**The Rise of Blockchain: A Deep-Dive into the Bitcoin Transaction World and the Ethereum Revolution**

By:

Sarosh Petkar

Committee Members:

Committee Chair: Jonathan Weissman

Advisory Board: Garret Arcoraci

In partial fulfillment of the requirements for the degree of

Master of Science in Computing Security

Rochester Institute of Technology

B. Thomas Golisano College of Computing & Information Sciences

Department of Computing Security

November 27, 2017

The Rise of Blockchain: A Deep-Dive into the Bitcoin Transaction World and the Ethereum Revolution

Author: Sarosh Petkar

Committee Chair: Jonathan Weissman

Advisory Board: Garret Arcoraci

Department of Computing Security, Rochester Institute of Technology

*ABSTRACT*

*In early 2009, the first block of Bitcoin was mined thereby, launching the world’s first cryptocurrency and since then, Bitcoin has grown over $10 billion in market capitalization.*

*Bitcoin’s rise has been spectacular. Its price has soared up almost thirty-fold. The rise in Bitcoin’s value signifies the speculation around its future value: The currency will have a long-term value as long as it is accepted as medium of exchange and value store. However, in current times, it is difficult to accept Bitcoin as a real currency due to its extreme volatility.*

*Furthermore, although the supply of individual cryptocurrencies is limited, their aggregate supply is still unlimited, as new cryptocurrencies seem to be created almost every month. At the same time, financial institutions are creating their own private cryptocurrencies to rival public cryptocurrencies like Bitcoin. [5]*

*While Bitcoin and other such cryptocurrencies have tremendous potential and value as a medium of exchange, it is the underlying distributed ledger technology, namely blockchain, which has emerged to truly capture the interest of entrepreneurs, venture capital firms, financial institutions and other corporations. [8]*

*A blockchain is defined as a list or a decentralized ledger of all transactions that takes place in a P2P network. In its purest form, it is a digital platform that aids in the handing over and verification of transactions in an open and tamper-free and revision-proof manner. Bitcoin, invented by Satoshi Nakamoto as the first blockchain application, became the first major digital currency in the world. Bitcoin’s successful application of blockchain technology as a cryptocurrency spawned a new wave of innovation within the blockchain environment. One of which is Ethereum, a platform that enables developers to develop a decentralized application to run on the blockchain. The platform is based on the concept of a smart contract, which is a piece of code that is stored on the blockchain, and executed by users via sending a transaction to the contract, the code is controlling. [30]*

*This project deals with the analysis of a bitcoin transaction with the security hat on, to understand what happens during a transaction between two parties. Furthermore, it will include an in-depth look into the Ethereum platform and how smart contracts are integrated into them.*

*The size and scope of applications are tremendous for blockchain technology, spanning a wide range of use cases in nearly every industry and thus such an undertaking will provide insight into that world. [25]*

Keywords: Blockchain, Ethereum, Bitcoin, smart contract

*Table of Contents*

[**I. INTRODUCTION**](#_od6drhuo3g44) **5**

[**II. PROJECT PROBLEM**](#_sby278pbqytm) **6**

[**III. LITERATURE REVIEW**](#_vs1imnt6nx7z) **6**

[**IV. PROJECT DESCRIPTION**](#_hr5y1u2bw6o7) **9**

[IV(a). Bitcoin](#_2q1h4hwcuj7e) 9

[IV(b). Ethereum](#_ukcnhky421rw) 25

[IV(c). Bitcoin vs Ethereum Comparison](#_2c1b16mxkg84) 36

[IV(d). The threat of Quantum Computing to Blockchain](#_c3vj7alkeor8) 39

[**V. CONCLUSION**](#_vmsvpwkn3j1w) **40**

[**VI. REFERENCES**](#_3tbpvmkaeg37) **42**

### 

*List of Figures and Tables*

Figure 1 - Inside a Bitcoin transaction ………………………………………………… 7

Figure 2 - Bitcoin transactional process ………………………………………………. 10

Figure 3 - Standard transaction to Bitcoin address ………………………………..… 12

Figure 4 - Bitcoin-qt client ………………………………………………………...……. 13

Figure 5 - Bitcoin blocks …………………………………………………..……………. 14

Figure 6 - Magic number ……………………………………………….………………. 14

Figure 7 - Blocksize …………………………………………………………..……...…. 15

Figure 8 - Block Header …………………………………………...…………...………. 15

Figure 9 - Transaction counter …………………………....…………………...………. 16

Figure 10 - List of transactions …………………………....…………………...………. 16

Figure 11 - Wireshark capture ………………………………..……………………...… 18

Figure 12 - Wireshark messages …………………………………….……………...… 18

Figure 13 - Bitcoin message structure ……………………....……………………...… 19

Figure 14 - Magic number and command field …………...………………………….. 19

Figure 15 - Message length …………………………………………………..……...… 19

Figure 16 - Bitcoin Version and other fields ……………………………...…………… 20

Figure 17 - Version ………………………………………………………….…………… 21

Figure 18 - Node services …………………………………………....…...…………… 21

Figure 19 - Remote node IP ………………………………………………...……..…… 21

Figure 20 - Block Start height …………………………………………...…..………… 21

Figure 21 - Hello World smart contract ………………………………...……...……… 28

Figure 22 - List of compilers …………………………………………...……….……… 29

Figure 23 - Smart contract deployment …………………………….……………….... 29

Figure 24 - Running the contract ……………………………………………...………. 29

Figure 25 - Smart Contract Kill Clause …………………………………….……….… 29

Figure 26 - Ethereum Platform Timeline …………………………….……..………… 34

Table 1 - Block Format Fields ……………………………………………...…………. 14

Table 2 - Block Header Fields ……………………………………………...…………. 15

Table 3 - Transaction fields …………………………………………………....………. 17

Table 4 - Message fields ………………………………………………………….……. 19

Table 5 - Version fields ……………………………………………………………....…. 20

Table 6 - Bitcoin vs Ethereum ……………………………………....…………………. 37

# *I. INTRODUCTION*

Throughout history, there are very few moments in time where there is an explosion of a new technology that tends to change the way that people live and do things. Many researchers believe that the world is on the cusp of another technological revolution and this change is being brought about by the rise of blockchain technology. This compendium presents a new technology, namely blockchain, wherein the key principle is its distributed nature and decentralization. Blockchain acts as a digital record of all data transfers on a network, updated chronologically, and distributed then sealed cryptographically. One of the important features of blockchain is the elimination of reliance on intermediaries present in the current digital economy. For example, in an environment where trust between parties can represent a weakness of a system, blockchain technology embraces the shift in power from one to many or from a central to a distributed relationship between entities.

The framework is a chain of blocks that collects a batch of timestamped transactions within the master ledger *(a global network of blockchains and self-governing nodes which stores data and executes transactions)* and is identified by a unique cryptographic signature. Each block refers to the unique signature of the block in the chain before it and therefore can be traced back to the first block ever created in the ledger. Thus, the blockchain contains an immutable record of all the transactions.

In the past, it was quite unimaginable to have transactions without having to trust a single central party. However, Bitcoin with the underlying blockchain technology has demonstrated that it is possible for two parties, who do not necessarily trust each other to perform important secure transactions without the aid of a central authority as an intermediary. Until recently, the blockchain technology has been primarily used in the crypto-currency sector, but now times have changed, and new potential areas have emerged. These include distributed storage and more importantly smart contracts, which extend the functionality of the blockchain and open avenues for new breakthroughs. [19]

Bitcoin, invented by Satoshi Nakamoto as the first blockchain application, incorporates such transactions as an integral part of their infrastructure. Since information about what occurs during a transaction is limited, this project will explore the process in detail to better understand it. Apart from Bitcoin, there are other platforms in play, such as Ethereum, it is a platform that enables developers to develop decentralized applications to run on the blockchain. The platform is based on the concept of a smart contract, which is a piece of code that is stored on the blockchain, and executed by users. [29]

Smart contracts can:

* Manage agreements between users.
* Have the ability to function as ‘multi-signature’ accounts, so that the funds can be transferred only when a certain percentage of the miners agree on it.
* Provide utility to other contracts.

# *II. PROJECT PROBLEM*

As all that glitters is not gold, similarly, the Bitcoin community as well as the Ethereum platform both face the issue of scalability but the first step at this juncture is to gain a complete understanding of what these two things are and what they are capable of and this requires a deep dive into the complex working of both these platforms. [29]

The goal of this project is two-fold:

1. Analyze what happens during a Bitcoin transaction to understand its inner workings.
2. To present an overview of the Ethereum platform and gain an understanding of how smart contracts work.

# *III. LITERATURE REVIEW*

Recently, Bitcoin and other cryptocurrencies have been all over the news, the furore over the topic compelled me to browse through a few articles on Forbes and other websites. Reading through those articles made me inquisitive about the inner-workings of this technology and motivated me to do conduct research on this topic. The biggest takeaway from those articles was the idea that it is important to see through the bubble around Bitcoin and focus on Blockchain -- this is where most experts think the future lies.

Blockchain is the new paradigm that is used as the core of various decentralized platforms. It is a data structure that can increase its size and be shared by different clients due to its peer-to-peer (P2P) architecture. It is structured as a chain of blocks (linked list) wherein each block has a set of instructions that it follows.

Blockchain is finding applications in wide range of areas: Banks can use blockchain to make quick, secure and low-cost transactions. It can also be used to put proof of existence on legal documents, health records, and loyalty payments in the entertainment industry and private securities*.*

Some of the benefits the blockchain technology provides are :

* Ownership of data
  + Possession of records and assets of any type can be proven.
* Uniqueness and proof of uniqueness.
  + The uniqueness of records and assets is guaranteed.
* Censorship resilient
  + Censorships or blocking access to data is not possible.
* Public transparency and traceability.
  + Everyone can see the content of the transactions and audit them.
* Trust-less and incorruptible
  + Allows building of trust-less systems and contracts that can be encoded without trusted parties.
* Guaranteed continuity
  + System continuity is guaranteed as long as nodes are present to run the chain.

As a result of the blockchain explosion, the original and starting revolutionary blockchain project that came to prominence was Bitcoin. Bitcoin per se is the ﬁrst Smart Contract ever developed. It is defined as a decentralized digital currency in order to produce a currency independent of any central authority with very low transaction fees. [15]

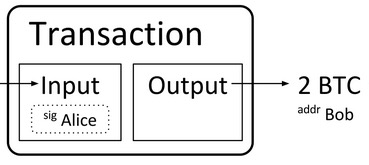
Technology-rooted movements like Bitcoin have demonstrated that through the power of consensus mechanisms and voluntary respect of contracts that it is possible to utilize the Internet to make a free to use decentralized value-transfer system. This system can be said to be a very specialized version of a cryptographically secure, transaction-based state machine.

More importantly, an integral aspect of Bitcoin is its transactions. Bitcoin transactions are classified as notes that are cryptographically signed that then have to undergo the process of verification by sending them out to the entire Bitcoin Network. All these transactions are done in the public domain and can be easily found on the digital ledger known as the blockchain.

An overview of a bitcoin transaction is represented below:

In the scenario that Alice wishes to transfer some bitcoins to Bob. Essentially, the bitcoin transaction would be comprised of three phases:

* **Input:** This is the actual record of the bitcoin address. Initially, the input is the location from where ‘Alice’ receives the bitcoin.
* **Quantity:** This is the specific quantity of Bitcoins (BTC) that Alice intends to send Bob.
* **Output:** This is referred to as Bob’s public key; essentially this is his ‘bitcoin address’.



*Figure 1: Inside a Bitcoin transaction [10]*

When it is said that someone “possesses bitcoins” what it actually means is that the person has access to a key-pair (2 keys) comprised of:

* Public key: Where some bitcoins were previously transferred.
* Private key: Authorizes that the BTC be sent to some other address.

The transaction takes place in such a manner that it is first broadcasted to everyone on the bitcoin network where a huge number of miners take turns to verify if Bob’s key has the ability to utilize the inputs that he claims to control. This process of confirming the identity is termed as ‘mining’ (also the process to create BTC) as it requires hardware and software intensive excavations/computations. The platform then in turn rewards these so called miners, in actual BTC, depending upon the number of blocks solved. [15]

While, Bitcoin is widely used as a successful decentralized ﬁnancial transaction system, various other platforms are trying to utilize other use cases in order to go beyond just the cryptocurrency. These platforms will thus enable numerous third-party projects to use such standards for data exchange. [27]

Another platform that is used to code, execute and share these kind of smart contracts, as a quasi- Turing complete program is Ethereum. Ethereum is a platform that attempts to build a technology on which all transaction based state machine concepts may be built. In slightly simpler terms, it aims to provide the end-developers a tightly integrated end-to-end system for building software on a trustful object framework. [31]

Some experts believe that bitcoins main objective is to disrupt popular services such as Paypal, Zelle, Venmo and other online banking systems, whereas it is suggested that ethereum’s goal is to use the blockchain technology to completely get rid of third parties on the Internet.

Using the example of cross-platform document-editing services like Evernote or Google Docs. With the use of Ethereum, the control of the data within these types of services will go back to its original owners in addition to handing over the creative power over to its author. This idea would lead to an environment where a single central entity will have to forfeit its control over to the user. In theory, it is an amalgamation of the past and the future, the past being that the user would have control over its data and the present ease-of-access that people desire. [1]

# *IV. PROJECT DESCRIPTION*

## IV(a). Bitcoin

*Origins*

Bitcoin’s was initially proposed in 2008 and its creation is credited to the inventor that goes by the alias of Satoshi Nakamoto, a man whose identity is still unknown. It is a open-source P2P technology that operates without a central authority wherein cryptocurrency (bitcoins) is issued collectively by the entire network.

The main principle behind the platform is decentralization (elimination of a central entity) and it works on the Proof of Work trust-based model. Within the trust model, in order for blocks to be created and added to the blockchain users are required to solve complex cryptographic problems. The Proof of Work (PoW) model is especially adept at providing increased security and validity during transactions. A trusted third party initially checks to see if the money is still available before allowing the transaction. [32]

The benefits of the model include:

* Protecting sellers from fraud by incorporating non-reversible transactions.
* Protecting buyers by having signed transactions.
* Entire transactional history is publicly available.
* Transactions can have multiple inputs and outputs.

*What are Transactions?*

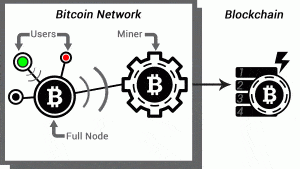
A transaction is a basic operation and a mechanism for spending currency in Bitcoin. It just does not simply move bitcoins from one address to another but does far more than that. In the network, all transactions take place with the aid of public keys that are owned by the users. Here, each user is entitled to use more than a single public key (stored in wallets).

Once a public key is used for a specific transaction, all of its related information is available for future analysis. [19]

*Prerequisite Understanding*

In order to send Bitcoins, a user needs a few things, namely a bitcoin client, bitcoin address, and a private key. The user obtains these bitcoins by purchasing it from an exchange, a prior transfer from an individual and finally by mining. The bitcoin address is a randomly generated alphanumeric sequence and the private key is the secret key only provided to a single user. A good analogy that is often used is that people must think of their bitcoin address’ as safety vaults. The vaults contents are precious and must remain secret hence only a private key in the possession of the user can be used to unlock it.

*Transactional Process*

**

*Figure 2: Bitcoin transactional process [26]*

1) Intention

User ‘A’ intends to buy some goods from user ‘B’ for 1BTC. In that case, user ‘A’ would send 1 bitcoin to ‘B’.

2) Broadcast

User ‘A’ then broadcasts the payment of 1 bitcoin to as many ‘Full Nodes’ (transaction-relaying wallet maintaining copy of blockchain) that are connected to user B’s wallet.

3) Propagation

Full nodes check for the integrity of user A’s transaction, they then broadcast the transaction across the entire network. At this stage the transaction has not yet been confirmed, this is where the miners play an important role.

4) Mining

Similar to full nodes, miners too have the ability to maintain a copy of the blockchain and as a result monitor the network. Miners compete against each other to complete the work in order to add the transaction to the block. Miners use the Proof of Work (PoW) mechanism to solve difficult computational problems. The more computer power in the possession of a miner the higher will be their hashrate and the greater will be their chances of solving problems quickly.

So how does mining work ?

The participants of the network form a consensus on the validity of the transaction and then aim to append it to the main block. But first, the transaction will be verified by the miners. This process involves the continuous computation of complex mathematical functions and is the principle that the security of the entire platform is built upon. The majority of the verification process is directed toward computing the complex SHA-256 hash. To solve a block, miners modify non-transactional data within the current block in a way that their hash result begins with a number of appended zeros and if the string was manually modified it would result in a 0. When more nodes/users are present the more difficult the hash gets, this is due to the fact that more zeros are prepended to create a race condition amongst miners. The entire purpose of mining is two-fold, verify and add new blocks to the main blockchain and secondly is to release new Bitcoins into the network.

Currently, the mining bounty is 25 BTC per block in addition to certain fees associated with the transactions within the block. In exchange for their effort, the miners are rewarded with transaction fees that is calculated using various methods. Some wallets allow for manual selection of transaction fees, whereas in some cases miners don’t even charge any fees for mining. One of the frustrating things about the fees is that it is not implemented strictly, as transactions without a fee will be given low priority by miners and may end up not being processed for many days or discarded completely. This entire process is termed as ‘mining’. Mining is very competitive and is an integral part of the security of the platform since it ensures that nobody can spam the system with malicious blocks.

5) Confirmation

The first miner that solves the block announces it to the entire network. After getting consensus on the completion of the work from the other full nodes, the new block is added to the blockchain. As soon as the block is recorded into the main blockchain, user A’s payment of 1 BTC goes through. User B can now feel secure to send over the items. However, it is good practice to wait for at least 5 such confirmations, as new blocks, when layered on top of the current block make it extremely difficult to reverse the transaction. All the transactions in a given block are considered to be verified once the specific block is followed by five other blocks, if this is not the case, then it is considered to be an ‘orphan block’. Within the orphan block, the transactions are added to another block and then go through the verification process again in order to be added to the main block. However, there is no incentive for miners to mine orphan blocks and hence it will be unused until five other blocks follow that block. [26]

*Transactional Process Summary and Special Cases*

The process takes approximately 10 minutes to complete and is composed of the following steps:

* 1. Assign the verifiable transactions to a block.
  2. Confirm sender’s private key.
  3. Confirm coins have not been exhausted.
  4. Repeat these steps for all transactions within that block.
  5. Calculate the hash (mine)
  6. Add the working block to the blockchain.

In the scenario that Alice wants to send bitcoins to Bob, she will utilize her private key (randomly generated 32-byte numbers) to sign the message along with the input (source address), output (recipient public key/address) and the amount (BTC). Bitcoins uses Elliptic Curve Digital Signature Algorithm (ECDSA) cryptography to generate a 64-byte public key, which is then hashed using SHA-256 and RIPEMD 160 algorithms. [23]

In certain cases, when Alice wants to send a specific amount such as 0.5 BTC to Bob but does not have the right number of bitcoins to add up to that amount then Alice will have to send one of the incoming transactions and the change will be returned to her. In such a case, she cannot split a transaction into smaller chunks. Hence, if Eve sent Alice 1 BTC then Alice will end up having two outputs of 0.5 BTC each. The first 0.5 BTC will go to Bob and then the second to a new escrow address which will eventually be returned to Alice. These transactions are not combined into one file inside the wallet but exist as separate transaction records.

*Related Information*

The Bitcoin scripting language

People might think that a Bitcoin transaction is signed by just including the signature into the transaction but it is far more complex. In reality, there is code within each transaction that gets executed to determine the transaction’s validity. The code is written in Bitcoin’s stack-based scripting language called ‘Script’, it does not contain any loops and is set to be Turing incomplete (A programming language is said to be Turing-complete if it can be shown to be computationally equivalent to a Turing machine). There are two scripts, the first is referred to as ‘scriptPubKey’ in the old transaction and ‘scriptSig’ in the new one. The Scriptpubkey is named so because it contains the public key whereas the scriptsig is named since it holds the private key.

To verify the transaction, the scriptSig is executed successfully followed by scriptPubKey otherwise the transaction is considered to be invalid. The motive of the scriptPubKey (puzzle) is that it defines the conditions for spending the currency whereas, scriptSig (solution) provides the data to satisfy the conditions.



*Figure 3: Standard transaction to Bitcoin address*

What is Elliptic Curve?

Elliptic curve is a curve that satisfies the equation *y2 = x3 + ax + b*. Moreover, Bitcoin uses a specific type of elliptic curve called ECDSA with the equation *y^2=x^3+7*. The ECDSA takes a hash and then performs ECC arithmetic using a combination of the actual message, the private key and a random number in order to generate a new point on the curve that will eventually supply the signature.

Why is RSA not used?

ECDSA offers the same level of security as RSA but with a much smaller footprint. In the scenario that more security is to be added, RSA keys can become more complicated and larger than ECDSA, and hence are not used by developers for the system that requires small packets to be sent around the network.

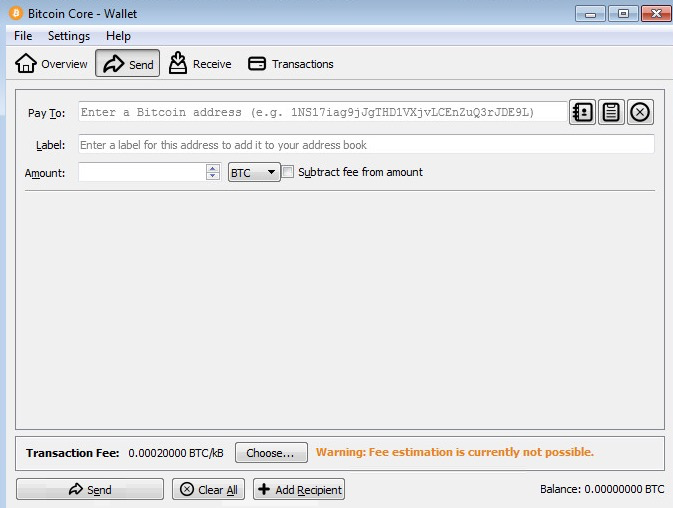
Note: Users with the public key, the message, and the signature can verify if the signature is valid. Whereas, only the user with the private key can sign a message.

*Analysis Approach*

To begin, it is important to study the outline of the Bitcoin block. The block is considered to be the basic building block of the protocol. It is crucial in creating more bitcoins and the addition of transactions to the block. As transactions are verified they are added to the ledger and each block contains the hash of the previous block thereby creating a pointer back to the parent block.

Experiment

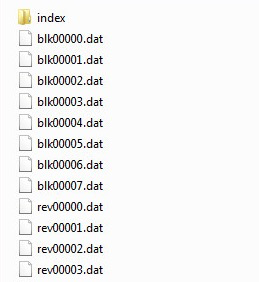
Install and launch the bitcoin-qt client on your machine. As the client is launched it will start downloading the blocks within the blockchain.



*Figure 4: Bitcoin-qt client*

These blocks are stored in

* **windows**: %APPDATA%\Roaming/Bitcoin
* **mac**: ~/Library/Application Support/Bitcoin/



*Figure 5: Bitcoin blocks*

Here, each and every *blk00\*.dat* file is a collection of several raw blocks that can be analyzed if desired.

Block Format

Each block is made to follow a well defined structure that begins with a magic number.

|  |  |  |
| --- | --- | --- |
| Field | Description | Size (bytes) |
| Magic number | Constant value | 4 |
| Blocksize | Size of the block | 4 |
| Block Header | Consists of version, time, nonce etc | 80 |
| Transaction counter | Integer for the transaction | 1-9 |
| Transaction | List of transactions | - |

*Table 1: Block Format Fields*

The first element of the block is a 4-byte magic number whose value is always a constant set at ‘0xD9B4BEF9’ (Bitcoin protocol uses little-endian representation for integers). This can be confirmed using a hex viewer on any of the block files.



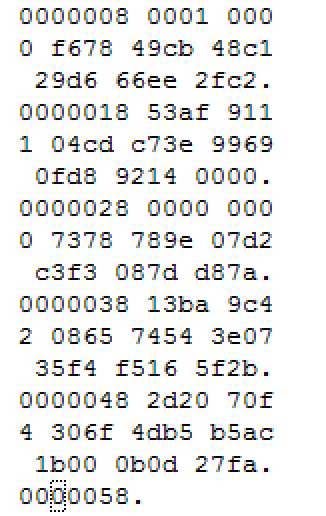
*Figure 6: Magic number*

This number is then followed by a 4-byte field that is the length of the block. The four bytes are ‘0x92200000’ which turns out to be ‘0x00002092’or 8338 bytes.



*Figure 7: Blocksize*

Next comes the 80-byte block header. This portion consists of 6 other fields.

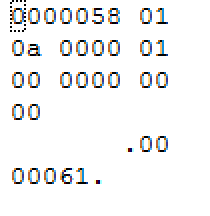


*Figure 8: Block Header*

|  |  |  |
| --- | --- | --- |
| Field | Description | Size (bytes) |
| Version | Block version number | 4 |
| Hash prev-block | Hash of the previous block | 32 |
| Hash Merkle-Root | Hash of all the transactions | 32 |
| Time | Timestamp | 4 |
| Bits | Current constant target number | 4 |
| Nonce | Random alphanumeric number | 4 |

*Table 2: Block Header Fields*

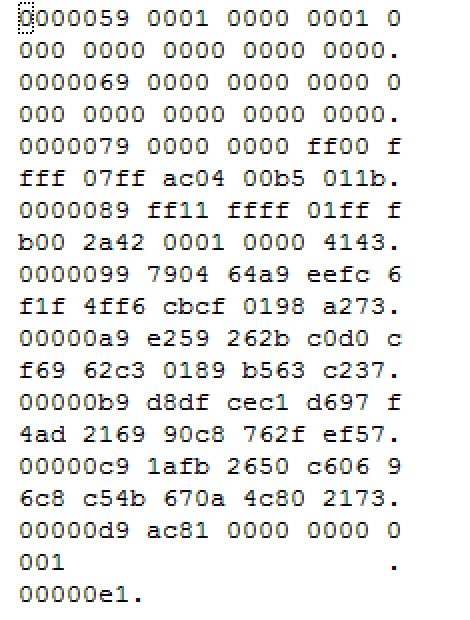
The next field that is made up of 1-9 bytes is the variable length transaction counter. This can be confirmed after skipping the first 88 bytes of the block. In this case, the counter is found to be 0x58 signifying that there are 88 (hex to decimal conversion) transactions.



*Figure 9: Transaction counter*

Transactions

It was discovered that there are 88 transactions in this current block. Next, we will dissect the first few transactions in order to gain a better understanding of the overall structure of a single transaction. This requires for us to skip the first 89 bytes of the block. This will reveal the very first special transaction (delimiter) within the particular block. This is also the place where the miner rewards themselves for performing the act of mining.



*Figure 10: List of transactions*

Further deconstructing this transaction it is seen that the transaction is made up of the following fields.

|  |  |  |
| --- | --- | --- |
| Field | Description | Size (bytes) |
| Version | Version number | 4 |
| In-counter | Integer counter | 1-9 |
| List of Inputs | First input of the transaction | Variable |
| Out-counter | Integer counter | 1-9 |
| List of Outputs | Output of the first transaction | Variable |

*Table 3: Transaction fields*

In this case, the version is ‘1’ while the in-counter and out-counter are both 1. Additionally, as this is the first transaction there is no input/previous transaction. However, the list of inputs parameter contains information related to another input script, and the list of outputs represents the amount of Satoshi’s (1 BTC = 108 satoshi’s) being transacted out as the output. [24] (Refer to Figure 10)

*P2P Network*

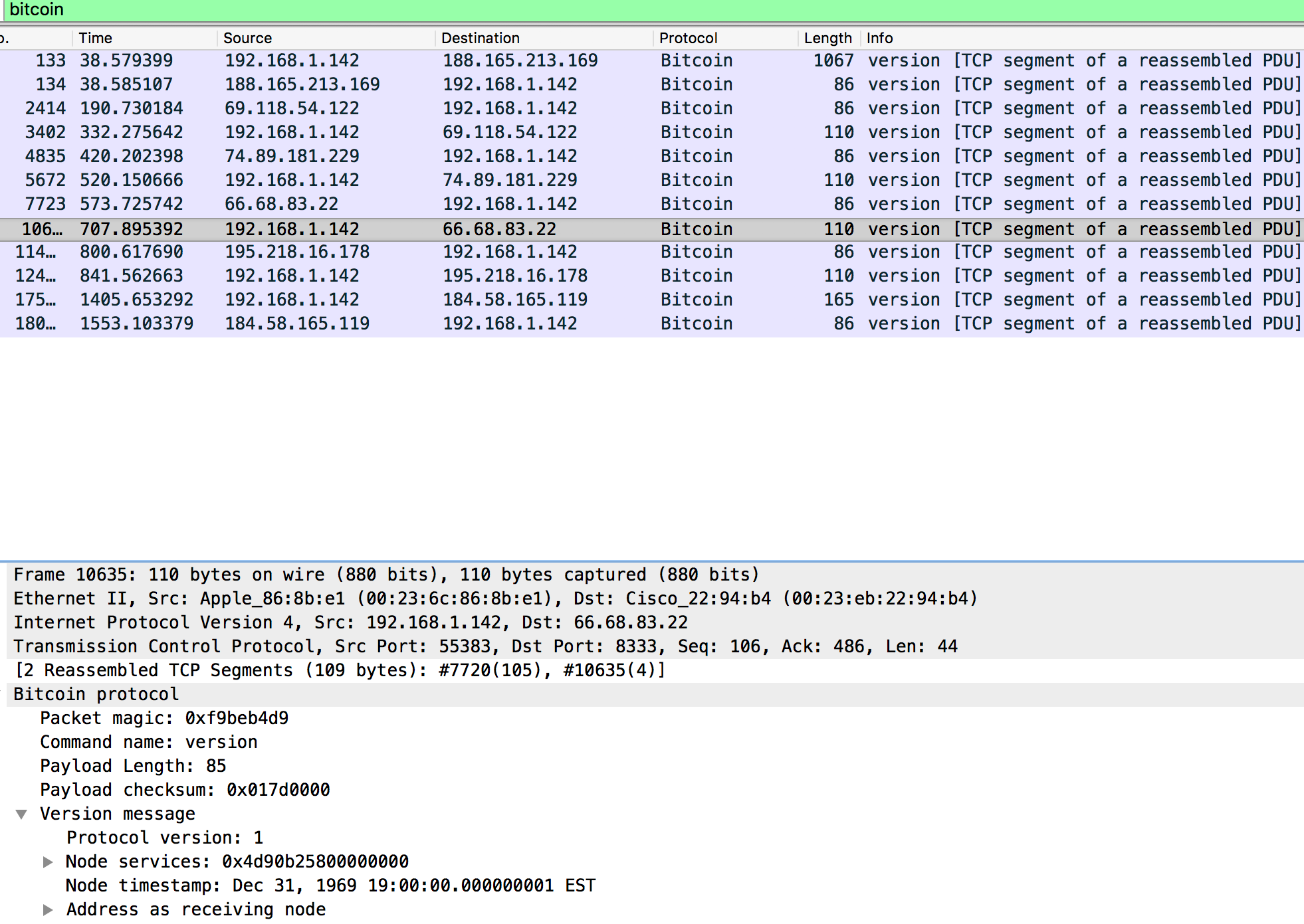
So far the conversation has been about the basic structure of the blocks within the blockchain. Now the conversation moves onto the Peer-to-Peer (P2P) network that exists between the nodes. The Peer to Peer decentralized network, consists of nodes that have the same privilege within the network wherein peers communicate with each other. During this communication, personal resources are are utilized in order to perform tasks for the entire community. Thus, the next section dives into what happens during a transaction from a network standpoint.

*Wireshark - Network Analysis*

The best and most easiest way to analyze bitcoin network traffic is using a packet analyzer such as Wireshark. Capturing Bitcoin network traffic provides plenty of information about what goes on during the transaction. The new version of Wireshark contains the ability to filter on the Bitcoin protocol, it operates via TCP on port 8333 for communication [16]

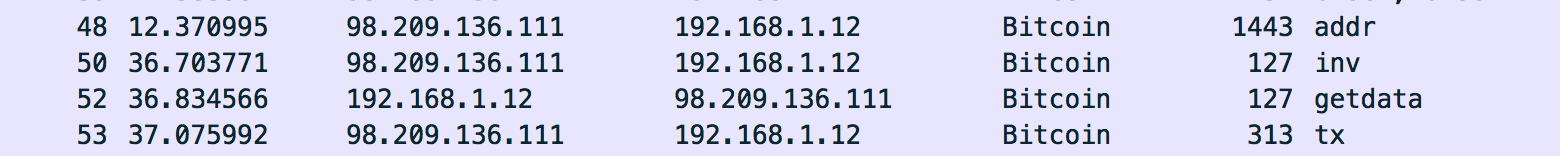
Procedure:

* After installing Wireshark, it can be started.
* You can use the filter tab to filter on the ‘bitcoin’ protocol.
* Now bitcoin-qt client must be started to capture and view network traffic.



*Figure 11: Wireshark capture*

Messages



*Figure 12: Wireshark messages*

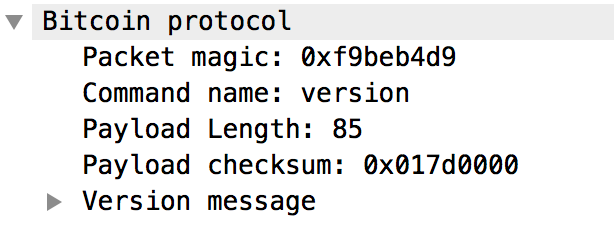
The protocol uses many messages types and has a well defined structure for them but the most important of them are the ‘inv’, ‘getdata’ and ‘tx’ messages. The inv messages are the first indication of the beginning of the transaction also an indication that the transaction has been accepted by the network.

The inv message is followed by the getdata message, it is the response from the host to the node. It contains the matching payload checksum to the parent inv and the transaction hash.

In return the node sends a ‘tx’ message. It contains the most publicly available information. Attached to it are the transaction details corresponding to the transaction hash in the previous two messages. The tx will contain the matching payload checksum to that of the first 4-bytes of the inv and getdata ‘Data’ hash value. [18]

Note: The actual value sent and the value observed in Wireshark has a difference in value of 108.

Message Structure



*Figure 13: Bitcoin message structure*

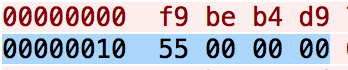
|  |  |  |
| --- | --- | --- |
| Name | Type (bytes) | Description |
| magic number | Unsigned int (4) | Magic value indicating message origin network, and used to seek to next message. |
| command | Char (12) | String to identify the contents of the message. |
| length | Unsigned int (4) | Length of the payload |
| checksum | Unsigned int (4) | Initial bytes of the SHA-256 hash |
| payload | Unsigned char | Data |

*Table 4: Message fields*

There is a 4-byte magic number to denote the main bitcoin network. This number is ‘0xD9B4BEF9’ and when it is sent over the network it gets little endian converted into ‘F9 BE B4 D9’.



*Figure 14: Magic number and command field*



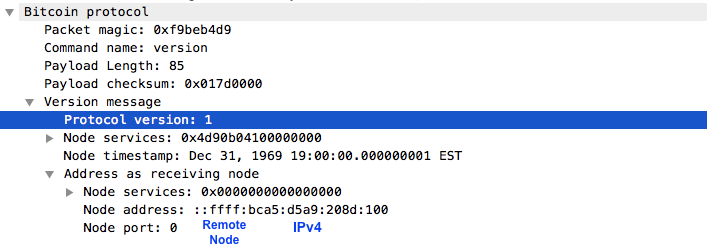
*Figure 15: Message length*

After the magic number comes the 12-byte ASCII command field indicating the type of message being sent over. Next comes the 4 byte little endian ‘length’ field, it is the number in bytes that indicates the length of the payload within the particular packet. In Figure 15 shown above, it is seen as 0x00000055 (hex) = 85 bytes. Following this is the 4 byte checksum of the payload. This number is created using the the SHA-256 hashing algorithm.

Version Message

The way each payload is decoded depends on the command and more importantly the version.

To establish a connection with another node, the first couple of things a client node does is set up the listener ports and then sends out version notifying messages. This is the first and most important step before two nodes can begin communicating. This announcement is a way of providing information regarding the capabilities of the node to other nodes.



*Figure 16: Bitcoin Version and other fields*

Version Structure

|  |  |  |
| --- | --- | --- |
| Name | Type (bytes) | Description |
| version | Int (4) | Protocol version used by the node. |
| services | Unsigned int (8) | Features to be enabled for this connection |
| timestamp | Int (8) | Timestamp |
| addr\_recv | Net\_Address | Receiver node address |
| addr\_from | Net\_Address | Transmitting node address |
| nonce | Unsigned int (8) | Random number |
| user\_agent | String | User Agent name |
| start\_height | Int (4) | Last block received |
| relay | Boolean | Should transaction be relayed |

*Table 5: Version fields*

The payload for an example version message sent over the wire looks like this:



*Figure 17: Version*

The payload starts with a 4-byte field detailing the version number. In the packet above, this is 0x00000001 = 1.

After this is a field indicating the features (node services) to be enabled for this particular connection.

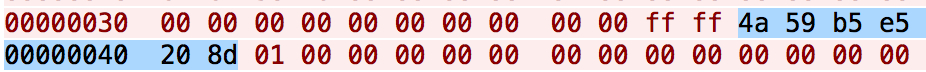


*Figure 18: Node services*

Consequently, the value of this 8-byte field is 0x0000000000000001.

After the node services information, comes the timestamp. For the current message, this would be Dec 31, 1969 19:00:00.000000001 EST:

Next is the address of the remote node that is receiving the message. The address is 12 bytes of 00 00 00 00 00 00 00 00 00 00 FF FF followed by the 4 bytes of the IPv4 address 74.89.181.229 (0x4a59b5e5). The last 2 bytes 0x208d combine to form a larger 4 byte big-endian integer 0x208d = 8333. Thus, this showcase that the node is connecting to the IP address 74.89.181.229 via port 8333.



*Figure 19: Remote node IP*

Next, comes the client node address. Similar to the previous field after the first 12 bytes is the IP address of the node which turns out to be 192.168.1.142.

Next is the 64-bit random number that is used as the nonce to detect and catch identical payloads. After the nonce is the variable length string detailing the name of the User Agent being used.

Finally, the last field is the block start height that signifies the height of the latest block within the database. The start height address can be updated if a connected node has a higher start address. In this case it is 114365. [24]



*Figure 20: Block Start height*

*The Myth of Anonymity*

Within the Bitcoin network users are identified solely by public-keys, as discussed in the previous section; however, anonymity within the network is a complex problem. For example, an attacker wishing to de-anonymize users can attempt to construct a 1-to-many mapping between the users and the public key and then associate this information externally. To prevent this from happening, Bitcoin stores the mapping between the user and the public key on the user’s current node and additionally limits the number of public-keys exhausted by an user.

Traditionally, the security of the Bitcoin platform has been maintained by the process of universal verification by everyone on the network. However, as collateral damage all the transactional data is available to the public which coincides with the idea of privacy.

Furthermore, insufficient privacy can have serious implications, as without adequate protection malicious actors have more freedom to conduct nefarious activities. It can also lead to loss of fungibility wherein some transactions are given higher priority than others further undermining the use of the platform.

Some researchers have done research to reveal that the Bitcoin network is not as anonymous as it claims to be. Puzis performed an exercise by simulating the monitoring of communications with the help of strategically located monitored nodes and found that it posed a significant threat to its anonymity. More famously, security researcher Dan Kaminsky independently performed an investigation of certain aspects of anonymity within the system and reported the findings at a security conference. He investigated the ‘linking problem’ by examining the TCP/IP operation of the underlying P2P network in order to expose the non-anonymity of user activity. He found out that by opening a connection to all public peers simultaneously he was able to map IP addresses to public keys and thereby leading to identity leakage. [22]

*Specialized Eclipse Attacks*

Eclipse attacks allow an adversary to control a substantial number of IP addresses in order to monopolize all incoming and outgoing connections to and from a victim node. The attacker then has the ability to perform a multitude of actions such exploiting the bot for mining and consensus abilities, an attacker with eclipsing capabilities can also engineer block races by hoarding blocks etc.

During a legitimate connection, each node has the ability to select amongst eight peers and at the same time accept up to 117 unsolicited incoming connections. As a result, these nodes can view and exchange the state of the blockchain with all peers. However, this mechanism at the same time makes it possible for nefarious actors to join the network and attack certain nodes.

The report also presents another set of attacks termed as off-path attackers wherein the attacker controls end nodes but do not have access to key infrastructure between the node and the main blockchain. In this attack, continuous rapid unsolicited incoming connections are sent to the victim. As a result, the victim has a high probability to form all of its eight connections with the attacker-controlled addresses.

Recently, large conglomerates, wallets and clients have been known to modify the bitcoin networking code in order to reduce the risk of such attacks. However, according to a Usenix report, the two best countermeasures against such attacks are :

* Disabling incoming connections
* Choosing reliable outgoing connections with peers.

There are a few problems with this solution, first if all incoming connections are restricted then how will new nodes join the network, second how does a particular node measure the reliability of a peer. [14]

The results of this report were disclosed to the bitcoin developers and some of the countermeasures were deployed. The developers incorporated the use of deterministic random eviction, random selection and the need to scale up the number of tried and new buckets. The ‘new’ bucket contains new addresses to which the client has never established a connection whereas the ‘tried’ bucket contains addresses to which there was at least one successful connection. Using the random eviction method an attacker is unable to increase the number of addresses stored using the same address during multiple connections (1 address 1 slot). Using random selection, attackers will be provided random addresses from both the tried and new buckets thereby decreasing their chances to exploit nodes. Finally, the most important countermeasure is to increase the number of new and tried buckets. This measure along with the increase in number of legitimate addresses stored within the tried bucket will make it difficult for an attacker to execute an attack. [14]

*Protections*

Bitcoin attempts to solve the privacy problem by using pseudonymous addresses. This mechanism makes it hard for users to determine who owns a specific address. With this information not being publicly known, other users will not be aware of your transactions and the approximate transaction amount you currently possess.

Another technique that can be deployed to improve the privacy within the Bitcoin platform is the adoption of merging transaction histories of users by enabling them to make joint payments. This method obfuscates the trail of bitcoins and breaks the notion that all input-addresses belong to a single specific user. However, this is a partial solution as this method is prone to Sybil attacks and BTC amounts tracking.

Finally, ‘confidential transactions’ is a new powerful basic cryptographic tool that helps to improve the privacy and security of the Bitcoin platform without too much overhead. This feature via a variation of homomorphic encryption (computation on ciphertexts) helps to keep the amounts transferred between parties only visible to the participants in the transaction. It not only makes the BTC amounts private but at the same time preserves the ability of the network to verify the ledger. [6]

*How to protect yourself while using BTC?*

A user can take several steps to protect their identity on the platform:

* It is considered good practice to generate a new public-private key pair for every transaction.
* Users must make sure to use trusted BTC wallets to which they possess the private key.
* They should avoid revealing any identifiable information in relation to their public-keys.
* Users should avoid making transactions immediately after a fork.

*What is a Fork?*

A fork is a modification of the digital currency software that creates two separate versions of the blockchain but with common ancestry. Forks can be soft, hard, temporary or permanent with the capability to split the network into two different digital currencies.

*Keeping up with the Forks*

* Bitcoin Gold (BTG) is a recently released hard fork that occurred on October 25. Its main feature includes the move from a Proof of Work (PoW) algorithm to an Equihash algorithm (memory-oriented PoW, that considers RAM) that is dominated by chinese miners. [20]
* A new fork currently in the works (at the time of writing) is called Bitcoin Diamond (BCD). It currently possesses 4.6 billions coins and more importantly aims to switch from a PoW algorithm to a PoS algorithm after the mining is completed. It claims to headline with privacy at its core and seems to have found a way to encrypt the balances and transactions of users. However, people assert that this will not be a hard fork but rather an altcoin release due to the release of new 210 million BCD. [12]

*Economics*

The first Bitcoin was transacted in January 2008 and by June 2011 there were 6.5 million but currently that number has risen to the astronomical amount of 16.4 million. These facts in conjunction with the plethora of benefits provides strong evidence that cryptocurrencies such as Bitcoin are going to be the money of choice for future generations. [28]

## IV(b). Ethereum

*Origins*

Ethereum came to the fore in 2014 and was seen as a realization of the future and the recognition of the various limitations of the bitcoin renaissance. It was at the time viewed as an attempt to apply the learnings from bitcoin’s network to challenges beyond value exchange. But on a more anthropological level, ethereum can be viewed as an outgrowth of an ideological subset of the bitcoin community that aimed to build additional functionality onto the network without creating a completely new standalone blockchain.

Buterin, one of the founders, positioned ethereum as a platform that would enable thousands of digital currencies to operate on the same network, with the goal being an “economic democracy”. However, as it is with most things, Ethereum is not just one thing but rather a compilation of many parts. Similar to the Internet, Ethereum is a sum of many different components. A non-exhaustive list of these components includes: a cryptographic token and address system, a network of validators (miners), a consensus algorithm, a blockchain ledger, the ethereum Virtual Machine (runtime environment for smart contracts), a set of programing languages (Solidity) and other complex economic structures. [13;11]

*Important Components*

* Ethereum follows a protocol called ‘Ghost’, which allows for stale blocks (blocks computed by others) to be discarded, as newer blocks need to be integrated into the blockchain. This process helps to reduce wastage of computing power, increase incentives for slower nodes and also for quick turnaround of transactions. One of the other more important pieces is Ethereum’s native programming language Solidity, it is often described as ethereum’s scripting language, but is actually a compiled language. The Solidity compiler turns code into EVM bytecode, which can then be sent to the network as a transaction in order to be given its own address. In general, it is quite similar to JavaScript and is the code that makes it possible to run programs.
* Ether (‘ETH’) is the unit of account and value on the ethereum blockchain, similar to bitcoins (BTC) on the bitcoin network. However, it is not meant to be used an alternate currency rather its purpose is to power the platform. It generates value by virtue of its ability to execute scripts and contracts on the network.
* In order to complement ether, the network introduced Gas. It is a throttling mechanism that determines in real-time how much ether would each contract cost and also aids in limiting the amount of work required for the transaction.

The Gas price is set by the initiator of the transaction. At the moment Gas has a fixed value and is currently set at 10 “szabo” (1 ETH = 1m szabo) which has to be paid up-front. The prime reason for running contracts based on the Gas throttle / ether limit is so that the it limits the potential for hackers to spam the network while at the same time sets a fixed amount on the transactions. [8]

*Supporting Technologies*

In addition to the main ethereum protocol, there are plenty of supporting technologies that help the network to run more efficiently. For example, new sets of protocols are being constructed to allow these programs to harness data from multiple blockchains. Some of these are:

* Whisper

Whisper is a communications protocol and tool-set that allows applications to talk to each other. It combines aspects of a distributed hash table and a peer-to-peer (P2P) communications system. It allows for the creation of open chat room-like apps or “secret” communications channels between parties. The use case for such an application is when, whistleblowers want to communicate with a journalist with their identity being anonymous.

* Swarm

Swarm is a peer-to-peer (P2P) file sharing system that is designed to store and retrieve data required in applications and contracts.The best analogy would be that it is essentially a BitTorrent for Ethereum.

* Oracles

Smart contracts require a well designed series of “if then” statements called ‘oracles’ in order to execute them properly.

* Mist

Mist is meant to used as a wallet for smart contracts. Its features include a GUI that allows users manage and set transaction fees.

*So what is the deal with Smart Contracts inside Ethereum ?*

Nick Szabo, a computer scientist, coined the term ‘Smart Contract’ to deﬁne a tool to automate human interactions. Smart contracts are the basic building blocks that help in the exchange of money, services, shares, or anything of value in an open and conflict-free way while completely avoiding the services of the middleman. All other structures are elaborate collections of these contracts. They are quite flexible and have the ability to be encoded in a variety of blockchain flavors, but typically Ethereum is preferred by certain users due to its extraordinary processing capability.

One way to describe smart contracts is to compare the technology to a vending machine. Generally, a person would go to a person of authority, pay the required fees in order to obtain the document. Additionally, smart contracts can be thought of as an elevator system. Imagine that the elevators run on smart contracts within the private blockchain. Individuals inside the elevator choose the button to press and then the smart contract system organizes a way in which the elevator will go the different floors in a specific order. With smart contracts, all a person has to do is insert a bitcoin into the automated machine (viz. ledger), and the escrow is available in his account. [29]

Accounts

There are considered to be two kinds of accounts in Ethereum, that tend to share the same address space. The first being ‘External accounts’, these are controlled by public-private keys, the second are ‘Contract accounts’, these are controlled by the code stored within the account. In external accounts, considered the basic form of an account, the account address is obtained from the public key while the address of the contract is determined at the time of contract creation (creator address & number of transactions sent from address). Whereas, in contract accounts, contracts execute the code, pull and push funds and other dynamic actions when they receive such instructions from an Externally Owned Account (EOA).

Transactions

A transaction is a message that is transferred over from one account to another, it is always cryptographically signed by the initiator and can include data in the form a payload and currency in the form of ether. In case, the target account contains code, then it is executed and the payload as provided as the input. Moreover, if the target account is a zero-account (address as 0) then the transaction creates a new contract between the two accounts.

This makes it straightforward to guard access to specific modifications of the database. In the example of the electronic currency, a simple check ensures that only the person holding the keys to the account can transfer money from it. In this case the payload is the EVM bytecode and the output is stored as the code of the contract. Thus in certain cases, actual code is not required to create a contract but the code that returns the code. [19]

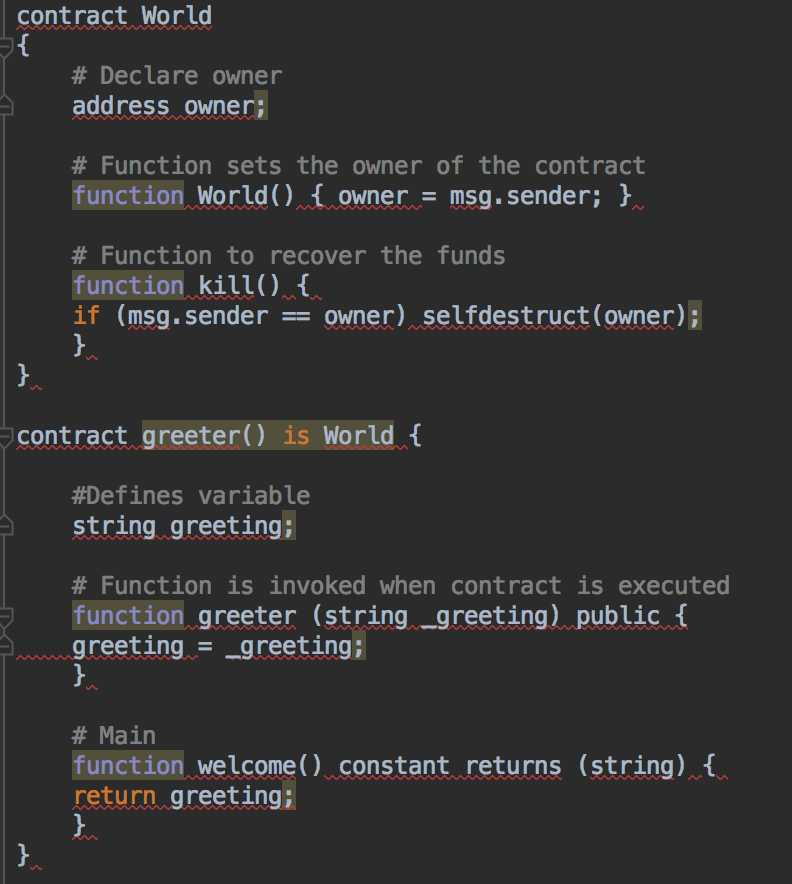
Getting Started

In order to start developing Ethereum apps, a user needs a client that connects to the network. It will act as a gateway to the distributed network, and provide a overview of the blockchain.

The most popular client for the protocol is ‘geth’ (A Go language implementation) others include Parity (Rust), Pyethapp (python) etc, however the best option according to many developers is the ‘testrpc’ node. Smart contracts are written in the Ethereum language Solidity. This, in addition with the Truffle development framework, helps with smart contract creation, deployment and testing.

What can you do with contracts? The simple answer is almost anything.

The easiest thing to start with is the classic “Hello World” contract using the ‘geth’ console, from there on a user can go on to build their own crypto based token.



*Figure 21: Hello World smart contract*

There are two different contracts here viz. “World” and “Greeter”. The image above displays a Solidity technique termed as inheritance, it allows for one contract to inherit features from another. This is extremely helpful feature as common traits of various contracts don’t need to be re-written every time but just referenced. [4]

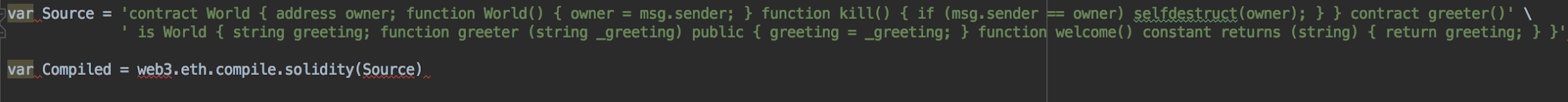
Before deploying the code, two things are needed: the completely compiled code and the Application binary Interface (Javascript object that defines how to interact with the contract).

Compiling the code requires the Solidity compiler, this can be checked using:



*Figure 22: List of compilers*

But before compiling the code, the contract should be void of line breaks and must be assigned to a single variable.



*Figure 23: Smart contract deployment*

After successful compilation, the code now needs to be set up for deployment, this process requires setting some variables like the output message.

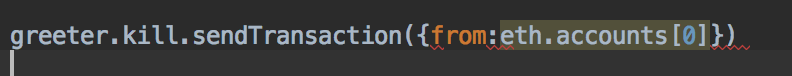
To run the greeter, use the command:



*Figure 24: Running the contract*

Additionally, an user may be required to "unlock" the account that is sending the transaction because they need to first pay for the gas costs in order to deploy the contract. Moreover, in order for other users on the network to run the contract, two things are required: The address of the contract and the ABI (code user manual).

Finally, after pushing the contract live, many users may go on to write further much more complex contracts, and in some cases may end up leaving abandoned contracts on the blockchain. Hence it is considered best practice that the account that created the contract include a kill clause so as not to live on the blockchain forever. [4]



*Figure 25: Smart Contract Kill Clause*

However, smart contracts are far from perfect and the list of challenges includes:

1. What if bugs get in the code?
2. What events would take place if the incorrect code was sent?
3. Send failures: When sending money, code should always have capabilities to counteract transfer failures.
4. Loops can trigger gas limit: Looping over state variables can grow the size of the code and make gas consumption hit the limits.
5. Timestamp dependency: Timestamps in critical parts of the code can instigate miners to manipulate them.

These situations of unexpected behaviors can lead to invalid transactions, theft or destruction of funds in your smart contract. The takeaway from this is: Always be careful when writing smart contracts as this piece of code handles real money. It is always recommended to use tests cases, do code reviews, andaudits. The best way to avoid such problems is to have a solid understanding of the language before diving into the world of smart contract creation.

*The DAO*

When smart contracts are combined they create what are called as DAO’s or DAA’s, which are acronyms for distributed autonomous organizations and distributed autonomous agents.

These are described as long-term contracts between many individuals that use some kind of voting system to manage their distribution. Thereby, they allow users to join the structure, exercise voting power and then exit the collaboration.

The most prominent ethereum project yet launched is the ‘DAO’, it was designed to collect ether investments and distribute those funds to projects voted on by an open community of donors and members. It consists of members who can create proposals in the form of transactions, and can cast votes to either approve or dismiss the proposal.

According to a Coindesk publication, in 2016, the project had collapsed following an incident in which an attacker was able to exploit a functionality in the DAO’s code. Using a “recursive call exploit”, the attacker repeatedly requested funds from the DAO, and the contract without checking approved these requests. As a consequence, Ethereum developers were considering a number of possible solutions to the loss. These included, a hard fork or alterations to ethereum’s code that would effectively reverse the hack, and a soft fork (backwards compatible), which would enact code preventing the stolen funds from being redeemed. A hard fork tends to split the single cryptocurrency in two, with both the old and new versions remaining valid. Such a move requires consensus of 51% of the entire Ethereum community. However, this step was taken in June 2016, as the DAO was forked. [7]

DApps

DApps can be comprised of a single DAO or multiple series of DAO’s that work in unison to create an application such as Excel or a game like Solitaire. Such applications have the feature of being implemented on the ethereum network and not locally on a single server or a computer.

Augur - The most famous DApp

Augur has been headlined as the first open-source decentralized prediction model. It aims to enable users to bet on the outcome of future events. It uses Ethereum to remove the need for users to trust a central entity and automates the process of ownership of funds through smart contracts. Within this application, information collected from the crowd is averaged into the most realistic possibility. Herein, correct predictions are rewarded, while incorrect reporting is penalised. In the end, Augur is quite a rare specimen amongst the pool of ethereum projects, as it leverages multiple blockchain technologies including the bitcoin currency. [7]

*Ethereum Platform Challenges*

Some of the challenges around the Ethereum platform include:

* Price of Gas: The economics of the platform in relation to the price of gas is a point of contention. As an example, in May it would cost around $250,000 to process 1 GB of transactional data. Thereby, the contract would cost 640,000,000,000 gas, or about 17,500 ETH, at $14 per ETH.
* Mining Monopoly: As recently as early 2016, one mining entity named ‘dwarfpool’, had amassed 48% of the network’s hashrate, leading to concerns about market share. As a result, the developers believe that a move towards Proof-of-Stake (PoS) model is a critical step in order to restore the original value proposition of the network.
* Scripting: Ethereum’s programming language has always been a constant work in progress.
* Turing Completeness: As discussed previously, ethereum is aimed to be “quasi-Turing complete”, but in reality, the system is constrained by memory, computation power, storage on the network. [7]

*Ethereum 2.0 Solutions*

* Proof of Stake Transition

One of the most-anticipated improvements to ethereum’s platform involves replacing the network from its current Proof-of-Work (PoW) transaction validation mechanism with one based on Proof-of-Stake (PoS).

PoW is a consensus algorithm that allows the system to prove that prior work was done in order to mine a block. Whereas, PoS validation discards the mining process. Within this system, the holders of the network’s tokens own stakes in the network based on percentage of ownership, and then they have the right to vote in order to validate and include blocks in the blockchain.

The integration of such a model comes with a lot of pros and cons. In a PoS model, miners will be replaced with validators who will no longer need to solve difficult cryptographic challenges. Instead validators will be required to own ether (ETH) and in order to validate a specific block will be required to put their owned ether on the line to certify the validity of a block. This way, if there are malicious validators then they will lose their stake which in this case is the ether owned by them.

Another difference is the method of reward. In the PoS model, the parties that want the transaction or contract to be executed will pay a fee (gas price) in order to have the block be added to the blockchain. Thus, instead of rewarding miners for creating blocks in the previous system, validators will earn transaction fees for each transaction and smart contract that they validate. This is good mechanism as it will put the focus on the bandwidth rather than on the hashrate. It will move the onus back onto collaboration rather than competition, as now the faster is not the one with the most rewards.

But, currently there are problems with the PoS systems today too. In the scenario that certain stakeholders gain the majority of ethers on the network, PoS could be used by them to have a monopolized influence on the network. This would create a hierarchical class system which the network was fighting against in the first place.

* Casper

Casper is an enhancement of the existing ‘Ghost’ mechanism, which replaces miners with ‘validators’. Within this mechanism nodes are responsible for estimating the way that the network state should look in order to verify the contracts, transaction and changes in ledger. The nodes broadcast this estimate to each other to evaluate and then coalesce around a single networks state.

One dilemma that has arisen from this mechanism is termed as the “nothing at stake” problem. Herein, the validators have nothing to lose by voting for more than one blockchain history which can then stall consensus. Casper’s solution to this problem involves “bonding”. Within ‘bonding’, validators need to post value in the form of ethers (ETH) inside the smart contract that would monitors their validation process. By doing this, the incentive to cheat and validate multiple blockchains is eliminated by making it more costly to lose the bonded value. The main purpose of Casper is to monitor the large number of nodes and at the same time detect “unethical” actions by validators. In the case, that Casper recognizes a “cheater”, it will then permanently terminate the bond and will consequently ban the node from becoming a validator in the future.

There will be several key benefits to this system:

* A focus on CPU power rather than GPU power, making the network more egalitarian.
* The capacity for more transactions per second.
* The possibility of even faster block times.

* State Channels

One partial solution which is a sort of an improvement involves state channels. State channels are a method of conducting transactions that could occur off of the main blockchain and are thus a critical component to scaling the protocol.

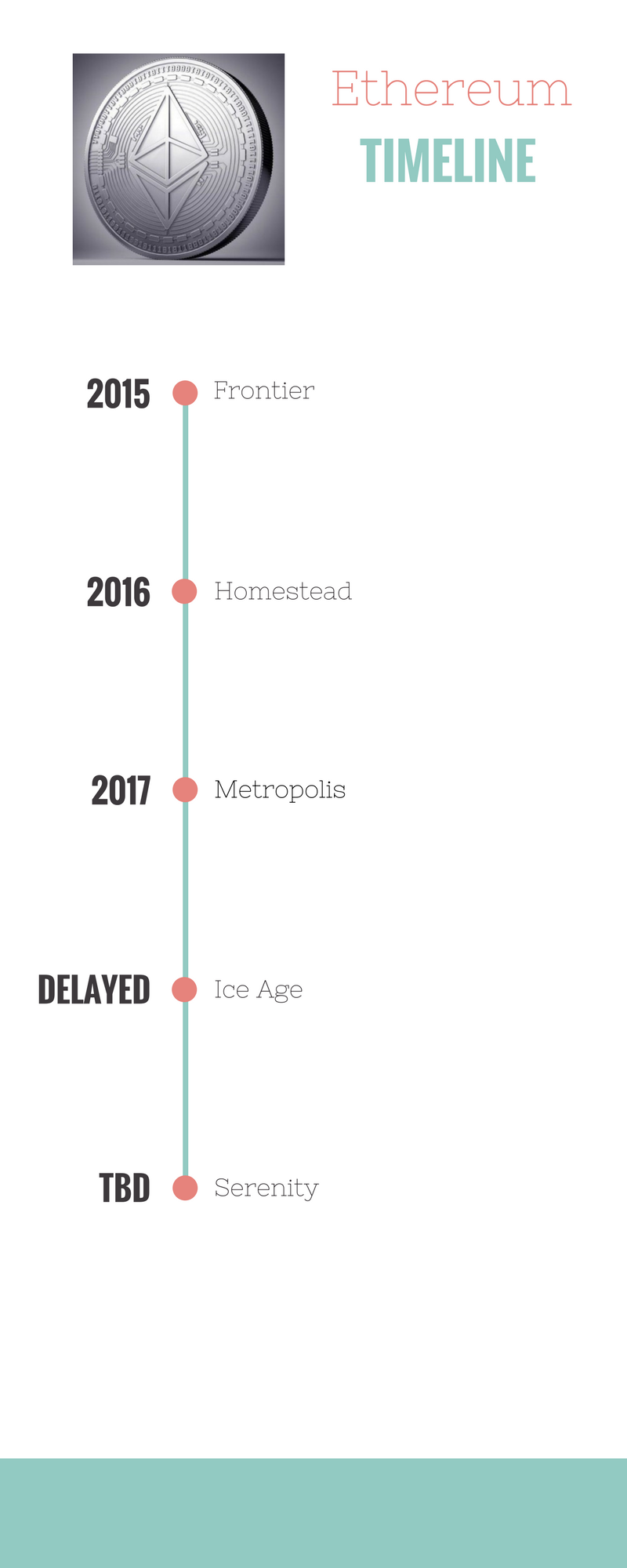
For this to work, both parties need to sign off on the validity of the transaction. The participants then submit the state to the main blockchain and the main blockchain must accept it as an update to the previous channel. This would help to move the value back into the main blockchain with the computational requirement being fulfilled without burdening the main-blockchain.

* Sharding

It attempts to utilize separate servers as a way to hold portions of the full database. By sharding the network into smaller chunks (shards) the network can be split. This is done to help spread out the load and thereby improve performance.

There is a strong belief within the community that distributing formerly centralized systems will be massively beneficial, both in removing the potential abuse and making them more fault tolerant. This challenge is one that faces all public blockchains, and ethereum offers no specific or special solution to this dilemma, at least today. [7]

*Ethereum Milestones*



*Figure 26: Ethereum Platform Timeline*

Frontier -:

Frontier was the first version of ethereum, described by the organization as a beta release.

Homestead -:

Homestead was described as the first “production version” of the network.

Metropolis -:

At time of writing, the latest major release of ethereum was Metropolis. Metropolis is the fully-featured version of the product, aimed at non-technical users. It includes security updates, smarter contracts and plenty of room for automation. Additionally, it will also include the Mist browser.

The Metropolis upgrade will be split into two stages, namely Byzantium and Constantinople.

Byzantium has just been released in October 2017 but unfortunately, there is no release date set for Constantinople (the second hard-fork) due to security concerns around it. [21]

Serenity -:

Serenity is the second calling termed as ‘Ethereum 2.0”. Serenity will see fundamental changes specifically in terms of the platform and the protocol. The most important change will be the migration from the POW mining process to a POS validation process. [7]

Ice Age -:

A drastic project pushed by Ethereum developers is called the Ice Age, it is so that people would have no choice other than to accept the PoS consensus. This will help to prevent miners from exploiting the platform and slowing down development. However, with the release of Metropolis, the beginning of the ice age has been postponed by 18 months, On top of that the miner reward has been decreased from 5 ethers to 3 Ethers per block, as a preparation for PoS.

*Economic Landscape*

Adoption

Ethereum is being adopted by an increasing number of application creators and users. This is evidenced by the fact that the number of transactions per day has been hitting the heights of around 40,000. Other positive indicators include the rising number of unique addresses indicating more users.

Node Distribution

As of mid-2016, Ethereum had 5,384 nodes connected to its network, a figure that is close to the 5,757 that was observed on the bitcoin network during its initial stages.

*Ethereum Summary*

Ethereum offers the Blockchain technology the opportunity to reach higher echelons; a potential path for artiﬁcial intelligence (AI), fundamental for an optimal realization of the “Internet of Things” and other technologies. Within the journey will emerge a lot of opportunities for research to be done in the convergence of machine learning and distributed ledgers. For example, a scenario using Deep Learning and Neural Networks powered by a distributed ledger. [29]

## IV(c). Bitcoin vs Ethereum Comparison

Overview

Both systems use blockchain technologies but have different goals in mind and this is visible through their embedded coding protocols.

Originally, Bitcoin was designed to function as a secure peer-to-peer (P2P) decentralized payment system, wherein due to the nature of the public ledger, there will be a guarantee that the transaction is legitimate. Bitcoin’s first priority has always been security, followed by speed. For example: A bitcoin transaction will be made available within as little as 1 hour and is considered to be very secure due to the nature of the code used.

Bitcoin operates on a proof-of-work (PoW) basis. ‘PoW’ means that in order to create blocks and add them to the blockchain, users must solve complex mathematical questions (mine). The current reward for mining is 25 bitcoins per blocks and this reward halves every 210,000 blocks. However, the next halving is estimated to take place sometime in 2020.

The PoW model, comes with its pros and cons. Even though it does provide security and validity on one end, on the other end it does not give miners an incentive to collaborate, neither is their anything of theirs at stake for them to not engage in malicious activity. The second issue with PoW is that the huge amount of energy required to validate the transactions.

Ethereum on the other hand is a decentralized platform that runs smart contracts. The Ethereum protocol is built to allow flexibility and functionality of multiple smart contracts within the system. Similar to bitcoins, the Ethereum platform currently works on PoW model (soon to be replaced by PoS) wherein ethers are released via the mining process at the amount of 3 ethers per block. However, in contrast to Bitcoin, Ethereum does not have a maximum total number of ethers but does cap the amount released each year. [11]

|  |  |  |  |
| --- | --- | --- | --- |
| No. | Topic | Bitcoin | Ethereum |
| 1 | Blockchain: Both ethereum and bitcoin operate global transaction ledgers achieving validation through the use of a Proof-of-Work (PoW) protocol. | In bitcoin, the transaction script is “stateless”, which means there is no state prior to execution of the script, and the update to that state is not saved after its execution. | Whereas, contracts on ethereum are considered to be “stateful”, which means they are aware about past information stored on the network and can be programmed to take actions in the future. |
| 2 | Blockchain Size: On both platforms, the more transactions that are executed, the more information all the peers on the network need to store. | Currently, Bitcoins blockchain is growing at the rate of 3GB per month. | Whereas, Ethereum is growing at 1GB per month. |
| 3 | Block Size | In Bitcoin, blocks are limited to 1 MB in size. This has been a point of contention for a while as it creates a cap on the amount of transactions processed per second (which is currently 7). | Ethereum has no such limit on the size of its blocks. This is in part due to its Turing completeness ability to executes scripts and contracts. |
| 4 | Block Timings | Speed has always been an issue within the blockchain community. Currently, bitcoin’s blockchain adds new blocks roughly every 10 minutes. | Whereas, Ethereum has set its target on 14-second block. |
| 5 | Inflation Rate | Within the bitcoin network, the maximum number of bitcoins that will ever exist is currently set at 21m BTC (a cap that would require consensus to change) | Ethereum, by comparison, has no hard limit at this point in time. |
| 6 | Scripting Language | The Bitcoin scripting language is not Turing complete, because it consists of very few capabilities. It has intentionally adopted a rudimentary scripting language in order to ‘push’ bitcoin transfers via the network to all other applications. | Ethereum, in contrast to Bitcoin, aspires to be “Turing-complete.” However, this functionality comes at the cost of reduced security. Ability for powerful scripting allows for greater function, but also create new avenues for potential attacks. |
| 7 | Consensus | Bitcoin utilizes what is referred to as “Nakamoto consensus”. This solution was an attempt to solve the problem known as Byzantine Fault tolerance by incorporating the idea that one cannot trust an entity that has a motivation to lie. | Ethereum’s ‘Ethash’ differs from Bitcoins “Nakamoto consensus” in various ways, at the forefront is the idea that it uses different cryptography for its hashing function viz. SHA-3 instead of SHA-256.  This mechanism is employed to make the platform resistant and more accessible to “lightweight” clients (allow users to use ethereum without downloading the blockchain on their device) |

*Table 6: Bitcoin vs Ethereum*

Transactions

The most notable difference between the two blockchains is that ethereum blocks contain both a transaction list and the most recent “state” of the ledger of these transactions.

* In Bitcoins model, newly mined bitcoin become an unspent transaction output in possession of the owner. During the transaction, these unspent transaction outputs (UTXO) become inputs for the next transaction. Thus, when these bitcoins are pushed, to another user, a brand new UTXO is created.
* Ethereum does not use transaction inputs or outputs, it deviates from the unspent transaction outputs (UTXO) model popularized by bitcoin. It uses a more familiar model, wherein it stores the current “state” of the network with a list of the accounts and their respective balances.

Note: Furthermore, if a transaction is valid, ethereum determines whether the sender has a sufficient balance. This feature becomes important when transactions have contracts as recipients. [11]

## IV(d). The threat of Quantum Computing to Blockchain

Quantum computers pose a major threat to the asymmetric encryption system, including blockchain. One way to defeat the system is to calculate the private key using the public key; this is extremely hard with current computer systems, but with quantum computer this can be solved easily. Quantum computers can achieve this feat by using ‘qubits’ (composed of photons). Rather than using a binary system of bits, qubits are made up of both 1 and 0 at the same time, thereby providing them with greater computing power for breaking the algorithm.

According to a research done at the National University of Singapore, it was found that that the elliptic curve scheme used by Bitcoin is at most risk, and could be broken by quantum computers as early as 2025. However, there are public-key schemes that are resistant to such threats, so it is conceivable that the Bitcoin protocol could incorporate certain quantum cybersecurity solutions to make the system safer. [2]

Some of these solutions include:

* Strengthening the existing encryption algorithm by adding quantum keys (stronger encryption keys).
* Developing a quantum-resistant algorithms to combat the calculation power of a quantum computer.
* Utilization of quantum networks, which uses quantum key distribution to send information by encoding them and severs the connection at the first hint of an hack. [9]

Furthermore, according to Ethereum founder, Buterin, there is a construct that helps to solve the problem without using RSA, ECC or any other traditional public-key systems, it is called Lamport signatures. Lamport signatures consist of only one ingredient - the hash function. Under this mechanism, the Bitcoin address will still be a 160 hash of the public key (SHA 256 + RIPEMD), the only change being that the public key will consist of 320 hashes instead of an elliptic curve point. Under this construct, it would take an adversary 280 steps to construct a fraudulent transaction or 280x80 steps (trillions of computations) to crack the hashes, a problem that might be too complex for quantum computers to solve. However, sudden advances in science and computing are always possible, and perhaps even these solutions could be defeated by something not yet known. [3]

# *V. CONCLUSION*

Blockchain technology today stands at a critical inflection point. The technology is understood in broader terms, it is still being applied by entrepreneurs in a variety of creative ways, yet the ecosystems around blockchain companies is still young. Early hype around it has somewhat subsided and now the question is not around the potential of the technology but how its applications will be incorporated by the market, as it sets it up to potentially disrupt a very wide range of industries.

As blockchain technology applications have begun to emerge, with Bitcoin and Ethereum we have discussed two of the most prominent state of the art representations of the blockchain technology. If successful, decentralized blockchain applications could play a major role in the emergence of the ‘new’ internet, by shifting the power from the big players back to the individual users. The statement is perhaps a little misleading and a little premature at this juncture.

However, in the future if the Internet were to become decentralized, the vision of the blockchain technology is to reduce the current barriers and limitations in order to establish trust and promote open transactions across the Internet.

Needless to say, blockchain has disrupted and eradicated outdated industries and truly marks the beginning of a new chapter in the realm of technology. At the time Bitcoin opened pandora’s box and enlightened the world to the idea of blockchain technology. Similarly, Ethereum is on the path of giving us a better view of this technology. It is definitely a leap in the right direction but it isn’t there yet.

The whole crypto industry is in its infancy and we must expect greater things as time progresses. There’s a ton of development still left to be done in Ethereum and it will take several years before there is a complete product out in the market. For the future, the switch from Proof-of-Work (PoW) to Proof-of-Stake (PoS) would be fantastic upgrade as it would greatly reduce the computational loads off of the network and the distributed storage solutions along with state channels would greatly expand its capabilities.

Bitcoin since its inception has grown to become a monster within the cryptocurrency industry. However, currently the biggest risk to this platform is parallel cryptocurrencies. This can be seen in the rise of the upcoming fork called as Bitcoin Diamond (BCD). Another recent hard fork called Bitcoin Gold (BTG) occurred in October 2017. Yet, die-hard bitcoin fans continue to believe that these will pose a risk as Bitcoin is considered to be the first in the pack. This defense is most likely quite weak as other currencies can step in and enjoy the same store value as Bitcoins thereby providing an equally good or better alternative. The questions continue to be raised as to whether Bitcoin is the gold of the 21st century or it is just a fad created by millennials ? The answer is not quite there yet but the only certainty is that the price of Bitcoins will continue to soar in current times. [17]

In contrast, Ethereum has made great strides in having its technology accepted as the standard when Microsoft Azure started offering it as a service in November 2015 as it felt that it provided the flexibility and extensibility that many customers desired. In the future Ethereum could be used to dislodge traditional banking institutions. Currently, every bank uses a SWIFT code to securely process transaction but with the inclusion of smart contracts, distributed ledgers could settle transactions more quickly and securely thereby saving up to $20 billion a year.

The current crisis has apparently not affected the value of the currency. The crisis in question is that ether in the range of $150m to $300m is now frozen. The currency is held up in cryptocurrency multi-sig wallets (wallets requiring more than one owner to “sign” a transaction before it can proceed) which happened due to a malicious actor exploiting a bug in the Parity wallet code. However, experts suggest these are minor bumps and still continue to believe that if Ethereum achieves its targets for the technology then the platform could taste the same success as Bitcoin is having.

Although both these platforms have somewhat similar philosophies and principles, the two are very different from each other in regards to the current use and the future potential of their assets. The future of Bitcoin, still has scope for growth and increase in value but experts believe it will not be at the current exponential rate for an extended period of time. As for Ethereum, the future is up in the air. It is definitely an attractive investment opportunity but huge returns should not be expected at this stage.

# *VI. REFERENCES*

[1] Aboulkheir, Moe. “Implementing the Ethereum Virtual Machine (Part I).” Nervous Systems, 12 Sept. 2017, nervous.io/clojure/crypto/2017/09/12/clojure-evm/.

[2] “Bitcoin Security Threatened by Quantum Computers, Say Cybersecurity Experts.” MIT Technology Review, MIT Technology Review, 8 Nov. 2017, www.technologyreview.com/s/609408/quantum-computers-pose-imminent-threat-to-bitcoin-security/.

[3] Buterin, Vitalik. “Bitcoin Is Not Quantum-Safe, And How We Can Fix It When Needed.” Bitcoin Magazine, Bitcoin Magazine, 31 July 2013, bitcoinmagazine.com/articles/bitcoin-is-not-quantum-safe-and-how-we-can-fix-1375242150/

[4] “Create a Hello World Contract in Ethereum.” Ethereum Project, www.ethereum.org/greeter.   
 https://www.ethereum.org/greeter

[5] Cheo, James. “Why Blockchain Is Real And Bitcoin Is A Mirage.” *Forbes*, Forbes Magazine, 11 Dec. 2017, www.forbes.com/sites/insideasia/2017/12/10/why-blockchain-is-real-and-bitcoin-is-a-mirage/#4b5272f54215.

[6] “Confidential Transactions.” Confidential Transactions, Content Privacy for Bitcoin Transactions, 9 June 2015, bitcointalk.org/index.php?topic=1085273.0.

[7] Dienelt, Jacob. “Understanding Ethereum Report.” *Understanding Ethereum*, CoinDesk, 2016, https://www.coindesk.com/research/understanding-ethereum-report/.

[8] Capital, Fairview. “The Rise of Blockchain – Fairview Capital – Medium.” *Medium*, Fairview Capital, 26 Jan. 2017, medium.com/fairview-capital/the-rise-of-blockchain-b4d63cf7ddd9.

[9] Friedson, Idalia. “How Quantum Computing Threatens Blockchain.” National Review, National Review, 28 Feb. 2018, www.nationalreview.com/2018/02/quantum-computing-blockchain-technology-threat/.

[10] Gavigan, Jack. “SNARKs for the Enterprise.” *Zcash Blog*, 19 Feb. 2018, blog.z.cash/zsl/.

[11] Harm, Julianne, et al. *Ethereum vs Bitcoin*. Creighton University, www.economist.com/sites/default/files/creighton\_university\_kraken\_case\_study.pdf.

[12] Hertig, Alyssa. “Bitcoin Gold: What to Know About the Blockchain's Next Split.” CoinDesk, 24 Oct. 2017, www.coindesk.com/bitcoin-gold-know-blockchains-next-split/.

[13] Hertig, Alyssa. “What Is Ethereum? - CoinDesk Guides.” CoinDesk, CoinDesk, 31 Mar. 2017, www.coindesk.com/information/what-is-ethereum/.

[14] Heilman, Ethan, and Alison Kendler. *Eclipse Attacks on Bitcoin’s Peer-to-Peer Network*. 24th USENIX Security Symposium, Aug. 2014, www.usenix.org/system/files/conference/usenixsecurity15/sec15-paper-heilman.pdf.

[15] “How Bitcoin Transactions Work – Bitcoin.com.” Bitcoin.com, 8 June 2017, www.bitcoin.com/info/how-bitcoin-transactions-work.

[16] Kear, Sam. “Analyzing Bitcoin Network Traffic Using Wireshark.” Sam Kear, 23 Aug. 2016, www.samkear.com/networking/analyzing-bitcoin-network-traffic-wireshark

[17] Konto, Stelios. “Bitcoin, the Future or Just a Gamble?” ForexAnalytix - Blog, 15 Jan. 2017, www.forexanalytix.com/blog/bitcoin-future-just-gamble.

[18] Miller, Preston. Analysis of Cryptocurrency Desktop Wallet Software. Marshall University, 2014, www.marshall.edu/forensics/files/DPM-Internship-Paper1.pdf.

[19] Muller, Christian, and Dalmir Hasic. “Blockchain: Technology and Applications.” 29 July 2016, www.softwareresearch.net/fileadmin/src/docs/teaching/SS16/Seminar/Seminar\_Paper\_Hasic\_Mueller.pdf.

[20] Palog. “Bitcoin Forks Chronology – The Ultimate List of Forks.” Steemit, 1 Nov. 2017, steemit.com/cryptocurrency/@palog/bitcoin-forks-chronology-the-ultimate-list-of-forks.

[21] Petrovic, Ante. “Ethereum's Development Roadmap - What Is Metropolis?” Bitfalls, 2 Oct. 2017, bitfalls.com/2017/10/02/ethereums-development-roadmap-metropolis/.

[22] Reid, Fergal, and Martin Harrigan. “An Analysis of Anonymity in the Bitcoin System.” Bitcoin-Article, Clique Research Cluster, www.item.ntnu.no/\_media/studies/courses/ttm4546/bitcoin\_article.pdf.

[23] Shirriff, Ken. “Ken Shirriff's Blog.” Bitcoins the Hard Way: Using the Raw Bitcoin Protocol, 2014, www.righto.com/2014/02/bitcoins-hard-way-using-raw-bitcoin.html.

[24] “The Bitcoin Protocol – 1 – Block Dissected.” Coin Logic, 9 Mar. 2014, coinlogic.wordpress.com/2014/02/18/the-protocol-1-block/.

[25] “The Rise of Blockchain.” Fairview Capital: The Rise of Blockchain, Fairview Capital, 2017, www.fairviewcapital.com/application/files/7914/9369/3742/Fairview\_Capital\_Rise\_of\_Blockchain.pdf.

[26] Tuwiner , Jordan. “What Is Bitcoin Mining?” What Is Bitcoin Mining and How Does It Work?, 28 June 2017, www.buybitcoinworldwide.com/mining/.

[27] Ugarte, Héctor. “A More Pragmatic Web 3.0: Linked Blockchain Data.” Academia.edu, 1 June 2017, www.academia.edu/31894545/A\_more\_pragmatic\_Web\_3.0\_Linked\_Blockchain\_Data.

[28] Vishwanathan, Vivina. “All You Wanted to Know about Bitcoin, the Most Popular Cryptocurrency.” Https://Www.livemint.com/, Livemint, 6 Nov. 2017, www.livemint.com/Money/gP9TohBCj63BxfXPaXpybI/All-you-wanted-to-know-about-bitcoin-the-most-popular-crypt.html.

[29] “What Are Smart Contracts? A Beginner's Guide to Smart Contracts.” Blockgeeks, blockgeeks.com/guides/smart-contracts/.

[30] Wilson, Steve. “Blockchain Explained in Plain English.” ZDNet, ZDNet, 22 May 2017, www.zdnet.com/article/blockchain-explained-in-plain-english/

[31] Wood, Gavin. “Ethereum: A Secure Decentralized Generalized Transaction Ledger.” gavwood.com/paper.pdf.

[32] Zambre, Deepak, and Ajey Shah. Analysis of Bitcoin Network Dataset for Fraud. Stanford, 10 Dec. 2013, snap.stanford.edu/class/cs224w-2013/projects2013/cs224w-030-final.pdf.