Uncovering the Secrets of Bitcoin's Success
by
Karthic Prasad Kosgi
B.E. Electrical & Electronics Engineering
Osmania University 2008

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
February 2016

© 2016 Karthic Prasad Kosgi. 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
Author........

Signature redacted
Karthic Prasad Kosgi
System Design and Management Program
Jan 11, 2016

Signature redacted
Certified by........
Dr. Barbara Wixom
Principal Research Scientist, MIT Sloan Center for Information Systems Research
Thesis Supervisor

Signature redacted
Accepted by........
Patrick Hale
Executive Director, System Design and Management Program
Uncovering the Secrets of Bitcoin’s Success

by

Karthic Prasad Kosgi

Submitted to the System Design and Management Program
on Jan 11, 2016, in partial fulfillment of
the requirements for the degree of
Master of Science in Engineering and Management

Abstract

Bitcoin is a cryptocurrency and a decentralized payment system. The transactions between two parties are approved not by a central institution but by the peers of the network. Bitcoin uses cryptography and software algorithms to control the units of generation and to verify the transactions on the network. However, bitcoin is not the only cryptocurrency with these capabilities. There are more than 600 cryptocurrencies in the market. Nonetheless, bitcoin is the most successful cryptocurrency to date with the highest market cap, transaction volume, merchant adoption, and venture capital investments.

In this thesis, the author investigates why bitcoin is the most successful cryptocurrency to date. The author’s research identified that bitcoin’s success is rooted in its ability to become an effective multi-sided platform with network effects.

Thesis Supervisor: Dr. Barbara Wixom

Title : Principal Research Scientist, MIT Sloan Center for Information Systems Research
Acknowledgements

I would like to thank my thesis advisor, Dr. Barbara Wixom, for your continuous support and feedback in writing this thesis. It has been an honor working with you as Research Assistant for the past two years and I am fortunate to have you as my mentor. You always set high work standards and you are always there to guide me to meet those standards when needed. The best part is I enjoyed working with you.

I would like to thank Jeanne Ross for giving me an opportunity to do research at the Sloan Center for Information Systems Research (CISR). This opportunity had a huge impact on my overall MIT experience.

I would like to thank Pat Hale, for leading a fantastic and flexible System Design and Management (SDM) program. This program gave me two of the best years of my life.

I would like to thank my fellow SDM friends, especially the social chairs, and others outside of SDM who made my stint at MIT even more memorable.

I would like to thank my friends outside of MIT - Viswa, Ramana, Karthik, Satish and many others who encouraged and supported me during this journey.

Saving the best for the last, I would like to thank my family for their unconditional love and support. Mom, Dad, Anna, Vadina and Saanvi, this thesis is dedicated to you people!
[This page intentionally left blank]
# Table of Contents

Abstract .......................................................................................................................................................... 3  
Acknowledgements ..................................................................................................................................... 5  
List of Tables .............................................................................................................................................. 10  
List of Figures ............................................................................................................................................. 12  
Chapter 1: Introduction ............................................................................................................................. 14  
1.1 Motivation ........................................................................................................................................... 14  
1.2 Thesis Structure ..................................................................................................................................... 15  
1.3 Introduction to cryptocurrencies ........................................................................................................... 16  
Chapter 2: Bitcoin, Advantages and Challenges ....................................................................................... 22  
2.1 Bitcoin ................................................................................................................................................... 22  
2.2 Technical Concepts in Bitcoin .............................................................................................................. 24  
2.3 Working details of bitcoin ...................................................................................................................... 27  
2.4 Advantages of Bitcoin ............................................................................................................................. 30  
2.5 Challenges ............................................................................................................................................ 34  
Chapter 3: Bitcoin Landscape ...................................................................................................................... 37  
3.1 Users ....................................................................................................................................................... 38  
3.2 Merchants................................................................................................................................................. 39  
3.3 Wallet Service Providers ......................................................................................................................... 40  
3.4 Exchanges ............................................................................................................................................... 42  
3.5 Miners ..................................................................................................................................................... 44  
3.6 Payment Processors ............................................................................................................................... 46  
3.7 Regulators .............................................................................................................................................. 47  
3.8 Venture Capitalists ................................................................................................................................. 48  
3.9 Bitcoin Developers ................................................................................................................................. 50  
Chapter 4: Multi-Sided Platforms ............................................................................................................... 53  
4.1 Introduction ............................................................................................................................................ 53  
4.2 Platforms ............................................................................................................................................... 54  
4.3 Multi-Sided Platforms ............................................................................................................................. 56  
4.3.1 Factors influencing the success of MSPs ........................................................................................... 58
List of Tables

Table 1.1: Top 10 cryptocurrencies based on market cap................................................................. 16
Table 2.1: SHA256 sample values...................................................................................................... 24
Table 3.1: Top 10 bitcoin exchanges based on trading volume......................................................... 43
Table A.1: Bitcoin generation............................................................................................................ 72
List of Figures

Figure 2.1: Total bitcoins Vs blocks .................................................................................................... 23
Figure 2.2: Simplified blockchain view ................................................................................................ 30
Figure 2.3: Bitcoin price chart ........................................................................................................... 35
Figure 3.1: Stakeholders of the Bitcoin Ecosystem .............................................................................. 37
Figure 3.2: Total wallets of individual Wallet Service Providers.................................................... 42
Figure 3.3: Bitcoin mining ecosystem .................................................................................................. 45
Figure 3.4: Venture Capital Investments in cryptocurrencies by year .................................................. 49
Figure 3.5: Venture Capital Investments by region ........................................................................... 50
Figure 4.1: Facebook as a multi-sided platform ................................................................................... 56
Figure 5.1: Bitcoin as a multi-sided platform ....................................................................................... 63
Figure 5.2 Bitcoin daily transactions ..................................................................................................... 65
Figure 5.3: Bitcoin related startups founded between 2011 and 2014 ............................................... 66
Chapter 1: Introduction

1.1 Motivation

When I travelled to Ghana from the United States last summer, I could not use the US dollars (USD) that I had because currencies in the United States and Ghana are different. I had no choice but to convert my US dollars into Ghana Cedi for my stay.

When I was admitted into Massachusetts Institute of Technology (MIT), I was both ecstatic and worried. I was ecstatic because MIT is the one of the best universities in the world. I was worried not only because I had to plan for high tuition fees, but also because I had to find an institution that offered good exchange rates to transfer money from India to the United States. After coming to the United States, I still worried about exchange rates when I sent money to my parents in India. Transaction fees for international transfers are high, representing 2-3% of the total transaction value.

During my time at MIT, I followed news about the Greek sovereign debt crisis, and I was struck by how centralized institutions such as banks have the power to impose restrictions on customers for little reason. During the debt crisis, Greek citizens were restricted from withdrawing more than 60 euros per day from bank ATMs.

Bitcoin offers solutions to all the problems described above. First, bitcoin is a global currency that can be used in multiple countries and that does not require currency conversion. Second, in bitcoin transactions, the transaction fees are small – in fact, almost zero. Finally, bitcoin represents a decentralized peer-to-peer network in which transactions are authorized by the entire network rather than a centralized institution, thus eliminating centralized power.
Bitcoin, however, is not the only cryptocurrency with the capabilities to solve these problems. There are quite a few cryptocurrencies in the market that offer similar capabilities. Nonetheless, Bitcoin is the most successful cryptocurrency to date in terms of user adoption, transaction volume, market capitalization and merchant adoption. In my thesis, I intend to investigate the reasons for bitcoin’s success.

Hypothesis: Bitcoin is the most successful cryptocurrency to date because it is a multi-sided platform with strong network effects.

1.2 Thesis Structure

Chapter 1 presents the motivation for the thesis. Cryptocurrencies are introduced in this chapter along with several participant groups of the cryptocurrency ecosystem.

Chapter 2 introduces Bitcoin and explains its technical concepts and working details. The chapter also discusses advantages and challenges of bitcoin.

Chapter 3 introduces various stakeholders of the bitcoin ecosystem and describes the role of each stakeholder.

Chapter 4 presents a literature review of Platforms and Multi-Sided Platforms.

Chapter 5 explains why Bitcoin is the most successful cryptocurrency to date using the Multi-Sided Platform literature.

Chapter 6 presents conclusion, limitations, and future research for the thesis.
1.3 Introduction to cryptocurrencies

Cryptocurrencies are digital currencies that use cryptography and software algorithms to generate the units of currency. Cryptocurrencies also act as payment systems by allowing users to transfer units of currency over the internet. The creation of units of currency and the verification of transactions are not controlled by a trusted third party institution or government but by the participants, nodes, or peers of the network, making it a completely decentralized system. The transactions are stored on publicly available distributed ledgers. As of December 22, 2015, there are 667 cryptocurrencies that have been created in the world, which vary in ways, such as unique cryptographic algorithms and product features. Please find below in Table 1.1 a list of the top 10 cryptocurrencies based on the market capitalization as of December 22, 2015.

<table>
<thead>
<tr>
<th>S.No.</th>
<th>Name</th>
<th>Market Capitalization</th>
<th>Price</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Bitcoin</td>
<td>$6,551,201,134.00</td>
<td>$436.99</td>
</tr>
<tr>
<td>2</td>
<td>Ripple</td>
<td>$207,844,930.00</td>
<td>$0.01</td>
</tr>
<tr>
<td>3</td>
<td>Litecoin</td>
<td>$149,724,605.00</td>
<td>$3.43</td>
</tr>
<tr>
<td>4</td>
<td>Ethereum</td>
<td>$67,888,331.00</td>
<td>$0.90</td>
</tr>
<tr>
<td>5</td>
<td>Dash</td>
<td>$15,224,902.00</td>
<td>$2.50</td>
</tr>
<tr>
<td>6</td>
<td>Dogecoin</td>
<td>$14,609,008.00</td>
<td>$0.00</td>
</tr>
<tr>
<td>7</td>
<td>Peercoin</td>
<td>$9,349,040.00</td>
<td>$0.41</td>
</tr>
<tr>
<td>8</td>
<td>BitShares</td>
<td>$8,972,780.00</td>
<td>$0.00</td>
</tr>
</tbody>
</table>
Some of the differences among cryptocurrencies include:

- **Total coins:** Many of the cryptocurrencies generate a fixed number of units of currency, and the total possible units of currency that can be generated varies. For example, the total bitcoins (Bitcoin’s unit of currency) that can be generated is limited to 21 million; whereas, the total litecoins (Litecoin’s unit of currency) that can be generated is limited to 84 million\(^9\). Total units of currency generation influence the supply and demand of the cryptocurrency.

- **Generation strategies:** Different cryptocurrencies adopt different strategies to generate units of currencies. For example, Bitcoin cryptocurrency will reach the limit of 21 million bitcoin in 2140\(^{10}\); whereas, Ripple cryptocurrency created all of its units of currency (denoted by XRP) - of 100 billion XRP - when it originated. Ripple Labs, creator of XRP, owned around 66 billion XRP, and others owned 34 billion XRP\(^{11}\) as of November 2015. Generation strategies of the cryptocurrencies influence the supply and demand of the cryptocurrency.

- **Consensus mechanism:** Cryptocurrencies serve as payment systems. The transactions over the decentralized network are verified by peers of the network. Different cryptocurrencies use different algorithms to validate the transactions on the network. For example, Bitcoin uses ‘Mining\(^{12}\), a process of solving computational problem, to validate the transactions on the network. BitShares uses an algorithm called ‘Proof-of-Stake\(^{13}\) to validate the transactions on
transactions on Bitcoin are more secure but are costly to verify because of the computational resources involved in the process. BitShares transactions are less secure and are prone to attacks, but are less costly compared to bitcoin transactions; they require less computational resources. Consensus algorithms influence the security and costs of the network.

- **Hashing Algorithms**: Many cryptocurrencies use mining to generate new units of currency and to verify transactions on the network. Mining involves solving for a computationally difficult problem, and it requires computing power. Cryptocurrencies use different hashing algorithms. For example, Bitcoin uses 'SHA256'; whereas, Litecoin uses 'Scrypt'. Application Specific Integrated Chips (ASICs) are used for Bitcoin mining. ASICs are very costly and can perform very high computations. Personal computers can be used for Litecoin mining. Hashing algorithms influence whether miners choose to join a specific cryptocurrency mining community.

- **Confirmation time**: Confirmation time refers to the time taken by the cryptocurrency network to verify a transaction and to add the same transaction to the distributed ledger. For example, Bitcoin takes an average of 10 minutes to add a transaction to its distributed ledger; whereas, Litecoin takes an average of 2.5 minutes to add a transaction to its distributed ledger. Confirmation time influences the transaction processing speed of the network.

Cryptocurrencies are considered to be one of the greatest innovations of the decade because of their ability to settle transactions between two parties without central authority. The distributed ledger
offers a new kind of record keeping system, which is open yet secure. The activities below signal innovation activities and cryptocurrency adoption.

- There are more than 100 global startups working in the cryptocurrency space to solve problems in various industries, such as healthcare, real estate, and financial services\(^\text{19}\). For example, Factom\(^\text{20}\), a records management service provider, offers solutions
  - In healthcare, “to track communication data for HIPAA compliance, proving in real-time that all private patient data remained appropriately secure”.
  - In real estate, “to secure land titles or any kind of real property”.
  - In financial services, “to track and audit all financial trade data in real time”.

- As of Oct 2015, the venture capital funding in cryptocurrency-related startups was $927.36 million USD\(^\text{21}\). These investments were made across multiple continents and signal global activity in the area.

- In the United States, the National Science Foundation, a government agency that supports and funds research and education in the field of Science and Engineering, approved a grant of 3 million USD for research in the field of Cryptocurrency Systems and Smart Contracts in 2015. This research program is called the Initiative for Cryptocurrencies and Contracts (IC3),\(^\text{22}\) and IC3 includes researchers from Cornell University, University of Maryland and University of California Berkley.

- Some of the world renowned universities have introduced cryptocurrency courses. Massachusetts Institute of Technology\(^\text{23}\) offered two classes viz. ‘Future Commerce’ and ‘Blockchain Technologies’ in the fall of 2015. Imperial College London, Duke University,
Canada McGill University, New York University, and many others also offered programs for students about cryptocurrencies.

- Bank of England, the central bank of England, published an article about the role of digital currencies in driving the innovation of payment systems. Bank of England argued that the distributed ledger is the most important facet of digital currencies and that digital currencies open up new opportunities in the financial services industry.

- A consortium of more than 30 global financial companies was formed by a company called R3 to research collaboratively in the distributed ledgers space and to find use cases in the financial services industry.

- Consumers have used cryptocurrency to transfer money and to buy goods and services because of low transaction fees compared to traditional payment options.
Chapter 2: Bitcoin, Advantages and Challenges

The previous chapter introduced the concept of cryptocurrencies. In this chapter, the cryptocurrency bitcoin is introduced in detail. The chapter describes technical concepts, working details, advantages, and challenges of bitcoin.

2.1 Bitcoin

Bitcoin is a cryptocurrency; it uses cryptography and software algorithms to control the generation of the units of currency. 'Bitcoin' was proposed by Satoshi Nakamoto in 2008. The transactions of Bitcoin are stored on a distributed ledger called 'Blockchain'. With traditional currencies, such as USD and INR, central institutions control the market’s money supply. For example, the Federal Reserve controls the total USD supply to the market in the United States. The Reserve Bank of India controls the total INR supply to the market in India. In contrast, the bitcoin supply to the market is controlled by computer algorithms. Bitcoin is programmed such that the total bitcoin supply is limited to 21 million bitcoins (BTC). As of Oct 31 2015, the total bitcoin circulation in the market was 14,786,850 BTC.

New bitcoins are added through a process called 'Mining'. Entities that perform mining are called 'Miners'. During this process, new 'blocks' are generated. The total number of bitcoins in the market is calculated by the product of the total number of blocks and the value of each block. The value of blocks is halved after every four years or 210,000 blocks. The value of each block is 50 BTC during the first four years. Currently, the block value is 25 BTC. Please refer to Figure 2.1 and Table A.1 in appendix for additional information on bitcoin generation.

Karthic Prasad Kosgi | MIT SDM 2016
Figure 2.1: Total bitcoins Vs blocks

Bitcoin is a decentralized payment system. Bitcoin can be used to transfer units of currency over the network to other individuals or to buy goods and services locally and globally. These transactions are approved not by central institutions such as banks and credit card companies but by peers of the network\(^\text{34}\). The transaction costs in the bitcoin payment system are much smaller as compared to transaction costs in centralized systems\(^\text{35}\).
Low transaction fees and decentralization are two of the key factors that drive bitcoin adoption. In the next sections, technical concepts and working details of bitcoin are presented to understand how bitcoin works.

2.2 Technical Concepts in Bitcoin

**Cryptographic Hash Functions:**

A Cryptographic hash function is a function that takes a string of any length as input and returns an output of fixed length. If ‘m’ is the input string or message and ‘H’ is the hash function, then the hash value ‘h’ = H(m). ‘MD5 (Message Digest Algorithm), ‘SHA256 (Secure Hash Algorithm), ‘RIPEMD (Race Integrity Primitives Evaluation Message Digest)’ are a few examples of hash functions. Bitcoin uses SHA256 as a hashing algorithm. SHA256 takes an input of any length and converts into an output of 256 bits. The hash values of two words ‘Blockchain’, ‘Block’, ‘block’, and ‘blockchain’ are calculated using an online tool in Table 2.1 for SHA256.

<table>
<thead>
<tr>
<th>Input</th>
<th>Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Blockchain</td>
<td>625da44e4af58d61cf048d168aa6f5e492dea166d8bb54ec06c30de07db57e1</td>
</tr>
<tr>
<td>Blockchain</td>
<td>ef7797e13d3a75526946a3bfc00daec9fc9c4d51ddc7cc5d888f74dd434d1</td>
</tr>
<tr>
<td>Block</td>
<td>211d0bb8cf4f5b5202c2a9b7996e483898644aa24714b1e10edd80a54ba4b560</td>
</tr>
<tr>
<td>Block</td>
<td>496aca80e4d8f29f88e8cd816c3afb48d3f103970b3a2ee1600c08ca67326dee</td>
</tr>
</tbody>
</table>
Some properties of hash functions include:

- Hash functions are efficiently computable. It is straightforward to compute the hash of a message and to return the output.
- Hash functions are ‘Collision-resistant’. It is infeasible to find two distinct values ‘x’ and ‘y’ such that H(x) = H(y).
- Hash functions are ‘Pre-image resistant’. It is infeasible to find the message ‘m’ given the hash value of the message h = H(m).
- Hash functions are deterministic. Hash functions return the same hash value for a given input string irrespective of number of trials.

In Bitcoin, these properties are used to verify if a valid ‘proof-of-work’ for the block is submitted to the network during the ‘mining’ process. ‘Proof-of-work’ and ‘mining’ are explained in detail in the ‘Working details of bitcoin’ section of this chapter.

Digital Signatures:

A digital signature is a mathematical scheme used to verify the authenticity of the document. A digital signature scheme typically consists of three algorithms.

1. Key Generation Algorithm: This algorithm generates a key pair by taking the key size as the input. The key pair is a combination of a public key and a secret key. The public key is shared with anyone and is used for the verification of the signature. The secret key is used to sign the documents by the user and is not shared with anyone.
(sk, pk) := generateKeys(keysize)

keysize is size of keys. Eg: 1024 bit keys, 2048 bit keys etc

sk is secret key

pk is public key

generateKeys is the function that generates keys

2. Signing Algorithm: This algorithm generates a signature for a given message and a secret key.

\[ \text{sig} := \text{sign}(\text{sk}, \text{message}) \]

\[ \text{sig} \] is the generated signature

sign is the function that generates signature

3. Signature verification algorithm: This algorithm verifies the authenticity of the signature. It takes the message, public key and signature and returns a boolean value depending on the validation.

\[ \text{isValid} := \text{verify}(\text{pk}, \text{message}, \text{sig}) \]

\[ \text{isValid} \] is true if it is a valid signature, false for invalid signature

Some applications of digital signatures:

- Digital signatures are used to authenticate the source of the document. It is impossible to replicate the sender's signature as long as the secret key is not compromised.
- Digital signatures are used in maintaining the integrity of the message between sender and receiver. The signature will be invalidated if the message is changed after signing the message.
- Digital signatures help in non-repudiation situations because of the presence of the signature.
Bitcoin uses Elliptic Curve Digital Signature Algorithm (ECDSA). Digital signatures help in validating the ownership of coins during transactions in Bitcoin.

2.3 Working details of bitcoin

This section communicates the working details of bitcoin by describing the steps that happen when a transaction occurs between two parties. ‘Alice’ and ‘Bob’ are the two parties involved in this transaction example. Bob intends to transfer money to Alice using bitcoin, and Alice does not own bitcoins to date.

In order to send or receive bitcoin, Alice first installs a ‘Wallet’. A wallet is a software application that is used to make transactions on the Bitcoin network. There are different kinds of wallets available (more detail about wallets is provided in the next chapter). In general, a wallet contains the private and secret keys that will help Alice sign the transactions. Wallet software also determines the total bitcoin value owned by Alice, and it relays its transactions to the entire network. Alice also needs a wallet to create an ‘Address’. The address is a 160-bit hash of the public portion of the public/private ECDSA key pair.

Once a new address is generated using the wallet software, Alice can use this address to receive bitcoin. Once her wallet is set up, Alice can receive bitcoins from someone who owns bitcoins, or Alice can buy bitcoins on ‘Exchanges’. Exchanges allow users to trade between bitcoin and other assets, such as fiat currencies and cryptocurrencies. Exchanges are explained in detail in the next chapter.

Bob initiates a bitcoin ‘Transaction’ to Alice by sending Alice a transaction using the private key in his wallet. A bitcoin transaction includes an ‘input’, an ‘output’ and a ‘value’. An ‘input’ is the reference to the previous output transaction, thereby confirming the transfer of ownership from the previous
owner to Bob. An ‘output’ is the reference to Alice’s address, and ‘value’ is the number of bitcoins to be transferred to Alice. There can be multiple output and input values. If Bob owns 100 BTC and is transferring only 25 BTC to Alice, there will be two outputs created: one to Alice’s address and the other to Bob’s address. The difference between the input bitcoins and output bitcoins is called the ‘Transaction Fees’. The transaction fees are charged to process the transaction. The miner who processes the transaction receives the fees. A transaction that is present on the blockchain is called a ‘Confirmed Transaction’. A transaction, which is yet to be added to the blockchain, is called an ‘Unconfirmed Transaction’.

A newly created transaction is broadcasted to the entire network through nodes on the network. All of the unconfirmed transactions in the network are stored in a pool called ‘Memory Pool’ or ‘Mempool’. Bob’s transaction, along with other transactions in the Mempool, is included in a 'block'. A block consists of a 'block header' and a list of transactions. A block includes a ‘Coinbase’ transaction, which consists of reward to miners for proof-of-work. Currently, the reward is 25 BTC. These rewards can be spent after 100 blocks.

The first block on the Bitcoin network is called the ‘Genesis block’. This block does not have a reference to a previous block. Every other block on the Bitcoin network has a reference to the previous block. The chain of blocks with references to previous block is called ‘Blockchain’. Please refer to Figure 2.2 for simplified illustration of blockchain. Blockchain is a publicly available distributed ledger, which maintains a record of all transactions in the chronological order on the bitcoin network. Blockchain is used by all nodes in the network as a reference to validate transactions on the network and to avoid double spending. Because blockchain is a chain of blocks that are chronologically linked, it is easy to verify transactions by validating the ownership and value for a given address. If a malicious
user wanted to change transaction data that was already added to the network, the user must redo all the proof-of-work, which might not be profitable because of the computing power required.

The 'Block Header' consists of the hash of the previous block, the hash of root of the Merkle tree, the current time, difficulty and nonce. The 'Merkle tree' is formed by pairing each transaction id with another transaction id and hashing them together. If there is an odd number of transaction ids, the last remaining transaction id is paired with itself. If there is an odd number of hashes, then the last single hash is paired with itself. This process is repeated until there is only one element, which is called the root of the Merkle tree.

'Difficulty' is the measure of how difficult it is to solve the problem set by the Bitcoin protocol. In order for the block to be added to the blockchain ledger, a miner has to perform a 'proof-of-work', which involves solving a computational problem. This requires both time and computing resources. Even though the computational problem is difficult to solve, it is easy to verify because the computational problem consists of finding the hash that meets the conditions set by the network.

Bitcoin uses 'Hashcash' proof-of-work, which was proposed by Adam Back in 1997. Once a miner solves a computational problem, that solution, also known as 'proof-of-work', is included in the block and published to the network. All other nodes on the network verify this solution before adding the block to the blockchain. Difficulty is updated after every 2016 blocks and is calculated based on the time taken to solve problems associated with previous blocks. All other parameters being constant, 'Nonce' is 32 bit number that is incremented continuously until the solution is found. This process of adding a block to the blockchain is called 'Mining,' and entities that perform mining are called 'Miners'. Once the block that contains Bob's transaction is added to the blockchain, the transaction can be verified on the blockchain.
Figure 2.261: Simplified blockchain view

2.4 Advantages of Bitcoin

In this section, various advantages of bitcoin are described. These advantages influence the adoption of bitcoin by various stakeholders.

User empowerment:

In the transaction process explained above, there was no central authority or single institution that approved the transaction. The transaction was approved by the distributed nodes that participated in the network with predetermined consensus rules. More importantly, this system was open for participation by any entity. This is quite different from traditional payment systems. The absence of centralized institutions provides autonomy and empowerment for the users.
During the Greek Sovereign Debt Crisis\textsuperscript{62}, restrictions were imposed on the citizens of the country that no more than 67 USD could be withdrawn from an ATM, and banks were closed for weeks denying access to savings. This was possible because governments and banks had the ability to set rules, which conflicted with the interest of customers. In the case of Bitcoin, the users always have control over the bitcoin that they own. Additionally, it is quite challenging to bring down the Bitcoin network of because nodes operate from different parts of the world.

\textbf{Security:}

Bitcoin uses principles of cryptography and game theory to secure the network. Bitcoin uses cryptographic algorithms, such as Secure Hash Algorithm (SHA 256) and Elliptic Curve Digital Signature Algorithm (ECDSA). The security of the network is also enforced by its incentive schemes, such as block rewards designed in the system. Although malicious activities within the bitcoin network are possible, malicious activities may not be profitable. For example, if a malicious user wants to transfer bitcoins that have been spent, he or she would have to redo and submit the proof-of-work to the network. Considering the current difficulty levels of the bitcoin network, this would entail huge computing power. Even in a case where a malicious user owned greater computational power than honest nodes on the network, also known as a ‘51% attack’, it would not be profitable; in this case, the value of bitcoin would decrease, thereby not resulting in financial gain.

Bitcoin offers security from data breaches. Unlike credit card payments, which record personal information of the user such as name, credit card number etc., bitcoin payments record only the
transfer of ownership of coins. This can help in avoiding data hacks at merchant stores such as what happened with Staples and Target.

**Transaction fees:**

Bitcoin offers low transaction fees when compared to traditional payment systems. Payment processors, such as Visa and MasterCard charge 2-3% of the transaction as fees to process the transaction. Bitcoin transaction fees depend on the size of the transaction, the priority and value of the transaction. Miners who process the bitcoin transactions on the network charge little or no transaction fees. Instead, miners earn revenue in the form of block rewards, which were 25 BTC per block in 2015. This fee arrangement might change in the future after the blocks on the network are mined and if the Bitcoin network scales to facilitate a higher number of network transactions.

**Privacy:**

Transactions in Bitcoin are stored in a public ledger called 'Blockchain'; however, the ledger stores information about change of ownership addresses, not the identities associated with the addresses. A single user can use multiple addresses for multiple transactions. Using multiple addresses makes it difficult to identify user details, thereby providing privacy to the user. Even during the initial wallet setup, a bitcoin user need not provide identification details. In contrast, in traditional banking systems, a user’s identity is stored in the bank’s database along with his or her transactions, offering less privacy for the bank’s customer.
Universalness:

With traditional fiat currencies, a person travelling from one country to a different country has to carry the local fiat currency to cover his expenses – or convert to the local currency upon arrival. In the case of bitcoin, a traveler can use the bitcoin wherever his or her destination, and the bitcoin value will be the same regardless of locale. Bitcoin saves time and effort required to make currency conversions.

Ease of use:

A bitcoin user needs a wallet and a recipient address to make a transaction. No additional information of the user is required. Bitcoin transactions on average take ten minutes for confirmation. In contrast, traditional payment systems require bank accounts. To get a bank account, identities issued by governments are required, and it takes days to get account access after all documents are submitted. It takes hours or even days to process a transaction between two bank accounts. Further, the timing depends on multiple factors, such as the country to which money is transferred, the bank, and the day of the week (holiday vs working day). In the case of Bitcoin, these factors do not come into play because bitcoin transactions are approved by the decentralized nodes on the network.
2.5 Challenges

In this section, the challenges of bitcoin are described that influence the adoption of bitcoin by various stakeholders as a currency and a payment option.

Volatility:

One of the biggest challenges that Bitcoin poses is its volatility. Bitcoin's volatility makes it difficult for users to conduct day-to-day transactions; value fluctuations make the currency unreliable in the short-term. Even though it is common for any fiat currency to have some value fluctuations, the magnitude of fluctuations is a big concern in the case of bitcoin. For example, in one case, Bitcoin experienced a change in value of more than 100% in a span of three months (refer to Figure 2.3). On August 24, 2015, the value of Bitcoin currency was 213.24 USD, and the value changed to 437 USD by November 4, 2015. These fluctuations are not just related to the demand and supply of bitcoin. They also can occur because of news related to illegal use of bitcoins, regulation announcements, and new partnerships among global banks.
Scalability:

In order for Bitcoin to become a global payment system, it must support thousands of transactions per second. VISA on average handles 2000 transactions per second, and VISA’s peak transaction volume is approximately 56000 transactions per second. Bitcoin currently can handle 7 transactions per second due to the limit on the block size. Bitcoin developers are working to increase the block size and thereby facilitating higher transaction volume; however, it is unclear how long this process will take. Consensus regarding the block size increase needs to occur through an open-source development process. If Bitcoin does not scale above current levels, confirmation times for transactions will increase because it will take more time for a new transaction to be included in a block.
Chapter 3: Bitcoin Landscape

In the previous chapter, technical and working details of bitcoin are explained along with advantages and challenges of bitcoin. This chapter describes the various stakeholders of Bitcoin ecosystem; see Figure 3.1 for the set of Bitcoin stakeholders.

Figure 3.1: Stakeholders of the Bitcoin Ecosystem
Bitcoin stakeholders are colored in blue and green in the above figure because blue stakeholders represent direct participants of the network and green represents indirect participants of the network. Direct participants involve in bitcoin transactions and indirect participants may work with some or all direct participants but do not involve in bitcoin transactions.

3.1 Users

Bitcoin users are people who use bitcoin to transfer money between two parties living in any part of the world and to buy goods and services on the internet. Bitcoin users can engage in a variety of transactions. For example, a person can buy apps and games for Windows, Windows Phone, and Xbox in the online store of Microsoft with bitcoin\(^7\). In another example, subscribers of DISH network can make payments in bitcoin\(^2\). DISH network is one of the largest satellite service providers in United States with more than 14 million pay-tv subscribers\(^3\). In these examples, people use bitcoin primarily as a currency and payment option.

Some users use the bitcoin transaction process to store information on the blockchain because the information is difficult to alter and easy to verify. For example, the MIT Media Labs is working on a project where digitally-issued certificates are registered on the bitcoin blockchain\(^4\) so that certificates are not lost and are easy to verify when needed. In another example, Everledger, a London based startup, is working on solving fraud and theft problems in the diamond industry. Everledger is using the bitcoin’s blockchain to register diamond certificates\(^5\). Note that these use cases are beyond the scope of this thesis; this thesis will focus on the currency and payment system aspect of bitcoin.
Bitcoin value is based on transaction volume\textsuperscript{76}. Transaction volume is dependent on the numbers of users using bitcoin. Thus, bitcoin users influence the success of bitcoin in that greater numbers of users increase bitcoin’s value.

3.2 Merchants

Merchants are participants of the bitcoin ecosystem who accept bitcoin as a payment option in exchange for goods and services. The total number of businesses that accept bitcoin is currently in thousands if not in millions\textsuperscript{77}. Furthermore, companies that accept bitcoin represent a variety of industries. Some examples include:

- Overstock, a large on-line US retail company, (Overstock was the first major business to accept bitcoin as a payment option. This occurred in early 2014.)
- Large technology companies such as Microsoft, Google, and Dell\textsuperscript{78}
- Large media firms such as Bloomberg and TimeInc
- Social media companies such as Reddit
- Gaming companies such as Zynga
- Non-profit organizations such as Khan Academy

In order for Bitcoin to gain widespread adoption as both currency and payment option, Bitcoin has to be accepted by merchants. Merchants influence the value of the bitcoin because the more merchants that accept bitcoin as a payment option, the greater the transaction volume, which results in greater bitcoin value. Merchant acceptance also will encourage users to see value in bitcoin for buying goods
and services. Some of the barriers for merchants to accept the bitcoin payments are the inherent volatility in bitcoin currency, unfamiliarity with cryptocurrencies and the infrastructure needed to process the transactions.

3.3 Wallet Service Providers

Wallet services providers are companies that offer key management services—called wallets—to bitcoin users. Wallets secure bitcoins by storing the private keys, which are required to perform transactions on the bitcoin network. Wallet service providers safeguard assets associated with bitcoin transactions by offering web authentications, hardware wallets, and insurance for the digital assets.

Wallet service providers vary based on how they protect keys.

- Some wallets offer *storage of keys locally* in a file. Keys are stored in a pre-configured file system path. These wallets also allow file encryption using a password, offering increased security. An example of such a wallet is ‘Bitcoin Core’.

- ‘Paper wallets offer *offline storage of keys*, which can be printed on paper. Paper-wallets contain the information about the public and private keys that are used for the transactions. These wallets offer greater security because they are impossible to hack programmatically, but they can be lost easily. ‘BitAddress’ is an example of paper wallet.

- Some wallets offer *air-gapped key storage* where a secondary device generates, signs and exports transactions but is never connected to the internet. The outputs that are created by
these wallets are transferred to a device that is connected to the internet to perform transactions on the bitcoin network. 'Armory' wallet is an example of air-gapped key storage.

- **Hardware wallets** manage keys in hardware modules. 'Ledger', 'Case', and 'Trezor' are examples of hardware wallets.

- Finally, **web wallets** host keys of the users on a company server. In all other cases, users are responsible for their keys. In this case, companies store the keys but provide users with access to transactional functionalities using standard web authenticating mechanisms. ‘Blockchain’ and ‘Coinbase’ are the most popular wallets of bitcoin. Blockchain crossed the landmark of 4 million wallets in August 2015. Coinbase had 2.9 million users and hosted 4.4 million wallets as of December 2015. Refer to Figure 3.2 for various wallet numbers of various wallet service providers.

Wallet service providers reduce barriers to entry for users who want to use bitcoins and therefore influence the adoption of bitcoin among users. However, not all users who own these wallets might be actively using bitcoins; some users may simply be experimenting with bitcoin. Most of the wallet service providers offer services to individual customers; however, there are some companies such as Coinkite that offer services to enterprise customers as well.
3.4 Exchanges

Bitcoin exchanges are businesses that allow customers to trade bitcoins for other assets, such as fiat currencies and other digital currencies\textsuperscript{84}. There are approximately two dozen bitcoin exchanges that accept transactions associated with almost 50 different currencies\textsuperscript{85}. See Table 3.1 for top 10 bitcoin exchanges based on trading volumes. Like traditional exchanges, bitcoin exchanges act as matching platforms between buyers and sellers by offering buy and sell bids. Bitcoin exchanges typically earn
revenue by charging money for these services; charges can be based on transaction volume or a monthly or annual fixed fee.

Exchanges are prone to security threats because exchanges deal with high volumes of bitcoin transactions. Malicious hackers mostly target exchanges for high returns. Mt Gox, one of the world’s first bitcoin exchanges, accounting for up to 80% of the overall bitcoin trading volume during its peak, was reportedly hacked. This resulted in a loss of 744,400 BTC worth approximately $350 million USD\textsuperscript{86}.

Bitcoin exchanges facilitate the onboarding of new users into the bitcoin ecosystem.

Table 3.1: Top 10 bitcoin exchanges based on trading volumes

<table>
<thead>
<tr>
<th>Exchange</th>
<th>Volume (BTC)</th>
<th>Market Share</th>
</tr>
</thead>
<tbody>
<tr>
<td>Huobi</td>
<td>19.4M</td>
<td>42.87%</td>
</tr>
<tr>
<td>OKCoin</td>
<td>18.4M</td>
<td>40.71%</td>
</tr>
<tr>
<td>bitFinex</td>
<td>2.07M</td>
<td>4.58%</td>
</tr>
<tr>
<td>btcChina</td>
<td>2.06M</td>
<td>4.56%</td>
</tr>
<tr>
<td>lakeBTC</td>
<td>920k</td>
<td>2.03%</td>
</tr>
<tr>
<td>Others</td>
<td>802k</td>
<td>1.77%</td>
</tr>
<tr>
<td>bitStamp</td>
<td>650k</td>
<td>1.44%</td>
</tr>
<tr>
<td>Btce</td>
<td>350k</td>
<td>0.77%</td>
</tr>
<tr>
<td>bit-x</td>
<td>302k</td>
<td>0.67%</td>
</tr>
<tr>
<td>Coinbase</td>
<td>272k</td>
<td>0.60%</td>
</tr>
</tbody>
</table>
3.5 Miners

Bitcoin miners verify and validate the bitcoin transactions on the network and then record these transactions on the Blockchain public distributed ledger. In this process, new bitcoins are created, which are awarded to miners in the form of block rewards. In order to add new blocks to the blockchain, miners have to solve a problem that requires high computing power and time. Miners ensure the safety and security of the bitcoin network by authorizing valid transactions and rejecting invalid transactions.

Miners employ hardware known as Application Specific Integrated Circuits or ASICs\textsuperscript{87} that can perform computations. By doing so, miners increase their chances of earning the block reward. When Satoshi Nakamoto proposed the decentralized electronic cash system, he envisioned a system where any individual with a computer could participate in the mining process. Even though theoretically it is still possible to participate in mining with normal computers, it is not profitable to do so. A traditional CPU can perform less than 10 Mega-hashes/Sec; whereas, ASICs can perform 500 Giga-hashes/Sec\textsuperscript{88}. The difficulty level of the bitcoin network in 2015 was 586, 372, 584 Giga-hashes/Sec\textsuperscript{89}, which made it nearly impossible for an individual to earn bitcoins. To put this in perspective, in 2015 the entire computing power of the bitcoin network was 525 times the computing power used to maintain all of the products and services of Google\textsuperscript{90}.

If a miner (individual or a company) operates independently, he or she must match the hashing rates of the network and solve the computational problem faster than other nodes on the network. At that point, other network nodes should accept the block. Miners use different strategies to increase the probability of receiving block rewards. One strategy is to form groups known as mining pools to share
the resources as well as profits from mining. These mining pools collectively try to solve the computational problem by using shared resources. The rewards are shared based on the computations performed to solve the problem. Mining pools increase the probability of getting the reward because they use greater computational power. GHash.io, F2Pool, AntPool are examples of mining pools that mined on the bitcoin network as of 2015. See Figure 3.3 for various mining pools and companies.

Miners influence the adoption of bitcoin among other stakeholders by maintaining the security of the network.

Figure 3.3: Bitcoin mining ecosystem
3.6 Payment Processors

Payment Processors are companies that work with businesses and organizations that accept bitcoin as a payment option. Payment Processors provide the necessary infrastructure that enables bitcoin transactions to occur. Payment processors earn revenues by charging commission fees on the transactions that they execute. Some examples of bitcoin payment processors include Coinbase and BitPay. In 2015, Coinbase worked with more than 41,000 businesses and organizations to enable bitcoin as a payment option. In that same year, BitPay worked with more than 60,000 businesses to enable bitcoin as a payment option.

Payment processors shield merchants from bitcoin's volatility. Volatility in bitcoin discourages merchants accepting transactions in bitcoin because the percentage change in currency can be greater than the profit spread, resulting in a net loss for the transaction. Payment processors solve this problem by offering services that convert the bitcoin currency immediately to fiat currencies, thereby reducing the risk.

Payment processors increase the value of bitcoin by enabling merchants to accept bitcoin as a payment option; the more merchants that accept bitcoin payments, the greater the transaction volume, which creates an increase in bitcoin.
3.7 Regulators

Bitcoin regulators provide guidelines for the businesses to operate to protect the interests of the consumers and to eliminate criminal activities. Regulators for traditional currencies control the money supply to the market and provide guidelines for businesses that offer services to customers, such as banks. Regulators for cryptocurrencies do not control the money supply to the market; however, regulators do provide guidelines for businesses offering customer services, such as wallet and mining companies.

Bitcoin regulations are different in different countries because bitcoin is a global currency. For the purposes of this thesis, only bitcoin regulations in the United States are presented.

- In 2013, US Department of Treasury’s Financial Crimes Enforcement Network (FinCEN) issued guidance on the compliance obligations of virtual currencies under the federal bank secrecy act (SBA). Because bitcoin and other digital currencies were not legal tender under any sovereign jurisdiction, they were classified as virtual currencies. FinCEN also provided clarification on who needs to register as money service businesses (MSBs). According to FinCEN regulation, bitcoin users who use bitcoin solely for transactions are not required to register as MSBs, but Miners and Exchanges are required to register as MSB. MSBs are responsible for recordkeeping and should report large transactions, suspicious activity, comply with the money laundering regulations and collect information about customers as traditional financial institutions are required to do.

- In 2014, New York became the first state in United States to propose a regulatory framework for virtual currencies called ‘BitLicense’. Benjamin Lawsky, superintendent for New York’s
Department of Financial Services communicated that the goals of these regulations were to ensure customer asset protection, root-out illegal activity and at the same time foster innovation in the virtual currency community. The regulation also mandated that all businesses in the virtual currency space should educate customers on the risks associated with Bitcoins and should provide high security to protect the assets of the customers from hackers.

Companies in the bitcoin community had mixed reactions to new regulations. Some companies that felt it was important to work with regulators for their long-term success did apply for licenses. Circle, a wallet service provider, became the first company to receive a BitLicense from the New York State Department of Financial Services. However, companies such as Shapeshift, GoCoin, and BitQuick shutdown their operations in New York after the creation of new regulatory framework in New York because they felt that collecting customer information was against the privacy norms of bitcoin.

Regulators that exist in the bitcoin ecosystem environment can influence the dynamics of bitcoin ecosystem when they impose legal and other constraints on the bitcoin network participants. Regulators are an important environmental – or indirect – influencer of the bitcoin ecosystem.

3.8 Venture Capitalists

Venture capitalists invest in bitcoin-related startups. Venture capital investments in bitcoin-related startups grew steadily since early 2012. By Oct 2015, the venture capital funding in cryptocurrency-related startups was close to 1 billion USD (927.36 million USD). Venture capital investments were not specific to a particular region; investments were spread across multiple continents. Influential
companies in the venture capital community, such as Andreessen Horowitz and Khosla Ventures have significant investments in bitcoin-related startups. Marc Andreessen, co-founder of Andreessen Horowitz, was one of the early investors and supporters of Bitcoin and Blockchain technology. His firm invested approximately 50 million USD in Bitcoin-related startups. Traditional financial services companies such as Visa, NASDAQ, Goldman Sachs, and Capital One also invested in bitcoin-related startups through their venture capital arms. Please refer to Figure 3.4 and Figure 3.5 for venture capital investments in cryptocurrencies by year and by region respectively.

Venture capitalists indirectly influence the bitcoin ecosystem by inspiring innovation. Venture capital investments provide financial support to companies offering services such as wallets, payment processors, exchanges, and mining.

Figure 3.4: Venture Capital Investments in cryptocurrencies by year
3.9 Bitcoin Developers

Bitcoin is an open-source project whereby any individual in any part of the world can contribute. Bitcoin developers improve the bitcoin protocol by adding new features, such as “Multi-Sig Transaction Distribution[100]. The source code of bitcoin is openly available, and the Bitcoin Core software is released under an MIT License[101]. Communication among bitcoin developers happens via bitcoin IRC channels[102] and on a development and technical forum[103]. Developers propose changes through these
platforms, which are called Bitcoin Improvement Proposals (BIPs)\textsuperscript{104}. Once the open-source community accepts these BIPs, core developers\textsuperscript{105} pull changes to the Bitcoin Core.

Bitcoin developers indirectly influence adoption of bitcoin among various stakeholders. Bitcoin developers create trust among stakeholders such as users, merchants and service providers to use bitcoin as a currency and payment system by supporting legitimate, respected development processes that are decentralized, transparent and open.
Chapter 4: Multi-Sided Platforms

The previous chapter described the stakeholders of bitcoin and their influences on bitcoin. This chapter presents a literature review of multi-sided platforms, which represents a concept that will be used in the next chapter to explain bitcoin’s success as a cryptocurrency.

4.1 Introduction

Multi-sided platforms are technologies, products or services that enable interactions between two or more participant groups to create value\textsuperscript{106}. Some of the fastest growing businesses of the last decade have used multi-sided platforms as a core component of their business models. An example of a multi-sided platform company is Airbnb. Airbnb has over 1.5 million accommodation listings in 34,000 cities and 190 countries\textsuperscript{107}. The company is valued at over 20 billion USD. Airbnb does not own real estate in the countries in which it operates; instead, it provides a platform for interaction between people who want to host and people who want to rent. The success of multi-sided platforms is primarily dependent on the interactions between various participants of the network.

In the following sections, a literature review of platforms and multi-sided platforms is presented.
4.2 Platforms

Platforms are reusable components which can be used to produce products of different variety. "A platform is a set of subsystems that form a common structure from which a stream of derivative products can be efficiently developed and produced".108 Reusability and customization are key characteristics of platforms.109

Platforms can be used by companies that make physical or intangible products. An example of a company that produces physical products is Ford. During the second industrial revolution, Henry Ford, the renowned automobile manufacturer, revolutionized the automobile manufacturing by using platforms. A classic platform example was the Ford Model T. Ford released eleven different models (i.e., Touring, Touring Fore-door, Runabout, Commercial Runabout, Coupe, Town, Tourster, Torpedo, Coupe' let, Sedan 4-door and Tudor) that were based on the Model T. "The Model T's overall underbody was common, including the engine, pedals, switches, suspensions, wheels, transmission, gas tank, steering wheel, lights"110, representing platform reusability. Each derivative product had a different body, signifying platform customization.

An example of a company making intangible products is Microsoft. Microsoft's windows operating system is used in personal computers, laptops, smartphones, and tablets, signifying platform reusability.111 Different products in each product line signify platform customization. For example, Lumia 950 and Lumia 550 are two smartphones that run on the same windows operating system112.
Companies create platforms for two primary reasons:

- Platforms help companies improve the speed of production because it reduces the amount of testing of products that is needed for different models using the same platform. This ultimately reduces the overall costs required to manufacture the product\textsuperscript{113}.
- Companies employing platforms will be in a better position to offer more product options to the customers. This can be observed in the Ford’s strategy of offering of multiple products that are based on the model T platform.

Companies face several challenges when creating successful platforms.

- Companies must decide “which market segments to enter, what the customers in each segment want, and what product attributes will appeal to those customers\textsuperscript{114}” because, these decisions influence the investments and resources needed to build the platform. These represent difficult decisions because they involve uncertainty and trade-offs.
- Platforms require coordination among various organizational entities, such as engineering, marketing, design and manufacturing in order for a company to build a strong underlying platform architecture\textsuperscript{115}. Because different departments have unique priorities, this coordination can be challenging.

The platforms described above focus on reusability and customization to offer better product variety derived from the common platforms. These platforms help companies develop internal capabilities such as efficient and reconfigurable manufacturing processes. In the next section, multi-sided platforms are introduced; these offer value by reducing the transaction costs for its external participant groups\textsuperscript{116}.
4.3 Multi-Sided Platforms

Multisided platforms (MSPs) are technologies, products or services that enable direct interactions between two or more customer or participant groups to create value. By enabling interactions between multiple participant groups, these platforms create 'network effects'. A network effect is the effect that one user of a product has on the value of that product to other people.

Multi-sided platforms are explained in detail below using Facebook as an example. As of 2015, Facebook represented the largest social networking website, with a market capitalization of more than 300 billion USD. At that time, Facebook had more than 1 billion monthly active users on its network. Content providers and game or app developers are other participants on the Facebook platform.

![Figure 4.1: Facebook as a multi-sided platform](image-url)
Facebook facilitates interactions among users, advertisers, and content creators. Users use Facebook to connect with friends and family on the social networking platform. As a user connects with more friends on Facebook, Facebook becomes more valuable to the user because it is easier for users to communicate with all of the people who matter to them. Network effects that are created through the direct interaction between a platform such as Facebook and one of its participants such as users are called 'direct network effects' or 'same-side network effects'. These interactions are highlighted in green in Figure 4.1.

The other key participant groups on the Facebook platform are advertisers and content creators. The goal of advertisers is to raise awareness of their brands. Advertisers generate revenues by selling their products to customers. The primary goal of content creators is to create content that is widely consumed. Content creators earn revenues by charging customers directly or through advertising revenues. Both advertisers and content creators require a large user base that will consume their advertisements and content. Facebook solves this problem by providing its user network.

Facebook creates network effects among its various participants groups such as users and advertisers, advertisers and content creators and users and content creators. These network effects are called 'indirect network effects' or 'cross side network effects' because they do not interact with the platform directly. Users consume advertisements and buy products of advertisers. Advertisers use the content to display advertisements to users. Users consume the content to interact with other users or to gain knowledge. These activities increase the value of the entire platform and also of the individual participants. These interactions are highlighted in blue in Figure 4.1.
4.3.1 Factors influencing the success of MSPs

In this section, some of the key factors that influence the success of multi-sided platforms, such as network effects, pricing and switching costs are described in detail.

Network effects:

Network effects are the effects that one user of a product has on the value of that product to other people\(^2\). Network effects drive adoption of a platform among its participant groups. Network effects increase adoption of platforms exponentially because new participants increase the value for existing participants.

Multi-sided platforms create strong network effects by:

- Offering direct value to the participant groups in order to encourage platform adoption.
- Offering indirect value to the participant groups by enabling interactions among the participant groups. It should be more valuable for the participant groups to interact through the platform than to interact directly.

Multi-sided platforms address this value exchange by offering solutions to the business problems of the participant groups and by making it cost-effective, convenient, or easy to participate on the platform.

For example, Uber is a multi-sided platform with strong network effects. Uber creates network effects by offering on-demand taxis for riders and customers for drivers. Uber offers

- For riders,
  - Easy means to hail a taxi using its mobile platform.
- Improved predictability of taxi arrival.
- Better ride experience as the payments are made through mobile app.
- Better fares compared to traditional taxis.

- For drivers,
  - Better predictability in finding customers.
  - Costs savings in taxi medallions.

It is more profitable for riders and drivers to interact through the Uber platform than interacting directly. Without Uber, riders have to make reservations by calling taxis or wait on roads to hail a taxi. When making a reservation, a rider has no guarantee that the taxi will arrive in time. For drivers, there is no predictability on the potential customers. Drivers have to be on move continuously looking for customers, which is not efficient and which incurs fuel costs. Moreover, taxi drivers have to deal with taxi medallions, which cost hundreds of thousands of dollars.

In sum, network effects increase the overall value of the platform by driving the adoption of the platform among the participant groups. As more users use the platform, there is greater opportunity for platforms to generate more revenues from the participant groups.

**Pricing:**

Pricing in multi-sided platforms refers to subsidizing or offering free services to some participant groups and charging other participant groups of the platform. Multi-sided platforms use pricing structures:

- To coordinate the demand on the platform among various participant groups and
To generate revenues\textsuperscript{126} from one or more participant groups of the platform.

For example, Lyft, a competitor of Uber, coordinates the demand for its platform by offering incentives to users with credits worth 50 USD for new users\textsuperscript{127} and referral bonuses up to 500 USD for new drivers. This helps Lyft increase the volume of drivers and riders on its platform. Lyft does not charge its users for using the mobile app platform and for connecting with drivers. Instead, Lyft generates revenues by charging drivers a commission fee of the total ride value. To sustain in the long run, platforms such as Lyft must generate profits higher than that of the incentives and subsidies offered on the platform. For multi-sided platforms, it is recommended to have pricing structures that drive the adoption of platforms among the participant groups and that result in sustained profits.

**Switching costs:**

'Switching costs' refer to the costs incurred by users to abandon a multi-sided platform and switch to a competing multi-sided platform\textsuperscript{128}. A classic example of a MSP with high switching costs for users is Facebook. Switching costs for users on Facebook is high because the users need to migrate their full network of connections to a different platform to equal Facebook's value.

High switching costs discourage participant groups of the platform to adopt competing platforms. Multi-sided platforms create high switching costs by offering unique services that differentiate themselves from the competitors as described in the Facebook example.
Chapter 5: Discussion

The previous chapter introduced the concepts of platforms and multi-sided platforms. This chapter uses the multi-sided platform literature to help explain why bitcoin is the most successful cryptocurrency to date.

Bitcoin is the most successful cryptocurrency to date, as evidenced by the following:

- The market capitalization of bitcoin is approximately 6.4 billion USD as of December 31, 2015. This is more than 90% of the total cryptocurrencies market capitalization\(^\text{129}\).
- Bitcoin has the highest average transaction volume per hour (6,517) of all cryptocurrencies. Dogecoin has the next highest transaction volume per hour (808)\(^\text{130}\). Dogecoin has approximately 12% of Bitcoin's average transaction volume.
- More than 100,000 businesses accept bitcoin as a payment option\(^\text{131}\).
- Bitcoin has the highest amount of venture capital investments when compared to other cryptocurrencies\(^\text{132}\).

The reason for bitcoin's success is explained below. My thesis research identified that bitcoin's success is rooted in its ability to become an effective multi-sided platform. In Figure 5.1, bitcoin is represented as a multi-sided platform with same-side network effects in green and cross-side network effects in blue.
Bitcoin is a multi-sided platform with strong network effects.

Bitcoin has three participant groups:

- Bitcoin users who use bitcoin as a payment option to transfer money to other users on the network and to buy goods and services over the internet.
- Merchants who accept bitcoin as a payment option.
- Service providers such as payment processors, wallet providers, exchanges and miners who help users and merchants in bitcoin transactions.
Other stakeholders such as Venture Capitalists, Regulators and Bitcoin developers are not included in the below multi-sided platform discussion because they do not directly contribute to bitcoin transactions. Please refer to chapter three to understand the roles of Venture Capitalists, Regulators, and Bitcoin developers.

5.1 Network Effects

Bitcoin has been the most successful cryptocurrency because of its ability to create strong network effects among its participant groups. Bitcoin created value for its participant groups by solving existing problems for some of them. Bitcoin solved user and merchant problems by offering an alternate low-cost payment option. Before bitcoin, traditional payment companies, such as Visa and MasterCard charged 2-5% of the total transaction value as transaction fees.

Bitcoin offered new business opportunities for other participant groups – for example, mining and wallets. Bitcoin miners verify the transactions on the network and maintain the security of the network. Miners earn revenue through block rewards and transaction fees. Wallet service providers offer key management services to individual and enterprise customers.

Network effects drive exponential adoption of platforms as described in chapter 4. The network effects of the bitcoin platform are evident from the below facts:

- The transaction volume of bitcoin increased continuously (refer to Figure 5.2) due to:
  - Increase in transactions among users.
  - Increase in transactions between users and merchants.
- Increase in the number of businesses accepting bitcoin as a payment option. Currently, there are more than 100,000 businesses accepting bitcoin as a payment option\textsuperscript{134}.

- Increase in the number of service providers such as wallets, miners, payment processors and exchanges (refer to Figure 5.3\textsuperscript{135}). This can be observed from the below chart, which represents the service provider companies founded each year.
5.2 Pricing

Bitcoin coordinates its platform demand across various participant groups using a portfolio of different pricing strategies. Bitcoin directly incentivizes miners on the network by paying block rewards when miners verify bitcoin transactions. Miners also receive transaction fees.

Other service providers such as wallets, payment processors, and exchanges, receive no direct incentives from the bitcoin platform. However, bitcoin offers revenue-generating opportunities through transaction fees for wallets, payment processors, and exchanges. Because the cost structures associated

---

1 Only startups with at least one round of funding are considered. Startups in 2015 are not considered for this reason. A startup may be working on more than one cryptocurrency.
with bitcoin are less as compared to traditional payment systems, service providers can charge small transaction fees and still earn a profit.

The other participant groups such as users and merchants enjoy low transaction fees as compared to fees associated with other payment options.

5.3 Switching costs

Switching costs for participant groups of bitcoin are high because it requires other participant groups' to adopt the competing platforms to match the value they receive from the bitcoin platform. Cryptocurrencies other than bitcoin do not yet have a strong network of users, merchants, and service providers. This is evident from the transaction volume of the other cryptocurrencies. Low transaction volumes also indicate low interaction among the participant groups.
Chapter 6: Conclusion

6.1 Conclusion

My thesis research suggests that bitcoin is the most successful cryptocurrency to date and that it will continue to be the most successful cryptocurrency because of its strong network effects. Further, bitcoin is a technological innovation that has applications beyond the financial services industry – the idea of tracking ownership and creating trust among various participants without any central authority has myriad applications. Bitcoin introduced a new record management system that is open yet secure; these capabilities can have diverse applications such as smart contracts, identity management, healthcare record management, and property title management.

The key will be identifying the use cases that can disrupt incumbent models. Bitcoin introduced us to borderless payments that are more fast, secure, and cost-effective than other payment systems. Borderless payments offered direct benefits to bitcoin users and merchants, and it rapidly drove adoption. A new use case such as healthcare record management must offer similar direct value to patients and doctors. The value can manifest as cost savings, convenience, privacy and/or security. If such a new platform can create sufficient network effects, adoption will increase exponentially; otherwise, it is likely to fail.
6.2 Limitations

This thesis uses the multi-sided platforms literature and supporting quantitative bitcoin performance data to describe why bitcoin is the most successful cryptocurrency to date. One limiting factor for the thesis is the availability of better quality quantitative bitcoin performance data. For example, in this thesis, transaction volume represents the interaction between users and merchants. The growing number of merchants is used to determine merchant adoption, but a better data source would be the volume of transactions in dollars, or percentage of bitcoin transactions relative to total transactions. For users, the growing number of wallets is used to determine the user adoption, but there is no way to confirm if new wallets actually contribute to transaction volume.

6.3 Future research

Bitcoin is the first application of a new technology that allows for a decentralized and secure record keeping system. The new technology can have applications in different industries. This topic can be explored in future research that identifies different use cases and execution strategies that deliver value.
### Table A.1: Bitcoin generation

Bitcoin's supply to market reaching 21 million (End BTC column).

<table>
<thead>
<tr>
<th>Block</th>
<th>BTC/block</th>
<th>Start BTC</th>
<th>BTC Added</th>
<th>End BTC</th>
<th>BTC Increase</th>
<th>End BTC % of Limit</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>50</td>
<td>0</td>
<td>10500000</td>
<td>1050000</td>
<td>infinite</td>
<td>50.00%</td>
</tr>
<tr>
<td>210000</td>
<td>25</td>
<td>10500000</td>
<td>5250000</td>
<td>1575000</td>
<td>50.00%</td>
<td>75.00%</td>
</tr>
<tr>
<td>420000</td>
<td>12.5</td>
<td>15750000</td>
<td>2625000</td>
<td>1837500</td>
<td>16.66666666700%</td>
<td>87.50%</td>
</tr>
<tr>
<td>630000</td>
<td>6.25</td>
<td>18375000</td>
<td>1312500</td>
<td>1968750</td>
<td>7.1428571400%</td>
<td>93.75%</td>
</tr>
<tr>
<td>840000</td>
<td>3.125</td>
<td>19687500</td>
<td>656250</td>
<td>2034375</td>
<td>3.3333333300%</td>
<td>96.88%</td>
</tr>
<tr>
<td>1050000</td>
<td>1.5625</td>
<td>20343750</td>
<td>328125</td>
<td>2067185</td>
<td>1.6129032300%</td>
<td>98.44%</td>
</tr>
<tr>
<td>1260000</td>
<td>0.78125</td>
<td>20671875</td>
<td>164062.5</td>
<td>20835937.5</td>
<td>0.7936507900%</td>
<td>99.22%</td>
</tr>
<tr>
<td>1470000</td>
<td>0.390625</td>
<td>20835937.5</td>
<td>82031.25</td>
<td>20917968.75</td>
<td>0.3937007900%</td>
<td>99.61%</td>
</tr>
<tr>
<td>1680000</td>
<td>0.1953125</td>
<td>20917968.75</td>
<td>41015.625</td>
<td>20958984.38</td>
<td>0.1960784300%</td>
<td>99.80%</td>
</tr>
<tr>
<td>1890000</td>
<td>0.09765625</td>
<td>20958984.38</td>
<td>20507.8125</td>
<td>20979492.19</td>
<td>0.0978473600%</td>
<td>99.90%</td>
</tr>
<tr>
<td>2100000</td>
<td>0.04882812</td>
<td>20979492.19</td>
<td>10253.9052</td>
<td>20989746.09</td>
<td>0.0488758500%</td>
<td>99.95%</td>
</tr>
<tr>
<td>2310000</td>
<td>0.02441406</td>
<td>20989746.09</td>
<td>5126.9526</td>
<td>20994873.05</td>
<td>0.0244259900%</td>
<td>99.98%</td>
</tr>
<tr>
<td>2520000</td>
<td>0.01220703</td>
<td>20994873.05</td>
<td>2563.4763</td>
<td>20997436.52</td>
<td>0.0122100100%</td>
<td>99.99%</td>
</tr>
<tr>
<td>2730000</td>
<td>0.00610351</td>
<td>20997436.52</td>
<td>1281.7371</td>
<td>20998718.26</td>
<td>0.0061042600%</td>
<td>99.99%</td>
</tr>
<tr>
<td>2940000</td>
<td>0.00305175</td>
<td>20998718.26</td>
<td>640.8675</td>
<td>20999359.13</td>
<td>0.0030519400%</td>
<td>100.00%</td>
</tr>
<tr>
<td>3150000</td>
<td>0.00152587</td>
<td>20999359.13</td>
<td>320.4327</td>
<td>20999679.56</td>
<td>0.0015259200%</td>
<td>100.00%</td>
</tr>
<tr>
<td>3360000</td>
<td>0.00076293</td>
<td>20999679.56</td>
<td>160.2153</td>
<td>20999839.77</td>
<td>0.0007629400%</td>
<td>100.00%</td>
</tr>
<tr>
<td>3570000</td>
<td>0.00038146</td>
<td>20999839.77</td>
<td>80.1066</td>
<td>20999919.88</td>
<td>0.0003814600%</td>
<td>100.00%</td>
</tr>
<tr>
<td>3780000</td>
<td>0.00019073</td>
<td>20999919.88</td>
<td>40.0533</td>
<td>20999959.93</td>
<td>0.0001907300%</td>
<td>100.00%</td>
</tr>
<tr>
<td>Value</td>
<td>Percentage</td>
<td>Value</td>
<td>Percentage</td>
<td>Value</td>
<td>Percentage</td>
<td>Value</td>
</tr>
<tr>
<td>--------</td>
<td>------------</td>
<td>--------</td>
<td>------------</td>
<td>--------</td>
<td>------------</td>
<td>--------</td>
</tr>
<tr>
<td>3990000</td>
<td>0.00009536</td>
<td>20999959.93</td>
<td>20.0256</td>
<td>20999979.96</td>
<td>0.0000953600%</td>
<td>100.00%</td>
</tr>
<tr>
<td>4200000</td>
<td>0.00004768</td>
<td>20999979.96</td>
<td>10.0128</td>
<td>20999989.97</td>
<td>0.0000476800%</td>
<td>100.00%</td>
</tr>
<tr>
<td>4410000</td>
<td>0.00002384</td>
<td>20999989.97</td>
<td>5.0064</td>
<td>20999994.98</td>
<td>0.0000238400%</td>
<td>100.00%</td>
</tr>
<tr>
<td>4620000</td>
<td>0.00001192</td>
<td>20999994.98</td>
<td>2.5032</td>
<td>20999997.48</td>
<td>0.0000119200%</td>
<td>100.00%</td>
</tr>
<tr>
<td>4830000</td>
<td>0.00000596</td>
<td>20999997.48</td>
<td>1.2516</td>
<td>20999998.73</td>
<td>0.0000059600%</td>
<td>100.00%</td>
</tr>
<tr>
<td>5040000</td>
<td>0.00000298</td>
<td>20999998.73</td>
<td>0.6258</td>
<td>20999999.36</td>
<td>0.0000029800%</td>
<td>100.00%</td>
</tr>
<tr>
<td>5250000</td>
<td>0.00000149</td>
<td>20999999.36</td>
<td>0.3129</td>
<td>20999999.67</td>
<td>0.0000014900%</td>
<td>100.00%</td>
</tr>
<tr>
<td>5460000</td>
<td>0.00000074</td>
<td>20999999.67</td>
<td>0.1554</td>
<td>20999999.83</td>
<td>0.0000007400%</td>
<td>100.00%</td>
</tr>
<tr>
<td>5670000</td>
<td>0.00000037</td>
<td>20999999.83</td>
<td>0.0777</td>
<td>20999999.91</td>
<td>0.0000003700%</td>
<td>100.00%</td>
</tr>
<tr>
<td>5880000</td>
<td>0.00000018</td>
<td>20999999.91</td>
<td>0.0378</td>
<td>20999999.94</td>
<td>0.0000001800%</td>
<td>100.00%</td>
</tr>
<tr>
<td>6090000</td>
<td>0.00000009</td>
<td>20999999.94</td>
<td>0.0189</td>
<td>20999999.96</td>
<td>0.0000000900%</td>
<td>100.00%</td>
</tr>
<tr>
<td>6300000</td>
<td>0.00000004</td>
<td>20999999.96</td>
<td>0.0084</td>
<td>20999999.97</td>
<td>0.0000000400%</td>
<td>100.00%</td>
</tr>
<tr>
<td>6510000</td>
<td>0.00000002</td>
<td>20999999.97</td>
<td>0.0042</td>
<td>20999999.97</td>
<td>0.0000000200%</td>
<td>100.00%</td>
</tr>
<tr>
<td>6720000</td>
<td>0.00000001</td>
<td>20999999.97</td>
<td>0.0021</td>
<td>20999999.98</td>
<td>0.0000000100%</td>
<td>100.00%</td>
</tr>
<tr>
<td>6930000</td>
<td>0</td>
<td>20999999.98</td>
<td>0</td>
<td>20999999.98</td>
<td>0.0000000000%</td>
<td>100.00%</td>
</tr>
</tbody>
</table>
References

14 “Proof-of-Stake - Wikipedia, the Free Encyclopedia.”
15 “What Is the Difference Between Litecoin and Bitcoin?”
17 “What Is the Difference Between Litecoin and Bitcoin?”
21 “Bitcoin Venture Capital Funding.”

“Bitcoin-papers/BitcoinGlossary.md at Master · Oleganza/bitcoin-Papers · GitHub.”


“Block Hashing Algorithm - Bitcoin Wiki.”


“Developer Guide - Bitcoin.”

“Greeks Can Only Get $67 From ATMs; Banks Shut for Week.”


“BitCoin vs. Visa - Transaction Fees - TabletsandTech.com.”

“Transaction Fees - Bitcoin Wiki.”


“Certs.media.mit.edu,” accessed December 2, 2015, https://certs.media.mit.edu/8ca9cad234bdc2136532072e4a01b4898d45ef128d0cec499e76903787b9430d.


“Crypto-Currency Market Capitalizations.”


“Digital Currency Exchanger - Wikipedia, the Free Encyclopedia.”


“How to Set up a Bitcoin Miner.”


“Coinbase - Buy and Sell Bitcoin.”

“BitPay – Accept Bitcoin.”

“Crypto-Currency Market Capitalizations.”


“History of Bitcoin.”


“Bitcoin Improvement Proposals - Bitcoin Wiki.”


113 Robertson and Ulrich, “Planning for Product Platforms.”
114 Robertson and Ulrich, “Planning for Product Platforms.”
115 Robertson and Ulrich, “Planning for Product Platforms.”
116 “Strategic Decisions for Multisided Platforms.”
117 “Strategic Decisions for Multisided Platforms.”
121 Gawer and Cusumano, “Industry Platforms and Ecosystem Innovation.”
122 Gawer and Cusumano, “Industry Platforms and Ecosystem Innovation.”
123 “Network Effect - Wikipedia, the Free Encyclopedia.”
126 “Strategic Decisions for Multisided Platforms.”
128 “Strategic Decisions for Multisided Platforms.”
130 “Bitcoin, Litecoin, Namecoin, Dogecoin, Peercoin, Quarkcoin, Worldcoin Stats.”
131 “Coinbase - Buy and Sell Bitcoin”; “BitPay – Accept Bitcoin.”
132 “Bitcoin Venture Capital Funding.”
134 “BitPay – Accept Bitcoin”; “Coinbase - Buy and Sell Bitcoin.”
135 “Bitcoin Venture Capital Funding.”

Karthic Prasad Kosgi | MIT SDM 2016
136 “Bitcoin, Litecoin, Namecoin, Dogecoin, Peercoin, Quarkcoin, Worldcoin Stats.”