_a_ponzi_scheme_the_internet_currency_will_collapse.html; Matt O'Brien, *Bitcoin Revealed: a Ponzi Scheme for Redistributing Wealth from one Libertarian to Another*, THE WASHINGTON POST (Jan. 14, 2015), http://www.washingtonpost.com/blogs/wonkblog/wp/2015/01/14/bitcoin-is-revealed-a-ponzi-scheme-for-redistributing-wealth-from-one-libertarian-to-another/; Bruce Richards, *Bitcoin a Ponzi Scheme, Fraud: Marathon's Richards*, BLOOMBERG BUSINESS (Feb. 25, 2014), http://www.bloomberg.com/news/videos/b/c6454137-4042-4d83-a1e4-ed77253b7652. *But see* Andy Bay, *Bitcoin is Not a Ponzi Scheme*, TED CONVERSATIONS (Mar. 18, 2014), http://www.ted.com/conversations/23415/bitcoin_is_not_a_ponzi_scheme.html; Evander Smart, *World Bank: Bitcoin is Not a Ponzi Scheme*, CRYPTOCOINS NEWS (Nov. 19, 2014), https://www.cryptocoinsnews.com/world-bank-bitcoin-not-ponzi-scheme/.

[36] See Charles Mackey's chapter on the "Tulipomania" that occurred among the Dutch in the 17th Century. CHARLES MACKAY, EXTRAORDINARY POPULAR DELUSIONS AND THE MADNESS OF CROWDS, 89–97 (2d Ed. 1890).

[37] Brian Domitrovic, *Aug. 15, 1971: A Date Which has Lived in Infamy*, FORBES (Aug. 14, 2011, 7:36 PM), http://www.forbes.com/sites/briandomitrovic/2011/08/14/august-15-1971-a-date-which-has-lived-in-infamy/.

[38] *Id.*

[39] ABOUT BITSHARES, http://bitshares-x.info/about.php (last visited Dec. 1, 2014).

economists are concerned with the government's ability to print new money whenever it wants, which causes inflation. The total number of Bitcoin, on the other hand, is permanently fixed at 21 million coins. Bitcoin users also like the fact that the transactions are made and controlled by the people, with complete transparency and a record of every Bitcoin transaction available to anyone who wishes to view it.

Other advantages of Bitcoin include: the ability to send or receive money at any time of day or night, including weekends and holidays; lower transaction fees than what are charged by banks and credit card companies;[40] low risk of fraud for merchants since transactions are irreversible; and the transparent nature of the Blockchain.[41]

That said, confidence in Bitcoin due mainly to external events has created a lot of volatility in the currency in the past few years. The first Bitcoin transaction occurred in 2009, but it was not until February 2011 that Bitcoin's value matched the value of the U.S. Dollar.[42] At the start of 2013, a single Bitcoin was worth $13. A year later, Bitcoins were selling for around $900.[43] By December 2014, Bitcoins were selling for around $400.[44] At its peak in December 2013, a single Bitcoin was worth $1,145.[45] The volatility has greatly decreased in the past year with the average price of a Bitcoin staying right around $300.[46]

---

[40] "While credit card networks charge merchants fees in the range of 3 to 4 percent of the total amount of a transaction, and the average cost of international remittances is 8.5 percent, a Bitcoin transaction can cost less than 1 percent." Jerry Brito et al., *Bitcoin Financial Regulation: Securities, Derivatives, Prediction Markets, and Gambling*, 26 COLUMBIA SCIENCE & TECH. L. REV. 144, 150 (2014).

[41] Frequently Asked Questions, What are the Advantages of Bitcoin?, https://bitcoin.org/en/faq#what-are-the-advantages-of-bitcoin (last visited May 24, 2015).

[42] Loz Blain, *The Rise of Bitcoin: Bonanza or Bust?*, GIZMAG (Feb. 19, 2013), http://www.gizmag.com/bitcoin-creation-value-overview/26325/.

[43] The values represent Bitcoin purchases in Salt Lake City as of January 2, 2014. BITCOIN CHARTS, http://bitcoincharts.com (last visited Jan. 2, 2014).

[44] Id.

[45] Michael J. Casey, *Bitcoin Trading Platform Atlas Partners with National Stock Exchange*, WALL STREET JOURNAL (Apr. 23, 2014, 12:16 AM), http://www.wsj.com/articles/SB10001424052702304049904579518224044905190.

[46] The average Bitcoin sold for $325 in 2015. BITCOIN CHARTS, http://bitcoincharts.com (last visited Nov. 1, 2015).

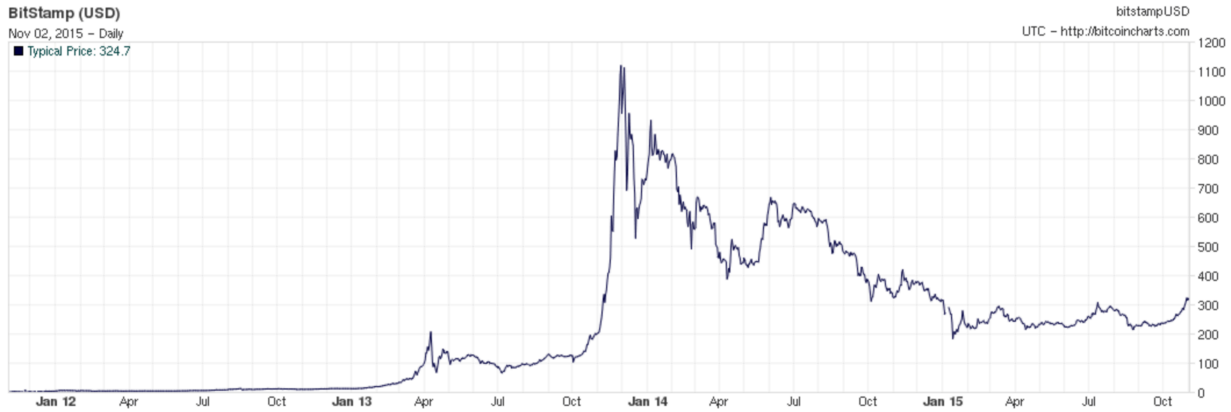


Chart showing the value of 1 Bitcoin from 2011–2015. Created at bitcoincharts.com.[47]

II. BITCOIN'S TECHNOLOGY—THE BLOCKCHAIN

Bitcoin is a digital currency. Unlike traditional currency and coin, Bitcoin does not have a physical form. This means that Bitcoins are stored, transferred, bought, and sold completely online—using the Blockchain. These transactions can be performed completely peer-to-peer, meaning without the assistance and verification of a trusted third party (such as a bank). Or, Bitcoin users can go through an exchange to complete this process for them. Either way, the technology behind the Bitcoin transfers is the same.

This section first provides an introduction to the Blockchain and its unique characteristics, including transparency, decentralization, mining, and use of cryptography. Second, the section walks through an example of how a peer-to-peer transaction works on the Blockchain, from the individual transaction level to incorporating the transaction into the Blockchain to completing the proof necessary to ensure the transaction's validity. Third, the section looks at some of the concerns associated with the proof stage of the Blockchain and some of the alternatives to this system. Finally, the section explains how the Blockchain could be implemented for peer-to-peer stock trading on a cryptosecurities market.

[47] BITCOIN CHARTS, http://bitcoincharts.com/charts/bitstampUSD#rg1460ztgTzx (last visited Nov. 1, 2015).

A. The ABCs of the Blockchain

1. Transparency and Anonymity

The Blockchain acts as a public ledger or transaction database and allows any person who downloads the Bitcoin software onto his or her computer to view a complete history of every Bitcoin transaction ever completed. This ledger may also be viewed online at https://Blockchain.info. Each individual Bitcoin may be traced from its inception through to present day.

While the transactions are entirely transparent, the identity of the users conducting the transactions is more difficult to determine. Although many Bitcoin users operate under the assumption that the Blockchain allows for anonymous transfers—see, e.g., Ross Ulbricht of Silk Road[48]—the reality is that, while the identity of the users is difficult to trace, it is still possible to trace user identity through a variety of different methods, including tracking IP addresses.[49]

2. Decentralization

The Blockchain does not have a central bank, a CEO, intermediary, or anyone else in charge. Like Wikipedia, Craigslist, and the ocean starfish that cling to rocky shorelines,[50] the

[48] On February 4, 2015, Ross Ulbricht was convicted of creating the black market illegal drug website Silk Road. Ulbricht operated under the assumption that his dealings were private, however Ulbricht "misplaced trust in a handful of technologies" and the FBI was able to trace Ulbricht as the Dread Pirate Roberts. Joab Jackson, *5 Technologies that Betrayed Silk Road's Anonymity,* PCWORLD (Feb. 9, 2015, 2:36 PM), http://www.pcworld.com/article/2881772/four-technologies-that-betrayed-silk-roads-anonymity.html. Ironically, eighteen months after the Silk Road shutdown, two federal agents involved in taking down the site and Ulbricht were arrested for stealing millions of dollars of Silk Road money and depositing it into their own personal accounts, believing that anonymity would protect these illegal transfers. Andy Greenberg, *DEA Agent Charged with Acting as a Paid Mole for Silk Road*, WIRED (Mar. 30, 2015, 1:40 PM), http://www.wired.com/2015/03/dea-agent-charged-acting-paid-mole-silk-road/.

[49] Alex Biryokov et al., *Deanonymisation of Clients in Bitcoin P2P Network* (Nov. 2014), http://orbilu.uni.lu/bitstream/10993/18679/1/Ccsfp614s-biryukovATS.pdf.

[50] Much like the Blockchain, "the starfish doesn't have a head. Its central body isn't even in charge. In fact, the major organs are replicated throughout each and every arm. If you cut the starfish in half, you'll be in for a surprise: the animal won't die, and pretty soon you'll have two starfish to deal with." ORI BRAFMAN & ROD BECKSTROM, THE STARFISH AND THE SPIDER 35 (2006).

Blockchain is completely decentralized. Any person in the world with an internet connection can download the software and will have access to what everyone else within the system has, including the ability to mine Bitcoin. This design was not by accident; "indeed the lack of such centripetal features was a core design goal for Bitcoin; as Nakamoto once wrote, '[a]t some point I became convinced there was a way to do this without any trust required at all and couldn't resist to keep thinking about it.'"[51]

An advantage of this type of decentralized financial system is that it cannot be censored. "For example, while PayPal froze the accounts of WikiLeaks after it released secret State Department cables, and prevented its customers from making donations to the group, such transactional prior restraint would not be possible on the Bitcoin network because there is no intermediary."[52]

Any other financial exchange system before Bitcoin required trust—in the form of a trusted third party that verifies each transaction. Rather than trust, the Blockchain relies on "proof" to determine if a transaction is authentic.[53] This proof allows the system to operate autonomously, with each user looking out for its own best interest and, in the process, keeping the entire system honest and secure. For Bitcoin, the proof is established through use of computational power (CPU). The users that devote the most CPU are able to prove that the transaction is accurate and authentic. This proof is discussed further in the Proof-of-Work section *infra*.

---

[51] Shawn Bayern, Of Bitcoins, Independently Wealthy Software, and the Zero-Member LLC, 108 NW. U.L. REV. Online 257, 259–60 (2014) (quoting Satoshi Nakamoto, Re: Transactions and Scripts: DUP HASH160 ... EQUALVERIFY CHECKSIG, BITCOIN FORUM (June 18, 2010, 4:17 PM), https://bitcointalk.org/index.php?topic=195.msg1617#msg1617.

[52] Jerry Brito et al., Bitcoin Financial Regulation: Securities, Derivatives, Prediction Markets, and Gambling, 26 COLUMBIA SCIENCE & TECH. L. REV. 144, 149 (2014).

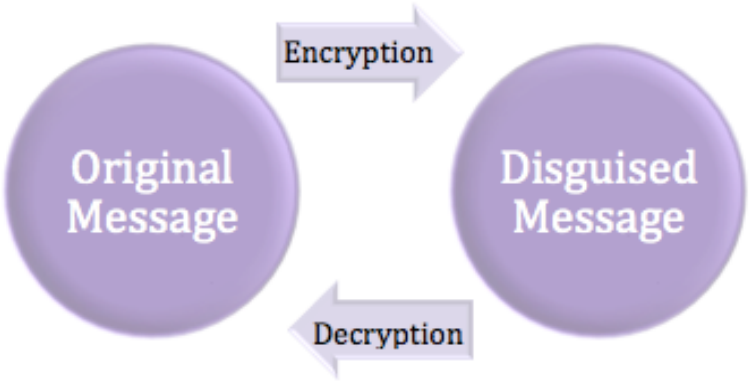
[53] The "proof of work" method is discussed more in Part C, *infra*.

3. Mining

The Blockchain is managed by people called "miners" or "nodes." The miners keep the system running and ensure double transactions are not taking place and that each transaction is legitimate. As Bitcoin transactions become more complex, miners are increasingly working in teams rather than individually to more quickly solve the computational problem. The amount of CPU miners put into a given transaction works effectively as a vote, where the transaction that devotes the most computational power or votes wins and gets added to the chain.

4. Cryptography

The Blockchain uses cryptography to secure its transactions. Cryptography is "the art of creating and using methods of disguising messages, using codes, ciphers, and other methods, so that only certain people can see the real message."[54] Cryptography is derived from the Greek words *kryptos* (hidden) and *graphein* (writing).[55] If Alice wants to send Bob a secret message using cryptography, Alice would *encrypt* the message which would convert the original message into a disguised message, and then Bob would *decrypt* the message to convert the disguised message back into the original message.[56]



[54] A. Michael Froomkin, The Metaphor Is the Key: Cryptography, the Clipper Chip, and the Constitution, 143 U. PA. L. REV. 709, 713 (1995).
[55] Monica Pawlan, *Cryptography: The Ancient Art of Secret Messages* (Feb. 1998), http://www.pawlan.com/monica/articles/crypto/.
[56] A. Michael Froomkin, *supra* n. 54 at 714.

Cryptography can range from very simple to extremely complex. Probably the most simple way to send a cryptographic message is to merely rearrange the letters in a message. Julius Caesar used a simple form of cryptography to send messages to his generals by replacing each letter in a word with a letter three positions down in the alphabet (e.g. a=d, m=p).[57] This is called the Caesar Cipher.[58]

One type of cryptography that Bitcoin employs is called SHA-256. This type of cryptography is one way, meaning the disguised message can never be encrypted back to the original message. For example, if Alice wants to send Bob a love letter using SHA-256, she will start with her original message, which can be of any arbitrary length. If she puts "I love you Bob" through SHA-256, the encrypted message is called a "hash" and will be always be exactly 64 numbers and characters in length.[59] In this case, the disguised message/hash is: 48ab675a2c361fbbd496ee7b1a962eab12abbf2f38c372a7b9b8485a36e628d5.

If the only information you have is this hash or disguised message, it is impossible to know that the original message was "I love you Bob." However, if you know the input is "I love you Bob," you can easily put it through the SHA-256 converter and will always end up with the

[57] Caesar Cipher, PRACTICAL CRYPTOGRAPHY, http://practicalcryptography.com/ciphers/caesar-cipher/.
[58] Id.
[59] Calculate your own SHA-256 hashes at: http://www.online-convert.com/result/146b3767c52e975cc1c24e64e805c6f7.

same resulting hash. If, however, you change *anything* in the original message including punctuation or capitalization, the result is a completely different hash. For example, "I lov you Bob" becomes: d63ea03682f1849bfc1c876fad349c44207cfb77935720dbef1e8adbf64f2d15. To understand how cryptography fits into the Blockchain, I will walk through a step-by-step example of a Bitcoin transaction.

B. An Example of How Transactions Are Processed and Incorporated on the Blockchain—The Story of Alice and Bob

To understand how these transactions work and fit in to the Blockchain, it is easiest to start at the micro level and then expands to the macro level.[60] This section first discusses what goes on at the individual transaction level, then how the transactions are incorporated into the blocks on the Blockchain, and then how proof of work keeps the blocks in order and prevents double spending.

1. The Transaction—Alice Buys a Pizza

Most of the transactional steps below are accomplished automatically through software programs and users rarely know this level of detail about their Bitcoins. However, it is helpful to know the process of these transactions to better understand how this same technology could be used in a cryptosecurities market.

[60] This is a very high level summary of how this technology works. For an excellent and greatly detailed explanation of the minutiae of these transactions, *see* ANDREAS M. ANTONOPOULOS, MASTERING BITCOIN (2014).

Step 1 – The Bitcoin Wallet

Let's say Alice wants to buy a pizza from Bob using Bitcoin.[61] If Alice were using cash, she would reach into her back pocket or purse and pull out her wallet, select the desired amount of cash, and then give the cash to Bob. Since Alice wants to pay with Bitcoin, she will go into her *Bitcoin wallet*—stored either on her computer or online—which holds all of Alice's Bitcoins.

Step 2 – The Message

Alice will then create a message to the effect of "I want to transfer one Bitcoin to Bob."[62] The message will also include a "hash" from the last time this Bitcoin was used. For example, say Alice's dad gave Alice the Bitcoin for her birthday. The transaction between Alice and her dad results in a digest or transaction hash. This hash is used as part of her message in the Alice-Bob transaction. Once the Alice-Bob transaction is complete, it will create a new hash that will be used when Bob is ready to transfer his Bitcoin to someone else. This is how it is possible to track each Bitcoin all the back to its inception.

[61] A lot of the information from this example comes from: *Bitcoin: Transaction Records*, KHAN ACADEMY, https://www.khanacademy.org/economics-finance-domain/core-finance/money-and-banking/bitcoin/v/bitcoin-transaction-records.

[62] For simplicity's sake, I will use one Bitcoin for this example, although that would be an incredibly expensive pizza. Also, the very first thing ever purchased with Bitcoin was a pizza, so it is fitting.

Step 3 – The Keys and the Bitcoin Address

Bitcoin uses a system of keys and cryptography—called public-key cryptography—to allow its users to trade safely without giving away any sensitive information.[63] The keys allow for "many of the interesting properties of bitcoin, including decentralized trust and control, ownership attestation, and the cryptographic-proof security model."[64] First, Alice and Bob will both need to create a *private key*, which is like a debit card pin number. Only the holder of the key should know this number and it is important to keep it backed up because if it is lost, it is gone forever. The private key will later be used to sign the transaction. Bitcoin wallet software will create a random private key number, made up of 256-bit binary numbers—meaning 256 random digits of zero or one.[65] This very long number can be compressed into a hexadecimal[66] format of 64 digits, where each digit represents 4 bits. For example: 1E99423A4ED27608A15A2616A2B0E9E52CED330AC530EDCC32C8FFC6A526AEDD.[67]

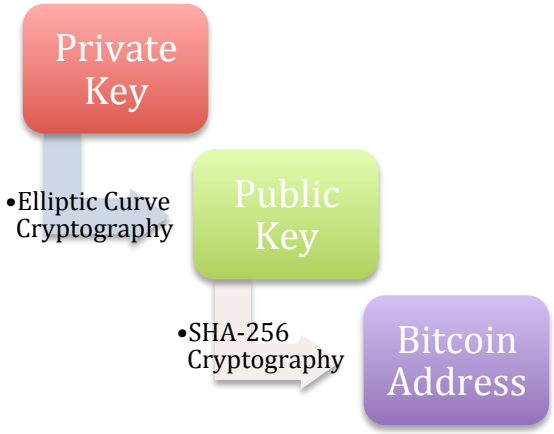
Using their private keys, Alice and Bob will each create a corresponding *public key*. The private to public key conversion is accomplished by using elliptic curve cryptography, which is mathematically different from SHA-256 but for our purposes it is similar in that it is one-way cryptography so anyone with the public key will never be able to figure out the private key, but if you have the private key you will always get the same public key result.[68]

Then, the public key will again go through a cryptographic transformation—this time using SHA-256—to come up with the *Bitcoin address*. The Bitcoin address is a string of

---

[63] Jerry Brito et al., Bitcoin Financial Regulation: Securities, Derivatives, Prediction Markets, and Gambling, 26 COLUMBIA SCIENCE & TECH. L. REV. 144, 149 (2014).
[64] ANTONOPOULOS, supra n. 60.
[65] Ckwop, *What Does 128-Bit Encryption Really Mean?*, http://www.ckwop.me.uk/What-does-128-bit-cryptography-really-mean.html (last visited May 24, 2015).
[66] Hexadecimal format includes the first 6 letters of the alphabet and the numbers 0-9.
[67] ANTONOPOULOS, supra n. 60.
[68] For a thorough explanation of elliptic curve cryptography, *see* DARREL HANKERSON, GUIDE TO ELLIPTIC CURVE CRYPTOGRAPHY (2004).

alphanumeric characters that signifies where Alice will send Bob's Bitcoin.[69] Bitcoin addresses start with the number "1", for example: 1J7mdg5rbQyUHENYdx39WVWK7fsLpEoXZy.[70] A Bitcoin address is similar to an invoice that a merchant sends out to its customers. Bob should create a new Bitcoin address for every transaction just like he would use a new invoice number for each customer. Bitcoin users can create as many keys and Bitcoin addresses as they wish. Alice will either need to know the exact address in which to send her Bitcoin, or more likely Bob will have a scannable QR code to which Alice may send the Bitcoin.[71]

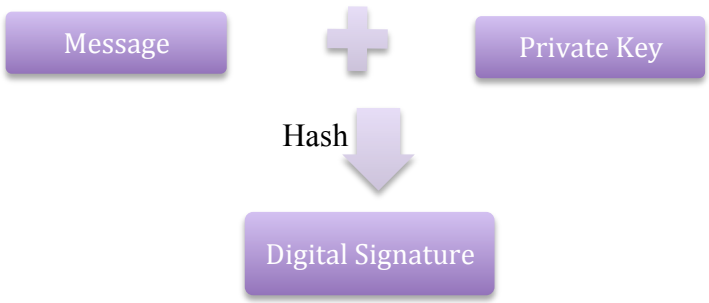


Step 4 – Signing the Transaction

Once Alice is ready with the message ("I want to send one Bitcoin to Bob" + last transaction hash) and Bob's Bitcoin address, Alice will sign this transaction using her *digital signature*. Just like the public key and Bitcoin address are derived from the private key, the digital signature is also cryptographically derived from the private key and the message. This is like signing a credit card receipt except that it is much more difficult to forge this signature. Note

[69] Melanie Swan, Blockchain: Blueprint for a New Economy 3 (2015).
[70] Example take from ANTONOPOULOS, supra n. 60.
[71] Timothy B. Lee, *12 Questions About Bitcoin You Were Too Embarrassed to Ask*, WASHINGTON POST (Nov. 19, 2013), http://www.washingtonpost.com/blogs/the-switch/wp/2013/11/19/12-questions-you-were-too-embarrassed-to-ask-about-bitcoin/.

that any change in the message will alter the resulting digital signature, because the digital signature is derived from both the message and the private key.



Step 5 – Broadcast to the Network

Up to this point, everything can be done offline. Once all the correct parts are in place, Alice will need to connect to the Bitcoin network. Alice will then submit the request to transfer her Bitcoin to Bob and almost instantaneously everyone in the Bitcoin network can view this request including Bob's Bitcoin address and Alice's public key. This is where the *miners* come into play. Miners are essentially computers hooked up to the Bitcoin network that both serve to verify individual transaction, and to place those transactions within blocks on the Blockchain.

Miners will be able to determine the authenticity of Alice's signature just by knowing her public key number.[72] They do not need to know Alice's private key. They will take the message, digital signature, and Alice's public key number and this will create the transaction hash number

[72] Jerry Brito et al., Bitcoin Financial Regulation: Securities, Derivatives, Prediction Markets, and Gambling, 26 COLUMBIA SCIENCE & TECH. L. REV. 144, 149 (2014).

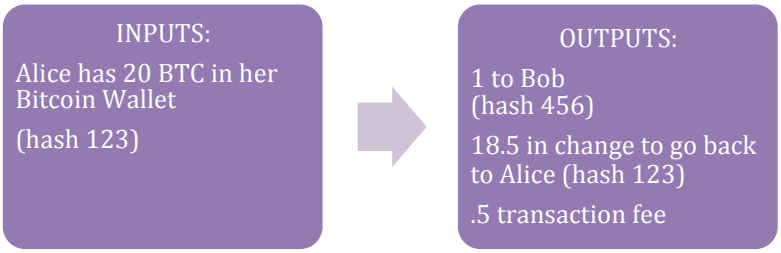
for this particular transaction. Bob's new Bitcoin will remain encumbered until he is able to verify with his signature that he owns the Bitcoin address that he told Alice to use.[73]

Step 6 – Transaction Fees

For simplicity in the above example, I left discussion of transaction fees out until now. A common misconception about Bitcoin is the idea that there are no transaction fees. In actuality, miners get a transaction fee on every transaction they successfully mine. There are two ways to earn transaction fees. First, anytime Alice wants to transfer Bitcoins to Bob, she must designate a portion of the transfer to go to the miners as a transaction fee. Second, any time a new block is successfully added to the Blockchain, brand new Bitcoins are released as a reward. For now, I will focus on the individual transaction fee.

Bitcoin transactions consist of inputs and outputs. The input consists of the previous transaction information—i.e. the amount and transaction hash from the Dad-Alice exchange. The output will always equal to the same amount as the input,[74] just like it would on a balance sheet. The output will specify the amount to go to Bob, the amount that will need to remain with Alice in the form of change, and the transaction fee. Sometimes it takes several inputs to make one large output (e.g. if Mom, Dad, and Grandpa each gave Alice small amounts that equaled one Bitcoin), or Alice could use one input for several outputs (e.g. she wanted to pay Bob for pizza but Charlie for soda). Below is a modification of the above example where Alice's dad originally gave her 20 Bitcoin instead of one, and how this would break down as inputs and outputs:

[73] ANTONOPOULOS, supra n. 60.
[74] In actuality, the transaction fee is not listed explicitly in the Blockchain but is rather inferred, as the output will always be slightly less than the inputs.

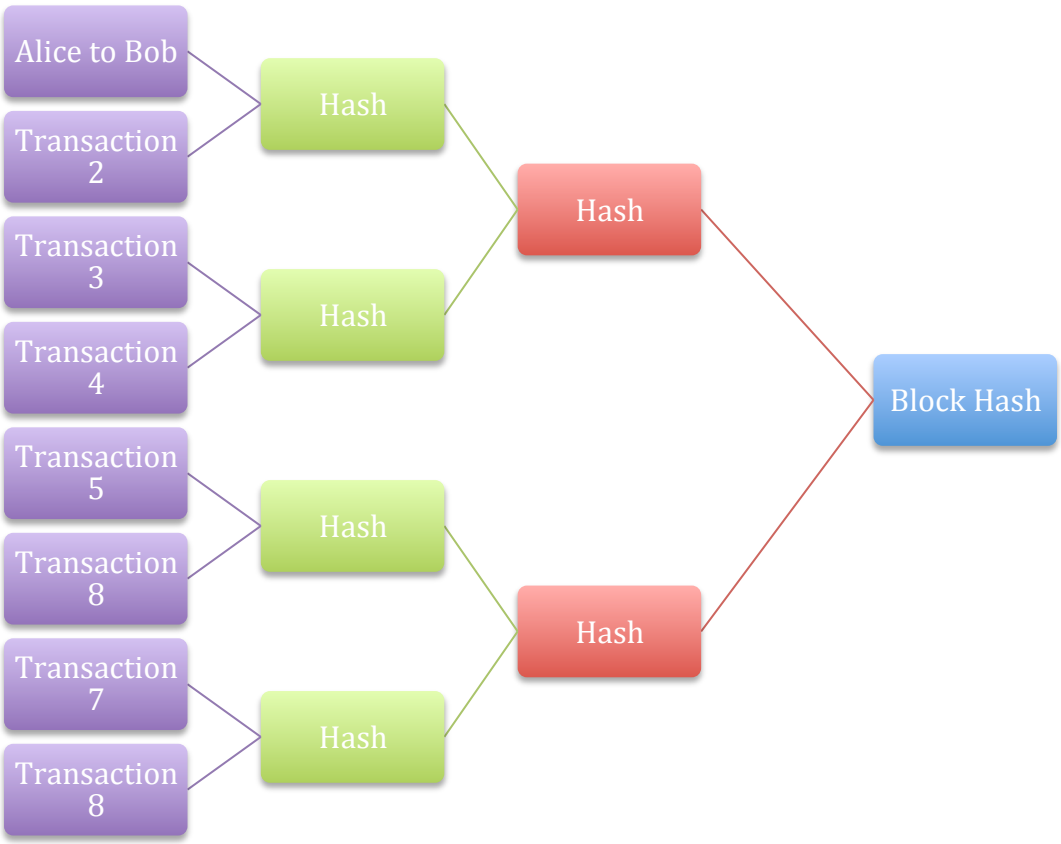


2. Incorporating the Transaction into the Blockchain

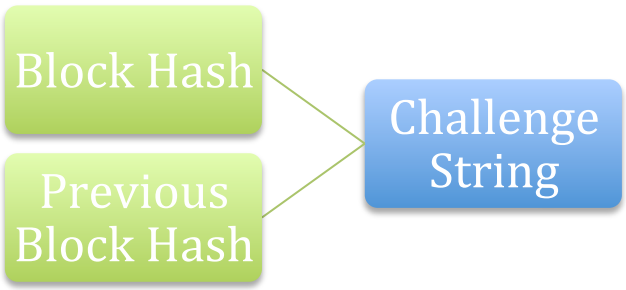
Once the transaction has been verified, it will sit on the network unconfirmed until it is packed into several other transactions in a *block*. This process takes around ten minutes and this is the main aspect of the miners' job. The first step the miners will take is to collate all the recent transactions into a single transaction block. Think of a transaction like a proposed entry in a ledger and the block as a page out of the ledger.[75]

Once all of the recent transactions are organized into a proposed new block, the miners will go through a series of SHA-256 cryptographic hashes until all of the transactions result in one hash. To do this, miners will start with hashing all the transactions in pairs. The miners will then take those hashes and hash them in pairs, and will keep performing these iterations until finally there is just one final hash.

[75] *Bitcoin: Transaction Block Chains*, KHAN ACADEMY, https://www.khanacademy.org/economics-finance-domain/core-finance/money-and-banking/bitcoin/v/bitcoin-transaction-block-chains.



Then, miners will combine the block hash with the block hash from the previous block. Going all the way back to the *genesis block*—the very first block on the Blockchain—each block contains the block hash from the block before it. This is just like how each transaction contains a piece of the transaction before it in order to track Bitcoin transfers back to their individual inception. Miners will take the two block hashes and will run another SHA-256 hash to result in the hash that will be used in the proof-of-work formula (described further in the next section). This is called a *challenge string*. Miners will use this challenge string to help them solve a mathematical puzzle called proof of work and once this puzzle is solved the block will officially be added to the Blockchain.



3. Proving the Work

A Proof-of-Work system is sort of like a puzzle, requiring the miners to go through a lot of computational work in order to prove that a transaction is legitimate. Once the initial computational work is performed and the puzzle is solved, it is much easier to verify that the answer is the correct answer.

To break this concept down into something tangible,[76] imagine someone gave you the number 589 and then asked you to figure out the two prime numbers that make up 589. To figure it out, you would need to go through a lot of trial and error before finally discovering that 9 and 31 multiplied together equals 589. Once this initial work is performed, it is much easier for anyone else in the system to verify that this is correct by simply multiplying 9 and 31 together and seeing that 589 is correct.

Bitcoin's proof of work operates in this way but on a much more difficult level that requires very high computational effort. Bitcoin's puzzle is more like starting with a can of mixed paint and trying to figure out what colors and in what quantity went into the can. Of course, Bitcoin miners themselves are not trying to figure out these incredibly complex formulas with pen and paper or a calculator; their computers are doing these for them by making millions

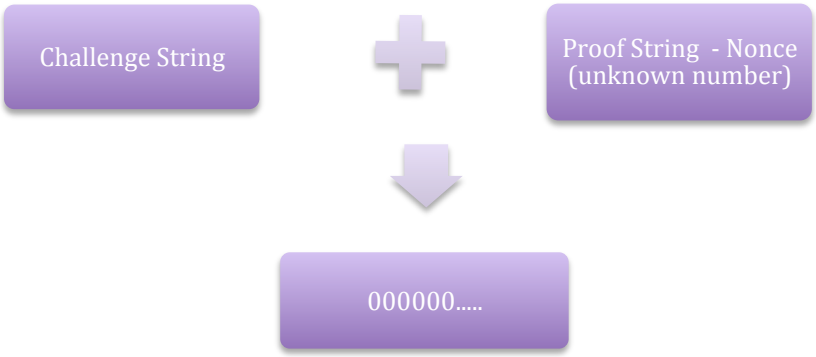
[76] This example comes from James Lyne, *Everyday Cybercrime—And What You Can Do About It*, TED (Feb. 2013), https://www.ted.com/talks/james_lyne_everyday_cybercrime_and_what_you_can_do_about_it?language=en.

of guesses per second to try and solve the problem. This takes an immense amount of computational power and takes on average ten minutes to solve the puzzle.

First, miners will start with the challenge string (the final hash from the current block hashed with the previous block). Miners are going to search for the "proof"—that is the answer to the challenge. This proof string is also called a *nonce*. Miners know that when the challenge string and the correct proof string are taken together and hashed, the end result will be a number with certain mathematical properties—specifically the final result must contain a specified number of zeroes at its start.

For example, in order to add the block containing Alice and Bob's transaction to the Blockchain, miners will be given a problem to solve and they will know the end result will start with 40 zeroes. In order to come up with a proof string that when combined with the challenge string and then hashed comes out to a number with 40 zeroes, miners will try a trillion different possibilities, and at some point one of the miners will come up with the correct answer. Once a miner discovers the correct proof string, he will broadcast the new block to all other active miners in the system.[77] The other miners will immediately shift from trying to solve the puzzle to verifying that all of the transactions are valid and that the proof string really solves the puzzle. The number of verifications a proof string receives acts as votes and the block with the most votes wins. The block will officially be added to the Blockchain and a new reward will be released. Miners will then begin working on the next block, using the hash of the previously accepted block.

[77] Nakamoto, supra n. 3 at 3.



a. Coinbase/Generation Reward

The reward released as a new block is added to the chain is called a *coinbase reward* (also called a generation reward). Just like mining for gold or any other precious metal, the more Bitcoin that is mined the more difficult it is to receive a reward. At Bitcoin's inception, a new block resulted in a 50 Bitcoin reward. Today, a new block results in a 25 Bitcoin reward. The coinbase reward will halve every few years until all 21 million Bitcoins are released, which is expected to happen in 2040.

Year	# of new coins generated per block[78]
2009	50
2012	25
2016	12.5
2020	6.25
2024	3.125
2028	1.56
2032	0.78
2036	0.38
2040	0.19

[78] Controlled Supply, BITCOIN WIKI, https://en.bitcoin.it/wiki/Controlled_supply (last visited Dec. 1, 2014).

b. Difficulty Level

Nakamoto designed the level of difficulty in generating a new block to change every two weeks so that each transaction takes an average of ten minutes to process.[79] This is accomplished by changing the number of zeroes required at the beginning of the answer to the proof and challenge strings. The more zeroes, the more difficult the problem becomes to solve. If it starts taking less than ten minutes, then the number of zeroes goes up, requiring more time to solve the problem. If it takes more than ten minutes, then the number of zeroes required will adjust downward. As more and more people are mining Bitcoin, the difficulty has increased exponentially in the past few years. Currently, it takes around forty billion attempts to come up with one correct proof string.[80]

c. Simultaneous Solving/Orphan Blocks

One last topic that is important to understand is the concept of simultaneous solving and orphan blocks. It is possible that two miners will solve for the proof string at the same time and create two identical blocks. This makes it confusing for the rest of the miners in trying to figure out which block to use for building on the next block. The tie is broken when the next proof is found, and one of the branch becomes longer than the other. In other words, the block with the most computational power (CPU) associated with it will be the one that other miners accept as being the most accurate and verified block. Miners "express their acceptance of the block by working on creating the next block in the chain, using the hash of the accepted block as the

[79] Protocol Rules, BITCOIN WIKI, https://en.bitcoin.it/wiki/Protocol_rules (last visited Dec. 1, 2014).
[80] Anthony Volastro, *CNBC Explains: How to Mine Bitcoins on your Own*, CNBC (Jan, 23, 2014, 1:48 PM), http://www.cnbc.com/id/101332124.

previous hash."[81] The rejected or *orphan blocks* will not last long as the rest of the system will stick with the accepted blocks.

C. Proof of Work Concerns and Alternative Systems

Although proof of work really revolutionized the way transactions are processed by allowing transactions to be handled peer-to-peer without a third party intermediary, it has some significant disadvantages. This section will address those disadvantages and then will highlight a few alternatives to proof of work.

1. Disadvantages of Proof of Work

The three most often cited disadvantages of proof of work are: (1) the computational effort required; (2) diminishing returns; and (3) a 51% attack. The alternative systems that will be discussed below mainly focus on fixing the first and most serious problem—the computational effort required. But first, each of these three issues will be discussed in turn.

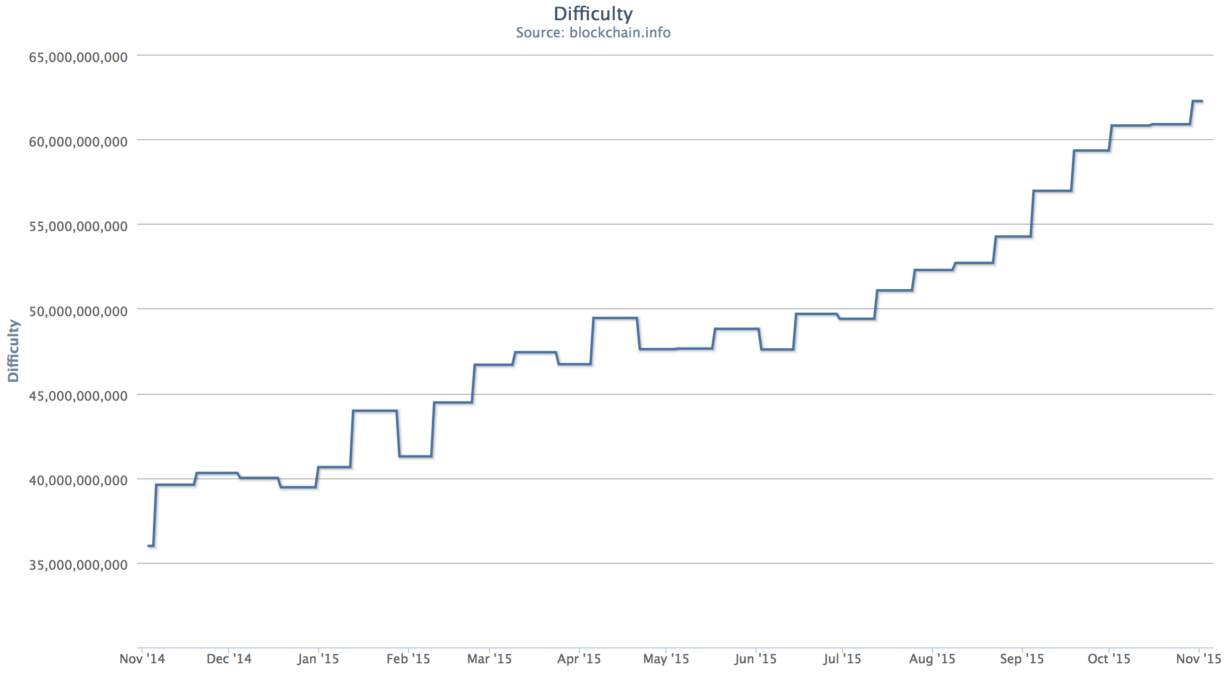
a. Required Computational Effort (CPU)

Rather than giving each miner one vote and allowing majority vote to rule the day ("one-IP-address-one-vote"[82]), the Blockchain was designed with computational power (CPU) in mind ("one-CPU-one-vote"[83]). Initially this seemed like a good idea because with majority vote "an attacker could game the system by creating numerous fake identities."[84] Proof of work is designed so that it is very costly to game the system.

---

[81] Nakamoto, supra n. 3 at 3.
[82] Nakamoto, supra n. 3 at 3.
[83] Id.
[84] Rainier Bohme et. al., *Bitcoin: Economics, Technology, and Governance*, 29 J. OF ECON. PERSPECTIVES, 213, 218–19 (2015).

However, the disadvantage of using CPU power as proof is the significant amount of energy that is required. Currently, performing these proof-of-work calculations burns through "173 megawatts of electricity continuously. For perspective, that amount is approximately 20 percent of an average nuclear power plant."[85] The energy required is estimated to cost around $600 million.[86] As mentioned above, as interest in Bitcoin has grown and more and more miners have joined the system, the difficulty level has adjusted upward and it results in a much higher level of energy expended.



b. Diminishing Returns

[85] *Id.* at 218.
[86] William Mougayer, *The Blockchain is the New Database, Get Ready to Rewrite Everything*, STARTUP MGMT. (Dec. 27, 2014), http://startupmanagement.org/2014/12/27/the-blockchain-is-the-new-database-get-ready-to-rewrite-everything/.

The concept of diminishing returns has many in the media concerned.[87] As more and more Bitcoins are mined, the coinbase reward will continue to get smaller until it disappears entirely. The argument is that once the reward disappears, miners will no longer be incentivized to mine, and because very few people will mine, the security of the entire system will be jeopardized. However, this concern may be overblown for two reasons. First, the fact is that most miners get their fees from the individual transactions and not from adding a new block to the chain, so it is unlikely that miners will be disincentivized to mine once all 21 million Bitcoins are released. Second, the Bitcoin system is designed with adjusting difficulty to take into account the changing number of miners and to ensure that mining is profitable.

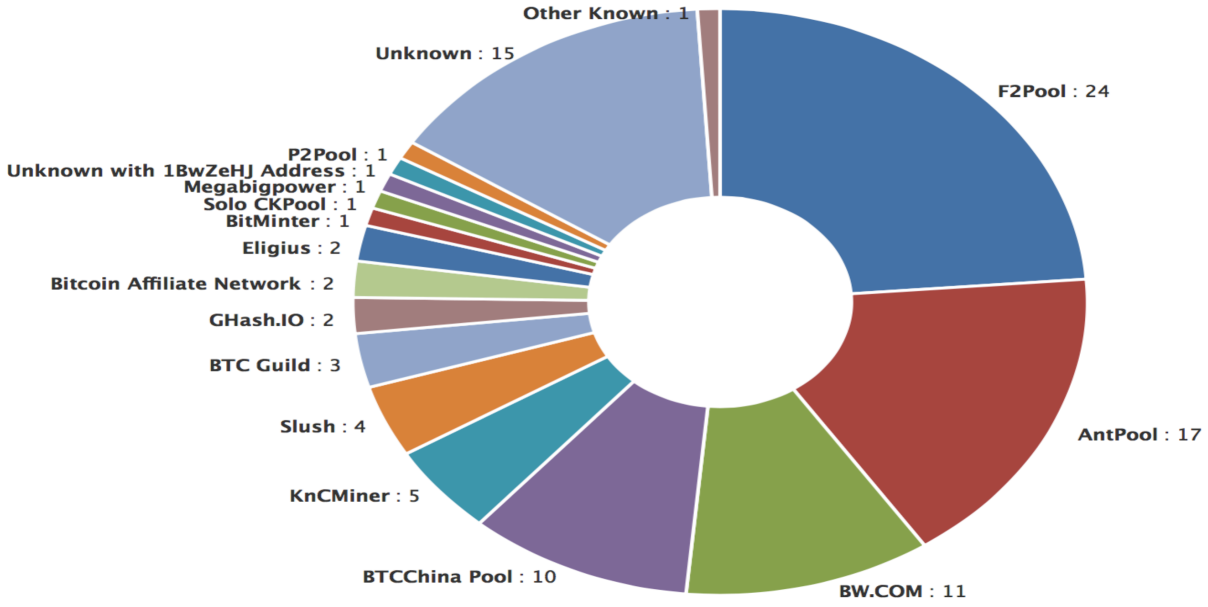
c. 51% Attack

Although the Blockchain is incredibly secure, it is not immune from attack. Hacking typically occurs when someone breaks into an online exchange or online wallet provider and steals the Bitcoin keys stored on the site. Thus far, no one has ever broken into the actual Blockchain and stolen Bitcoins through that directly; it has always been through third-party Bitcoin storage providers.

In order for the actual Blockchain to be hacked, a miner or a pool of miners would have to attain 51% of the computing power, and then rewrite the Blockchain's history. At the beginning of Bitcoin's history, it was fairly easy to mine and required little computational power, and the potential for a 51% Attack was a lot higher. However, "as time goes on and more powerful devices run legitimate copies of the software, it becomes extremely difficult for any

[87] Maria Korolov, *Bitcoin Approaching Diminishing Returns*, HYPERGRID BUS. (Feb. 21, 2014), http://www.hypergridbusiness.com/2014/02/bitcoin-approaching-diminishing-returns/; Alec Liu, *A Guide to Bitcoin Mining: Why Someone Bought a $1,500 Bitcoin Miner on eBay for $20,600*, MOTHERBOARD (Mar. 22, 2013, 9:45 AM), http://motherboard.vice.com/blog/a-guide-to-bitcoin-mining-why-someone-bought-a-1500-bitcoin-miner-on-ebay-for-20600; Alec Liu, *How to Really Get Rich From Bitcoins*, MOTHERBOARD (Apr. 10, 2013, 9:40 AM), http://motherboard.vice.com/blog/how-to-really-get-rich-from-bitcoins.

single party to disrupt the system."[88] That said, as mining becomes more difficult, the demographics of miners have changed. "Individual home miners have given way to large operators that invest substantial money in mining farms in far away places with low temperatures and low electricity costs."[89] Additionally, many miners have joined mining *pools* that allow them to collectively solve the proof of work and then split the reward between them. Below is a chart showing the percentages of Bitcoin mined by pools.[90]



These pools present a risk of centralization. This is not something Satoshi Hashimoto had in mind for Bitcoin,[91] but is becoming increasingly common. Last year some of the largest pools voluntarily split into smaller pools because the top two pools actually held a majority of the CPU power. The fear with centralization is that if one group holds a majority of the mining power

[88] Shawn Bayern, Of Bitcoins, Independently Wealthy Software, and the Zero-Member LLC, 108 NW. U.L. REV. Online 257, 262 (2014).
[89] Giulio Prisco, *Mining Bitcoin is Big Business—the Economist*, CRYPTOCOINS NEWS (Jan. 10, 2015), https://www.cryptocoinsnews.com/mining-bitcoin-big-business-economist/.
[90] HASHRATE DISTRIBUTION, https://blockchain.info/pools (last visited May 24, 2015). "Unknown" represents either individual miners, or more likely private or mining pools that require an invitation. Blockchain.info.
[91] Nakamoto, supra n. 3 at 1.

(51%), then this group could effectively rewrite the entire Blockchain. As mentioned above, while it is theoretically possible that one group could hold the majority of mining power, even if it did it is not likely it would want to rewrite the Blockchain.[92] As soon as the majority CPU began rewriting the Blockchain, everyone else in the network would notice and the price of Bitcoin would plummet. Therefore, the fear of this threat appears to be overblown.

2. Alternative to Proof of Work—Proof of Stake

Proof of stake is an alternative to using proof of work to verify digital transactions. Where proof of work weighs votes based on the amount of computational power devoted to the system, a proof of stake system weighs votes based on the number of Bitcoins a user owns.[93] Therefore, a person holding 1% of the total Bitcoins could mine 1% of the blocks.[94] This solves the problem with majority vote mentioned above (one-IP address-one-vote), because users must have a stake in the system before they can cast their votes. This is thought to be a better system because some are concerned that with the diminishing returns referred to in the previous section, the security of Bitcoin transactions will decrease over time. If instead the votes are based on the miner's ownership, the miner is incentivized to ensure the transactions are accurate because it has a "stake" in the future performance of the currency.

Where the fear with proof of work is diminishing returns, the fear with proof of stake is monopoly problems. In proof of stake, if a user gains 51% of the outstanding coins, then it

[92] Awhile back a mining group was getting close to reaching a majority, and it voluntarily split into several small groups in order to ensure the integrity of the system. This is another reason why it is unlikely that a mining group would be able to throw the entire system. Robert McMillan, *Bitcoin Stares Down Impending Apocalypse (Again)*, WIRED (Jan. 10, 2014, 6:30 AM), http://www.wired.com/2014/01/ghash/.

[93] This idea is thought to have originated on a bitcointalk thread in 2011 by member QuantumMechanic. *Proof of Stake Instead of Proof of Work,* BITCOIN TALK (July 11, 2011 4:12 AM), https://bitcointalk.org/index.php?topic=27787.0.

[94] PROOF OF STAKE, https://en.bitcoin.it/wiki/Proof_of_Stake (last visited Dec. 1, 2014).

> could use these resources to impose conditions on the rest of the network. Potentially, the monopolist could choose to do this in malicious ways, such as double spending or denying services. If the monopolist chose a malicious strategy and maintained his control for a long period, confidence in bitcoin would be undermined and bitcoin purchasing power would collapse.[95]

However, just like with proof of work, anyone reaching a majority of the control of the number of Bitcoins would be unlikely to undermine the system because then Bitcoin would lose its value and potentially billions of dollars. Other users will quickly notice that the fifty-one percenter is up to no good and then "the public will lose faith in Bitcoin, and the value of Bitcoins will plummet. So the act of stealing will render the fruits of the theft worthless."[96] Following is a chart showing a summary of proof of work versus proof of stake:

	Proof of Work	Proof of Stake
How Voting Works	Computational power (CPU)	Stake in the currency
Advantages	• Ensures accuracy/validity of transactions • Not required to own a lot of Bitcoin – removes incentive to hoard	• low CPU required • allows those with the most "stake" or skin in the game the highest votes
Disadvantages	• Uses a lot of power – bad for the environment • Diminishing returns • Potential for 51% attack	• Potential for monopolization • Encourages hoarding

a. An Example of Proof of Stake—NXT

To date, the most successful Bitcoin alternative (*altcoin*) using a pure proof-of-stake system is *NXT*. Instead of miners, the system uses "forgers" who forge the transactions into blocks.[97] Forgers are selected to forge a particular block at random with the odds of selection being proportional to the forgers' stake in the network—i.e. the number of NXT coins they

[95] Id.
[96] Ed Felten, *Bitcoin Mining Now Dominated by One Pool*, FREEDOM TO TINKER (June 16, 2014), https://freedom-to-tinker.com/blog/felten/bitcoin-mining-now-dominated-by-one-pool/.
[97] About NXT, Proof of Stake, http://nxt.org/about/proof-of-stake/ (last visited May 24, 2015).

hold.[98] A new block can be added to the chain every two minutes, instead of ten minutes.[99] One unique feature of NXT is that it allows users to forge on their cell phone or home computer—there is no need for fancy mining hardware like that required by Bitcoin. Another interesting feature is that forgers do not get a reward for each new block in the system, they only get transaction fees from the individual transactions.

NXT also solved the potential 51% attack problem by implementing "transparent forging," which is defined as the following:

> Although the [forger] which forges a block is random in the long term, in the immediate future it is highly predictable. This means the network knows where the next block should be forged. If a [forger] does not forge the block it is expected to (perhaps because it is working to build a fraudulent chain instead), it is excluded from the network for a period of time. The likelihood of that [forger] being chosen is instead redistributed across the remaining members of the network.[100]

NXT is also designed not just for cryptocurrency but also to include asset transfer, an online marketplace, private messaging, and the option to create your own currency that is backed by NXT.[101] In the future, NXT plans on adding voting capabilities, smart contracts, and instant transactions.[102]

b. A Twist on Proof of Stake—Delegated Proof of Stake

The company Bitshares uses delegated proof of stake to secure its Blockchain. Delegated proof of stake requires 51% of the stakeholders to agree on the new transactions before they can be added to the Blockchain. However, to save time and increase efficiency, the system allows stakeholders to "delegate their voting power to a delegate. The top 100 delegates by total votes

[98] Id.
[99] HOW TO ISSUE A CRYPTOSECURITY, https://o.info/index.php/How_to_issue_a_cryptosecurity (last visited May 24, 2015).
[100] *Id.* (emphasis removed).
[101] About NXT, What is Transparent Forging?, http://nxt.org/about/proof-of-stake/ (last visited May 24, 2015).
[102] About NXT, Upcoming Features, http://nxt.org/about/upcoming-features/ (last visited May 24, 2015).

take turns generating blocks on a defined schedule."[103] In order to become a delegate, a user must post a small bond. When a delegate behaves badly, i.e. signing n invalid block, failing to produce a block, or failing to reference the previous block, the system will "automatically vote against that delegate the next time their user makes a transaction until that delegate is no longer" able to perform the role of delegate.[104]

3. Mixed Proof of Work/Proof of Stake

Most of the other altcoins that do not rely exclusively on proof of work use some sort of combination of proof of work plus proof of stake or something else entirely. In August 2012, *Peercoin* was the first altcoin "to use a hybrid proof-of-work and proof-of-stake algorithm to issue new currency."[105] Peercoin uses proof of stake to keep the Blockchain secure and uses proof of work to enable the reward associated with completing a new block.[106] Like Bitcoin, the difficulty level is adjusted so that there is ten minutes between transactions, however with Peercoin this difficulty level adjusts after every block is completed and not once every two weeks. This allows for the difficulty level to more accurately reflect reality and keep the transaction time as close as possible to ten minutes.

The company NEM uses "proof of importance" to reward the users who "actively participate in the economy. The balance of an account, who transacts with them, and how much they transact to others are all combined to calculate an account's importance."[107] Instead of

[103] Daniel Larimer, *Delegated Proof of Stake*, BITSHARES (Apr. 3, 2014), http://bitshares.org/blog/delegated-proof-of-stake/.
[104] Id.
[105] ANTONOPOULOS, supra n. 60.
[106] Sunny King & Scott Nadal, *PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake*, PEERCOIN (Aug. 19, 2012), http://peercoin.net/assets/paper/peercoin-paper.pdf.
[107] Alireza Beikverdi, *NEM Launches, Targets Old Economy with Proof-of-Importance*, COINTELEGRAPH (Apr. 1, 2015, 8:14 AM), http://cointelegraph.com/news/113839/nem-launches-targets-old-economy-with-proof-of-importance.

miners or forgers, NEM uses harvesters to do the work verifying transactions.[108] Harvesters must have a stake or vested balance of at least 10,000 of NEM's currency (called "XEM").[109] New blocks are harvested once every minute in NEM's system.[110]

4. Other Innovations

The Blockchain is already being used for a variety of purposes outside of just cryptocurrency transfers. Currency exchange and remittances, smart contracts, smart property, charitable proof of work, and domain name registration are just a few of the innovations currently available.

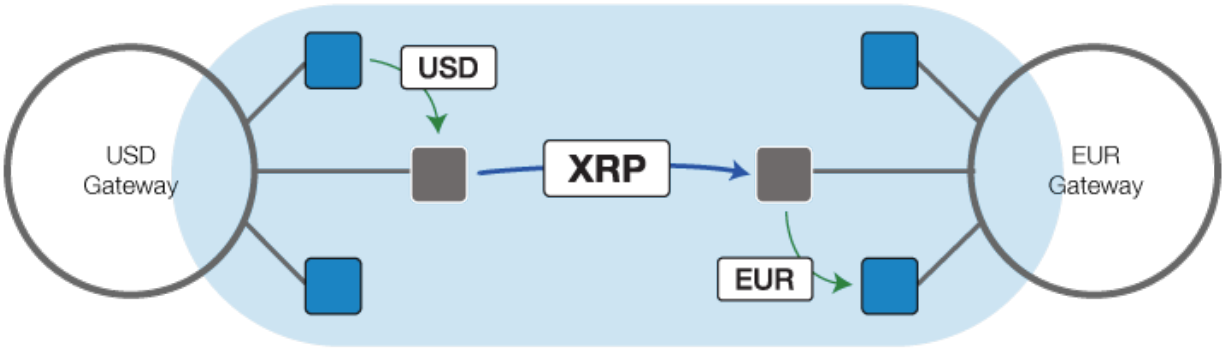
a. Currency Exchange and Remittances—Ripple

Ripple has the second-highest market capitalization next to Bitcoin at $220 million.[111] Ripple created a cryptocurrency called ripples (XRP), but also acts as a currency exchange and remittance network. Ripple supports fiat currency (U.S. Dollars, euros, etc.), other cryptocurrencies (Bitcoin, Litecoin, etc.), commodities, and even frequent flier miles. Ripple uses a Blockchain called the "Ripple ledger" that keeps track of all the transactions in the system.

Ripple also uses "gateways" to enable transfers from one form to another. Gateways are other people or companies that use the Ripple network to make exchanges. Typically, one gateway will convert the asset into ripples which will act as a vehicle currency to enable the exchange into another asset. For example, if Alice has $200 and she wants to trade it for euros, she will send her money to one gateway that will convert her money into ripples and then will

[108] FAQs, http://www.nem.io/faq.html (last visited May 24, 2015).
[109] Id.
[110] Id.
[111] CRYPTO-CURRENCY MARKET CAPITALIZATIONS, http://coinmarketcap.com (last visited May 24, 2015).

send the money to another gateway that will trade the ripples for euros and then send it back to her.



Exchanging U.S. Dollars into Euros, using ripples as the transaction vehicle[112]

The biggest advantage of Ripple is probably for expatriates wishing to send money back to their home countries. Depending on the country and currency, it can take several days and cost a lot of money to make these remittances.[113] Transaction fees can eat up to 12% of these hard-earned payments.[114] Transaction fees on Ripple comes out to around 1/100th of a penny.[115] Also, Ripple is incredibly fast compared to traditional remittance services and even fast compared to Bitcoin. It takes anywhere from two to twenty seconds to confirm a transaction.[116]

Ripple uses a consensus algorithm to approve new transactions that is similar to delegated proof of stake. Ripple miners work in small groups to approve transactions, and 80% of the group must approve before the transaction is approved.[117] This means that 80% of the network—as opposed to 51%—would have to be acting maliciously before someone could upset

[112] RIPPLE FOR MARKET MAKERS, https://ripple.com/trade/ripple-for-market-makers/ (last visited May 24, 2015).
[113] Tom Simonite, *Making Money: Ripple Labs*, MIT TECH. REVIEW (Feb. 18, 2014), http://www.technologyreview.com/featuredstory/524566/making-money/.
[114] Id.
[115] Ariella Brown, *10 Things you need to know About Ripple*, COINDESK (May 17, 2013, 11:00 AM), http://www.coindesk.com/10-things-you-need-to-know-about-ripple/.
[116] RIPPLE FOR MARKET MAKERS, https://ripple.com/trade/ripple-for-market-makers/ (last visited May 24, 2015).
[117] David Schwartz et al., *The Ripple Protocol Consensus Algorithm*, RIPPLE LABS (2014), https://ripple.com/files/ripple_consensus_whitepaper.pdf.

the network. Ripple also employs proof of work in order for the miners to join the small groups.[118] The existing miners will generate a challenge string that the new miner will need to answer before he or she can join the group. This makes the cost of attacking the system prohibitively expensive.[119]

b. Smart Contracts—Ethereum

In 1997, Nick Szabo first introduced the concept of smart contracts in his paper "The Idea of Smart Contracts."[120] Smart Contracts are "automated programs that transfer digital assets within the blockchain upon certain triggering conditions."[121] Like the Blockchain itself, smart contracts "subsist independently of any moral or legal entity."[122] Instead, two parties use coding to create

> a little program that you can entrust with a unit of value (as a token or money), and rules around that value. The basic idea behind smart contracts is that a transaction's contractual governance between two or more parties can be verified programmatically via the blockchain, instead of via a central arbitrator, rule maker or gatekeeper . . . . [The parties] can bake the terms and implications of their agreement programmatically and conditionally, with automatic money releases when fulfilling services in a sequential manner, or incur penalties if not fulfilled.[123]

The Blockchain replaces the role of the third party typically required to resolve disagreements. As an example,

---

[118] PROOF OF WORK, https://wiki.ripple.com/Proof_of_Work (last visited May 24, 2015).
[119] Id.
[120] Nick Szabo, The Idea of Smart Contracts, Nick Szabo's Papers and Concise Tutorials (1997), http://szabo.best.vwh.net/idea.html.
[121] Joshua A.T. Fairfield, *Smart Contracts, Bitcoin Bots, and Consumer Protection*, 71 WASH. & LEE L. REV. ONLINE 36, 38 (2014).
[122] Primavera de Filippi, *Tomorrow's Apps will Come from Brilliant (and Risky) Bitcoin Code*, WIRED (Mar. 8, 2014, 6:30 AM), http://www.wired.com/2014/03/decentralized-applications-built-bitcoin-great-except-whos-responsible-outcomes/.
[123] William Mougayar, *The Blockchain is the New Database, Get Ready to Rewrite Everything*, STARTUP MGMT. (Dec. 27, 2014), http://startupmanagement.org/2014/12/27/the-blockchain-is-the-new-database-get-ready-to-rewrite-everything/. *See also* Melanie Swan, *Blockchain Thinking: The Brain as a DAC (Decentralized Autonomous Organization)* (Apr. 2, 2015), http://www.melanieswan.com/documents/BlockchainThinking_SWAN.pdf.

> imagine a red-widget factory receives an order from a new customer to produce 100 of a new type of blue widget. This requires the factory to invest in a new machine and they will only recoup this investment if the customer follows through on their order. Instead of trusting the customer or hiring an expensive lawyer, the company could create a smart property with a self-executing contract. Such a contract might look like this: For every blue widget delivered, transfer price per item from the customer's bank account to the factory's bank account. Not only does this eliminate the need for a deposit or escrow—which places trust in a third party—the customer is protected from the factory under-delivering.[124]

Smart contracts could be used for virtually anything that can be owned—tangible property like homes, cars, phones, and computers, and intangible property such as intellectual property rights could all be purchased using smart contracts.[125] This could easily be implemented with car purchases. A car could contain code that is tied to the smart contract.[126] If the borrower becomes late on a car payment, the parties could agree on a code that would forbid the keys from opening the car until the default is cured. If it gets to the point where the lender needs to repossess the car, the code could automatically provide that the lenders keys could open the door in that situation. Finally, when the final payment is made, the smart contract could provide that the lender no longer has any legal rights to the car, and the borrower has full rights.

Ethereum is the most highly-anticipated platform for smart contracts. Rather than building off of the Bitcoin network, Ethereum created its own Blockchain from scratch.[127] It uses some of the proof of work and proof of stake aspects of other Bitcoin but also includes a built-in Turing-complete programming language.[128] This means that instead of creating a different platform for each individual application, Ethereum developed one programming language that is

---

[124] Josh Blatchford, *4 Ways Blockchain Technology will Change the World*, VENTUREBEAT (Mar, 28, 2015, 7:00 AM), http://venturebeat.com/2015/03/28/4-ways-blockchain-technology-will-change-the-world/.
[125] SMART PROPERTY, https://en.bitcoin.it/wiki/Smart_Property (last visited Dec. 1, 2014).
[126] Nick Szabo originally gave an example like this in his 1997 paper. Szabo, *supra* n. 120.
[127] Ethereum, *Vitalik Buterin Reveals Ethereum at Bitcoin Miami 2014*, YOUTUBE (Feb. 1, 2014), https://www.youtube.com/watch?v=l9dpjN3Mwps.
[128] Vitalik Buterin, *A Next-Generation Smart Contract and Decentralized Application Platform*, GITHUB, https://github.com/ethereum/wiki/wiki/White-Paper#blockchain-and-mining (last updated Apr. 29, 2015).

powerful enough to build any other program or application of top of the underlying language.[129] This is like how gmail, Facebook, and countless other applications are built on top of JavaScript. Ethereum supports several programming languages, including C++ and JavaScript.[130]

Ethereum also uses a stack-based language in order to create a virtually unlimited number of stages in the contract. With Bitcoin, the transactions are binary—the Bitcoin are either spent or not spent. With Ethereum, the contract does not have to be fulfilled or unfulfilled, but can be in stage one pre-negotiation, stage two offer, etc.

Ethereum also created its own cryptocurrency called *ether*. Ether is used as a token to represent the asset virtually. Users can create their own currencies on top of ether just like NXT. Ethereum plans to release 15 million ethers each year, and, unlike Bitcoin, there is no cap.[131] Ethers are required in order to create contracts or even to run Ethereum's software, and is referred to by Ethereum's founders as the "platform's programming 'fuel.'"[132]

c. Colored Coins

Colored coins takes Bitcoin and adds on a piece of code in order to represent an asset—like smart property. In effect, it changes the color of the coin so that you know the type of asset, where the asset has been, and where it is going. For example, you could use colored coins technology to add code to a Bitcoin specifying that the Bitcoin represents your house, changing the Bitcoin into effectively a token to represent the value of your house. This could be done with securities, cars, or any other type of property. Ethereum used the concept of colored coins as a

[129] Ethereum, *Vitalik Buterin Reveals Ethereum at Bitcoin Miami 2014*, YOUTUBE (Feb. 1, 2014), https://www.youtube.com/watch?v=l9dpjN3Mwps.
[130] Robert McMillan, *Project to Turn Bitcoin into an All-Powerful Programming Language Raises $15M*, WIRED (Sept. 10, 2014, 6:30 AM), http://www.wired.com/2014/09/ethereum-backers-raise-15-million/.
[131] Id.
[132] Id.

facet of its platform, only with Ethereum the colored coins are not tied to Bitcoin but rather ether.

d. Charitable Proof of Work

Several alternative cryptocurrencies have been proposed or are now in motion that use the proof of work process to perform something useful for society, meaning they solve problems using their algorithms. One such example is CureCoin, who partnered up with Stanford University's Folding@home program.[133] The Folding@home program seeks to use the power of the cloud to study and find cures for cancer, Alzheimer's, Parkinson's, and many other diseases.[134] Instead of Bitcoin miners solving some arbitrary puzzle, CureCoin miners use their computational power to fold proteins and receive CureCoin rewards based on the amount of computational power contributed. Another proof-of-charity company is Primecoin, who uses proof of work to discover new prime numbers.[135]

e. Namecoin

Namecoin was the first Bitcoin fork—meaning the first company to take the Bitcoin Blockchain and create its own Blockchain using the exact same technology.[136] As such, Namecoin is very similar to Bitcoin with ten minute transaction time, 21 million cap on the total number of Namecoin, and same rewards released with each new block. One major difference is that with Namecoin users can store information in addition to just the transaction information on the Blockchain. Specifically, Namecoin is a decentralized Domain Name System (DNS). The DNS allows internet users to type in a URL address rather than requiring a specific IP address.

[133] WHAT IS CURECOIN, https://www.curecoin.net/index.php/knowledge-base/14-knowledge-base/about-curecoin/19-what-is-curecoin (last visited May 24, 2015).
[134] START FOLDING, https://folding.stanford.edu (last visited May 24, 2015).
[135] Id.
[136] NAMECOIN, https://namecoin.info (last visited May 24, 2015).

For example, entering "'google.com' into your browser will trigger your computer to check its DNS server for Google's IP address."[137] The benefit of a decentralized DNS is that it cannot be censored or shut down, just like Bitcoin.

D. Platform Recommendations for a Cryptosecurities Market

A cryptosecurities market would require certain unique features. First, unlike Bitcoin, shares cannot be divided into small units but can trade only in whole numbers. Second, Bitcoin miners are paid transaction fees in Bitcoin, but in a cryptosecurities market you cannot pay the miners with shares. Third, the securities will need to have technology that enables issuers to specify the type of security, whether stock, bond, etc.

The technology already exists to create a cryptosecurities market. Using a platform such as Ripple or Ethereum, a cryptosecurities system could easily be built onto the existing code. Then, the colored coins technology could specify the type of security offered, and any restrictions on the securities. Ethereum has the capability of processing transactions in less than a minute, and Ripple confirmations take only a few seconds.

III. PROBLEMS WITH THE STOCK MARKET AND HOW A CRYPTOSECURITIES MARKET WOULD ADDRESS THESE ISSUES

Many argue that the stock market is broken.[138] Occupy Wall Street, the Wolf of Wall Street, and high frequency trading are all notorious examples illuminating why there is a problem, and why now is the time to address these problems. This section highlights some issues

---

[137] David Gilson, *What are Namecoins and .bit Domains?*, COINDESK (June 18, 2013, 1:30 PM), http://www.coindesk.com/what-are-namecoins-and-bit-domains/.

[138] After the publication of "Flash Boys"—the latest book by author Michael Lewis—SEC Chair Mary Jo White defended the stock market by claiming that it is not rigged and that the "U.S. markets are the strongest and most reliable in the world." Peter Hamner, *Wall Street and SEC Chief Respond to 'Flash Boys' Book*, KNOWLEDGE EFFECT (May 8, 2014), http://blog.thomsonreuters.com/index.php/wall-street-and-sec-chief-respond-to-flash-boys-book/.

with the current stock market, and how a cryptosecurities market would address and solve these problems. Just as cryptocurrencies are an alternative to traditional currencies for those wishing to use them, the cryptosecurities stock market would be an alternative to the current stock market and not a replacement. Investors may choose to use this market in addition to or instead of traditional stock using traditional exchanges or brokerages.

A. Problems with Stockbrokers

There is likely not a better embodiment of all that is wrong with stockbrokers than that of Jordan Belfort—the self-proclaimed "Wolf of Wall Street." Belfort scammed investors out of more than $100 million dollars before being convicted and sentenced to federal prison. His over-the-counter brokerage firm, Stratton Oakmont, participated in several "pump and dump" schemes, wherein the company would purchase cheap stock, issue false and misleading statements in order to pump up the price of that stock, and then sell or dump the stock at the artificially inflated price. A reporter likened Belfort to a "twisted Robin Hood who takes from the rich and gives to himself and his merry band of brokers."[139]

While Mr. Belfort's actions stand out as particularly culpable, stockbrokers and dealers often engage in various activities that range from outright fraudulent to slightly less than legal. Although a large amount of trading today happens online, these trades must still go through an online brokerage, and that brokerage gets to decide how the trade will be executed (whether it will go through an exchange, market maker, etc.[140]) and gets to collect a commission on every trade.

---

[139] Brian Solomon, *Meet the Real 'Wolf of Wall Street' in Forbes' Original Takedown of Jordan Belfort*, FORBES (Dec. 28, 2013, 12:24 PM), http://www.forbes.com/sites/briansolomon/2013/12/28/meet-the-real-wolf-of-wall-street-in-forbes-original-takedown-of-jordan-belfort/.

[140] TRADE EXECUTION: WHAT EVERY INVESTOR SHOULD KNOW, http://www.sec.gov/investor/pubs/tradexec.htm (last updated Jan. 16, 2013).

If an investor prefers an actively managed mutual fund, then the brokers get an even bigger cut. Numerous studies have shown that actively managed mutual funds generate a lower return for investors than mutual funds sold to the investors directly.[141] It is illegal to switch a customer from one mutual fund into another when the new investment will not result in any net gain to the customer. But brokers do this all the time to generate commissions, and this is called "churning."

A cryptosecurities market would solve the broker problem simply by eliminating the mandatory requirement of going through a broker. Of course, less savvy or less involved investors could still choose to go through brokers, exchanges, actively managed funds, and other investment trusts, but others could make trades completely on their own or peer-to-peer, just like many Bitcoin users today.

B. High Frequency Trading

Just as trading floors replaced outdoor curbside stock markets, high frequency trading (HFT) has replaced trading floors by allowing computers to replace the work of human traders. HFT has allowed an exponential growth in the number of quotes. In 1999, around 1,000 quotes were received per second. By 2013, with the help of HFT computers, around 2,000,000 quotes go through every second even though there is less trading overall.[142] High-frequency trading firms make up around 50% of all stock trades.[143]

---

[141] *See, e.g.*, Diane Del Guercio & Jonathan Reuter, *Mutual Fund Performance and the Incentive to Generate Alpha*, 69 J. OF FINANCE 1673 (2014).
[142] Richard Finger, *High Frequency Trading: Is it a Dark Force Against Ordinary Human Traders and Investors?*, FORBES (Sept. 30, 2013, 8:41 AM), http://www.forbes.com/sites/richardfinger/2013/09/30/high-frequency-trading-is-it-a-dark-force-against-ordinary-human-traders-and-investors/.
[143] Peter J. Henning, *'Spoofing,' a New Crime With a Catchy Name*, NEW YORK TIMES (Oct. 6, 2014, 12:39 PM), http://dealbook.nytimes.com/2014/10/06/a-new-crime-with-a-catchy-name-spoofing/.

Proponents of HFT argue that it lowers costs, tightens spreads, and adds liquidity to the markets.[144] The bid-ask spread is "the difference in price between the highest price that a buyer is willing to pay for an asset and the lowest price for which a seller is willing to sell it."[145] The bid-ask spread has decreased over the past thirty years from about .20 percent to around .0002 percent, and some claim this is due to high frequency trading and the resulting increased liquidity.[146]

But critics of HFT argue that HFT firms are getting all the reward without taking any of the risk. Traditionally, market makers were obligated to keep the markets in order and would "step in and be the buyer of last resort."[147] HFT firms are not taking on that kind of risk and have even bragged about not having a single day of trading losses over the course of several years.[148] Stephen Weiss of Short Hills Capital argued that HFT firms are "not adding liquidity. They're sucking it out and returning it at a higher price after they've scalped you."[149]

Some major issues with HFT could be solved by using cryptosecurities. First, experiences like the flash crash would be avoided because it takes time to verify the transactions—even the fastest crypto-technologies require several seconds before transactions are completed. Second, spoofing and naked short selling would be impossible because you must actually hold the

[144] Bruno J. Navarro, *High-Frequency Trading Benefits Investors: Advocate*, CNBC (Apr. 2, 2014, 2:46 PM), http://www.cnbc.com/id/101549113#.
[145] BID-ASK SPREAD, http://www.investopedia.com/terms/b/bid-askspread.asp (last visited May 25, 2015).
[146] Tim Worstall, *HFT Really Does Reduce the Bid Ask Spread; Making Michael Lewis Wrong About HFT*, FORBES (Apr. 1, 2014, 12:16 PM), http://www.forbes.com/sites/timworstall/2014/04/01/hft-really-does-reduce-the-bid-ask-spread-making-michael-lewis-wrong-about-hft/.
[147] Finger, *supra* n. 142.
[148] MICHAEL LEWIS, FLASH BOYS: A WALL STREET REVOLT 109 (2015). "Virtu Financial publicly boasted that in five and a half years of trading it had experienced just one day when it hadn't made money, and that the loss was caused by 'human error.' In 2008, Dave Cummings, the CEO of a high-frequency trading firm called Tradebot, told university students that his firm had gone four ears without a single day of trading losses. This sort of performance is possible only if you have a huge informational advantage." *Id.*
[149] Henning, *supra* n. 143.

cryptostock before you could make a trade. If a trader does not have the stock in his crypto-portfolio, he will not be able to create the private and public keys necessary to make the trade.

1. The Flash Crash

On May 6, 2010, something unprecedented happened to the stock market. In only twenty minutes, investors lost around $862 billion.[150] Throughout history, the market has experienced crashes, but this was the largest single day point drop for the Dow Jones Industrial Average.[151] What makes this day truly unique among all other market crashes, however, is that within fifteen minutes, the market had bounced back up to almost exactly where it started that day.[152]

> Over the same fifteen minutes, individual stocks traded wildly, with huge and evidently illogical price swings. Proctor & Gamble--a blue-chip component of the benchmark Dow Jones Industrial Average ("DJIA")--dropped by 36% in less than four minutes, and then fully recovered in less than a minute. 3M experienced a similarly rapid collapse and recovery. Accenture, a multi-billion dollar consultancy firm, saw its stock price fall from $40 per share to a penny in a matter of seconds, and then rocket back to $40 just as quickly. Shares of Apple, which had been trading at around $250 per share, changed hands at the outlandish price of $100,000 per share. Hundreds of other securities experienced similar chaos.[153]

Because it takes an average of ten minutes for a new block to be added to the Blockchain, it allows enough time to verify each transaction before it is added to the ledger as a verified transaction for everyone to see. Likewise, a cryptosecurities market would require several minutes for a transaction to process, which would help smooth out the issues caused by computer algorithms responding to imaginary signals that the market is starting to drop.

Of course, the SEC could create new rules requiring transactions to be verified and slow down before being added to the system. However, this would not solve the other issues: brokers

---

[150] Edgar Ortega Barrales, *Lessons from the Flash Crash for the Regulation of High-Frequency Traders*, 17 FORDHAM J. CORP. & FIN. L. 1195, 1196 (2012).
[151] *Id.* at 1196–97.
[152] Charles R. Korsmo, *High-Frequency Trading: A Regulatory Strategy*, 48 U. RICH. L. REV. 523, 525 (2014).
[153] Id.

would still be required and traders could not trade peer-to-peer without third parties, and the trades could not be completed anonymously. Finally, a cryptosecurities market would not need to replace the stock market; it is merely an alternative that investors may use in addition to what is already out there.

2. Spoofing and Naked Short Selling

Another issue gaining attention with high frequency trading is "spoofing" or "layering." Spoofing occurs when a "trader places orders with no intention of having them executed but rather to trick others into buying or selling a stock at an artificial price driven by the orders that the trader later cancels."[154] The Dodd-Frank Act specifically lists spoofing as one of its prohibited transactions.[155]

A similar issue occurs with naked short selling. First, a short sale occurs when a trader borrows shares and then sells those shares without actually owning them. Say ABC stock is selling at $100 per share.[156] Bob wants to buy 50 shares. Alice borrows 50 shares from a brokerage and sells them to Bob at $100 per share. The brokerage will deliver the shares to Bob and after three days the transaction is finalized.[157] When it comes time to pay for the borrowed shares, ABC stock has dropped to $80 per share. Alice therefore made a profit of $20 per share minus fees charged by the brokerage. Conversely, if ABC stock rises after Bob buys the shares at $100 to $120, then Alice would lose $20 per share.

---

[154] Press Release, SEC Charges N.Y.-Based Brokerage Firm with Layering (Sept. 25, 2012), http://www.sec.gov/News/PressRelease/Detail/PressRelease/1365171484972#.VD1Vf77XFG4.
[155] Dodd-Frank Act, 7 U.S.C. 6c(a)(5)(C) (2012).
[156] This example is loosely based on one found in this article: James J. Angel & Douglas M. McCabe, *Business Ethics of Short Selling and Naked Short Selling*, 85 J. BUS. ETHICS, 239, 240 (2009).
[157] Once trades are completed, the trades are not settled until the third business day after the trade has processed, meaning the buyer does not actually pay for the shares or receive the stock certificate until the settlement date. *Id.*

Naked short selling occurs when a seller has no intention of delivering the purchased shares on the settlement date (usually the third business day after the trade), or possibly has no intention of delivering the shares *at all*. The latter typically occurs when a trader is purposely trying to drive the stock price downwards to an artificially low stock price, which in turn "may cause serious damage to the firm by damaging its reputation as a going concern or by preventing the firm from obtaining needed financing."[158] The trader will not even borrow the shares before the "sale" takes place because the trader has no intention of completing the transaction. Settlement failures, whether purposeful or accidental, account for approximately 20% of total trades.[159]

A cryptosecurities market would cure any issues with spoofing and naked short selling because the system is not updated with the trade until the trade is complete. If a person places an order and then withdraws before the order is completely, it simply never shows up on the Blockchain ledger. This should increase the overall stability of the market and the stock value of the participating companies.

C. Other Advantages of a Cryptosecurities Market

The other main advantages of a cryptosecurities market are transparency, the fast settlement periods, the ability to trade 24 hours per day, and cheaper transaction costs.

1. Transparency

All transactions on the Blockchain are public and can be traced from origin through to present day. There are two types of traders that will appreciate this transparency. First are the traders dissatisfied with the status quo and dark pool trading, who feel that the system is corrupt

[158] *Id.* at 242.
[159] Id.

because of all the secret trading and problems on Wall Street. The second group of traders are those technologically savvy traders who enjoy the new technological aspect of trading on a cryptosecurities market. Therefore, the traders will include the two groups from the broad ends of the spectrum.

2. Improved Speed

Although high frequency traders can make trades in microseconds, the actual transfer of stocks takes up to three days.[160] This is how spoofing and naked short selling is able to occur. Because cryptosecurities trade on the Blockchain and are verified in less than one minute, this makes ownership rights clear and removes the opportunity for traders to take advantage of the system by spoofing or naked short selling. Additionally, the Blockchain runs 24 hours per day so traders would never have to worry about after-hours trading.

3. Cheaper Transaction Costs

There is a potential to significantly cut down on transaction costs with this a cryptosecurities market. With removing the requirement of brokers, and removing the need for transfer agents, the only fees left will be to the crypto-exchanges (unless the traders trade directly peer-to-peer) and to the SEC. The SEC charges exchanges fees that are kept "as close as possible to the amount of the regular appropriation to the Commission by Congress for that fiscal year. If transaction volume in a given year increases, the SEC will lower the fee rate because each transaction has to contribute less to the target collection amount."[161] Currently these fees are set

[160] ABOUT SETTLING TRADES IN THREE DAYS: T+3, http://www.sec.gov/investor/pubs/tplus3.htm (last updated May 21, 2004).
[161] "SEC FEE"—SECTION 31 TRANSACTION FEES, http://www.sec.gov/answers/sec31.htm (last updated Sept. 25, 2013).

at $18.40 per million dollars of trades.[162] Exchanges delegate the responsibility for fee collection to brokers, who then collect the fees from the investor, equaling a few pennies on each trade.

D. The Costs and Benefits of Completely Replacing the Traditional Stock Market

There is no need to outlaw the traditional stock market in favor of a cryptosecurities market. A complete replacement is impractical and—due to institutional inertia—impossible unless Congress were to significantly rewrite the statutes governing securities laws. Many of the players in the traditional stock market would be displaced overnight, including transfer agents, brokers, and the traditional stock exchanges. Therefore, just as there is still a need for people to use the post office to send traditional email even though e-mail technology has been around for more than twenty years, it is unlikely that a cryptosecurities market will ever completely replace the traditional stock market.

IV. REGULATING THE CRYPTOSECURITIES MARKET

Surprisingly, most of the existing regulatory framework would remain the same with a cryptosecurities market. The responsibilities and regulation of issuers, purchasers, or the exchanges would not change. One major change with a cryptosecurities market is that brokers will no longer be required to be involved in trades, leaving traders the ability to trade directly through the exchanges or peer-to-peer. Another major change involves the role of transfer agents—the Blockchain used in a cryptosecurities market would completely obviate the need for transfer agents.

[162] Press Release, Fee Rate Advisory #4 for Fiscal Year 2015 (Feb. 27, 2015), http://www.sec.gov/news/pressrelease/2015-42.html.

A. Broker-Dealers

If I want to buy traditional stock listed on NASDAQ or the NYSE, I first would have to place an order through my broker.[163] My broker then would send the order to the exchange and the exchange matches the order with a willing seller. Then the exchange confirms the trade with my broker and my broker will alert me that the trade is complete. I have three days to send the money to my broker to pay for this trade, the broker pays my money to the seller, and then the seller will send the stock certificates (proof of ownership) to my broker. I can request the certificate from my broker but it will likely cost extra money.

Anytime I buy or sell, I have to pay a commission to my broker. If I use a full-service brokerage, the commission could be as high as $300 for one trade.[164] If I go through a discount brokerage—i.e. I make my trade online through a broker's website without any interaction with an actual person—then the average fee is around $10 with some discount brokers charging as low as $5 per trade.[165]

A cryptosecurities market would do away with the requirement that traders must go through brokers in order to complete trades. Of course, inexperienced traders may still use a broker for broker-assisted trades. However, traders should be able to purchase or sell their cryptosecurities directly on the exchanges or directly peer-to-peer. Traders who purchase on the exchanges will still need to pay a fee for every trade, but that fee will be significantly less than even the cheapest discount brokerage fee of $5.

---

[163] Example largely taken from Larry Harris, Trading and Exchanges: Market Microstructure for Practitioners 14 (2002).
[164] Patrick Gleeson, *How Much is the Average Stock Brokers Commission?*, THE NEST http://budgeting.thenest.com/much-average-stock-brokers-commission-31078.html (last visited May 25, 2015).
[165] *A Quick Guide to Stock Broker Commissions*, WISE STOCK BUYER (May 31, 2012), http://www.wisestockbuyer.com/2012/05/guide-to-stock-broker-commissions/.

Traders can also sell directly peer-to-peer on the Blockchain if they are able to find someone willing to buy or sell at the desired price. The only parties involved in this transaction would be the buyer, the seller, and the network users verifying the transaction. It may be difficult even on a cryptosecurities market for buyers and sellers to find each other without the traditional matchers—exchanges, market makers, or broker-dealers.

B. Transfer Agents

Transfer agents are the record keepers of the stock market, and even predate the SEC.[166] A transfer agent's role is to "record changes of ownership, maintain the issuer's security holder records, cancel and issue certificates, and distribute dividends."[167] There are 450 registered transfer agents in the U.S., managing "roughly 276 million shareholder accounts for about 1.5 million issuers."[168] Transfer agents are required to register with the SEC and are regulated by Section 17A(c) of the 1934 Exchange Act and SEC rules and regulations.[169] Transfer agents are not governed by the exchanges.[170]

A cryptosecurities market would obviate the need for transfer agents. Paper certificates will no longer be necessary to prove ownership—the Blockchain will maintain a clear and reliable record of who owns what. SEC Commissioner Luis Aguilar spoke of the transfer agents' "'unique position' to identify and prevent unregistered, restricted shares from being sold

---

[166] *Who is the STA?*, SECURITIES TRANSFER ASSOCIATION, INC., http://www.stai.org/who-is-the-sta.php (last visited May 25, 2015).
[167] TRANSFER AGENTS, https://www.sec.gov/divisions/marketreg/mrtransfer.shtml (last updated June 24, 2010).
[168] Sarah N. Lynch, *SEC Eyes Transfer Agents in New Front Against U.S. Stock Fraudsters*, REUTERS (Jan. 12, 2015, 4:57 AM), http://www.reuters.com/article/2015/01/12/us-sec-transferagents-insight-idUSKBN0KL0BD20150112.
[169] Id.
[170] If the transfer agent is a bank, it will also be regulated by the Comptroller of the Currency, the Federal Reserve System, and the Federal Deposit Insurance Corporation (FDIC). TRANSFER AGENTS, https://www.sec.gov/divisions/marketreg/mrtransfer.shtml (last updated June 24, 2010).

illegally."[171] However, using technology like Colored Coins, issuers will be able to add code on top of the underlying shares that automatically provides for the necessary restrictions. Unregistered securities can be coded as unregistered, shares with restrictions on resell can be coded with the exact resell restrictions so that there is no confusion on when the shareholder may sell the shares.

C. Issuers

Issuers will have enormous flexibility with cryptosecurities offerings. Issuers will be able to easily issue stocks, bonds, or other types of securities with technology such as Colored Coins adding code onto the base security to give it unique features. Issuers will also easily be able to enforce the 180-day lock-up period required for company insiders by adding on code that forbids transfers for 180 days. Likewise, if the issuer is engaging in a private offering, the issuer will be able to implement resell restrictions through code rather than relying on the transfer agent to create a legend written on a paper stock certificate.[172]

This will flow fairly seamlessly for new cryptosecurities offerings. But what about the situation where an issuer or its traders wish to convert traditional securities into cryptosecurities? If traders want to convert, then they should be able to subject to being fully informed of what the transfer may mean. Just because it is the same issuer and the securities may even have identical rights, the two systems are otherwise completely separate and will have different valuation. Overstock's traditional stock may be trading around $25[173] a share, while the separate cryptosecurities shares could be selling for $15. In effect, it is like two different classes of shares.

---

[171] Lynch, *supra* n. 168.
[172] Although this paper focuses on public offerings, issuers engaging in private offerings could also use Blockchain technology to track the sale of private cryptosecurities. This will likely be my next paper topic.
[173] $24.95 as of April 13, 2015. OVERSTOCK.COM, INC., http://www.marketwatch.com/investing/stock/ostk.

Due to these differences, issuers should be allowed to create new offerings of cryptosecurities but should not be able to convert its outstanding shares to cryptoshares without full approval from its existing shareholders. Otherwise it would be like converting preferred stock into common stock without permission, which is unacceptable. It is only the shareholders who are able to effectuate this conversion if they hold convertible preferred stock, and not the issuer. This concept should be used in the situation of converting traditional securities into cryptosecurities and vice versa.

D. Exchanges

Long before traders made trades electronically or on the floor of a stock exchange, trades were completed outside in the open air.[174] Even as far back as 1788, traders would gather every day outside at what is now 68 Wall Street under a buttonwood tree to conduct their trades.[175] What would eventually become the New York Stock Exchange (NYSE) eventually moved indoors in 1817, but traders continued to conduct business curbside.[176] As late as the Civil War, the majority of trades in the stock market were believed to have been conducted outside.[177]

Because the SEC has limited resources, it has delegated part of its regulatory function to the exchanges. The exchanges therefore play two roles: one as a publicly-traded company in competition with other public companies; and the other role as a Self-Regulatory Organization (SRO). Stock exchanges enjoy certain immunity when acting in their role as SRO. As SROs,

---

[174] The New York Curb Market: History, Organization, Listed and Unlisted Requirements, Execution of an Order, American Stock Exchange (1928) *available at* http://babel.hathitrust.org/cgi/pt?id=mdp.39015076045650;view=1up;seq=16.
[175] *Id.*; *The New York Curb Market Building—113–123 Greenwich Street*, DAYTONIAN IN MANHATTAN (Oct. 16, 2012), http://daytoninmanhattan.blogspot.com/2012/10/the-new-york-curb-market-building-113.html.
[176] Id.
[177] Id.

exchanges are responsible for regulating themselves (as evident by their name), their customers, and their competitors.

The exchanges' role as SRO should not greatly change with the advent of a cryptosecurities market. The traditional stock market is made up of public and private companies selling all manner of securities, whether through an exchange, over the counter, or directly. Many of these trades (see dark pools) happen outside the public eye, and only a portion of these trades happen on the exchanges. There will still be a need for stock exchanges to enable the buying and selling of cryptostock just like many Bitcoin users transfer on the Bitcoin exchanges rather than directly on the Blockchain.

Therefore, the exchanges will still play a role and their role and responsibilities with the SEC should remain largely the same, although parts of the exchanges' job will become automated with the Blockchain—e.g. specialists will likely play a much smaller role. More importantly, traders would not be required to go through a broker to effectuate trades, and could trade completely peer-to-peer. Traders should be able to log on to the exchange and trade their stock directly on the exchange, just as Bitcoin users are able to exchange Bitcoin directly on the exchanges.

There are two categories of exchanges capable of serving the cryptosecurities market in the near future. First are the national exchanges—such as NYSE and NASDAQ. These exchanges are in the best position to operate on the cryptosecurities market because they are well established, already have regulatory approval, and should be able to add on the necessary additional capacity.

Another category of exchanges that could transition to cryptosecurities is the existing Bitcoin exchanges, such as Coinbase[178] and Bitstamp.[179] Although these currency exchanges do not yet have the SEC regulatory approval, they do have experience with the Blockchain technology and how best to make Bitcoin transfers happen. Coinbase is the first U.S.-based licensed Bitcoin exchange, and it is actually backed by the NYSE.[180] With the support of the NYSE, I would argue that Coinbase is the top candidate for becoming a cryptosecurities exchange because it will bring to the table experience in both stock markets and cryptocurrency markets.

CONCLUSION

Whether or not the stock market is broken, this article explores an alternative trading system that addresses several of the current problems with the traditional regime. Using Bitcoin's underlying technology—the Blockchain—issuers will be able to create cryptosecurities that will allow anyone in the public to be able to see each transaction as it is taking place, which will remove some of the shroud of secrecy surrounding much of the high frequency and dark pool trading occurring today. This alternative market will also allow traders to trade completely peer-to-peer or directly through an exchange—cutting out several layers of intermediaries including brokers and transfer agents. The key is that a cryptosecurities market would not require the replacement of the traditional stock market; rather it would be an alternative market for users dissatisfied with the current regime. It is likely there will always be a need for both systems, just as with the advent of email there is still a need for the post office to manage traditional letters.

[178] https://www.coinbase.com.
[179] https://www.bitstamp.net.
[180] Bensinger, *supra* n. 16.

GLOSSARY OF BITCOIN TERMINOLOGY

51% attack	If more than 50% of the computing power (CPU) on the Bitcoin network is controlled by one miner or pool of miners, then that group could effectively hack into the Blockchain and rewrite the Blockchain's history.
Altcoin	Cryptocurrencies offered as an alternative to Bitcoin. Examples of popular altcoin include Ripple, NXT, Bitshares, and Ethereum.
Bitcoin	Bitcoin is the term to describe two separate concepts: (1) Bitcoin as the digital currency; and (2) Bitcoin as the entire network/protocol. Bitcoin is abbreviated as either BTC or XBT.
Bitcoin Address	A Bitcoin address is used to receive and send transactions on the Bitcoin network. It contains a string of alphanumeric characters, but can also be represented as a scannable QR code. The Bitcoin address is the only information that you need to give out in order for someone to pay you with Bitcoin. For security reasons, it is recommended that users create a new Bitcoin address per transaction.
Bitcoin Whitepaper	Satoshi Nakamoto authored "Bitcoin: A Peer-to-Peer Electronic Cash System" in November, 2008. This whitepaper lays out the fundamentals of the peer to peer network and the proof of work technology that would be implemented with the Bitcoin network.
BitPay	The most popular payment processor for Bitcoin. Merchants use BitPay to accept Bitcoin payments, using a scannable QR code.
Block	Blocks are like a page out of a ledger book, where the ledger is the Blockchain. Each block is connected to the previous block in order to form one long chain from the very first block (see genesis block) through the present day. Anywhere from hundreds to thousands of transactions will be entered and verified on a single block.
Blockchain	The Blockchain is the public ledger of every Bitcoin transaction ever made. It proceeds in chronological order from the very first Bitcoin block (see genesis block) through the present day. The Blockchain may be viewed by downloading the Bitcoin software or by viewing it online at blockchain.info. NOTE: Blockchain may also refer to the company that posts real-time Bitcoin transactions and is also a wallet software.
Block reward	This is the new Bitcoin creation reward that is given out to the miner who successfully adds a new block to the Blockchain. This reward started out at 50 Bitcoin, is currently at 25 Bitcoin, and will continue decreasing until all Bitcoin have been mined.
BTC	The currency abbreviation for bitcoins.
Client	See "miner."
Confirmation	The process of successfully adding a new block to the Blockchain is called confirmation. Satoshi Nakamoto designed the system to take approximately ten minutes per block, with the difficulty level adjusting every two weeks to keep transaction times as close as possible to ten minutes.
Colored coins	Code added onto Bitcoins that create additional attributes, such as the ability to mark a particular Bitcoin as a stock or car. This allows users to trade Bitcoins

	as tokens for other property.
CPU	Stands for Central Processing Unit—the hardware on a computer. Today Bitcoin users typically must invest in something more powerful than a regular computer to do the mining work.
Coinbase transaction	This is another term for the Bitcoin reward that is released once a new block is successfully mined. Note: Coinbase is also the name of the first licensed U.S. Bitcoin exchange, backed by the NYSE.
Cryptocurrency	A type of currency that is completely digital and typically relies on cryptography in order to secure the system.
Cryptography	Cryptography is a type of mathematics involving codes and ciphers created in order to encrypt (secure) information. Cryptography is used in order to secure the Blockchain.
Cryptosecurity	Stocks and bonds that can be traded completely peer-to-peer and recorded on a public ledger for anyone to see.
Difficulty	Refers to the amount of effort that is required in order to add a new block to the Blockchain. Difficulty is automatically adjusted based on the amount of computational power devoted to solving the proof of work puzzle in order to keep transaction confirmation time at ten minutes.
Double Spending	Spending Bitcoins twice. This is possible if someone accepts a Bitcoin payment without waiting until the payment has been confirmed (ten minutes).
Elliptic Curve Cryptography	The Elliptic Curve Digital Signature Algorithm is the type of cryptography used to transform Private Keys into Public Keys. Abbreviated as ECDSA.
Exchange	A venue for exchanging one type of currency or asset for another.
Fiat Currency	Currency which derives its value from government regulation or law.
Fork	This occurs when a company creates a new cryptocurrency using the existing code of an established cryptocurrency. Namecoin is an example of the first cryptocurrency to create a fork from the Bitcoin Blockchain.
Genesis Block	The very first block in the block chain. This block does not contain any inputs (i.e. a hash from the previous block). Every other transaction leads back to the genesis block or to the coinbase transaction.
Hash	Used in cryptography to change an arbitrary input into a fixed output with certain properties. Because the output is meant to be random, it is almost impossible to determine what the original input was. Any change made to the input—even as small as change in capitalization or punctuation—will completely change the hash.
Input	The information on a Bitcoin transaction that shows where the Bitcoin came from. The public will only see the Bitcoin address.
Miner	This refers to the people—and their computers—who run the Blockchain. Also called a “node” or “client.” As a reward for devoting the computational effort required to verify transactions, Bitcoin miners are able to collect a transaction fee for each individual transaction that they confirm, and also receive a reward for each block that they successful add to the Blockchain.
Mining	The act of generating new Bitcoin by solving cryptographic problems using computing hardware.

Node	See “miner.”
Nonce	A nonce is the proof string that miners search for when solving the proof of work puzzle. Miners will try billions of different nonces before discovering one that solves the puzzle. Once someone has figured out the nonce, it is much easier to verify that this is the correct solution, and the block that receives the most verification will be added to the Blockchain.
Orphan Block	A block that does not become valid on the Blockchain. Also called a “rejected block.”
Output	Where the Bitcoin will be delivered to.
Peer to Peer (P2P)	These are decentralized transactions that involve only the two parties in the transaction—the buyer and the seller. There are no third-party intermediaries (such as a bank) involved in peer-to-peer transactions.
Pool	A group of miners who collectively mine blocks and then split the reward between them.
Private Key	An alphanumeric string of data that proves that someone has the rights to the Bitcoin. Like cash, if someone loses their private key, their Bitcoin is gone forever. These are typically stored on a Bitcoin wallet, and it is recommended to store this information offline. Users should never reveal their private key to anyone. This is also used to sign transactions.
Proof of Stake	An alternative to proof of work, in which your existing stake in a currency (the amount of that currency that you hold) is used to calculate the amount of that currency that you can mine.
Proof of Work	A system that ties mining capability to computational power. Blocks must be hashed, which is in itself an easy computational process, but an additional variable is added to the hashing process to make it more difficult. When a block is successfully hashed, the hashing must have taken some time and computational effort. Thus, a hashed block is considered proof of work.
Public Key	An alphanumeric string of data that is derived from the private key, and once it goes through cryptographic hashing, will become that Bitcoin address that can be made available to the public.
satoshi	The smallest unit of Bitcoin that may be transferred, equal to one millionth of a Bitcoin (0.00000001).
Satoshi Nakamoto	The name used by the original inventor of the Bitcoin. It is likely this name is a pseudonym for a person or group of individuals. During Bitcoin’s first few years, Satoshi Nakamoto was active on blogs, but has not been heard from since 2010.
Satoshi Nakamoto Whitepaper	See Bitcoin Whitepaper.
Signature	Created by hashing private and public keys together in order to prove that a bitcoin transaction came from a particular address. This is required for every transfer of Bitcoin.
SHA-256	The cryptographic function that is used as the basis for the Blockchain.
Stale	Once a block has been successfully added to the system, any other efforts at mining that block become “stale.” There is no reward associated with working on a stale block.

Ten Minute Transactions	The Bitcoin protocol is set to ensure ten minutes in between block confirmations. This is accomplished by adjusting the difficulty level once every two weeks. If transactions begin taking less than ten minutes to confirm, the difficulty level is adjusted upwards. Likewise, if transactions begin taking more than ten minutes, the difficulty level will be adjusted downward.
Transaction fee	A small fee imposed on Bitcoin transactions. Although this fee is not explicit, it is implied as the output will always equal a small amount less than the input. These fees are given to the miners who successfully confirm the transaction.
Wallet	Like a physical wallet, a Bitcoin wallet stores a person's Bitcoin for later use. It will also contain the private key, public key, and Bitcoin addresses that a user creates. Bitcoin wallets will display a user's total balance and allows users to designate specific amounts to send to another user.