Analysis of Bitcoin as a Peer-to-Peer Network for International Payments

by

Sascha Böhme

M.A. in Business Administration
Ludwig-Maximilians-Universität, 1998

SUBMITTED TO THE SYSTEM DESIGN AND MANAGEMENT PROGRAM
IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE DEGREE OF

MASTER OF SCIENCE IN ENGINEERING AND MANAGEMENT
AT THE
MASSACHUSETTS INSTITUTE OF TECHNOLOGY

JUNE 2014

©2014 Sascha Böhme. All Rights Reserved.

The author hereby grants to MIT permission to reproduce
and to distribute publicly paper and electronic
copies of this thesis document in whole or in part
in any medium now known or hereafter created.

Signature redacted

Sascha Böhme

System Design and Management Program
May 2014

Certified by: ____________________________

Michael A. Cusumano
SMR Distinguished Professor of Management
Thesis Supervisor

Accepted by: ____________________________

Patrick Hale
Director
System Design and Management Program
Analysis of Bitcoin as a Peer-to-Peer Network for International Payments

by

Sascha Böhme

Submitted to the System Design and Management Program
On May 14, 2014 in Partial Fulfillment of the
Requirements for the Degree of Master of Science in
Engineering and Management

Abstract

The payment system is due for an overhaul. The antiquated infrastructure that runs the funds transfer network belongs to the pre-Internet era. As a result, international payments are expensive, slow, cumbersome, and not as secure as they could be.

This thesis argues that the cryptocurrency Bitcoin is the answer to the problems facing millions of consumers, merchants, and remitters worldwide.

The analysis is based on two frameworks. The first one is used to measure how well Bitcoin's attributes meet the needs of the users of the payment system. The second one is used to decide if the payments industry is likely to have one or more dominant platform leaders.

Thesis Supervisor: Michael A. Cusumano
Title: SMR Distinguished Professor of Management
Acknowledgments

I want to dedicate this thesis to my father, who will never be able to read it. Through his endless love and support, he guided me on a lifelong path that ultimately led me to MIT.

I thank my mother for always believing in me and supporting me in all my ventures, no matter how far from home they took me.

I want to thank professor Michael Cusumano, for agreeing to be my thesis supervisor, for his patience with me, and for proposing to use Bitcoin for this research in the first place.

Finally, I want to thank Pat Hale, Chris Bates, Bill Foley, Melissa Parillo, Amal Elalam, Jasmine Robledo, Joan Rubin, Lois Slavin, and Lesely Perera from the SDM program for making the past two years at MIT one of the best and most meaningful experiences of my life.
Contents

1 Introduction ................................................................................. 1
  1.1 Research Motivation and Objective .................................. 1
  1.2 Research Approach ......................................................... 2
  1.3 Thesis Structure .............................................................. 2

2 International Payments .......................................................... 3
  2.1 Money ............................................................................. 3
  2.2 Payment System ............................................................ 4
    2.2.1 Overview ............................................................... 4
    2.2.2 Payment Instruments ............................................. 6
    2.2.3 Drivers of Change ................................................. 8
  2.3 Regulation ...................................................................... 9

3 Bitcoin .................................................................................. 13
  3.1 Introduction ..................................................................... 13
    3.1.1 What is Bitcoin? ................................................... 13
    3.1.2 History of Bitcoin .................................................. 15
    3.1.3 Idea and Motivation Behind Bitcoin ...................... 16
    3.1.4 Concept ............................................................... 18
  3.2 Architecture .................................................................... 18
    3.2.1 Peer-to-Peer Network ........................................... 18
    3.2.2 Mining the Block Chain ....................................... 21
    3.2.3 Transactions: Digital Signatures and Public Key Cryptography ........................................... 27
  3.3 Features and Properties .................................................. 29
  3.4 Uses, Challenges, and Value .......................................... 35
    3.4.1 Uses ........................................................................ 35
    3.4.2 Challenges ............................................................ 37
    3.4.3 Value ...................................................................... 41
  3.5 Ecosystem ....................................................................... 43

4 Bitcoin as a Platform for International Payments .................... 49
  4.1 Customer Needs Analysis ............................................... 50
    4.1.1 Capability ................................................................ 51
    4.1.2 Cost ........................................................................ 51
    4.1.3 Convenience ........................................................ 52
    4.1.4 Coverage ............................................................. 54
    4.1.5 Confidence ............................................................ 55
    4.1.6 Confidentiality ........................................................ 56
    4.1.7 Verdict ................................................................. 57
  4.2 WTAoM Analysis ........................................................... 57
    4.2.1 Network Effects: Strong ......................................... 57
    4.2.2 Differentiation: Currently High/Potentially Low ......... 59
    4.2.3 Multi-Homing: Common ....................................... 59
    4.2.4 Verdict ................................................................. 60

5 Conclusion ............................................................................. 60
  5.1 Summary of Findings ...................................................... 60
  5.2 Outlook and Future Work ............................................... 62

6 References .............................................................................. 63
1 Introduction

“There is no reason, in principle, why final settlements could not be carried out by the private sector without the need to be cleared through the central bank.”

Mervyn King, Governor of the Bank of England, 1999 [1]

1.1 Research Motivation and Objective

A safe and efficient payment system is of fundamental importance for economic and financial activities and is essential for the maintenance of financial stability. Historically, banks and other financial institutions have been the primary providers of payment and financial services to end users, as well as important owners and users of the systems for processing, clearing, and settlement of funds and financial instruments. The central bank, as the issuer of the currency, the monetary authority and the “bank of banks”, has a key role to play in the payment system and possesses unique responsibilities [2, p. 16].

Despite, or possibly because of, their importance for the national and global economy, payment systems have changed little over the past decades. While the world has witnessed the invention of the PC in 1975, and the advent of the Internet in 1993, innovations in the payments industry have been few and far between. The rails that form the foundation of today’s payment system are decades old. In addition, the financial institutions that own and operate these systems are in a position of power to extract a hefty rent from their users. As a result, these systems are burdened with considerable inefficiencies, making international money transfer unnecessarily expensive, slow, cumbersome, and at times insecure.

In contrast, information and communications technology (ICT) has evolved at a staggering pace, giving free Email to every household in the world with an Internet connection, and free video conferencing to every smartphone, making it possible for anyone to connect to anyone else in the world in real-time. Meanwhile, the payment system infrastructure has remained stuck in the pre-Internet era. Innovation in payments has come mainly on top of the existing system, in the form of products and services like PayPal, that improve the lives of consumers and merchants through the provision of online payment instruments.

That is, until an unidentified programmer known as Satoshi Nakamoto published his paper on Bitcoin in December of 2008. Bitcoin is a cryptocurrency, i.e. it is a currency and a peer-to-peer network, that does not require a trusted third party such as a clearing house or central bank to transfer money. Thus, it is a new form of currency, payment instrument, and infrastructure for payments all at once.

The objective of this thesis is to determine whether this decentralized and distributed network of trust, that is not owned or controlled by any government or corporation, can support international payments equally or more reliable, efficient, and effective than the existing payment system.
1.2 Research Approach

The evaluation of Bitcoin as a technology for international payments requires a framework.

According to Crawley [3] a concept maps function to form and a product or system architecture is the implementation of that concept. The function, i.e. what a system does, should meet the needs and goals of the primary beneficiaries of that system, i.e. it should do what it is supposed to do. To evaluate how good an architecture is, you can measure how well the attributes of the system meet the needs of the primary beneficiaries. In the case of Bitcoin as a peer-to-peer network for international payments, the primary beneficiaries are the users who wish to transfer money. Blockley and McDowell's framework "The 6 Cs that drive consumer choice in payments" has been identified as suitable for that purpose.

Since Bitcoin is a platform, and is being analyzed in the context of the payments market, Cusumano's "Winner Take all or Most" framework will be used in a second step to evaluate if that market is likely to have one or more dominant platform leaders.

1.3 Thesis Structure

This thesis is organized in five chapters.

Following the introduction, chapter 2 frames the problem. Since Bitcoin is a currency, among other things, the chapter starts with an excursion on money, describing its uses and explaining why it has value. Next follows an overview of the international payment system and relevant terminology. After describing important payment instruments, the system's stakeholders and drivers for change will be discussed. The final section is on financial regulation, which provides important context for the analysis of Bitcoin as a platform for payments.

Chapter 3 explains in detail the motivation behind Bitcoin, its architecture and technology, the attributes and properties that emerge from it, and the benefits and challenges of Bitcoin in the context of its use cases. Following a discussion of the potential value of Bitcoin, the chapter closes with an overview of the ecosystem surrounding the platform.

Chapter 4 analyzes Bitcoin as a platform for international payments. Two frameworks will be used. The first one is Blockley and McDowell's "The 6 Cs that drive consumer choice in payments", which focuses on the needs of the users of payment instruments. The second one is Cusumano's "Winner Take All or Most" framework, used to analyze the potential for dominant players in platform markets.

Chapter 5 summarizes the major findings and provides an outlook on the future of Bitcoin.
2 International Payments

2.1 Money

The International Monetary Fund [4] describes money as a

- medium of exchange, something that people can use to buy and sell from one another;
- unit of account, providing a common basis for prices;
- store of value, which means people can save it and use it later.

Without money there would be only barter trade where buyer and seller would have to exchange goods with each other. If the buyer had nothing suitable to offer the seller, or not in the desired amount, the trade would fall through. But with money, you don't need to find a particular individual. All that is required is a market where goods are exchanged for a common medium of exchange. This increases specialization, as everyone can focus on what they do best, instead of producing and accumulating different goods to barter with. As people become more specialized, they produce more, leading to more trade and, hence, more demand for money.

Thus, money holds value over time, is widely accepted, and makes it possible to attach a price to goods and services. It is fungible, divisible, transportable, durable, and should be hard to counterfeit.

How much money is worth depends on the value ascribed to it. The first forms of money were valued according to their alternative uses and replacement costs. Grain, for example, could be consumed as food or stored. Although anybody could grow it, that took time, so consumption would reduce the money supply. The value people ascribed to these attributes put a floor to its price. However, most things don't last forever or can't be divided or transported easily, making them unsuitable as money.

But precious metals serve all three needs well. Also, they are hard to obtain, there is a finite supply, and they last over time. Precious metals were used as money for a very long time, until their drawbacks became salient. Although they are transferable and divisible, they are difficult to transport over great distances in large quantities, and dividing or combing them frequently is cumbersome. That is when precious metals were stored in banks and instead notes were used for payment, which claimed ownership on the metals. The notes could be exchanged into the metals at the banks at any time. Eventually, the paper claim was delinked from the metals and fiat money was born.

Fiat money has no material value. It only has value because a nation collectively agrees to ascribe value to it. Today's money only works because people believe it will. The source for fiat currency are the central banks whose job it is to keep the demand for and supply of money in balance to avoid deflation or too much inflation. The reason why governments should not have direct control over the money supply is their tendency to abuse that power and print money to pay their debts, pay more salaries, and spend more overall, without regard for a stable currency. If that balance gets out of control people may lose trust in their currency, leading to hyperinflation as witnessed, for example, in Germany during the second world war, or Brazil.
and Argentina in the 1980s. Once that trust is lost, it is very hard to regain. The people in those Latin American countries started using the U.S. dollar because it was a more stable currency. And during the global financial crisis in 2008, someone decided to create his own currency: Bitcoin.

2.2 Payment System

2.2.1 Overview

The financial system consists of the three core components markets, institutions, and the payment system. The payment system is of fundamental importance for the functioning of the financial system. Its primary objective is to facilitate transactions between economic agents and the allocation of resources in the economy. The payment system consists of payment instruments and the market infrastructure for payments and financial instruments. A payment instrument is a tool or a set of procedures enabling the transfer of funds from the payer to the payee, whereas infrastructure relates to the institutions, systems, rules, procedures, and processes of the payment system.

Payments refer to the transfer of funds and encompass their processing, clearing, and settlement. Payments can be classified based on the types of payer and payee involved. Wholesale payments are made between financial institutions. Retail payments are made between non-financial institutions and include person-to-person transactions between private households (money transfer), person-to-business transactions (payments made for the purchase of goods and services), and business-to-business transactions [2]. A term often associated with international payments is remittances. Remittances are payments sent by migrants back to their families, can be domestic or international, and are usually made on a recurring basis [5].

The focus of this thesis is on international retail payments. Therefore, the following definitions apply:

- *payments* are defined as non-cash person-to-person and person-to-business transactions
- *remittances* are defined as cross-border person-to-person money transfer of relatively low value
- *international payments* are defined as cross-currency payments (i.e. cross-border payments requiring a currency conversion); they encompass purchases and remittances.

Life Cycle of a Payment

According to the European Central Bank [2, pp. 25–27] a payment is a process that involves

- a payment instrument;
- processing (including clearing), which involves the exchange of payment instructions between banks (and their accounts);
• *settlement*, i.e. the compensation of the payee's bank by the payer's bank.

The stylized life cycle of a payment looks as follows (see Figure 1 for an illustration).

1. **Choice of payment instrument and submission of payment instructions**
   Depending on the payment instrument (see section 2.2.2), either payer or payee submit instructions to the bank (for example account and routing number of the recipient).

2. **Payer's bank's internal processing**
   The sending bank verifies and authenticates the payment instrument, checks for available funds (or overdraft lines), and debits the account of the payer.

3. **Interbank processing (clearing)**
   Transmission, reconciliation, sorting, and confirmation of transfer orders prior to settlement. Clearing can take place bilaterally through correspondent banking or through multilateral arrangements.

4. **Interbank settlement**
   Funds are transferred from the sending bank to the receiving bank bilaterally or multilaterally through agents.

5. **Receiver's bank's internal processing**
   The receiving bank credits the payee's account.

6. **Information and communication**
   Receipt of the payment is communicated to the payee via account statements.

Figure 1: Stylized Life Cycle of a Payment [2, p. 26]

Although infrastructure exists to settle payments in real-time, these are reserved for large corporations and wholesale payments. Retail payments are generally processed in batch runs several times per day. Since each bank has to run the batch, and potentially an intermediary as well, even domestic retail payments can take one or two days to settle [2, pp. 48–55]. Because of the increased complexity, international payments take even longer.

**International payments**

International payments take place in a similar manner as described above, extended by one or more additional steps at the point where funds cross borders, change payment systems, and switch currencies. Since market opening hours may not be aligned when payments cross
multiple time zones, they often require a foreign exchange settlement institution acting as a trusted third party to ensure simultaneous crediting and debiting of the involved bank accounts at the same foreign exchange rate [2, p. 62]. Because of the additional overhead, international payments are more expensive and slower than their domestic variants.

Remittances are an especially important segment of international payments. The global remittance market in 2013 was worth nearly $550 billion\(^1\). $414 billion of that amount went to developing countries and is expected to reach $540 billion by 2016 [6, p. 1]. Remittances don't always travel through formal or legal channels, for various reasons. The recipient country may not have the required financial or IT infrastructure in place, or capital controls and other legal barriers make these channels overly expensive and slow [7, p. 7]. Coverage, speed, and cost are some of the important aspects for comparing payment options and will be discussed in detail in section 4.1. Figure 2 illustrates the various remittance channels.

![Figure 2: Remittance Channels](image)

2.2.2 Payment Instruments

Payment instruments are methods of payment such as cash, credit/debit cards, and wire transfers (also known as electronic funds transfer or EFT). They are to be distinguished from financial instruments (securities and derivatives) and financing instruments (bonds and other instruments for businesses to obtain financing).

Since the focus of this research is on international payments, which implies remote transfer of funds, only electronic payment instruments (EPIs) are considered, as opposed to physical forms like cash. EPIs comprise the two building blocks EFT and electronic credit/debit cards, and online EPIs like PayPal, which build on the existing financial infrastructure of bank accounts and credit/debit cards [8]. Mobile payments are included insofar as they relate to payments made with mobile devices using the internet and are subsumed under online EPIs. Local mobile transactions at the point of sale (POS) using technologies like near field communication (NFC)

\(^1\) The true size of the market including unrecorded flows is believed to be significantly greater.
are not suitable for international money transfer. Mobile money, i.e. tools like M-Pesa that allow payments through the networks of telecommunication providers, plays only a small role in international payments. This technology provides for an important research topic on how to bring financial services to the developing world, but it is largely confined to domestic payments [9].

**EFT**

EFT or wire transfer is a transfer of funds from one bank to another where the processing occurs in electronic form. In a credit transfer, the instructions are sent by the payer to his bank, which will transfer the funds to the account of the payee. In a debit-based transfer, the instructions authorizing the debiting of the payer's bank account are initiated by the payee, based on the authorization of the payer [2, p. 31].

**Credit/Debit Cards**

Cards are physical devices used to authorize a debit directly from the cardholder's account (debit card) or to draw on a line of credit from the card issuer (credit card). Cards are issued via a card scheme (for example Visa, MasterCard, or American Express) and settled via clearing and settlement agents.

Credit and debit cards can be seen as identical in their function of transferring money to a payee. They can both be used to pay locally at a point of sale (POS) or remotely in "card-not-present" transactions and to withdraw funds at ATMs. The difference is that credit cards have additional features bundled together, such as a credit line, buyer protection, insurance, etc. [8, p. 34].

**Online EPIs**

There has been a trend over the past few years away from 'traditional' payment methods. The market share for credit cards, for example, is shrinking because of consumers' fears over credit card fraud and the increase in alternative payment methods especially online [10]. Online EPIs are payment instruments that utilize EFT and cards for the debiting/crediting of the respective payer/payee accounts. By providing a web interface to the user, they abstract from the mechanics necessary to use cards or sending payment instructions to banks. To make a payment, all the payer needs is his password and the payee's Email address, greatly simplifying the process, especially for international payments. In addition, none of the payer's account information is transmitted to the receiver, increasing security. In order to participate, one or both parties have to register with the provider. PayPal is the best known representative of this category. Transfer is nearly instant as long as the funds stay with the provider. Cashing out requires the funds to be sent to a user's bank account via EFT.
2.2.3 Drivers of Change

Despite the wide variety of choices in payment instruments and providers, all of them have not only strengths but also weaknesses. As mentioned above, the payment system supports the financial system and on a larger scale the entire economy. Innovation in the payment system comes about when there is demand for change, for example, from a growing economy and ever-increasing international trade and globalization. However, innovation occurs only if it creates value for at least some of the stakeholders in a system. In order to understand the payments industry, it is necessary to understand what actors are involved. Following Crawley’s framework [3] there are stakeholders and beneficiaries. Stakeholders have a stake in the system, either by producing an output that fulfills others’ needs, or because they are important to the system otherwise. Beneficiaries are those actors whose needs are addressed by the system’s outputs, or who the system is important to otherwise. This leads to three different stakeholder types

- Primary Beneficiary
- Beneficial Stakeholder
- High Leverage Stakeholder

The stakeholders in the payments industry are as follows.

**Primary beneficiaries** simply receive a benefit without producing anything in return. These are the users of the payment system, i.e. payers and payees, consumers and businesses.

**Beneficial stakeholders** receive a benefit and at the same time fulfill a need. These are all the producers who fulfill users' or other producers' needs, generally in return for financial compensation. This group consists of banks, credit card companies, payment processors and other financial institutions, and payment system providers [11, p. 11].

**High leverage stakeholders** are important to the producers and the system as a whole, without requiring any compensation. These are typically government entities such as regulators and policymakers, and central banks. This stakeholder group is high leverage because its output — the approval — is absolutely required for the producers' and the system's ability to operate, but it cannot be negotiated with because it requires nothing in return.\(^2\)

For the purpose of simplicity, going forward the term *stakeholders* will be used to refer to the entire group of stakeholder types. Figure 3 illustrates the relationship between the stakeholders.

---

\(^2\) This refers to the direct output of the system. Of course, the state requires taxes to function and lobby groups produce outputs (for example donations and votes) that are beneficial to the government. However, these needs are out of scope for the purpose of this thesis.
As Pogor [8, pp. 16-19] pointed out, while all stakeholders play a role in the evolution of payment instruments, it has usually been the banks who innovate. The reason has been that banks control the core payment infrastructure and are heavily invested in it. Their decisions are based on long-term cost/benefit analyses. For that reason, and enabled by technological advances, there is continuous, albeit incremental, innovation in the industry. Often, new technologies are implemented to reduce costs and raise profits, not necessarily to increase customer value. Although, no new payment instrument will be successful if it doesn't get adopted by its intended users. However, his assertion that "the support of the banks is imperative in driving and implementing new ideas in EPIs" shows just how much has changed with the invention of Bitcoin. This is the first time that consumers decided to design and implement a payment instrument with the intention to fulfill their own needs, regardless of those of the financial services industry or of governments. Blockley and McDowell [10] proposed a framework around the drivers of consumer choice in payments which will be used in section 4.1 to analyze how well Bitcoin and current EPIs actually meet the demands of the primary beneficiaries.

But before getting into the analysis of Bitcoin and its suitability for international payments, it is first necessary to understand the impact of the high leverage stakeholders by looking at pertinent financial regulation.

2.3 Regulation

Regulators grapple with the fact that Bitcoin does not neatly fit any existing definition of currency, financial asset, or even institution. It falls into a grey area and it is therefore difficult to know which laws apply and how. This situation is not uncommon with the emergence of new technologies and is reminiscent of the uncertainty surrounding the Voice over Internet Protocol (VoIP). When VoIP first emerged, the Communications Act and Federal Communications Commission (FCC) had only been looking at voice communication over the traditional telephone network and was primarily concerned with keeping a monopoly from forming. Like Bitcoin, VoIP was often peer-to-peer, less expensive, and competed with long-standing incumbents in a highly regulated market. Luckily, Congress and the FCC managed to clear much of the
regulatory ambiguity without burdening the technology with heavy-handed legacy regulation that would stifle innovation. As a result, the technology flourished, increased competition, and led to lower prices for customers. One can only hope that policymakers will do the same for Bitcoin.

Since Bitcoin has the properties of a payment instrument and system, a currency, a commodity, and a network, among other things, several agencies are faced with questions on how to regulate it. These are very well explained in Jerry Brito’s "A Primer for Policymakers" [12] and will be discussed in the remainder of this section.

**Private Currency**

Bitcoins are not being issued by a federal government. But as a cryptocurrency they are used as money. The first question is if that is legal. The answer seems to be yes. The U.S. Constitution only prohibits states from minting money. Privately issued currencies are legal and are actually in circulation. Local currencies such as the Cascadia Hour Exchange in Portland [13] have been created by local business people and lawmakers to promote trade and economic growth in their region. What private currencies may not do is resemble US money. This is clearly not an issue with Bitcoin.

**Money Transmission Laws**

A business that transmits funds from one person to another is a *money transmitter* and must obtain a license where it wants to operate in 48 states and the District of Columbia under non-bank license laws [14], and is subject to the Bank Secrecy Act (BSA), as implemented by regulations from the Financial Crimes Enforcement Network (FinCEN) [15]. Operating an unlicensed money transmission business is also a criminal offense under the USA PATRIOT Act of 2001 [16].

Because money transmitters aren't banks, they normally don't have FDIC insurance, which means that consumers may end up losing their funds if the transmitter doesn't send the money to the payee. For that reason, State licensing has been enacted for consumer protection.

The purpose of the BSA, on the other hand, is to prevent or detect money laundering and terrorist financing. It requires the affected businesses to register with FinCEN, keep transaction and customer records, implement anti-money laundering (AML) procedures, and report any suspicious activity such as transactions above a certain threshold.

Since Bitcoin is not actually a company but a global peer-to-peer network, it cannot be treated as a money transmitter per se. But if actors in its ecosystem exhibit the properties of a money transmitting business, they might still be subject to the same regulation. In 2013 FinCEN has issued guidance on the application of the BSA on virtual currencies which can be used to test if someone who is involved with Bitcoin falls under these laws. It has defined three categories of persons:
A user is a person that obtains virtual currency to purchase goods or services. An exchanger is a person engaged as a business in the exchange of virtual currency for real currency, funds, or other virtual currency. An administrator is a person engaged as a business in issuing (putting into circulation) a virtual currency, and who has the authority to redeem (to withdraw from circulation) such virtual currency. [17]

FinCEN defined a user category that is exempt from FinCEN's regulations. However, under the definition a user is only someone who obtains bitcoins "to purchase goods or services." It doesn't state how someone who doesn't want to purchase anything should be treated. People buy bitcoins for many reasons. For example, as a speculative investment, or a long-term stake in the system because they believe in its success, or because they want to send remittances to their families abroad. None of these constitute a purchase of goods or services, so the user definition doesn't apply. It is not clear if such activities expose someone to money transmission laws or not. This ambiguity creates uncertainty that dampens the adoption of Bitcoin.

An exchanger is a more straightforward case. If someone engages in the "business" of exchanging bitcoins for fiat currency or vice versa then he is considered a money transmitter and subject to FinCEN's regulations. Because states often look to FinCEN for guidance, it is likely that exchangers also may have to obtain licenses.

Most problematic is the interpretation of this guidance for miners who create bitcoins (see section 3.2.2 for a detailed explanation of what Bitcoin mining is and how it works). At first glance, it looks as if miners fall into the administrator category, but that definition only applies to centralized virtual currencies with a central authority that creates the currency, similar to a central bank. Bitcoin however is a decentralized and distributed peer-to-peer network where miners are just another node, so this definition doesn't apply. Therefore, the guidance has a section on decentralized virtual currencies which can be interpreted such that a miner who uses his bitcoins "to purchase real or virtual goods and services" is considered a user and does not have to comply with FinCEN's regulations. But if he sells his mined bitcoins "to another person for real currency or its equivalent" then he is considered a money transmitter and thus subject to regulation. The problem is that miners can't launder anyone's money this way nor are there any consumers to protect, calling into question who would benefit from such burdensome consumer protection and AML regulation.

CFTC Regulation

As mentioned, bitcoins can be viewed as currency or commodity, among other things. Therefore, the U.S. Commodity Futures Trading Commission (CFTC), which regulates commodity futures and their markets, as well as some foreign exchange products, is also looking into Bitcoin [18]. The question is, if it considers bitcoins to be a currency or a commodity.

While the Commodity Exchange Act [19] defines forwards and swaps, which are both a form of foreign exchange derivative, it does not define foreign exchange or foreign currency. Thus, if
the CFTC wants to apply its foreign-exchange regulation to Bitcoin transactions, it will have to justify why it considers bitcoins to be a foreign currency. The 2009 Dodd-Frank Wall Street Reform and Consumer Protection Act, which established the CFTC's authority over foreign exchange, defines foreign exchange as "the exchange, for compensation, of currency of the United States or a foreign government for currency of another government" [20]. Bitcoins clearly fall outside this definition, because they are not the currency of any government.

On the other hand, bitcoins can easily be treated as commodities. The Commodity Exchange Act defines commodities as all "goods and articles ... and all services, rights, and interests ... in which contracts for future delivery are presently or in future dealt in." Because bitcoins are articles that can be traded and made subject of future contracts they qualify as commodities. However, most Bitcoin transactions are currently done instantaneously and not as part of futures contracts. Since the CFTC's authority is not over commodities themselves but over commodity futures, regulation may not apply in those cases. Bitcoin futures on the other hand certainly fall under CFTC regulation.

Electronic Fund Transfer Regulation

Regulation under the Electronic Fund Transfer Act (EFTA) [21] is also a possibility for regulation that needs to be examined. Its purpose is consumer protection. It establishes the rights and responsibilities of consumers and financial institutions that take part in electronic funds transfers, which are defined as:

"any transfer of funds, other than a transaction originated by check, draft, or similar paper instrument, which is initiated through an electronic terminal, telephonic instrument, or computer or magnetic tape so as to order, instruct, or authorize a financial institution to debit or credit an account."

A financial institution is defined as:

"a State or National bank, a State or Federal savings and loan association, a mutual savings bank, a State or Federal credit union, or any other person who, directly or indirectly, holds an account belonging to a consumer."

These definitions assume the presence of accounts and financial institutions in an electronic funds transfer. That is not the case for Bitcoin. As mentioned earlier, Bitcoin is a peer-to-peer network and neither a company nor a financial institution. Bitcoin addresses therefore, which can be thought of as ID numbers of the associated bitcoins, cannot be considered accounts of financial institutions. In fact, there is no financial institution or any third party that "debit[s] or credit[s] an account." Electronic funds transfers on the network are carried out between users alone. The control over sending bitcoins resides entirely with their owner. As will be explained in the following chapter, bitcoins are generally stored in electronic files (wallets) that can reside on a user's computer or with a service provider on the Internet where the user holds an "account". One could argue that these service providers should be regarded as financial institutions, in which case they would fall under EFTA regulation. However, transfers are
generally "initiated" by the user, not the online service, who provides only storage and software to the customer. From that point of view, these services may not count as financial institutions.

Finally, there are regulations by the Consumer Financial Protection Bureau (CFPB) aimed at remittance-transfer providers. These rules require the providers to disclose exchange rates and fees associated with international transfers and, more importantly, require that consumer get 30 minutes to cancel a transfer and get their money back if they do [22]. This is incompatible with the Bitcoin protocol, because all transactions are final and irreversible. It is possible to insert artificial delays into the protocol, but that would be entirely at odds with the purpose of Bitcoin, which will be presented next.

3 Bitcoin

"The only way to confirm the absence of a transaction is to be aware of all transactions."

Satoshi Nakamoto, 2008

3.1 Introduction

3.1.1 What is Bitcoin?

Bitcoin is a cryptocurrency and a peer-to-peer payment network [23]. It is a "peer-to-peer, decentralized, digital currency that relies on cryptography for validation and generation" [24]. As a result, it serves two purposes simultaneously:

- As a currency, it has the properties of money (see section 2.1), i.e. it is a medium of exchange, a unit of account, and a store of value.
- As a peer-to-peer payment network, it is a system that enables fast and secure transfer of money between participants, without the existence of a central authority [25].

This dualism sets Bitcoin apart from other virtual currencies such as Linden Dollars, the currency used in the virtual world of Second Life, and from online payment networks such as PayPal. It is what makes Bitcoin the first completely decentralized payment system [12].

The term "cryptocurrency" actually understates Bitcoin's capabilities. It is not just about money. With Bitcoin, there is for the first time a way to transfer a unique piece of digital property securely over the Internet so that the transfer is irreversible and ownership cannot be challenged, because everyone knows it has taken place and it was valid. The property could be money, but it can also be a contract, or shares in a company, or any other kind of property that can be digitized. The fact that a unique piece stays that way is the real breakthrough. Digital music or Email can also be sent safely and securely, but they can also be multiplied. A person can buy a song once and then copy and sell it as often as he wishes. The fact that it is illegal to do so doesn't make it impossible. For a currency this would be the end. If it weren't scarce or hard to obtain it would have no value. Bitcoin has solved this double spending problem. Digital property, represented by bitcoins, is exchanged through a distributed network of trust that does not required a central third party to operate, because the network itself takes over its
functions. Only the owner of an asset can send it, only the intended recipient can receive it, and the asset can exist only at one place in time, preserving is uniqueness [26]. Exactly how that is accomplished will be explained in detail in this chapter.

This thesis aims to evaluate Bitcoin only by how well it performs as a payment network in fulfilling the needs of the stakeholders in the system. The functions of money will be addressed solely to clearly delineate the two dimensions and in the discussion around the price history that we have witnessed to date.

Before diving deeper into the discussion of Bitcoin, it is important to note that many cryptocurrencies other than Bitcoin, so called altcoins, exist. In fact, at the point of writing, there are at least 280 of them, according to one source [27]. Table 1 lists the top ten cryptocurrencies by market capitalization. The reasons for this diversity are numerous. Some currencies have been created with a different purpose in mind. Mastercoin, for example, was launched in September of 2013 as an extension of the Bitcoin protocol, introducing new products such as contracts for difference and smart property. Others are aimed at the apparent shortcomings of Bitcoin. Litecoin, for example, was launched back in October 2011 with the goal to improve upon Bitcoin with a different hashing algorithm for its proof-of-work function, called scrypt. It mines faster – a new block every 2.5 minutes instead of 10 – and ultimately more (84 million LTC instead of 21 million BTC). The algorithm also has some extra "memory-hard" requirements that don't give custom processors and advantage over normal CPUs as is the case with Bitcoin [28]. All have distinct communities that further their purpose. And while the jury is still out on which will ultimately become dominant, Bitcoin has a big head start and is by far the most successful cryptocurrency to date. Not just by market cap relative to the rest of the field, but also measured by the adoption among consumers and merchants, and the maturity of the platform, measured by the amount and diversity of complementors and the number of revisions of the core Bitcoin client. That is the reason why the author chose Bitcoin for this thesis.

Table 1: Top Ten Altcoins by Market Cap [27]

<table>
<thead>
<tr>
<th>#</th>
<th>Name</th>
<th>Market Cap</th>
<th>Price</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Bitcoin</td>
<td>$5,600,615,030</td>
<td>$438.77</td>
</tr>
<tr>
<td>2</td>
<td>Litecoin</td>
<td>$294,632,158</td>
<td>$10.40</td>
</tr>
<tr>
<td>3</td>
<td>Ripple</td>
<td>$47,383,512</td>
<td>$0.006252</td>
</tr>
<tr>
<td>4</td>
<td>Peercoin</td>
<td>$44,937,540</td>
<td>$2.10</td>
</tr>
<tr>
<td>5</td>
<td>Dogecoin</td>
<td>$34,847,919</td>
<td>$0.00045</td>
</tr>
<tr>
<td>6</td>
<td>Nxt</td>
<td>$31,413,119</td>
<td>$0.031413</td>
</tr>
<tr>
<td>7</td>
<td>Namecoin</td>
<td>$17,672,739</td>
<td>$2.02</td>
</tr>
<tr>
<td>8</td>
<td>Mastercoin</td>
<td>$16,726,685</td>
<td>$29.70</td>
</tr>
<tr>
<td>9</td>
<td>Darkcoin</td>
<td>$11,233,848</td>
<td>$2.63</td>
</tr>
<tr>
<td>10</td>
<td>BlackCoin</td>
<td>$8,374,172</td>
<td>$0.11</td>
</tr>
</tbody>
</table>
3.1.2 History of Bitcoin

Bitcoin was created in 2008 by one or more individuals known only under the pseudonym "Satoshi Nakamoto" [25] [29]. The first bitcoins were created on January 3rd 2009 by Satoshi when he mined the first block, yielding 50 bitcoins (BTC) [30]. The transaction was accompanied by a note in the ledger saying "The Times 03/Jan/2009 Chancellor on brink of second bailout for banks", presumably to demonstrate that this transaction indeed happened that day, and possibly as a hint towards his motives for creating Bitcoin as an alternative to the failing banking system [31].

The USD price of a bitcoin at the time was zero since there was nobody willing to exchange it for fiat currency or any other asset or service. The first recorded price for a bitcoin on Mt.Gox, a once popular Bitcoin exchange that since has shut down, was $0.0769 on August 17, 2010 [32]. Since then, the price and diffusion of bitcoins has increased dramatically.

Table 2 highlights the main events in the history of Bitcoin and the USD price of a bitcoin at the time.3

<table>
<thead>
<tr>
<th>Date</th>
<th>Event</th>
<th>USD/BTC</th>
</tr>
</thead>
<tbody>
<tr>
<td>1998</td>
<td>The concept of cryptocurrency is being described for the first time [33].</td>
<td>-</td>
</tr>
<tr>
<td>1-Nov-08</td>
<td>Satoshi Nakamoto publishes his paper on Bitcoin [34], [25].</td>
<td>-</td>
</tr>
<tr>
<td>3-Jan-09</td>
<td>First bitcoins mined – the “Genesis Block” is created.</td>
<td>-</td>
</tr>
<tr>
<td>12-Jan-09</td>
<td>First Bitcoin transaction, from Satoshi to Hal Finney [30].</td>
<td>-</td>
</tr>
<tr>
<td>May-10</td>
<td>Someone bought pizza worth USD 41 for 10,000 BTC, which implies a price of less than a cent for a bitcoin [35], [36].</td>
<td>$0.0041</td>
</tr>
<tr>
<td>17-Aug-10</td>
<td>The first recorded price for a bitcoin on Mt.Gox.</td>
<td>$0.0769</td>
</tr>
<tr>
<td>Jul-11</td>
<td>First signs of security issues including theft of virtual wallets cause the price to drop [37].</td>
<td>$17</td>
</tr>
<tr>
<td>Jul-12</td>
<td>Bitcoin is growing in acceptance and the platform’s first complementors such as Coinbase arrive.</td>
<td>$7</td>
</tr>
<tr>
<td>Apr-13</td>
<td>Bitcoin’s market cap passes the billion dollar mark. The rise is partly fuelled by the Winklevoss brothers' buying of large amounts of bitcoins, Bitcoin startup OpenCoin receiving VC funding, and growing demand from China [38].</td>
<td>$198</td>
</tr>
<tr>
<td>Jul-13</td>
<td>The Winklevosses file an SEC proposal for a Bitcoin ETF, giving investors exposure to the price of Bitcoin without having to hold them directly, while a ponzy scheme in Texas involving Bitcoin is revealed.</td>
<td>$91</td>
</tr>
<tr>
<td>Sep-13</td>
<td>SecondMarket creates the Bitcoin Investment Trust, another vehicle for gaining</td>
<td>$130</td>
</tr>
</tbody>
</table>

3 Value in USD per bitcoin. If no source for the value was found, it was estimated by the author.
4 The timeline has been modified by the author to include events that were not in the original source but deemed relevant.
5 Average BTC price as reported on http://blockchain.info
indirect exposure to the price of Bitcoin.

Oct-13 Silk Road, the illegal marketplace in the dark web which accepts bitcoins, and which was rumored to be responsible for about half the Bitcoin transaction volume, is shut down. The price drops temporarily but recovers quickly, as the elimination of illegal activities in the Bitcoin ecosystem is ultimately viewed as a boon [39]. At the same time, the world's first Bitcoin ATM is being installed in a café in Canada [40]. $105

18-Nov-13 A U.S. Senate hearing involving policymakers, regulators, and a panel of experts from the Bitcoin ecosystem opine favorably on the legitimacy and usefulness of Bitcoin. The bitcoin price jumps from $463 to $583 within a day. $583

30-Nov-13 The price of a bitcoin exceeds that of Gold for the first time [41]. This is an all-time high. The market cap is more than $13 billion. $1,120

28-Feb-14 Mt.Gox, once the world's largest Bitcoin exchange, files for bankruptcy amidst a scandal involving security breaches and fraud. 850,000 bitcoins where lost, worth nearly $500 million [42]. $578

1-May-14 At the time of writing there are 12,712,075 bitcoins in circulation, with 25 coins being added about every 10 minutes. At a current price of $460 USD/BTC the respective market cap is $5.8 billion [43]. $460

Figure 4 illustrates the USD price history of a bitcoin, annotated with the events from Table 2.

Figure 4: Bitcoin Price Chart

3.1.3 Idea and Motivation Behind Bitcoin

In his first post on a cryptography listserv Satoshi Nakamoto announces the invention of Bitcoin (see Figure 5). In that same thread Satoshi replies to questions with regards to his original post. One of his answers in particular leads us to assume that his work was at least partially politically motivated:

... we can win a major battle in the arms race and gain a new territory of freedom for several years. Governments are good at cutting off the heads of
The idea behind Bitcoin is explained in detail in the paper he referenced in that post. There, he describes his vision of a peer-to-peer network that would allow for electronic cash to be transferred directly between parties that don’t know or don’t trust each other, without having to go through a financial institution or another trusted third party [25]. This is revolutionary and would dramatically reduce friction in the global payment system, lowering costs to a minimum and increasing transfer speeds to be almost instantaneous.

Figure 5: Satoshi Nakamoto Publishes His Bitcoin Paper [34]

Bitcoin P2P e-cash paper

Satoshi Nakamoto Sat, 01 Nov 2008 18:16:33 -0700

I've been working on a new electronic cash system that's fully peer-to-peer, with no trusted third party.

The paper is available at:
http://www.bitcoin.org/bitcoin.pdf

The main properties:
Double-spending is prevented with a peer-to-peer network.
No mint or other trusted parties.
Participants can be anonymous.
New coins are made from Hashcash style proof-of-work.
The proof-of-work for new coin generation also powers the network to prevent double-spending.

Bitcoin: A Peer-to-Peer Electronic Cash System

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without the burdens of going through a financial institution.

Others in the community have since taken on leading roles in defining what Bitcoin is, can, and will be. Nicolas Cary, Blockchain.info’s second employee, said “...we’re going to build something that makes a better world through better money” [44].

---

6 Blockchain.info is the leading open-source service in the Bitcoin ecosystem, whose purpose is to provide as much transparency about the network as possible, including a website with an easy-to-use tool to traverse the blockchain of all transactions ever made, a free and secure wallet and several APIs for programmers to access and consume all of the service’s data [32].
3.1.4 Concept

As noted in the introduction, a concept maps function to form and an architecture is the implementation of that concept. In the language of Professor Ed Crawley's [3] Needs-to-Architecture framework (see Figure 6 for an illustration) Satoshi devised a concept whose function consists of the Bitcoin network as the specific system operating and bitcoins as the specific operand, in order to fulfill the central goals of allowing

- people (beneficiaries) to send e-money directly and instantaneously to each other;
- who don’t have to know each other and can be anonymous;
- without the involvement of a (costly) trusted third party;
- while avoiding risks such as double spending;
- while maintaining the functions of money (including management of inflation).

The corresponding form that implements that concept and enables the function of the system comprises several technologies that individually have been in existence for some time, but whose combination yields the unique hybrid of cryptocurrency and secure payment network that is Bitcoin:

- Decentralized and distributed peer-to-peer networks
- Proof-of-work
- Cryptographic hashing
- Public key cryptography
- Digital signatures

These technologies will be explained in detail in the next section.

3.2 Architecture

This section discusses the technologies that are comprised in the Bitcoin architecture. While the peer-to-peer technology makes it decentralized and distributed, proof-of-work, public key cryptography, digital signatures, and cryptographic hashing are what makes Bitcoin a secure network of trust without the need for a third party to verify and validate transactions. This is achieved by time stamping each transaction and creating a chain of events that was witnessed by everyone on the network and that cannot be changed [25]. The result are secure and irreversible payments and, more generally, decentralized information verification, which opens up a myriad of possible use cases for Bitcoin beyond the transfer of money.

3.2.1 Peer-to-Peer Network

A peer-to-peer (P2P) network is a type of decentralized and distributed network architecture in which individual nodes in the network (peers) act as both suppliers and consumers of
resources. This is in contrast to the centralized client-server model where client nodes request access to resources provided by central servers [45]. Bitcoin is a distributed, decentralized, and democratic system of trust over transactions without the need for a third party and, therefore, a true peer-to-peer network.

Distributed means that work is split up between members of a network who communicate with each other in achieving a common goal.

Decentralized means that this work is not coordinated by a single resource that decides which node does what work or that assembles the individual work results back together [46]. The fact that Bitcoin possesses these two properties and thus qualifies as peer-to-peer is evident in the fact that each node on the network does essentially “what it wants”, without taking orders from a central authority. For example, when a node receives a message about a transaction, it forwards this message to all other nodes it is connected to. Similarly, a node that is mining a block is individually trying to find the answer to the cryptographic hash problem and, when it finds a solution, broadcasts it to all the nodes it is connected to, who in turn disseminate that message throughout the network.

Democratic means that each unit of computing power gets one vote [25], and the majority of the network’s computing power decides what the truth is. On the other hand, this does not preclude groups of nodes combining and coordinating efforts with each other on top of the Bitcoin protocol to achieve a common goal, as is for example the case with mining pools (see section 3.5).
In the peer-to-peer network each node speaks directly with each other node it is connected to, whereas in the centralized network based on the client-server model, all communication goes through a central service. The advantage of peer-to-peer is fast, secure, and reliable delivery of communication, but at the price of increased coordination costs as each new node does not just have one new connection to the central hub, but one new connection to potentially every other node on the network. This introduces scalability issues, as the number of connections grows exponentially in a peer-to-peer network [47, pp. 21–23]. Figure 7 illustrates the difference between the two network models.

![Figure 7: Peer-to-Peer vs. Centralized Networks [45]](image)

Traditional payment systems have been built in pre-Internet times, when central hubs such as banks and clearing houses aggregated supply and demand for payments from and to parties that were not in direct contact with each other. Nonetheless, attempts at peer-to-peer payment platforms have been made before and turned into startups such as Transferwise\(^7\) and peerTransfer\(^8\), but they fall short of the true peer-to-peer definition. Instead, they lie somewhere along the spectrum between peer-to-peer and centralized network, as they rely on banks and clearing houses as critical elements in their infrastructure. Only the “last mile” to the end-user has been disintermediated by these startups. But crucially, transacting parties still don’t speak to each other directly and thus the system is not fully decentralized and distributed. In that respect, these competitors rather disintermediate the aggregation function of banks by bundling supply and demand from a large number of customers away from banks, before ultimately moving money on a wholesale basis through the international payment system just as the incumbents do.

The steps to send money internationally through Transferwise are as follows.

\(^7\) https://transferwise.com
\(^8\) https://www.peertransfer.com
1. Payer fills out an online form with the desired currency, amount, and payee’s bank details
2. Payer sends money from his bank account to Transferwise.
3. Wait several days.
4. Payee receives funds in his account.

In contrast, one way to send money internationally using Bitcoin exchanges would currently be as follows.

1. Payer buys bitcoins at an online exchange; simultaneously, the exchange sends a debit request to his bank account.
2. Depending on his verification status with the exchange, the payer immediately gets his bitcoins or has to wait until the exchange receives the funds, which can take several days, depending on the payer’s local bank infrastructure.
3. Payer sends bitcoins to destination address using an online form to fill in the amount of bitcoins to send and the payee’s Bitcoin address.
4. Payee immediately receives the bitcoins; the actual confirmation on the network takes about 10 minutes.
5. Payee sells bitcoins on the local exchange in his currency; settlement of funds takes several days depending on local bank infrastructure.

Thus, the difference between current solutions advertised as "peer-to-peer" and a transfer based on Bitcoin lies not so much in the short-term user experience. Both require similar amounts of time, user interaction, and the passing-on of bank details. But the underlying technology is vastly different, with the long-term implications and potential uses being far greater for Bitcoin.

3.2.2 Mining the Block Chain

A fundamental innovation in Bitcoin is the shared public ledger. A ledger is an accounting book that records all transactions and where no entry can be erased. To reverse a transaction, a second, opposite transaction has to be entered. Because Bitcoin’s ledger is shared and public, all transactions ever made are known to everyone on the network. This is the reason why proponents of Bitcoin claim that fraudulent behavior such as double spending becomes nearly impossible. In Bitcoin, the public ledger is called the block chain [48]. It came alive on January 3rd, 2009 at 18:15 UTC [49] with the Genesis Block [50].

The block chain consists of individual blocks. A block is a record of the most recent Bitcoin transactions that have not yet been recorded in any prior blocks [51]. Blocks are linked to each other in chronological order to form the block chain. The chain can be used to calculate the amount of bitcoins associated with an address, simply by summing up all incoming transactions to and subtracting all outgoing transactions from the address. To know if an incoming transaction was valid, i.e. if it was spent by someone who had the required amount of bitcoins,
the balance of that originating address itself can be calculated by again summing up all of its previous incoming transactions and making sure that all its outgoing transactions have not exceeded that amount. Therefore, the chronological order of all transactions is crucial to the integrity of the system and must be protected against tampering. This integrity is enforced through mining.

Mining, or generating, is the process of appending blocks with new transaction records to the block chain. A block is mined about every 10 minutes. Once a transaction is recorded in a block, it is considered confirmed. The award for the first block mined was 50 bitcoins. For every 210,000 blocks solved, the number of bitcoins yielded per block is cut in half [49][52]. Currently, the number is 25. In the year 2140, at a final amount of 21 million bitcoins mined [33], the creation of bitcoins will cease and no more bitcoins will be awarded for mining. The actual number in circulation will be lower due to bitcoins lost, for example, when the physical storage a bitcoin was held in gets destroyed [53]. After 2140, blocks will still be mined, but no new bitcoins will be granted as reward [54]. Miners are already asking for transaction fees attached to a transaction by the sender in order for it to be prioritized in the mining process, and it is likely these fees will increase to offset reduced mining awards in the form of new bitcoins [49][52].

During the mining process, a complicated cryptographic hashing problem is solved as proof-of-work [55]. The proof-of-work is a way to implement a timestamp server on a distributed network without the need for a third party. The goal is to avoid double spending [25].

Double spending is the attempt to try and spend bitcoins to two different recipients at the same time. In the traditional banking system, one cannot spend one's money twice because the bank keeps a record of all transactions, including time and date. If someone with $100 in his account took $100 in cash from an ATM and at the same time wrote a check for $100 to another person, that check would bounce, because by the time it arrived at the payer’s bank several days later, his balance would have been reduced to $0 by the earlier ATM transaction. In the Bitcoin network, the transaction that gets mined first is confirmed. The other one will be rejected by the network. Bitcoin mining and the block chain are there to create a consensus on the network about which of the two transactions will confirm and be considered valid [56], making Bitcoin immune against double spending.

Running the network

The steps to run the network and build the block chain are as follows.

1. New transactions are broadcast to all nodes.
2. Each node collects new transactions into a block.
3. Each node works on finding a difficult proof-of-work for its block.
4. When a node finds a proof-of-work, it broadcasts the block to all nodes.
5. Nodes accept the block only if all transactions in it are valid and not already spent.
6. Nodes 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 previous hash.
Nodes always consider the longest chain\(^9\) to be the correct one and are working on extending it. If two nodes happen to find a proof-of-work at the same time and broadcast their blocks simultaneously, some nodes will receive one block first, and some the other. Nodes will always work on the first block they receive, but save the other one (which has now created a fork in the chain) in case that branch becomes longer. The race between the two branches is over when the next proof-of-work is found and one of the two branches wins and becomes longer. The nodes that were working in the losing branch will switch and start working on the longer one.

New transaction broadcasts do not have to reach all nodes. As long as they reach enough nodes, they will ultimately end up in a block. Block broadcasting is also able to handle dropped messages. Should a node not receive a block, it will request it when it receives the next block and realizes it missed one [25, p. 3].

**Cryptographic Hashing**

To gain a better appreciation of the importance of proof-of-work for securing the network, it is helpful to have some understanding of encryption and cryptographic hashing. The purpose of *encryption* is to make plain information secure in such a way that it can only be read by the intended recipient. Thus, the author of information \(x\) (*plaintext*) transforms it into a different set of symbols \(y\) (*ciphertext or code*) using an algorithm \(H(x)\) (*cipher*). Without that algorithm, it is not trivial to reverse the transformation to get the plaintext \(x\) from the ciphertext \(y = H(x)\) \[57\] \[58\]. The more elaborate the algorithm, the harder it is to guess and thus the harder to decrypt the ciphertext through sheer luck or brute force.

One particular type of algorithm is *hashing*. In Bitcoin, each block must contain a proof-of-work to be considered valid. This proof-of-work is verified by other Bitcoin nodes each time they receive a block. Bitcoin uses the hashcash proof-of-work function, specifically hashcash-SHA256\(^2\) \[49\]. The square means that the result of the first hash is hashed again for increased security, especially against birthday attacks (which SHA256 is not susceptible to anyway due to its pre-image resistance (see below), but this conservative approach makes it even safer) \[59\]. *Hashcash* is not a new concept and neither is SHA. SHA has been developed by the NSA \[60\]. The hashcash proof-of-work function was invented in 1997 and has been used in many applications to avoid DoS attacks and spam, including Microsoft Exchange and Outlook \[61\][49][62\]. It is a form of hashing algorithm, which in turn is a form of cipher. The resulting ciphertext, called hash, is completely random. Apart from being encrypted, it has the additional property of always having the same length, independent of the length of the plaintext \[63\]. In SHA256\(^2\) the length is 256 bits \[64\]. Figure 8 illustrates how cryptographic hashing works and shows that the output is completely unpredictable, no matter how similar or different the inputs are.

---

\(^9\) *Longest chain* means the chain on which the most processing power has been expended, not the one with the most blocks or transactions in it \[51\].
The reason why hashing is so popular is that it is easy to generate hash values from input data and easy to verify that the data matches the hash. The same input will always give the same hash. It requires only one calculation. But, it is hard to fake a hash value \( H(x) \) to hide malicious data in the message \( x \). Because hashing is random, with a strong cryptographic hash function there are so many possible results, it makes it computationally too expensive to randomly generate a message \( x \) that results in a specific hash \( H(x') \) whose message \( x' \) is known. As a consequence, if two transactions have the same hash, one can be confident they are identical [63]. That way, the cost of encrypting data is low (e.g. encrypting Emails including the sender's address) but the cost of decrypting is very high (e.g. for a spammer to find people's Email addresses within the hash), which makes hashing a very efficient way to secure data.

Figure 8: Cryptographic Hash Function [65]

This is important in eliminating the risk of double spending. If a transaction that contains information about the sender, receiver, and amount is hashed, and the hash is used as proof for this transaction, it is conceivable that a malicious user could try to generate another transaction whose hash looks exactly the same (hashes and the block chain are public) and which would then be equally valid. With SHA256 \(^2\) this is for all intents and purposes impossible and is referred to as second pre-image resistance.\(^1\)

The hashcash problem used in Bitcoin mining is to find a 256-bit hash \( H(x) \) that has less than a certain number of leading zeros\(^1\). The more zeros required, the fewer possible hashes there are. Hashes are random because their output is unpredictable. Therefore, it is a matter of trial and error to put in so many different values for \( x \) until the result \( H(x) \) contains the minimum required number of leading zeros. Furthermore, the input into the hash function is not purely a random number \( x \). The result of hashing is a block. In order to link all blocks in the block chain, the input for a new block is the hash of the previous block (more precisely its header), plus

\(^{10}\) For further details on the feasibility and probability of staging a successful second pre-image attack on SHA256 see for example [66][60][67].

\(^{11}\) A 256-bit number is a sequence of 256 digits consisting only of 0s and 1s.
some nonce $c$ which acts as a counter for each miner, plus a random seed $s$ given to each miner so as to avoid two miners using the same inputs. Thus, the function becomes $H(s, x, c)$ [59].

A hash with many leading zeros simply means it is a small number. For example, for a 3-bit hash, the binary number has 3 digits. Since each digit can only be either 0 or 1 in the binary system, there are eight ($2^3$) possible combinations. The binary number 000 equals the decimal number 0, the binary number 001 equals the decimal number 1, and so on. 110 equals 7, and 111 equals 8. So, if two leading zeros are required, the only two binary numbers acceptable are 001 and 000. Since there are eight possible numbers [000, 111] the chances of randomly finding a solution is $2/8 = 25\%$. On average, one has to make four attempts ($8/2$) to find a solution.

Generally, the number of attempts required can be written as

$$\frac{2^n}{2^{n-k}} = 2^k$$

with $n$ being the number of bits in the hash (256 in Bitcoin), and $k$ the number of leading zeros. $2^n$ is called the maximum target and $2^{n-k}$ is the current target. The goal then, is to find a hash that is below the current target:

$$H(s, x, c) < 2^{n-k}$$

The higher $k$, the higher the number of attempts required. For $k = 20$ there would be 1,048,576 attempts on average [59].

The minimum number of attempts in Bitcoin is set to $2^{32}$, i.e. $k = 32$ and $2^{n-k} = 2^{224}$. This number is a 256-bit number with 32 leading zeros ($k = 32$) and is called the difficulty_1_target. Difficulty is Bitcoin's way of expressing how much computing power is required to solve a block. The formula for difficulty is:

$$\text{difficulty} = \frac{\text{difficulty}_1\text{_target}}{\text{current\_target}}$$

A difficulty of 1 means

$$\text{current\_target} = \text{difficulty}_1\text{_target}$$

I.e. $k = 32$. A difficulty of 2 means that $k = 33$ and current_target = $2^{223}$, requiring twice as many attempts. For difficulty 3 and $k = 34$ the number of attempts would double again, and so on [68]. The difficulty at the time of writing was 8,000,872,136, which means $k = 64.90$ and the current target is $2^{191.1}$ [69]. Accordingly, the number of attempts required is $2^{64.90} = 3.45 \times 10^{19}$. The time it takes in to find a solution, and for one lucky miner to receive 25 BTC, depends on how many attempts can be made in a certain amount of time. This number is called the hash rate.
Bitcoin's hash rate is the number of attempts currently made by all computers on the network combined. At the time of writing the hash rate was 66,817,886 GH/s\textsuperscript{12} [32]. Dividing the hash rate by the number of attempts required returns the time it takes the network on average to mine a block. In this case, the time is 514 seconds or 8:34 minutes. Close to the intended average of 10 minutes, but not quite.

Since difficulty describes how many attempts will be necessary to find a solution, for a given difficulty it takes less time if there are more nodes with more computing power on the network. But, since Bitcoin is designed to mine a block every 10 minutes on average and thus have a predictable rate of inflation, the difficulty has to be adjusted to variations in the hash rate. The hash rate changes constantly with miners coming on and off the network, but difficulty only gets adjusted every two weeks to the prevailing average hash rate, so the result will never be exactly 10 minutes. In any case, hashing is a random function and so the time to mine a new block fluctuates around the average indicated by the difficulty and hash rate. How the hash rate has changed over time is shown in Figure 9. Figure 10 shows the adjustments in difficulty over the same period.

\begin{figure}[h]
\centering
\includegraphics[width=\textwidth]{bitcoin_hash_rate_chart}
\caption{Bitcoin Hash Rate Chart [32]}
\end{figure}

\textsuperscript{12} GH stands for \textit{giga hashes}, i.e. 1 billion hashing operations. Thus, 66,817,885 GH/s means 66,817,885 billion hashing operations per second.
The entire concept of Bitcoin revolves around not needing a trusted third party but instead being able to trust the system without having to trust any one individual. To accomplish that goal Satoshi provides a solution which he calls the proof-of-work chain. It takes care of synchronizing the whole network to the valid ledger which represents the view shared by the majority of the computing power [34]. Hashcash and proof-of-work made a central authority which manages the money supply and acts as trusted third party obsolete.

### 3.2.3 Transactions: Digital Signatures and Public Key Cryptography

In a simplified way, a Bitcoin transaction can be seen as the transfer of bitcoins from one account to another, similar to traditional payments. These accounts are called wallets and each wallet has a Bitcoin address. What makes Bitcoin special is the fact that the addresses need not be tied to an identity in the real world, such as a bank account or credit card [12, p. 10]. In fact, a user can randomly create a new address for each transaction. Because there are so many possible numbers, it is virtually impossible to accidentally create an address that belongs to someone else. Bitcoin transactions are therefore anonymous. This is one of the biggest differences to traditional online payment systems. As a consequence, the Bitcoin network is often used by criminals for illegal activities such as fraud or money laundering, and even entire underground market places such as the infamous Silk Road.

To be precise, Bitcoin is not actually anonymous, but pseudonymous. While the true identities of senders and receivers are not required for the network to function, the Bitcoin addresses used in each transaction are recorded and distributed to every node on the network through the block chain. Thus, the block chain is a record of the entire history of all Bitcoin transactions ever made. Pseudonymity is not dissimilar to the way Email works. While an Email can be traced back to its sender, the true identity of that sender is unknown and he could create a new Email address for every Email he sends. Thus, Bitcoin is somewhere in the middle of the spectrum between cash and electronic funds transfer. It is similar to cash in that it allows nearly
instant transfer directly between two parties without a trusted third party in the middle. But unlike cash, each transaction gets recorded as with EFT and in addition is known to anyone who comes on the network. But unlike EFT, the parties are by default anonymous. However, because user-data such as IP addresses and bank account information are recorded when fiat currency is exchanged for bitcoins on Bitcoin exchanges, it is possible to tie a real-world identity to such a transaction [12, pp. 9–11].

In actuality, Bitcoin transactions are more complex. A transaction moves bitcoins from one address to another and gets included in the block chain. Each address has a private key associated with it which is used to sign the transaction. Each address also has bitcoins associated with it. As a consequence, only the owner of the private key can send the respective bitcoins. The signature provides mathematical proof that the coins come from the owner of the private key. Hence, it is imperative to not lose the private key, lest the bitcoins at that address cannot be spent and become worthless. Likewise, it is important to keep the private key secret, because anyone with the key, legitimate owner or thief, can spend the coins.

Each address also has a public key associated with it. Bitcoin uses the public/private key cipher technology with an asymmetric key algorithm, where different keys are used for encryption and decryption. The key pair is generated and mathematically linked together but one key cannot be deduced from the other. This makes it possible to make one key public without the loss of confidentiality. Whereas the private key is used to sign transactions, the public key is in fact the bitcoin address.

![Figure 11: Bitcoin Transactions][25]

The signature is combined with the hash of the previous transaction and the public key of the recipient to form the new transaction. Finally, the new transaction is cryptographically hashed and this hash is used to identify the transaction in the system. Besides proving ownership, the signature also prevents the transaction from being altered by anybody once the transaction has
been hashed. The transaction is then broadcast to the network and will be confirmed within about 10 minutes through mining [55], [70], [71]. See Figure 11 for an illustration of transactions from Satoshi Nakamoto's paper.

3.3 Features and Properties

This section describes the features and properties of Bitcoin that emerge from its architecture. They will serve as guidance for the discussion of Bitcoin’s suitability for international payments in chapter 4.

Satoshi’s paper [25] in combination with some of his posts [34] on the listserv thread already give some insights into what features he had in mind.

With regards to inflation through a drastic increase in computing power (according to Moore’s Law) he writes:

To compensate for increasing hardware speed and varying interest in running nodes over time, the proof-of-work difficulty is determined by a moving average targeting an average number of blocks per hour. If they’re generated too fast, the difficulty increases.

Likewise, Satoshi already anticipated that if demand outpaces the speed of production (mining) of bitcoins, their price will rise and early holders will reap the benefits:

If the supply of money increases at the same rate that the number of people using it increases, prices remain stable. If it does not increase as fast as demand, there will be deflation and early holders of money will see its value increase.

With regards to anonymity:

It’s not pseudonymous in the sense of nyms identifying people, but it is at least a little pseudonymous in that the next action on a coin can be identified as being from the owner of that coin.

On recourse:

Identities are not used, and there’s no reliance on recourse. It’s all prevention.

His thoughts on double spending:

There’s no need for reporting of "proof of double spending" like that. If the same chain contains both spends, then the block is invalid and rejected.

And finally, his take on security:
Right, it's ECC digital signatures. A new key pair is used for every transaction.

The following is a discussion of Bitcoin's attributes in more detail.

**Decentralized and Distributed**

Bitcoin is a decentralized and distributed network of trust. There is no central authority that issues new coins or takes existing ones out of circulation, that gets involved in the authorization, processing, or settlement of transactions, or keeps a (secret) ledger. Likewise, bank accounts and card networks are not required for clearing Bitcoin transactions [72]. This is achieved via full decentralization of the verification process (mining), the distributed public ledger (block chain), and thus the true peer-to-peer nature of the network.

**Democratic**

The fact that Bitcoin is democratic does not automatically follow from decentralization and distribution. Majority decision making could be undermined if the system were based, for example, on one-IP-address-one-vote. Whoever manages to allocate the most IP addresses garners the most votes. But through proof-of-work a one-CPU-one-vote system has been implemented. The majority decision is represented by the longest chain, which has the greatest proof-of-work effort invested in it [25].

**Without Double Spending**

The biggest challenge for digital currencies is the problem of double spending. Much like a text or audio file can be copied multiple times after purchase, and then re-sold, a digital currency could be 'copied' multiple times and thus spent more than once. The traditional solution is a trusted third party, a clearing house, that records every transaction and thus can be used to identify illegal copies and other types of fraud. Bitcoin solved the problem of a trusted third party through mining and the block chain as public ledger [73]. Double spending is countered by the fact that only the longest chain is valid, so if an input is spent in two different blocks, only one of them will be valid once one of the blocks ends up in the longest chain. Therefore, the receiver of a new input should wait several blocks before acting upon that input, for example by shipping goods to a customer, until that input is indeed confirmed to be in the longest block chain. The other receiver of an input from the same source will have his transaction rejected by the network. Since he should have waited for a confirmation before using those bitcoins, he should not have any damage. In fact, he could have already spent that bitcoin and the next receiver would then have his input cancelled as well [34].
With Predetermined Supply

The only source for new bitcoins entering the economy is mining, which happens at specific time intervals (every 10 minutes until the year 2140) and at specified quantities (the amount of bitcoins generated per block halves about every 4 years (every 210,000 blocks exactly). The rate of inflation is set and will be zero in the end. Conversely, there is no mechanism for taking bitcoins out of circulation. The only time their number decreases is when they are 'lost'. Lost bitcoins still exist, but they are no longer available to the economy because their owner has no access to the private key associated with their public address and so has no way of retrieving them. Bitcoin therefore is ultimately a deflationary currency. To account for an increase in computing power on the network while keeping the mining of new bitcoins at a 10-minute interval on average, the mining difficulty is being adjusted every two weeks based on a moving average of the hash rate, as explained in section 3.2.2.

Volatile

The supply of bitcoins is completely inelastic to demand. It is set by an algorithm to peak at 21 million bitcoins in 2140. However, due to some bitcoins getting lost over time, the supply will ultimately shrink. Demand on the other hand is highly volatile and unpredictable, especially at the current early stage of Bitcoin where not just regular users such as merchants and consumers transact on the network, but where speculators looking for quick profits come in and out of bitcoins in staggering amounts in very short time frames. Thus, the price of bitcoins currently is highly volatile. Once the euphoria has settled and a fair price has been established, demand will be more stable and become more predictable in line with the flow of goods and services paid for in bitcoins, including international money transfer and currency exchange. At that time, price fluctuations should decrease to levels normally seen in markets of similar size. The size of the current market at about $6 billion is another reason for the current volatility. It is not the actual number of bitcoins that matters - more than half of the final 21 million are already in circulation. It is the market capitalization, the volume in fiat currency, that matters. At the current market size an investor who wants to buy $1m worth of bitcoins will move the price much more than if the market were worth $6 trillion.

Transparent

The entire blockchain and thus all transactions ever done on the network are public and can be viewed by anyone. It is even possible to watch a live stream of all transactions in the Bitcoin economy on blockchain.info (see Figure 12). It is typically unknown who the sender and receiver are or what the specific motivation behind each transaction was, but they are all there. Be it a purchase on Overstock.com, a trade on Bitstamp or someone moving his coins from hot to cold storage. No other economy before allowed such an undiscriminating public view [44].
Pseudonymous

While transactions are public, the real identities of the owners of the addresses are not. In addition, a new address can be created for every transaction. Thus, even efforts to use pattern recognition to derive true identities from transaction data are severely hampered. However, due to the transparency afforded by the public block chain, Bitcoin is pseudonymous rather than anonymous. Therefore, Bitcoin cannot offer the same level of privacy as cash [33].

It does, however, afford a higher level of privacy compared to the traditional banking system. There, privacy is achieved by limiting access to information to the parties involved in a transaction and the trusted third party. In Bitcoin, all transactions are announced publicly on the block chain, so this method does not work here. But, privacy can still be achieved by keeping public keys anonymous, so they cannot be traced back to real world identities. An additional step to maintain privacy is to use a different public key for each transaction [25].

Instantaneous

Bitcoin transactions are instant, due to the true peer-to-peer nature of the network, with no clearing houses or other intermediaries required for processing. However, in order to be certain that the bitcoins received in fact come from a source who owned those bitcoins and did not double spend them, it is advised to wait at least for one if not more confirmations, which prolongs the transfer time.

Irreversible

Transactions are irreversible once confirmed and in the block chain. The only way to reverse a transaction is to do an equal and opposite one. The protocol itself also doesn't require any real identities being revealed in a transaction, so there is no real-world identity one could aim any proceedings against. There is no recourse. Exchanges and other financial services companies in the Bitcoin ecosystem do collect personal information of their users, not least because of regulation. And while the underlying protocol is pseudonymous, transactions done on these platforms can and will be tied to real identities, and therefore can be reversed by an opposite transaction. The question then is how disputes are resolved, which is an entirely different conversation outside of the Bitcoin protocol, centering around consumer protection and the laws regarding contracts between consumers and merchants.

Inexpensive for Users, Expensive for Miners

Transactions currently are virtually free. Thus, there are very low economic barriers to entry for users to get on the network. On the other hand, mining has become incredibly expensive in terms of the USD/BTC price relative to the cost for hardware and energy required to mine at the current difficulty. With so many CPUs on the network, the probability of a single CPU mining a block has become miniscule. This works as intended, as the increased difficulty keeps the block mining rate at its desired level of one block per 10 minutes, but it drives concentration of
most of the power to a few very powerful mining pools, increasing risks such as 51%-attacks and selfish mining (see section 3.5). The two biggest mining pools (BTC Guild and GHash.IO) currently control over 60% of the computing power on the network (see Figure 15). It is not uncommon for these pools to mine several blocks in sequence. In April 2013 (and several times thereafter) BTC Guild mined six blocks in a row [32][74]. This is a security concern as the system relies on the majority of nodes on the network being honest.

Secure

Through its combination of cryptographic hashing, public key cryptography, digital signatures, and the public ledger, Bitcoin provides several measures of security for the stakeholders and for the network itself. But it is not perfect and there are areas of weakness.

- Theft protection
  Nobody can spend someone else’s bitcoins and nobody can fake a transaction looking like it came from someone else unless they have their private key. In Bitcoin, actually stealing someone’s coins (similar to stealing someone’s cash) is the same as pretending to be someone else in a transaction without actually having their cash (similar to writing a check in someone else’s name), because the current balance of bitcoins is simply the sum of all previous incoming and outgoing transactions to an address, all of which are visible to the public through the general ledger.

- Fraud protection
  There is a high level of fraud protection from within the Bitcoin system. Nobody can create a block with a fake transaction in it due to the proof-of-work requirement. Defrauding other users through double spending is impossible and has already been discussed. The result is a much higher level of security compared to current payment instruments. When paying with a credit or debit card at a merchant in the store or online, the customer submits all the credit card information that is required to make a purchase, now and in the future. The customer has to trust the merchant to keep that information safe from fraud, by the merchant himself as well as from hackers who might steal that data. With Bitcoin, no sensitive data is transmitted that could be used by another party to make future payments. The private key is required to spend bitcoins, and the owner never has to disclose it. In that sense, Bitcoin is like cash.

However, protection against concealing flows and sources of external funds (i.e. money laundering) is rather limited. On one hand, the public ledger leaves a trail of all transactions and thus fraud can be detected either in real-time or forensically through suspicious pattern recognition. On the other hand, due to the pseudonymous nature of Bitcoin, fraudsters can easily obscure their identity and get away with money laundering. Even if a fraud were detected, as long as the perpetrators are at large, and their keys are safe, their funds could not be seized or frozen.
• Insurance
  There is no insurance in the Bitcoin protocol itself. However, there are several startups that develop products and services that provide various forms of insurance against the loss of bitcoins and hedges against adverse price moves.

Open Source

Bitcoin is an open source platform with low barriers to entry. It fosters innovation in the community, from the Bitcoin protocol itself to all kinds of products and services by complementors.

The Bitcoin protocol has evolved over time, often in reaction to adverse events. The fall of Mt.Gox, for example, has brought attention to the malleability exploit. Although widely considered a scapegoat to distract from gross negligence or outright malice by the operators, it has been known to cause problems for wallet implementations that did not take this exploit into account. In response, the Bitcoin reference client version 0.9.0 was released with a bug-fix [75].

APIs have been built that consume block chain data and react to it, such as trading algorithms that generate buy and sell recommendations from trading prices and volume data on exchanges, accessible through other APIs.

Figure 12: Stream of Latest Bitcoin Transactions on Blockchain.info [32]
3.4 Uses, Challenges, and Value

This section discusses the real world applications for Bitcoin, what risks and challenges it is facing on its way to mainstream adoption, and what the value of a bitcoin might be, given the currency’s properties described in the previous section.

3.4.1 Uses

It is difficult to overstate the potential uses and benefits of Bitcoin. Numerous applications come to mind when looking at its attributes. From easier online shopping, to faster and cheaper money transfer, to smart contracts with automated execution of clauses, and many more. An exhaustive discussion would go far beyond the scope of this thesis. But while there is a gap between the obvious uses that the media and most other people see, and the visions of programmers, technology enthusiasts, and entrepreneurs, almost all can agree on a number of concrete and immediate applications. Some of the most relevant ones will be described here.

International Payments

The first use case that is generally mentioned as the one having the largest immediate potential to change the way we transact on a global scale, and which happens to be the topic of this thesis, is international payments. As noted in chapter 2, the international remittance market has a volume of around $500 billion. Millions of low-income workers send hard-earned money back to their families in developing countries, often subsiding on the bare minimum. As the funds travel through the international payment system, financial companies in the value chain, like the traditional wire services Western Union and MoneyGram, extract fees of up to 10 percent, sometimes more. And the funds take days to arrive.

As an inexpensive funds transfer system with fees of around 0.0005 BTC, Bitcoin would lower the costs of remittances to a minimum and speed up the transaction. At that price, even a $25 transfer costs less than 1%, allowing migrants and guest workers to send payments more frequently instead of having to save them up to be able to afford the transaction. These benefits immediately help those most in need and increase their standard of living. In fact, it is hard to think of any other solution that can improve the lives of millions of people in such a short amount of time and with such little effort from the financial and entrepreneurial community.

Of course, the uses for international payments go beyond remittances. International students, expatriates, businesses, anybody with accounts in multiple locations, will benefit from near-instant transfer of funds at a fraction of the costs currently charged by banks. Now that Bitcoin ATMs have arrived, even tourists can save themselves from paying steep conversion rates to exchange agents at their destinations.

International payments will be further analyzed in detail in chapter 4.
Online payments

More efficient online payments is the use case that has gained the most traction so far, as more and more merchants recently started accepting bitcoins. Small businesses often operate on razor sharp margins. Many have an online presence to increase their reach, and while credit cards were very helpful in making transactions easier, they come with considerable costs to merchants. Businesses that want to offer credit card payments as an option to their customers first needs to pay for a merchant account with each credit card company. Depending on the terms and conditions, they must then pay a variety of authorization fees, transaction fees, statement fees, interchange fees, and customer-service fees, among other charges. These quickly sum up to an average of around 2%-3% per transaction plus running flat fees that eat up most of the additional profit.

Bitcoin removes those charges. Small business have already adopted BitPay, a payment-processing company, because of its ability to lower the costs of doing online commerce, even across borders. Even large online retailers like Overstock.com, and other big names such as Tesla, now accept Bitcoins as a way to avoid the costs of doing business with credit card companies. The early results indicate that consumers paying with bitcoins spend more on average, and are mostly new customers. Both effects add to the bottom line of businesses [76]. Others have adopted it for its speed and efficiency in facilitating transactions. And some merchants may not even qualify for being allowed to accept credit card, because they fail the credit check. That is the niche the payments company Square used as a beach head to start is business. Bitcoin companies can do the same, but even cheaper.

Accepting credit card payments also exposes business to chargeback fraud, where consumers initiate payment reversals, pretending that a product has never been delivered. Merchants can lose the payment for the goods and the item itself, and in addition they have to pay a fee for the chargeback. Bitcoin eliminates this kind of fraud because payments are irreversible.

Of course, chargebacks have benefits for honest consumers, because they protect them from the opposite risk of shady merchants keeping the payment and not sending the goods, as well as from honest merchant errors. And there are other benefits to credit cards such as rewards and insurance, that are funded by credit card fees and that consumers may want. Thus, many consumer and merchants will probably stick to credit cards, but Bitcoin offers more alternatives to everyone that haven't been there before. Merchants and consumers can pick what they like best.

Not having to pay merchant fees enables merchants who accept Bitcoin to pass the savings on to their customers. That is the business model of the Bitcoin Store, which sells thousands of consumer electronics at discounted prices and only accepts bitcoins. In this way, Bitcoin provides more low-cost options to bargain hunters and small businesses, without removing the option to use traditional credit card services that some consumers prefer [12, pp. 10–12].

---

13 https://squareup.com/
Micropayments

Lastly, because transaction fees are fixed at a very low price (less than $0.05 at current BTC levels) Bitcoin generates huge cost savings for large transactions and at the same time makes micropayments (transactions under $5) affordable [77, p. 25].

Micropayments have been touted as one of the main use cases for Bitcoin. The reason is that in today's financial system, transactions below $5 paid by credit card are uneconomical and fees for transactions below $1 are prohibitive. If, for example, a customer pays $0.99 for a song on iTunes and the credit card company charges Apple $0.20 as a fixed fee plus a %-fee on top, the fee paid by the merchant is over 20%. This is the reason why there are fees around 30% for in-app purchases on Android or Facebook for example. Many business models based on micropayments are simply not viable.

With fees close to zero, and near infinite divisibility, Bitcoin can change that. For example, in the area of content monetization. One reason media businesses such as newspapers struggle to charge for content is because they need to charge either all (i.e. pay the entire subscription fee for all the content) or nothing by selling ads, resulting in banners and pop-ups that annoy customers. With Bitcoin it becomes economically viable for businesses to charge tiny amounts. Now it's possible for consumers to pay a few cents to finish a WSJ article without having to buy a subscription, or to pay for Wi-Fi by the second on the go if you just want to check your Emails. The possibilities are endless.

Another potential use of Bitcoin micropayments is to fight spam. Future Email systems and social networks could refuse to accept incoming messages unless they came with a very small amount of bitcoins. Small enough so they don't matter to the sender, but large enough to deter spammers, who at present can send billions of spam messages for free.

There are many more benefits and possibilities that arise from Bitcoin, such as a strong stimulus for financial innovation and the possibility to fight poverty and oppression all around the globe. The uses go far beyond payments. A bitcoin can simply be thought of as a piece of space in the ledger that is owned by someone. That someone can keep that space or transfer ownership to someone else. This space can also be ‘colored’ to give meaning to its content. At the moment it's just a USD number, but that really is the price for the empty space that people are willing to pay. Soon, there may be something to put into that space, for example shares and other documents of ownership, or contracts [26]. Use cases will then include transfer of property, execution of contracts, identity management, issuing stocks or bonds, or electronic voting. The interested reader might want to look at these resources and the references therein: [12], [78], [79].

3.4.2 Challenges

Despite all the benefits to Bitcoin, it is not without its flaws. New users may not properly secure or lose their private keys, price fluctuations can cause hefty losses for those holding bitcoins for an extended period of time, and hackers and criminals undermine security and confidence. Thus, for Bitcoin to become mainstream and get accepted by the masses, several challenges
have to be met. The most urgent ones required to raise trust and confidence in the system are around price volatility, security, and criminal uses.

**Volatility**

Bitcoin has had several significant price adjustments since 2011 (see Figure 4). These adjustments are common in financial markets which are prone to speculative bubbles: overoptimistic media coverage of Bitcoin leads to waves of inexperienced investors jumping into the fray and drive up prices. The frenzy reaches a tipping point where the bubble bursts and the price plummets. Newcomer investors that are eager to get in run the risk of overvaluing the currency and losing their money in a crash. Bitcoin’s price fluctuations make many observers weary of the currency’s stability. But while some believe this is the reason why Bitcoin cannot succeed [80], others, including the author of this thesis, believe that these fluctuations will decrease in frequency and amplitude over time, just as they did with many of the former tech startups that are now household names, as mechanisms develop that counteract volatility.

But, volatility causes the most concern for those who view Bitcoin as a store of value or a unit of account. And that is understandable. It does not make sense to keep books and balance sheets in such a highly fluctuating currency, and neither do long term investments. At least not at this stage, where not only price stability, but the very existence of the currency are uncertain. If used exclusively as a medium of exchange, however, volatility is less of a problem. The price risk can be mitigated to a great extent by quoting goods in traditional currencies and adjust the BTC-equivalent, and immediately selling the bitcoins for fiat upon receipt. This service has been offered to merchants through BitPay and more recently in combination with Coinbase through a plugin on merchant sites similar to PayPal’s. And customers don’t care about the USD/BTC price. They simply care about a better USD price, made possible because of lower transaction costs. This is why Bitcoin adoption has been strongest among merchants [12].

Better user interfaces and apps make first time use and onboarding of new customers simpler, lowering barriers for adoption. It is conceivable that the price of bitcoins stabilizes as more people become familiar with the technology, increase market volume and thus liquidity, and develop more realistic expectations about its future. In addition, because Bitcoin is outside the traditional financial system, bankers and central banks currently don’t have an easy way, or a mandate, to intervene and stabilize the currency. Future regulation may make this a real possibility.

**Security Breaches and Fraud**

As a cryptocurrency, Bitcoin presents some specific security challenges around private keys. If people are not careful, they can accidentally delete or misplace their bitcoins. Once the digital file is lost, the money is lost, just as with paper cash. If people do not protect their private keys, they are vulnerable to theft and hacking. Bitcoin wallets can be protected by encryption, but users often must actively choose to enable that option. If a user does not encrypt his or her
wallet, bitcoins could be stolen through malware. Also, if there is no backup copy in digital or even paper form, an irrecoverable computer crash or a spilled cup of coffee could make the bitcoins inaccessible for anyone, forever.

Bitcoin exchanges have struggled with security, too. Since most new users now use web wallets to store their bitcoins, this is the main area for concern at the moment. There have been cases reported in the past. Hackers successfully stole 24,000 bitcoins from a Bitcoin exchange called Bitfloor in 2012 and mounted a massive series of distributed denial-of-service (DDoS) attacks against the most popular Bitcoin exchange at the time, Mt.Gox, in 2013. Bitfloor eventually repaid the stolen funds to its customers, and Mt.Gox ultimately recovered from the DDoS attacks [12]. However, those were just portents of what was to come. On February 7th, 2014 the mighty Mt.Gox halted trading in all customer accounts amidst a series of what was initially claimed to be technical issues. The BTC price plummeted to below $100 at one point before recovering. Communication from the exchange and its CEO, Mark Karpeles, over the coming days was highly unprofessional, only saying that the problem is being worked on, and refusing to speak in public, raising concerns in the Bitcoin community that there was much more to it. A week later, Karpeles resigned from the Bitcoin Foundation's board of directors and deleted all of Mt.Gox's tweets from its Twitter account. The U.S. Attorney's office was alerted to the possible theft of about $400 million from the Bitcoin exchange, which resulted in the issuance of a subpoena and investigation in Japan. Then, on February 28th, Mt.Gox filed for bankruptcy, claiming they had lost 750,000 bitcoins, worth nearly half a billion dollars, in a possible theft [81].

Of course, many of the security risks facing Bitcoin are similar to those facing traditional currencies. Dollar bills can be destroyed or lost, personal financial information can be stolen and used by criminals, and banks can be robbed or targeted by DDoS attacks. Bitcoin users should take care to learn about and prepare for security concerns just as they currently do for other financial activities. Even scandals on the scale of Mt.Gox are not unheard of. Banks have been fined billions of dollars for money laundering and doing business with countries on the list of nations suspected of financing terrorists [82]. And of course there was the collapse of LTCM in 1998, a Connecticut-based hedge fund with two Nobel laureates in its ranks, destroying billions of dollars worth of investors' money [83].

**Criminal Uses**

Because Bitcoin is pseudonymous, it is possible for criminals to use it to launder money and to get paid in bitcoins for illicit goods and services. Just like cash, it can be used for both, legal and illegal uses.

One example is the infamous black-market site Silk Road, which since has shut down [39]. Silk Road was used as a marketplace where one could mail-order drugs and other legal and illegal goods. Although the exchange of goods that resulted from fraud or harm was apparently prohibited by the site's administrators, like stolen credit cards or photographs of child exploitation, other illegal products like forged IDs and drugs could be traded with impunity. The pseudonymous nature of Bitcoin allows people to purchase illegal wares online in the same way
that cash has been used for the same purpose in face-to-face transactions for a long time. At one point, the market had a volume of over $770 million in transactions in one month.

Another concern is the use of Bitcoin for laundering money and financing terrorism. Although there is currently no proof that this is going on, the technology is certainly capable to do so. Case in point is Liberty Reserve, a private but centralized digital-currency service that was based in Costa Rica and has been shut down by authorities on charges of money laundering [84].

These cases tarnished the reputation of Bitcoin, which in the public eye got branded as a tool for criminals and techno-anarchists to pursue their illegal activities or subvert the government. But that is not the case. While Liberty Reserve and Bitcoin have similarities because they both provide digital currencies, there are important differences. Liberty Reserve was a centralized currency created and owned by a company, for the apparent purpose of facilitating money laundering. Bitcoin is not. Transactions in Liberty reserve were not at all transparent. In fact, users were promised total anonymity. While Bitcoin is often associated with anonymity, it really is an open decentralized currency with a public ledger. So, while the real identities of criminals may stay hidden, their transaction records are available for everyone to see, including law enforcement, without needing a subpoena. In addition, the new players such as exchanges that are coming on the Bitcoin platform, now generally comply with the applicable financial regulation such as BSA and state licensing [12].

As noted before, many of the downsides of Bitcoin are the same as that of traditional cash, which had historically been the medium of choice for criminals. But nobody would think of banning cash. What should be comforting to all Bitcoin skeptics is the reaction of the community in such instances, for example in the case of Mt.Gox. On February 24th, amidst all the turmoil, a joint statement (see Figure 13) was given by Bitcoin ecosystem leaders including the founders of Bitcoin's most successful exchange, Coinbase, Blockchain.info's CEO Nicolas Cary, and Jeremy Allaire, CEO of Circle Financial. In their statement they condemned the "... tragic violation of the trust of users of Mt.Gox ..." and the fallout the collapse has brought on the Bitcoin community and reassured that the community at large is trustworthy and is working together to wash out bad actors, maintain the highest levels of security, and protect its customers. If regulators also view Bitcoin from that perspective and stay away from overregulation, the odds that the Bitcoin community will meet its challenges are indeed promising.
Joint Statement Regarding Mt.Gox

Feb 24th, 2014

The purpose of this document is to summarize a joint statement to the Bitcoin community regarding Mt.Gox.

This tragic violation of the trust of users of Mt.Gox was the result of one company's actions and does not reflect the resilience or value of bitcoin and the digital currency industry. There are hundreds of trustworthy and responsible companies involved in bitcoin. These companies will continue to build the future of money by making bitcoin more secure and easy to use for consumers and merchants. As with any new industry, there are certain bad actors that need to be weeded out, and that is what we are seeing today. Mtgox has confirmed its issues in private discussions with other members of the bitcoin community.

We are confident, however, that strong Bitcoin companies, led by highly competent teams and backed by credible investors, will continue to thrive, and to fulfill the promise that bitcoin offers as the future of payment in the Internet age.

In order to re-establish the trust squandered by the failings of Mt. Gox, responsible bitcoin exchanges are working together and are committed to the future of bitcoin and the security of all customer funds. As part of the effort to re-assure customers, the following services will be coordinating efforts over the coming days to publicly reassure customers and the general public that all funds continue to be held in a safe and secure manner: Coinbase, Kraken, BitStamp, Circle, and BTC China.

We strongly believe in transparent, thoughtful, and comprehensive consumer protection measures. We pledge to lead the way.

Bitcoin operators, whether they be exchanges, wallet services or payment providers, play a critical custodial role over the bitcoin they hold as assets for their customers. Acting as a custodian should require a high-bar, including appropriate security safeguards that are independently audited and tested on a regular basis, adequate balance sheets and reserves as commercial entities, transparent and accountable customer disclosures, and clear policies to not use customer assets for proprietary trading or for margin loans in leveraged trading.

3.4.3 Value

The opinions about the value of Bitcoin, how high it is and if it has any at all, differ widely. Some prominent figures in finance have strongly negative views on that issue. Alan Greenspan thinks that "Money is worth something either because it has intrinsic value, like Silver or Gold, or because it is backed by someone or an institution with great credit standing. There doesn't seem to be any intrinsic value in Bitcoin, and it is not backed by anyone, so the current price has to be a bubble" [86]. Nouriel Roubini thinks that Bitcoin is a 'Ponzi Game': "Bitcoin is not a currency as it is not a unit of account or a means of payments or store of value" [87]. And Paul Krugman is "... still deeply unconvinced. To be successful, money must be both a medium of
exchange and a reasonably stable store of value. And it remains completely unclear why Bitcoin should be a stable store of value" [88]. Further arguments against Bitcoin are brought forward by the banking community and governments. Their main point of contention, aside from Bitcoin not being able to function as money, is its potential for use in illegal activities such as money laundering and drug trafficking due to its anonymous character. However, these arguments are weak, as they can easily be brought against any currency. Transactions done in cash are completely untraceable unless the actors leave a trail somewhere else. In fact, Bitcoin offers a higher level of security, since all transactions are recorded [89].

On the other hand, there are many positive opinions, and not just from inside the Bitcoin ecosystem: Simon Johnson, professor at MIT Sloan, thinks that "Bitcoin definitely addresses a need ... The payments industry is ready to be disrupted" [90]. And even Ben Bernanke, the former chairman of the U.S. Federal Reserve, is cautiously optimistic saying that virtual currencies " ... may hold long-term promise, particularly if the innovations promote a faster, more secure and more efficient payment system" [91].

Of course, the strongest proponents of Bitcoin are the leaders in the ecosystem. According to libertarian and early Bitcoin entrepreneur Erik Voorhees, anything that is useful and scarce has a value. If it is not scarce, air for example, then it has no value. If it is scarce but not useful, such as a fish with three eyes, then it has no value either. Bitcoin is two things: the network (Bitcoin) and a currency (bitcoins). The currency in itself may not be worth anything as it has no utility yet. But the network is worth a lot. It is a revolutionary protocol to transfer not just money but information in general, and network effects make it hard to switch to a new system that uses the same open source code. Thus, since the Bitcoin network has value and bitcoins are the only medium allowed on the network, and they are scarce, they must have value, too [92]. Bitcoin is neither a fiat currency that has value because it is backed by a government, nor is it a specie currency that can be converted into something precious like silver or gold. According to Gavin Andresen, board member of the Bitcoin Foundation and lead developer for the Bitcoin digital currency project, it has value much like any useful tool has a value [37]. And Jeremy Allaire believes that " ... global digital currency represents one of the most important technical and economic innovations of our time. Specifically, digital currency introduces advancements in electronic payments and money transfers, potentially materially lowering costs for businesses around the world, decreasing fraud risk for consumers and merchants, increasing consumer privacy and protection, and expanding the market for consumer financial products on a worldwide basis" [93]. Marc Andreessen, serial entrepreneur and co-founder of venture capital firm Andreessen Horowitz, who invested over $50 million in Bitcoin-related startups, describes the discussion around value and price as a chicken-and-egg problem: "It’s not as much that the Bitcoin currency has some arbitrary value and then people are trading with it; it’s more that people can trade with Bitcoin (anywhere, everywhere, with no fraud and no or very low fees) and as a result it has value" [26]. He argues that, although it was speculation that has driven up the price, it is actually that sufficiently high price for the currency that made payments possible in the first place, because now it can be used to transport meaningful volumes of fiat-currency through the network.

Amazingly, Nobel laureate Milton Friedman already predicted some form of virtual currency in 1999:
"The one thing that's missing, but that will soon be developed, is a reliable e-cash. A method whereby on the internet you can transfer funds from A to B, without A knowing B or B knowing A. The way in which I can take a 20 dollar bill and hand it over to you and there's no record of where it came from. And you may get that without knowing who I am" [94].

As noted earlier, Bitcoin is a currency, a protocol, and a platform. It is interesting to see that the two camps in this discourse focus on different aspects of Bitcoin. Its critics focus on Bitcoin's ability— or lack thereof—to function as money, whereas its proponents focus on its utility as a protocol and platform. The latter is also the focus of the evaluation of Bitcoin in chapter 4.

Several financial analysts have gone further and attempted to estimate the fair value of a bitcoin. Because Bitcoin is a payment network and a currency, calculations can take into account a multitude of variables, and results are heavily influenced by the assumptions made for the relevance (weights) of these factors and their distribution (possible values and likelihood of occurrence). An analysis by David Woo of Bank of America Merrill Lynch arrived at a fair value for a bitcoin of about $1,300, assuming a potential market capitalization of $15 billion based on Bitcoin becoming a major player in e-commerce and money transfer, and an accepted store of value [95]. An analysis by Wedbush Securities identified scenarios under which the price of a bitcoin could reach $10,000 or even $100,000, depending on the market share Bitcoin could achieve in the payments industry [96]. Yet another analysis even sees a bitcoin valued at $400,000 if the currency would be worth all of the world's gold ($8 trillion / 21 million bitcoins) [97]. Since bitcoins are divisible to eight decimal places, called a Satoshi, even if one Bitcoin were worth $1,000,000 one could still pay for items priced to the cent.

In contrast to intrinsic value, prices in a free market economy are driven by supply and demand, which again are influenced by many variables. Intrinsic value as described above is one of them, but there are others such as taxation, regulation, speculation and psychology. The price of Bitcoin is heavily influenced by demand fluctuations, because its total supply is deterministic and its market capitalization is small. Because Bitcoin is subject to heavy speculation based on short term sentiment by a growing number of investors who simply want to make a quick profit, news can lead to great buying or selling pressure, leading to large price swings [80][24].

The success of Bitcoin depends on how soon and by how much its volatility will decrease, especially for its function as a currency but also for its function as a technology, because volatility deters both, users of and investors in the Bitcoin ecosystem [37][80]. Since volatility depends on demand fluctuations relative to supply, it in turn will depend on its level of stable long-term adoption that is driven by a decrease in risk factors such as regulation and security, and a lowering of barriers of entry for users.

3.5 Ecosystem

Bitcoin is a foundation technology that is used beyond a single firm, brings multiple parties together for a common purpose, and whose value increases exponentially with more
complementary products and services and more users. Thus, according to Cusumano, Bitcoin is an industry platform [98, p. 24].

The actors in the ecosystem fall into six primary groups [79]:

- Miners
- Complementors
- The Bitcoin Foundation
- Consumers
- Merchants
- Policymakers and Regulators

Following Crawley's framework introduced in section 2.2, the ecosystem includes not only the providers of products and services that develop and influence the Bitcoin architecture (leaders and complementors), but also upstream and downstream stakeholders such as regulators and users. Figure 14 illustrates how they can be categorized into the different stakeholder groups.

**Figure 14: Stakeholders in the Bitcoin Ecosystem**

Miners

Miners are arguably the most important actors in the ecosystem. They create bitcoins, put them into circulation by selling bitcoins or spending them, and maintain the network and the block chain. Miners get rewarded for their work through bitcoins upon successfully mining a block, and through transaction fees paid by the rest of the users on the network, as explained in detail in section 3.2.2.

Theoretically, anyone can mine bitcoins by running the software on their computer. However, computing power on the network has become so high that, in order to have a meaningful statistical chance to mine a block, significant investments would have to be made to compete with large miners who spend millions of dollars on equipment specifically designed for bitcoin.
mining (ASICs\textsuperscript{14}), or with mining pools, which are networks of thousands of computers collaboratively working together and who share the mining rewards [49]. Mining pools can also be dangerous. With the vast power concentrated in their pools, they could take over the network and launch a 51%-attack.

Figure 15: Mining Pools [32]

A block, once hashed, cannot be changed, for example, by changing the details of a transaction inside it, and then hashed again to the same result. If a block cannot be changed, transactions in that block are confirmed ‘forever’ and the ledger is secured against tampering. Moreover, each block takes the hash of the previous block into account, so that in order to change a block that lies further in the past and have it validated, all subsequent blocks would have to be solved again, all the while the rest of the network continues mining new blocks. Thus, in order to change a past transaction, an attacker would have to race and overtake the rest of the network in building the longest chain, so that his chain will be accepted as the new truth. Because, on average, each attempt to solve the hash has the same probability, the probability of a slower attacker catching up diminishes exponentially as subsequent blocks are added. Thus, the

\textsuperscript{14} ASIC stands for application-specific integrated circuit
attacker would have to control more than 50% of the computing power on the network to have a chance better than 50:50, which is why this kind of attack is called a 51%-attack [99]. Because large mining pools such as BTC Guild have a high chance to generate several blocks in sequence, there is a chance the block chain can get compromised.

**Complementors**

The complementors on the platform are all the producers of goods and services around Bitcoin, namely exchanges, digital wallets, and payment service providers.

- **Exchanges** are service providers that allow users to buy or sell bitcoins in exchange either for fiat currency or for other virtual currencies. On some exchanges such as Coinbase, the company itself is the counterparty for the transaction, whereas on other exchanges such as bitcoin.de, the company is merely providing a market place for buyers and sellers to meet and the transaction is done directly between the two after they found each other through the price matching algorithm of the exchange. There is even a nascent market for derivatives. They can, for example, be traded on ICBIT and Predictious [100]. An example for derivatives and more widely financial innovation is the Winkelvoss ETF [101]. Even ATMs are now available in a few locations in the U.S. and around the world [102].

- **Payment Service Providers** such as BitPay [103] provide products in the form of plug-ins that merchants can integrate into their websites. These plug-ins allow merchants to accept and customers to pay with bitcoins as easily as with a credit card or PayPal, if they already own bitcoins. There is currently a great push towards making it easier for customers who don’t already own bitcoins and thus have no Bitcoin address or wallet, to make instant payments. An example for that is the payment URL technology by Coinbase, which redirects customers from the merchant website to Coinbase where they buy bitcoins in the exact amount required upon which Coinbase immediately sends those to the merchant wallet [104]. Generally, BitPay immediately exchanges the merchant’s bitcoins into fiat upon receipt, because for the time being most merchants don’t like to hold bitcoins while the currency is still highly volatile and would expose their revenues to unnecessary risk. Even PayPal, an incumbent payments processor from the pre-Bitcoin era is looking to accept bitcoins when regulatory uncertainties and price volatility have sufficiently subsided [105]. This exemplifies the fact that Bitcoin has reached a stage where the boundaries between old and new world start to blur. Incumbents are adopting the new technology, either as partners with or competitors to new Bitcoin companies.

- **Wallets** are products and services that store the public and private keys associated with bitcoins. Online wallets are software running on a desktop, mobile device, or the web, whereas offline wallets are not connected to the Internet and comprise digital hardware wallets such as USB sticks or in the simplest form a piece of paper [106].
The Bitcoin Foundation

The Bitcoin Foundation is made up of all the important complementors within the Bitcoin ecosystem such as Coinbase and Circle, and more than a thousand individual Bitcoin advocates (including the author of this thesis). It is open to anyone who would like to join. It sometimes gets confused with being "The Bitcoin Company", which it is not. Bitcoin is open source, it belongs to nobody and everybody. Rather, the Foundation’s mission is to help people exchange resources and ideas more freely, and its goal is to be an organizing body for Bitcoin to advance Bitcoin standards and security. This mainly translates into being a marketing channel for the Bitcoin community. In the first months of 2014, two of the founding board members resigned amidst scandals and huge losses for many Bitcoin users. Charles Schrem was arrested on charges of money laundering in relation to Silk Road [107] and Mark Karpeles had to resign in the wake of the previously mentioned fall of Mt.Gox.

Consumers

According to a Bizrate Insights survey of more than 7,000 online buyers, less than 1% have both heard of and used bitcoins (see Figure 16). They are roughly equally split between genders, on average younger than 45 years old, and they have a household income of less than $75,000. Consumers can buy bitcoins on an online exchange such as Coinbase, by linking to a bank or payment card account. Bitcoins can also be purchased with cash at Bitcoin ATMs and face-to-face in paper form (the keys are actually printed on the paper). To pay with bitcoins at a merchant’s website they simply select Bitcoin at the checkout when available. It will appear as another payment option besides, for example, credit cards or PayPal. Bitcoin payments can also be made via QR code, which is presented on the screen by the merchant or receiver of the funds, and which the sender can scan with his mobile device. The price the consumer pays in bitcoins is based on the exchange rate to the merchant's native currency at the time of the transaction. The consumer bears all of the volatility risk as the exchange rate fluctuates, whereas the merchant uses provider like BitPay to immediately exchange the bitcoins back to their native currency [79].

Merchants

There are currently over 4,000 websites and retailers that accept bitcoins for goods and services around the globe (see Figure 17). The largest and most notable is Overstock.com. Other notable merchants include Chicago Sun-Times, Fancy, Foodler, Gyft, Khan Academy, Newsweek, Reddit, the Sacramento Kings, Scan Computers International, TigerDirect, Tesla, and Zynga.
Policymakers and Regulators

As discussed in section 2.3, Bitcoin has attracted the attention of policymakers and regulators. As high leverage stakeholders, they will shape the future of Bitcoin as much as the complementors, especially if the platform is to cross the chasm into the mainstream and reach mainstream adoption. Luckily, many of the main Bitcoin advocates, like Circle's Jeremy Allaire, have learned from past experiments in virtual currencies and disruptive technologies like Napster, and are looking to work in close cooperation with regulators. It is the right way to go in order to separate illegal activity and fraudsters in the ecosystem from the majority who wants to build legitimate businesses on the platform.

Note on Platform Leadership

Cusumano defines platform leaders as "... companies that drive industrywide innovation for an evolving system of separately developed pieces of technology ..." and complementors as "...
companies that make ancillary products that expand the platform's market" [108]. It is too soon to declare a winner in the race for platform leadership in this ecosystem, but there are a few likely contenders. While some of the Bitcoin companies are clearly less suited to become leaders, for example, because they occupy niches such as producing hardware wallets, others look much more promising. It is companies like Circle or Coinbase who have the potential to influence the direction of the entire Bitcoin platform and the ecosystem, because they build products and services for mass adoption, with the goal for Bitcoin to cross the chasm into the mainstream. They aren't the first movers. Many Bitcoin projects came before. But that is all they were – projects that were never meant to become global corporations. The new generation of leaders are experienced entrepreneurs who take management and accountability seriously, and who have a proven track record of building billion dollar businesses with hundreds of millions of customers. And, crucially, they are vocal supporters of cooperation with regulators and policymakers, because they identified them correctly as high leverage stakeholders who have the power to either squash Bitcoin, or to support and strengthen the ecosystem with consumer-friendly regulation without stifling innovation.

Figure 17: Merchants Accepting Bitcoin [109]

4 Bitcoin as a Platform for International Payments

Based on the understanding gained in the previous chapter of how Bitcoin works, what its properties, uses, and challenges are, and what products and services are being offered and developed on the platform, this chapter will analyze its suitability for international payments.

The question will be approached with two frameworks. The first is an analysis of how well Bitcoin meets the needs of customers compared to the current electronic payment
instruments. The second will investigate if the international payments industry is a WTAoM market and assess Bitcoin's potential for success in it.

4.1 Customer Needs Analysis

This section discusses how well Bitcoin's attributes meet the needs of the primary beneficiary – the customer – represented by Blockley and McDowell's [10] 6 Cs that drive consumer choice in payments (see Table 3). Since the goal is to get an understanding of Bitcoin's potential to succeed in the competitive international payments industry, the analysis will be done in the context of the current EPls selected for this thesis: wire transfer, credit and debit cards, and online EPIs.

Table 3: The 6 Cs That Drive Consumer Choice in Payments [10]

<table>
<thead>
<tr>
<th>Capability</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Capability</td>
<td>Describes the functional ability to actually undertake a payment. Some new capabilities add value by changing or shortening channels or payment supply chains. This type of innovation can provide a way of entry for new participants, thereby challenging the role of traditional suppliers and intermediaries. PayPal, for example, is a mediating service facilitating person-to-person transfers without the seller having to register as a merchant, which challenges the traditional credit card players.</td>
</tr>
<tr>
<td>Cost</td>
<td>Describes the cost of the payments system to customers such as fixed or proportional transaction charges. Cost would normally be viewed as a strong driver of change. The impact of cost on payment choice, however, is a complex matter. The issue is complicated by consumer expectations and the fact that in most cases the marginal cost to the consumer of making a payment is zero.</td>
</tr>
<tr>
<td>Convenience</td>
<td>Describes how easy a payments method is to use, for example, the need for registration or the speed of payment. Consumers' expectations in terms of speed, real-time, electronic channels, etc. are constantly increasing, especially among the younger generation.</td>
</tr>
<tr>
<td>Coverage</td>
<td>Describes how widely a payments system is accepted by merchants and other recipients of payments. The increase in access to the Internet is also associated with an increase in the use of electronic commerce. Expanding coverage for consumers by making electronic payment options available in the real, as opposed to on-line, world often involves a major investment in systems.</td>
</tr>
<tr>
<td>Confidence</td>
<td>Describes a customer's belief that a payment will be successfully executed and completed, and that the value of a payments method will be respected. Providers of new, innovative payment systems need to convince consumers that their products or channels will operate as expected, and give confidence that the payment will 'go through'.</td>
</tr>
<tr>
<td>Confidentiality</td>
<td>Describes the integrity of the payment system in maintaining the privacy of customer information. Providers of new, innovative payment systems face a challenge to convince customers that their products or channels are trustworthy and secure, although new methods/systems that provide consumers with greater security, actual or perceived, of their confidential/personal information have attraction.</td>
</tr>
</tbody>
</table>
4.1.1 Capability

Bitcoin's ecosystem is still in its infancy, yet already rich in functionality. There are desktop, online, and mobile wallets to store, send, and receive bitcoins, exchanges and ATMs to buy or sell bitcoins for fiat currency, and over 4000 businesses that accept bitcoins. That alone is sufficient for international payments to function satisfactorily and to put Bitcoin at par with most EPIs. While wire transfers are suitable only for money transfers and credit and debit cards for purchases, only some online EPIs such as PayPal have bridged the gap. A payer can send money from his PayPal account to a payee anywhere in the world, and the same account can be used to buy goods online wherever PayPal is accepted. In addition, there are Bitcoin exchanges that offer a full range of trading features such as orders, limits, and even derivatives. Since the ledger is public, there are applications that provide real-time bookkeeping of a user's transactions and trading signals based on current buy or sell volumes and prices. As discussed in detail in chapter 3, because Bitcoin is an open source, decentralized, and distributed peer-to-peer network with virtually instant and free transactions, this platform offers innovation capabilities ranging from micropayments which now become a viable business model, to multi-signature contracts and smart money, and functionality that has not even been conceived. Bitcoin's potential capabilities are therefore far greater than those of current EPIs.

The advantage of current EPIs from a consumer perspective are credit and recourse. This does not mean that Bitcoin could not support credit functionality, which would probably be modeled as an input into the Bitcoin address from a Bitcoin lender, thus increasing the funds available. However, in its current form the Bitcoin ecosystem does not provide this capability, so credit cards and overdraft lines are the preferred choice in that respect. Recourse is by design not an attribute of Bitcoin. Transactions are supposed to be irreversible. However, since it is evident that consumer protection is an essential requirement for Bitcoin to become mainstream, it is conceivable that a multi-signature protocol will be developed on top of Bitcoin that would allow a third party such as Amazon or Coinbase to initiate a transaction that is equal but opposite to the initial BTC transfer from buyer to seller in case of a dispute. Such a recourse protocol would also include an expiration date after which this type of chargeback would no longer be possible and the transaction is final.

4.1.2 Cost

Because of the absence of a central monetary authority, of payment processors, and of trusted third parties that would introduce direct and indirect costs into the system, the use of Bitcoin is virtually free. The main costs incurred are for the exchange between fiat currency and bitcoins. Coinbase, for example, charges 1% plus $0.15 for the exchange between BTC and USD (for merchants, the first $1 million worth of BTC cashed out to USD are free). However, the cost structure will probably deteriorate as mining becomes less profitable and miners will start charging higher transaction fees (currently 0.0005 to 0.0001 BTC per transaction) [110], and as dominant players in the Bitcoin ecosystem emerge who will be able to charge a premium for their services. We can already witness a trade-off between the transaction fee a user pays to miners and the priority his transaction has for inclusion into the block. The higher the fees, the
higher the priority, speeding up confirmation of the transaction. This is the same model used by money transmitters and banks and in other time-sensitive markets such as the postal service.

By comparison, banks charge around $25 for international wire transfers, often on both sides of the transaction, plus a currency conversion fee of around 2.5%, so that even transfers of $1,000 cost more than 5% [111]. Smaller transactions become increasingly uneconomical. Money transmitters such as Western Union often charge even higher rates in return for better coverage, especially in the under banked regions of the world [112], [113]. For purchases, credit card transactions are more cost efficient. The consumer only pays around 2.5% for the currency conversion. However, the merchant has to pay an additional fee of 2% to 3% to the card issuer. To attract more business, merchants like the Bitcoin Store often pass on part of their savings to customers through lower prices if the goods are paid for with Bitcoin instead of credit cards by those who prefer a bargain over consumer protection [12, p. 14]. Even with PayPal the total cost is between 3% and 6% including currency conversion fees depending on location, size of the transaction, and if it is a personal transfer between individuals or a payment to a merchant. Furthermore, the $0.30 minimum fee makes micropayments under $1.00 prohibitive [114].

If the demand for payments through Bitcoin keeps rising, its volume will reach a market share that is significant enough for providers of current EPIs to experience a noticeable decline in revenues. At that point they will have to reduce their fees in order to stay competitive. In fact, the author predicts a convergence of fees between Bitcoin and current EPIs to the point where some EPI providers might charge less than Bitcoin companies, because they cannot compete in the other 5Cs.

A discussion of costs requires the inclusion of the bitcoin exchange rate. If demand grows, the price for bitcoins will rise because their supply is finite. However, the costs for individual transactions should not be affected, as an increase in the bitcoin price can easily be offset by a reduction in BTC units to reflect the same amount of fiat currency transferred. And since bitcoins are divisible at least to the eighth digit, this option remains independent of the BTC price level. However, volatility is currently so high that by the time it takes for a transaction to be processed and confirmed, including the exchange of the originating fiat currency into bitcoins and back out to the destination currency, price moves may have created a conversion loss, increasing the costs of the transaction.

4.1.3 Convenience

The transfer of bitcoins from one address to another requires only two pieces of data: the payee's Bitcoin address and the amount to be sent. This can easily be done from any desktop, web, or mobile wallet after login with a username and password. The destination address and amount are often provided to be copied and pasted into the Bitcoin client and can even be read from a website or a piece of paper with a QR reader, further simplifying the process. By comparison, international wire transfers require at least the recipient's name, account and routing number, and address of his financial institution and often a personal visit to the branch.

15 This number can be increased by a change in the Bitcoin software.
as many banks still don't provide this service online. Credit and debit card transactions are also more cumbersome than Bitcoin, requiring the entry of long and arbitrary card numbers, expiration dates, the security code and further details such as the cardholder's name and address [10]. PayPal on the other hand offers similar levels of convenience to Bitcoin, requiring only a username and password to login, the amount to be sent, and the Email address of the recipient.

The actual time for bitcoins to change hands can be measured in seconds, and it takes an average of only ten minutes for a transaction to be confirmed on the blockchain. Nevertheless, critics regularly point out that, while the actual transfer of bitcoins may be easy and fast, the setting up of a wallet and the acquisition of bitcoins is a cumbersome technical process that can take a week to accomplish. Thus, so the argument goes, Bitcoin is unsuitable for mainstream use and will remain confined to the domain of technophiles where it came from. It is true that the installation especially of some desktop wallets and the necessary research that comes beforehand take some time. The research in particular is important, because unlike checking accounts which basically all behave the same way with respect to storing and transferring funds and which differentiate themselves only in some terms and conditions such as overdraft lines or fees, Bitcoin wallets can behave very differently. Bitcoin Core, for example, a heavy desktop wallet, first needs to download and verify the complete blockchain before it is operational. Because the blockchain has grown to more than 16 GB in size, having doubled within the past 12 months [32], this process alone can take over 24 hours and will continue to take even longer going forward. In addition, a wallet can contain multiple addresses and it is common practice to use a different address for every transaction. Furthermore, each address within each wallet should have a password associated with it, apart from the unique private key that comes with each address, to avoid the loss of funds if the desktop gets lost or stolen. MultiBit on the other hand is a lightweight wallet which requires very little setting up, but is considered less secure and has fewer features. It simply listens to the network and reads the blockchain, whereas Bitcoin Core acts as a node, checking and relaying transactions and thus actively protecting the network [23]. Convenience, capability, and confidentiality have to be weighed against each other, requiring technical knowledge that exceeds the average user's abilities. Likewise, the argument that it takes several days to exchange fiat to bitcoins is valid, if only partially. Until recently, there have been two main ways to acquire bitcoins, other than mining. One is the face-to-face purchase of bitcoins for cash (or check if anonymity was not an issue), with websites such as LocalBitcoins.com acting as personal ad platforms similar to Craigslist where buyers or sellers could express their interest and preferred meeting location. The other alternative is an online exchange where the user opens an account and funds it with fiat currency via direct debit or credit or a card, and subsequently purchases bitcoins. The first option can take hours or days and is not scalable because the supply of bitcoins in any location constantly fluctuates with sellers running out of bitcoins or changing their minds from sell to hold if their expectations about future prices change. The second option takes about a week to complete due to account verification procedures implemented to satisfy regulatory requirements.

Fortunately, this issue has been identified as one of the main barriers to entry for new users by the community and great efforts are under way to solve this problem, with millions of dollars
being poured into Bitcoin startups addressing many of the shortcomings of the existing ecosystem [26], [115]. One solution are Bitcoin ATMs such as the ones from Liberty Teller or Robocoin that have become available in late 2013 and which allow the purchase of bitcoins with cash in less than a minute. Another one is a streamlining of the account verification and funding process, a project that is worked on by companies such as Coinbase and Circle.

The current EPIs by comparison either require a bank account to be set up or a credit card applied for and approved, or cash physically handed to a money transfer business, before a payment can occur. All of these options can be done within a matter of hours. The actual cross-border transfer on the other hand generally takes several business days for wires, with the option to pay a premium for faster transfer. Purchases with cards are instant, as are transfers within PayPal. However, the cashing out of a PayPal balance to a bank account can take several business days. Thus, while instant transfers are often touted as one of Bitcoin's strengths, it is important to note that there are many other payment instruments providing that particular kind of convenience, albeit at a higher cost.

4.1.4 Coverage

Anyone can send bitcoins from anywhere to anywhere just as they are able to send Email. And with ATMs as a recent addition to the ecosystem, Bitcoin has the potential for ubiquity that is not offered by any of the existing payment options. Many banks still don't allow international payments over the phone or online, let alone from an ATM. With Bitcoin on the other hand, it is possible to buy bitcoins at an ATM with cash and immediately send them to any address. Due to its decentralized and distributed nature, Bitcoin does not know national or regulatory barriers. A Bitcoin address is not linked to an account with a bank that resides in a specific country under a specific jurisdiction. Granted, there are only very few Bitcoin ATMs installed to date. But the machines proliferate at an increasing speed with new locations opening almost daily all around the globe [116]. What further mitigates Bitcoin's current lack of extensive ATM coverage is the fact that the world continually moves away from cash towards electronic money and payment instruments, generally weakening the case for ATMs. However, for the time being, cash is an important payment instrument, and a big advantage of money transfer businesses such as Western Union is their global network of agents that provide cash payouts without ATMs or the need for a bank account.

Of course, what currently severely limits the usefulness of Bitcoin is the low number of merchants and individuals that accept bitcoins compared to fiat currency through any of the current EPIs. Even fewer want to hold bitcoins for any longer than is necessary for fear of drastic price moves. Adoption is one of the big challenges ahead, and it is being addressed. BitPay is a prime example, allowing online merchants to accept bitcoins and turn them instantly into fiat currency. Because this mechanism is cheaper than credit cards, merchants are incentivized to adopt Bitcoin. Moreover, early data from Overstock.com, an online merchant that recently started to accept bitcoins, show that the average purchase value is higher when paid for with bitcoins than with dollars and that more than half of the Bitcoin orders come from new customers. This could be an indication that the early Bitcoin adopters are more affluent
than the average customer and an attractive segment to pursue, thus supporting the case for Bitcoin adoption even more [76].

4.1.5 Confidence

For a transaction on Bitcoin to succeed, several conditions must be met. First, the transaction has to be valid. This includes conditions such as there having to be at least as many bitcoins in the wallet as there are to be sent. This is the mechanism at the heart of Bitcoin that avoids double spending. Second, the transaction has to get included in a block for it to be confirmed. Even if a transaction is valid it may get rejected, for example if there are more than one valid transaction racing to be confirmed, as was the case with the transaction malleability exploit, or if a miner decides not to include a transaction that pays too low a fee. Third, the transaction must be included in the longest chain. Even if it is confirmed in a mined block, there may be a longer chain that does not yet have this transaction confirmed. This is generally not a problem, but sometimes a fork on the chain continues to exist for hours our days, during which the transaction cannot be considered successful. In the worst case, a 51%-attack deliberately creates a longer chain than the current one and invalidates any number of previously confirmed transactions. The upside is that all these measures are in place to prevent abuse of the system. If a transaction is legitimate it will go through unless the system is being attacked. A risk that plagues current EPIs just as much, for example in the form of large scale DDoS attacks on banks [117].

A further concern with Bitcoin payments are rapid exchange rate fluctuations. As mentioned above under Cost, due to the current high BTC volatility, the parties to a transaction cannot be confident that the desired amount will arrive at the destination when bitcoins get converted back to fiat currency. This problem is more muted for international wire transfer and card transactions. Although settlement and fee notification can take days and the exact time of currency exchange is not published, the exchange rate risk is generally much smaller since most fiat currency pairs are far less volatile than USD/BTC. Some services such as PayPal or Western Union even provide instant conversion at a given rate, with no foreign exchange risk at all.

On the other hand, Bitcoin’s public ledger creates never before seen transparency. Anyone can lookup any transaction, including the input and output addresses and the amount of BTC sent. In combination with the irreversibility of transactions once included in the block chain and the fact that most transactions are confirmed within ten minutes, this creates a very high level of confidence that, once a transaction succeeds, the funds belong irreversibly to the payee without recourse or risk of seizure by a third party. With current EPIs the pros and cons are reversed. The vast majority of transactions goes through if there are sufficient funds and the required information such as account or PIN numbers has been provided correctly. But even if a transaction has gone through it can be reversed, especially when paid for with credit cards and the payer disputes the transaction. This is a boon for the consumer but a risk and a cost for the merchant.
4.1.6 Confidentiality

As with confidence, confidentiality is tightly linked to security, but under a different aspect. As discussed in section 3.3 the Bitcoin protocol is highly secure and protects identities due to its pseudonymous nature and against double spending. Yet, there have been many incidents of lost bitcoins. The Achilles' heel of Bitcoin are the wallets' private keys. Whoever holds one has full control over the associated bitcoins. Thus, most incidents involve lost or stolen private keys. While forgotten or lost keys or deleted wallets are painful, they don't involve criminal activities and are solely the responsibility of the owner. In that respect, Bitcoin is similar to cash. Once it is lost, the owner has no way of getting it back [53]. The bigger threat are stolen private keys, either from a user's device through malware or by hackers from a web wallet, as was the case in 2012 where hackers stole 24,000 BTC from an exchange [12, p. 19]. However, the financial industry is not free from such incidents either, such as the theft of credit card details in the infamous Target breach and similar cases where merchants stored but insufficiently secured sensitive financial customer data [118]. This type of attack is not possible with Bitcoin because it is a digital bearer instrument. Private keys or other sensitive information are not transmitted to the merchant [26].

A troubling issue that cannot be addressed through better IT security are the many Bitcoin companies that operate with little or no supervision from regulators or auditors. If their operators intend to defraud their own customers there is little in their way to stop them. The two most famous cases are Silk Road and Mt.Gox, which resulted in the loss of bitcoins worth hundreds of millions of dollars. After Silk Road and all its assets were initially seized by the FBI, a second site was quickly put up. Before long, that one also closed down, with the CEO blaming the loss of all bitcoins on an attack by hackers while discussions in relevant Bitcoin forums point to a likely case of fraud by the operators. Similarly, Mark Karpeles, the former CEO of Mt.Gox, blamed a flaw in the Bitcoin protocol and the malleability issue on the loss of most of the exchange's bitcoins. Criminal investigations are currently under way to shed light on the case, but insiders believe this is also a case of fraud. A related concern is that most exchanges now require proof of identity such as passport copies and utility bills. In combination with bank account details provided by customer to fund purchases and cash out sales of bitcoins, this information can be readily abused for identity theft, entirely undermining the pseudonymity that is one of Bitcoin's main strengths.

While the protocol itself is secure, the immaturity of the ecosystem with its many dubious operators and lack of regulation has Bitcoin at a disadvantage versus current EPIs. The existing financial system is currently much better equipped to deal with security breaches than Bitcoin. Banks can always reset forgotten account passwords. Funds aren't automatically lost. In case of security breaches or fraud and subsequent financial losses, customers often get reimbursed, at least partially. This form of consumer protection weighs strongly in favor of current EPIs and is the reason why some of the higher costs compared to Bitcoin are justified. On the bright side, many governments around the world, especially in the U.S. and in Europe, are currently working hard to put Bitcoin regulation and oversight in place. The hope is they will find a balance, creating enough confidence to drive adoption without stifling innovation.
4.1.7 Verdict

This thesis has argued that current electronic payment instruments don't sufficiently meet customer needs. That is the reason for continuous innovation in the industry. As discussed, Bitcoin is equal to and in many aspects already superior to existing payment instruments. There is still a lot of work to be done to drive up mainstream adoption, especially around volatility, trust, and regulation. But while current EPIs fulfill some needs better than others and present customers with a trade-off between cost, speed, and coverage, Bitcoin has the potential to unify all strengths under one network and protocol. It is therefore a highly suitable instrument for international payments.

Equipped with such advantages, can Bitcoin become a dominant platform in the international payments industry given the market's characteristics? The next section will try to answer this question.

4.2 WTAoM Analysis

"It is a vision that says the whole of the ecosystem can be greater than the sum of its parts, if firms work together and follow a leader" [119].

According to Cusumano [119] the fundamental attributes of a platform are interdependency and innovation. While the actors in the international payments process (financial institutions, central banks, and clearing houses) are highly interdependent, technological innovation has generally been rare, incremental, and confined to national or regional level. Part of the problem is that innovation often requires industry-wide coordination and government support, which can be difficult to achieve [10]. Only recently has there been a spur of innovation in the industry, often by non-bank technology startups, especially around mobile and P2P payments, and mostly on a national level. Nevertheless, the international payments industry is a platform market with dominant players like VISA and MasterCard in the cards segment or Western Union and MoneyGram for remittances.

Bitcoin is also a platform and the ecosystem around it is growing fast. New startups with innovative products and services mainly around payments are being announced almost on a daily basis. This section will analyze if the payments industry is a Winner Take All or Most market and if the Bitcoin ecosystem lends itself to spring a leader to dominate it.

A WTAoM market has to meet three criteria. Strong network effects should exist between the actors on the platform, there should be little differentiation between competing platforms, and multi-homing should be difficult. Following are the tests for these three requirements.

4.2.1 Network Effects: Strong

The payments industry exhibits strong network effects. Payers will only adopt a new form of payment if there are payees who will accept it, and merchants will only invest in a new payment technology if they benefit from customers using it. Both sides benefit from more users
joining the network. This is linked to the concept of coverage discussed in section 4.1 and is one explanation why innovation in the payments industry has been lagging. There has to be a critical mass of payers and payees to create enough benefit to outweigh the costs of developing and implementing a new technology. If there is only one counterparty or one case for which to use a new instrument, neither side has an incentive to incur the startup costs in terms of time and money associated with learning new payment mechanics, changing existing processes, and developing or purchasing the required technology, and the innovation will not get adopted. It therefore often takes considerable financial resources, industry-wide cooperation, and time for a new payment instrument to take hold \[16\].

Bitcoin exhibits even stronger network effects than existing payment platforms. The more businesses accept bitcoins, the more people will start using bitcoins to buy goods that are cheaper and easier to pay for, attracting ever more businesses. The same users will start sending money around the world to their friends and family, creating an incentive for businesses to accept bitcoins in those regions as well. This positive feedback loop is similar to that of Email or eBay. Bitcoin is actually a four-sided network. Besides merchants and consumers the other two relevant stakeholders are the miners who ensure the integrity of the network and developers and businesses who are building new products and services. This last group is especially valuable in creating a mote around Bitcoin, because thousands of bright and motivated developers are joining outstanding entrepreneurs with a background in the financial industry to innovate on top of the Bitcoin platform, making it increasingly difficult for competitive technologies to evolve and surpass Bitcoin's adoption. It is this group of complementors where a potential platform leader might arise from [26].

Of course, the network effects extend beyond the payments industry. Every use case for Bitcoin, current and potential, increases the user base, creating further network effects with the platform and increasing the value for everyone as new users that join for one use case are now connected and potential users of other products and services. For example, once multi-signature contracts become available, real-estate agents and home buyers and sellers may come onto the platform to sign contracts and transfer ownership of the property. Once they use Bitcoin they become potential users of the payments infrastructure as well.

Furthermore, because Bitcoin is open source, there are strong network effects between the core software and its complements like wallets and exchanges. If innovators of products and services find that what they want to build is not possible with the core Bitcoin protocol they write their own software on top of it. If the result is deemed a useful extension of Bitcoin's capabilities by the community it can get incorporated into a future release of Bitcoin. Similarly, if the current version of the software causes problems for users and producers, as was the case in the recent malleability exploit, the core protocol will be improved in a concerted effort by the community.

\[16\] BPAY, a global bill payment system, took about five years to reach critical mass in Australia. That is the same time it took from inception of Bitcoin until the end of 2013, "The Year of Bitcoin" with big advances in adoption, products, and regulation [120].
4.2.2 Differentiation: Currently High/Potentially Low

There is a high degree of differentiation between current payment instruments with regards to the 6Cs as discussed in detail in section 4.1. While most offer a general trade-off between cost and speed, the market is highly segmented by customer type depending, for example, on transaction volume, frequency, and price sensitivity, and each segment is catered for by different providers. While migrants value the ability to make low cost, low volume payments on a weekly or monthly basis to regions with little or no banking infrastructure and are willing to pay a premium to money transfer businesses, multi-national corporations make payments worth millions of dollars in multiple currencies to a number of countries on a daily basis and pay their banks a fraction of the fees due to their negotiating power. Credit cards offer a vastly different set of features from wire transfer and online EPIs can be custom-built from these basic modules to serve the needs of different customer segments such as online merchants or migrants. The channels through which payments can be made include over-the-counter and ATMs, the telephone network for credit and debit cards, and desktop and mobile devices for the web presence of banks, money transmitters, and online EPIs. Country-specific regulation and national interests confer an advantage to local champions over foreign competitors, effectively adding another dimension to the coverage attribute. Lastly, security is a concern with many of the current EPIs and a variety of solutions such as PINs, mobile phone verification, and two-factor authentication create further differentiation.

Bitcoin on the other hand has the potential to replicate the strengths of the separate EPIs on one platform and introduce new capabilities that are not available anywhere else. Because of its peer-to-peer nature it can become a dominant technology which offers superior alternatives to most existing solutions, making these obsolete and reducing differentiation across a broad spectrum of attributes.

4.2.3 Multi-Homing: Common

There has long been a trend away from relationship banking to transactional banking. In the past most individuals and firms had one main bank for all their financial needs. A strong relationship was important because banks would give credit lines only to customers who they knew well enough to properly assess the counterparty risk and fee discounts would be subject to transaction volumes or average balances. Often a checking account could only be opened if it was where the paychecks would get deposited. These and similar conditions created a lock-in that made it difficult for customers to have more than one banking relationship. That is not the case anymore. Customers increasingly check on a transaction by transaction basis who offers the best solution, for example, in terms of price, transfer speed, or the quality of advice. The Internet has accelerated this trend, especially for products and services that require little human interaction. These offerings are designed for ease of use to attract more visitors and usually don't have a membership fee or other contractual agreements to lock in customers. It therefore costs little or nothing to open and own multiple accounts with different providers. International money transfer falls into that category, because the customer usually knows exactly how much they want to transfer, when, and where to. No consultation is required.
Thus, individuals frequently own multiple bank and online EPI accounts and credit cards, merchants accept a variety of payment options, and personal transfers are done either through banks, money transmitters, or online EPIs, depending on how well each solution meets the specific needs in a given situation. In addition, Bitcoin itself supports multi-homing with free wallets and exchanges built on top of an open source platform, and companies like Coinbase and Bitstamp provide simple and low-cost ways to move money between the existing banking infrastructure and Bitcoin. Having said that, Confidence is one of the 6 Cs that drive consumer choice and trust that the funds will arrive is arguably the most important requirement for a payment instrument to gain adoption. If the funds don't arrive it doesn't matter how fast or cheap they could have been there. Thus, while transaction banking is prevalent, a minimum level of confidence in and EPI is a pre-condition for its success. Bitcoin has not yet achieved that level of trust in the general public.

On the flip side, development and infrastructure costs for a platform have traditionally been extremely high, especially on an international scale, resulting in only a handful of providers to choose from (for example VISA versus MasterCard or Western Union versus MoneyGram). With Bitcoin, this fundamentally changes as the underlying peer-to-peer infrastructure already exists and is essentially free to use.

4.2.4 Verdict

Given the three tests above, there is no clear verdict in favor of or against the international payments industry being a WTAoM market. This result is supported by the fact that, despite there being leaders in certain segments, no dominant platform for the entire international payments industry exists. Despite strong network effects on each of the platforms, there is a high degree of differentiation among and between payment instruments with regards to the 6Cs and switching costs are low, encouraging multi-homing.

This verdict may change if Bitcoin successfully establishes itself as a dominant technology that reaches mainstream adoption in the payments market. Even if it won't dominate the entire industry, use cases like remittances hold great potential for Bitcoin to establish a foothold in at least some segments and niches. There would still be room for competing solutions and possibly platforms in specialized areas such as wholesale international money transfer between banks, so it is not clear if there would be one winner or multiple platforms that co-exist.

5 Conclusion

5.1 Summary of Findings

Bitcoin is a technology that is well suited for international payments. It already can fulfill user needs better than some of the current payment instruments. It shows clear advantages in capability, cost, and speed. Confidence and confidentiality will rise with the maturation of the ecosystem and increase in regulation. All these factors will have a positive impact on coverage,
as more individuals and businesses will join once they see their needs fulfilled and concerns alleviated.

It is also an attractive ecosystem for individuals, merchants, miners, and entrepreneurs with strong network effects that has the potential to become a dominant platform in the market segments that exhibit WTAoM characteristics. However, a consequence of such characteristics is that a less-efficient network standard may get adopted. Such standards truncate the value that flows to consumers and merchants who would prefer a unified payments platform that fulfills all their needs over a variety of choices that offer only partial solutions. While unsolved pain points might look like an attractive opportunity for new entrants to the market, once adopted a sub-optimal standard can survive for a very long time despite superior alternatives, as has been the case with the QWERTY key layout invented for type writers over a century ago and which is still the norm today [77, pp. 32–43]. The battle for dominance is therefore neither over nor is the result clear cut. However, once a new entrant successfully tips the market to his platform, he can benefit from WTAoM characteristics himself and become deeply entrenched in a dominant position. The author believes that Bitcoin is here to stay and that it is the front runner in the race to change the payments industry to an extent not seen since the revolution in the communications industry with the invention of the Internet.

This will not happen overnight. Instead, it is more likely that market segments will be taken over one by one, starting with the long hanging fruit with major pain points for which Bitcoin is the solution. Remittances are very expensive and are hurting those who have the least to spend [112]. The $500 billion remittance market is an ideal fit and therefore a likely first candidate for Bitcoin to have an immediate impact on a global scale.

This prediction is predicated on the continued growth and ultimate mainstream adoption of Bitcoin. In order for that to occur, three main challenges have to be met: regulation, volatility, and trust.

The outlook for regulation has recently become more positive. Initially there was the fear that governments would simply squash what they saw as a threat to their legal mandate over their national currencies. While China and Russia still take a negative stance on that issue, regulation in many of the most important global economies like the U.S. and Germany has been more favorable. A BitLicense is under way in the state of New York which should reduce ambiguity and drive adoption [121].

Volatility has been of great concern for investors and speculators who see Bitcoin as a currency. Its price rose from $14 at the start of 2013 to over $1,200 at year end, and has since dropped two-thirds from its peak. As a store of value it is therefore unsuitable at this point. But volatility has fallen in recent months as the speculative craze abated and more actual users joined the platform who see value in Bitcoin the network. The concern that merchants won’t adopt Bitcoin because of its high volatility is therefore unfounded. In any case, as discussed in this thesis there are tools that immediately exchange bitcoins for fiat currency upon receipt, largely negating the price risk. Growing adoption will reduce volatility which encourages more adoption in a positive feedback loop.
Security is the outstanding feature of Bitcoin. The way the network is protected through public key cryptography, digital signatures, and cryptographic hashing is revolutionary and facilitates secure and irreversible payments without a trusted third party. However, the ecosystem is still at an early stage and like any speculative bubble it has attracted some shady characters who intend to enrich themselves at the expense of the masses. Customer funds aren't secure in a vault if the banker has his keys stolen or robs the bank himself. The Silk Road seizure has demonstrated that Bitcoin can be abused for criminal activity and the fall of Mt.Gox has reminded everyone that bitcoins cost real money and that hundreds of millions of dollars can be wiped off people's accounts overnight. Incidents like these erode the trust Bitcoin has earned through the honest and hard work put into the development of the platform by the large majority of stakeholders. Sensible regulation that protects consumers and enforces standards will flush out the fraudsters and help regain the trust in Bitcoin, and with it adoption.

5.2 Outlook and Future Work

Bitcoin has come a long way since its inception in 2008. Having solved the double spending problem is truly revolutionary and the possibilities for innovation are endless. Not just in payments, but in business and communication in general. It has the potential to alleviate poverty and oppression on a global scale much like the invention of the Internet did. Its development is neither finished nor is it certain that Bitcoin will survive. The possibilities for failure are endless. It may fail as a currency or it could be replaced by a superior cryptocurrency. But it has already made its mark on history by putting cryptocurrencies on the map. Distributed networks of trust that allow strangers to transact remotely without the need for a neutral third party are here to stay.

Future work in this field could continue where this analysis left off by analyzing the competitive landscape further and recommending strategies for companies how to become platform leaders in the payments industry, and in the Bitcoin ecosystem. Another path of research would be to investigate the many other uses for Bitcoin besides payments, and what the likely next industries are that will get disrupted by cryptocurrencies.
6 References


@albertwenger, “Bitcoin As Protocol,” Union Square Ventures, 31-Oct-2013.

“Mining,” Bitcoin. 01-Apr-2014.

“Genesis Block,” Bitcoin. 19-Dec-2013.


“Controlled supply,” Bitcoin. 03-Mar-2014.


thepok, “This could have been a successful 51% attack from btcguild if they were evil :/ They are to strong! 6 Blocks in a row!,” *r/bitcoin*. May-2013.


“Coinbase and Overstock.com: The results are in!,” 04-Mar-2014.


E. Voorhees, “My Open Letter to Peter Schiff (followup from the debate today),” *r/bitcoin*. 02-Dec-2013.


