Abstract— Bitcoin is a well-known cryptographic currency system up to date which open a wide scope for digital currencies and impact several surrounding fields by prompting noteworthy researches and interests. This survey presents the structure of several research outcomes that develop the whole concept of crypto-currency. Our approach involve these steps: First, we introduce background about Bitcoin protocol and its building blocks. Second, we compare the online banking model with the Bitcoin model with key points further than decentralization. Third, we explore some attacks and vulnerability in Bitcoin structure along this survey and then include more attacks that does not mentioned until the end. In the process we explain and discuss, numerous essential methods that have the same concepts as the traditional currency transaction approach, which could influence what is more than one specific digital currency.

Keywords: Bitcoin, Cryptocurrency, Digital Currency, Block-chain, Electronic Money, Distributed Systems, Survey.

I. INTRODUCTION

We all acknowledge the important role of Internet through the last decades. The Internet has faced the born of numerous revolutions and fundamental applications where researchers can solve the problem in cooperative and distributed manner. A very well-known and widespread examples of thses community-driven and noncommercial systems are anonymous communication, PGP, Hash-cash and Bit-Torrent. In fact, when the idea of specific application had been considered and examined then the essentially applicable solutions existed. However, this rule does not applied for the digital money. The revelation of cryptotocurrency had been around from the early 1980s, but the process took a while before the full distributed solution become real and certain. (1; 2; 3)

The bank as a central authority was a requirement in the initial attempts to build a digital currencies. Then, the idea of interpret the solution to a cryptographic enigma a proof of work considered valuable with approaches like B-cash, Karma, RPOW, and bit gold. The concept of compare it to the traditional piece of valuable metal or a stamped coin was helpful. Applying this thought everyone can mining the money independently and become a digital gold digger. However, for maintaining the ownership records we still need the central instance. (4; 5; 6; 7)

Additionally, it is essential to distribute the ledger that represents the coins ownership in order to eliminate the bank completely. Nonetheless, double spending coins in digital currencies is a general and inherent risk and partially for the distributed currency. If someone issue two transactions in parallel where the digital copies are trivial, multiple recipients could receive the same coin from one sender. The bank in the online centralized set-up, would be able distinguish and avoid this problem. But, in the distributed systems is very complex to achieve similar set-up. Where there is a self-interested or malicious participants in distributed computing systems, the ability to keep the consistent state in the mutual agreement problem is challenging. Which is a summarizing to Byzantine Generals problem. (8; 9; 10)

Quorum systems has been employed to facilitate this problem. In the distributed environment, Quorum systems are a well-known tools that ensure the consistency and availability of replicated data despite of fault information and malicious entities existence. The notion of voting had been introduced, in condition that the majority of any subset of peers know as quorum is honest. Then, the election is used to obtain the state of correct ledger. Nevertheless, Sybil attack is likely to happen with this approach, which is the ability to subvert the election and infuse fault data by a malicious entity. Moreover, it leads to momentary inconsistency in distributed computing systems by ignoring the propagation delays. (11; 2; 10)

Satoshi Nakamoto announced the Bitcoin design which solved most of these difficulties in November 2008 used Cryptography mailing list. Bitcoin become viral quickly after its publised in 2009. The next year Nakamoto gone passive and hand over the project while his identity kept unknown and subject to questioning, like is he one person or group of people. For sure, a combinations of existing contributions from many years of research is what make Bitcoin cleverly possible. However, we cannot ignore the novel contributions that involve the cryptocurrency development which find an original and practical solutions for a fundamental problems. It used a scheme known as a proof of work to limit the number of votes for each entity and therefore render decentralization practical. (12; 4; 5; 13; 14; 15)

Until one of Bitcoin miners finds the solution of a par-
ticular puzzle, they keep collecting transactions in a block and vary a nonce. So, the transactions and the block which contain the solution are broadcast to the other entities, and update the distributed ledger which known as block chain. To determine the coin ownership we need to move cross the block chain until we found the respective coin even going to the recent transaction. Because of malicious manipulations or propagation delays, the idea of block chain forks is employed. So, by considering the longest fork as well as most of the work as consensus the problem is resolved. (2; 16)

Therefore, bind additions or votes to the block chain to proof-of-work contributions mitigates the Sybil attack or double spending attacks. Rewarding the miner with a new coins using the proof of work provide an endless supply. These procedures do not need a centralized coordinating authority which demonstrate the distributed digital currency feasibility. (17; 11; 18; 19)

The systems strengths and weaknesses and many and some comparing the paper and electronic money was discussed in the previous Bitcoin studies. In this survey, the area of full distributed digital currency is described and reflect that concept which fundamentally reaches beyond Bitcoin. However, Bitcoin marks the turning point that speeds up the whole research area and considered the most popular cryptocurrency system. Thus, in our survey we focus on the Bitcoin then we discover some related comparison criteria that make us explore more differences of concepts and attacks.

The objective of this review is to provide a technical point of view on distributed crypto-currencies which provide some necessary clarifications. Then, we investigate the design structure and reveal the reasons behind some individual outline choices.

II. Bitcoin Technical Overview

The Bitcoin protocol foundation and its core idea is discussed in this technical overview. we investigate the use of "proof of work" which eliminate the central bank approach and secure and decentralized the ledger. furthermore, the mining process and the components in the block chain are covered along with the transactions and scripting.

A. Centralized Digital Currencies

Lets follow the scenario where Alice would like to transfer a coin to Bob. She can use an arbitrary approach by generating a contract signed digitally saying smoothing as "I transfer one coin to Bob" and declare it in public. This contract might know as a transaction (TX) in Bitcoin terminology. It is a signed contract. Therefore, it can be verified by using Alice's public key. However, this method could not consider proof of forgery since it can be replayed; the appearance of duplicated copy of the contract, would not be easy to determine if Alice wants to trick Bob, or if she an honest person who really would like to transfer another coin to Bob, or in another situation if Bob would plan a replay attack on Alices account to claim several coins. (2; 12)

Thus, A unique identified coins are vital for solving ambiguities. One solution is to have a trusted source the can issue a serial numbers for each coin. This trusted authority is which known as the bank in centralized scenario. So, the bank would issues a unique serial number coins, then keep the ownership of these coins in a ledger which is simply mapping between the serial numbers and client accounts. The coin transaction contains Alice signature and the transaction announcement as this form for instance, "I transfer coin number 5599 to Bob". With the bank consultation, Bob can verify the ownership for coin number 5599. The ledger would be updated by the bank when the transaction is valid, and Bob accepted. At this time the coin's owner changes from Alice to Bob. (16; 10; 11)

These steps show the fundamental design of the banking model as an application of centralized digital currency. In fact, the online classic electronic payment protocols resemble in this case, despite that there is for sure more features and extended sharp lines involved. However, the ambition solution that Bitcoin aims for is to eliminate the central bank entirely. Thus, creating coins and maintaining the ledger must work sufficiently in a distributed setting. Achieving a consensus on a certain coin and its ownership without central element or mutual trust among participants is challenging. (16; 10; 2)

B. Decentralizing the Currency (proof of work)

A pragmatic method to eliminate the central bank was revealed by Bitcoin where the bank is everyone. Which means that a copy of the record would be kept with every participant and not the central bank as in the classical model. The distributed ledger consider a reflection to the entire transactions and their ownership. This distributed ledger in Bitcoin known as the block chain. (16; 8; 13; 11)
Nonetheless, other new cheating attempts by Alice would be allowed in this distributed storage of several block chain copies. For example, Alice can issue two separate transactions to Bob and Charlie as two different participants where they will receive the same coin. Double spending is the term for such cheating possibility. The inconsistent state of the block chain could be driven if Bob and Charlie verify and accept the transactions independently according to their individual local copy of the block chain.

Double spending in the banking model is prevented by letting the bank issued the serial numbers and controlled them. The transaction concurrent processing is prohibited in the centralized model which enforce a complete order. On the other hand, in the decentralized model when Bob accepts the transaction and announces his claim of it before Charlie, yet, the last could identify the transaction as attempt of double spending. Therefore, a synchronized distributed ledger consider a viable under the synchronous and resistant to jamming broadcast channel. This assumption which simplified the B-money proposal, does not hold in practice. Thus, there is must be a time balance in the prototypical distributed consensus problem between issuing a transaction and informing everybody about it.

In Bitcoin model, double spending would be noticeable by other participants since the transaction legitimacy can verified through the entire network. Bob in our example should only accept the transaction if the majority of participants agreed on the transaction existence and legitimacy. This method is similar to the known problem of Byzantine Generals which is related to the difficulty of international fault tolerance in distributed systems. So, the question of false identity arise with the Byzantine Generals problem: Sybil attack could be possible by an adversary. That means, the transaction could be confirmed by Alice when setting up many instances, i.e., constituting the majority which is consider a double spend. This could lead Bob to trust them and further accept the transaction.

The proof of work in Bitcoin protocol used for Sybil attacks prevention. Ahead of verifying any transaction and broadcast the news regarding it, participant should provide some evidence to demonstrate his/her "genuine" identity. The evidence is in form of cryptography puzzle that required high computation cost for transaction verification. In this case, the computing power is the base for verification the transactions where the number of identities is doesn't matter. The well-known assumption that it is easier to control the identities majority in the system than it is to control the computing power majority. Before Bitcoin the proof of work scheme had been used for other areas such as working against denial of service attacks and spam. The Hashcash is one of the popular examples that use this scheme also.

The transactions in new Bitcoin are communicated to all participants in the network. If the transactions are valid, they collected to form a block. In the distributed validation process of the puzzle used in proof of work scheme consists of hash calculation which formed the block and adjusting a nonce where the hash value is lower than or equal to a certain value that is targeted. The block with the respective nonce would be distributed in the network when one participant has found the required nonce. Then the local copy of block chain for each participant will be updated.

Finding a solution to the puzzle is difficult computationally and depend on the target value. SHA-256 hash function is used by Bitcoin, The only productive strategy to find the solution is to try different nonces, but the hash function for calculating the block hashes should not be broken. Less solution exist where the lower the target which make the puzzle more difficult. For instance, if the target required the binary hash to start with 42 zeros, the average number of attempts are needed is $2^{42}$ before solving the puzzle.

The chance of being the first one who can find the puzzles solution among all the network participants is proportional to the fraction total computing power. The participants who work racing to solve this computational puzzle for monetary rewards called miners. The tickets numbers for a certain participant is proportional to his/her computing power, these tickets known with analogy raffle tickets. In the raffle wheel, the total tickets number is proportional to the total computing power in the system. Therefore, for a certain user with a given computing power, the chances of
winning is reduced if he/she has more tickets in the raffle wheel. Nevertheless, the users chances could be enhanced by increasing the computing power which means buying more raffle tickets. (2)

The value that we aim for is adjusted every 2,016 blocks for stability and reasonable waiting times to validate a transaction. Then, it is re-chosen every 10 minutes to meet the verification rate of one block at that time approximately. Therefore, the target is recomputed on average every two weeks. The new target \( T \) is:

\[
T = T_p \frac{T_a}{(2016)(10\text{min})}
\]

Where \( T_p \) is the value of old target and \( T_a \) is the actual time span that took to generate the last 2,016 blocks. The overall computing power could increase, if the time span less than two weeks to generate 2,016 blocks which indicate that the proof of work difficulty should increase also. (12; 5; 3; 2; 7; 21)

### C. Block chain

Until now we explain the distributed ledger as the abstract block chain but there is more to explain in its structure. The most important part is to answer how Bitcoin maintains the blocks order and comes with a consistent consensus in a wide system. A total blocks order and transactions also is recommended to determine the coin ownership. Therefore, each block in the chain has a pointer to the previous validated block, it illustrated in figure 1. A hash of the preceding block included in the pointer implementation which make the block chain has a linked list structure. The blocks number from head to tail is called block height. At the time of getting into the block, a particular transaction should be existed and that was proved by the block. Along the lines of block, Bitcoin implements a distributed variant of a timestamp service. (13; 18; 20)

The block chain grows constantly because of the continuous mining. The transactions number has enormously increased due to the Bitcoin popularity in general and gamblers in particular. For example, on SatoshiDice, the sake and the payout are two transactions which are a result of bets that consider as at least one satoshi. The pseudo random number derived from hashing of everyday changing secret and extracting information form the transactions is what used to determine the winner. In June 2012, their transaction volume reach its peak with about 62,000 transactions a day. (2; 19)

However, this will inflate the size of the block and results in an undeniable size of block chain which is in the order of tens gigabytes currently. The high transactions number increases the validation procedure effort. Therefore, Bitcoin provides simplified payment verification (SPV) using Merkle trees in order to manage the block size and the low computation effort. It builds a hash tree on the top and the transactions on the leaves. The tree root is a hash value including transactions information and it is part of the block header. The hash tree enables the transactions verification without the complete transactions local copy. The branches from untrusted sources are loadable on demand because the known and secured root through the mining process. Thus, we can detect any tampering with the transaction which result a different hash values. (13; 18; 9)

Through the mining process, forks can occur because block validations are calculated in a distributed approach. Independent validations of the block simultaneously broadcast or one validated block is stalled due to propagation while the distribution. There are two or more versions of linked list in case of fork with potential other sets including transactions. Therefore, the block chain structure would be disagreeable among different participant in the system. The order of transaction might has no consensus consequently which means the unsettled ownership. This issue had been solved in Bitcoin using a simple but effective rule; continue mining on the longest known fork locally where the highest commutation effort involved. One fork will be broadcast validations before others by a minors at some point. Thus, once it propagated this fork will overtake the other and became the longest one which called main chain for participants. By this means, we restored the distributed consensus but double spending still possible in some cases. (11; 2; 20; 21)

### D. Transactions and Scripts

We mentioned the term transactions many times already but here we discuss further details. In Bitcoin a series of messages known as transactions. The most possible use for transactions is to publish in order to transfer currency between participants. As we note before that the longest and most growing list of transactions is the only state of Bitcoin. Thus, the notion of higher authority are eliminated but it exist only in concept of users, account balances or identities when they can imputed form the list of published transactions. (16; 2)

A transaction format contains inputs array and outputs array. The unique transaction ID is a hash of the entire transaction using SHA-256 which serve as global identification. Ad hoc binary format is used to represent transactions and that is an important detail about Bitcoin specification. The output value is an integer that accounts for a quantity of Bitcoin currency. This values precision limits the extent to which currency units could be subdivided; the smallest is Satoshi as we mentioned before. The primary unit of currency is ten Satoshi by the convention which called one Bitcoin, BTC or XBT. ScriptPubKey is a short code snippet that represents the conditions of redeeming the transaction output which also included in the next transaction as an input. (19; 2; 9; 10)
Transaction scripts is what the ScriptPubKey specified the hash of ECDSA public key and the routine of signature validation which refer to as pay to pub-key hash. We use the key with the specified has to sign the whole redeeming transaction. The vast majority of transactions in Bitcoin are pay to pub-key hash and often it is the only possibility to describe the system, but other types are also possible for the transactions. Ad hoc and non-Turing complete stack language is the scripting language. Also, with fewer than 200 commands called opcodes which include cryptographic operations support such as data hashing and signatures verifying. The scripting language is like the transaction format, its implementation in bitcoin is what specified it only. (22; 5; 9; 16; 10)

The transactions hash and output index with its array are what the transaction inputs refer to in the previous transactions. The inputs also include scriptSig which is a code snippet that redeems the transaction output. Using the same stack, the scriptSig and ScriptPubKey should have a successful execution after each other for a successful redemption of the previous transaction. The scriptSig is a complete public key and signature for the pay to pub-key hash transactions. (19; 10)

As we mentioned before that, each transaction input matches a previous transaction output, and the two scripts would have a successful execution if the transactions are valid and satisfy the necessary constraint. Furthermore, the sum of transaction outputs values must be less or equal to the sum of inputs values. Several remarkable properties are implied by the transaction format. The ownership of the Bitcoin does not use the identity inheriting notion or individual accounts. If a participant has a private key to make a signature which redeem a specific outputs that participant can own as many Bitcoins as he/she can redeem and that simply the concept of ownership. Public key hashes function as pseudonymous identities effectively within the system and refer to as addresses in pay to pub-key hash transactions. The requirements does not need a real name of any identity information. (19; 9; 16; 10)

We can argue that the Bitcoins transaction format has a profound innovation. However, specify redemption criteria using a scripting language and determine the entire system state by transactions realization are not visible design options if we look to the prior cryptocurrency systems. Both specifications have been standard in all subsequent essential models. The Bitcoin transactions semantics extended in some proposals usually by improving the scripting language without any effect on the other components. (19; 9; 16; 10)

E. Consensus and Mining

The current design still need global consensus in the block chain contents. Bob and Chris will be vulnerable to double spending attacks if they both saw two divergent block chain. The trusted central authority could be one solution to collect and public the transactions in signed block. However, the authority could freeze an assets of user by refusing to publish a certain transaction. This undesirable approach might happen when the authority go offline or fork block chain to double spend intentionally. (11; 9)

Nakamoto consensus in a decentralized and pseudonymous protocol that could use to establish consensus on the block chain. This idea is the core innovation of Bitcoin and crucial success ingredient. Adding to the chain can be done by any participant through collecting a set of valid pending transaction and use then to form a block. Using the challenging computational puzzle is the core ingredient to determine the partys block that might be considered in the chain as the next block. (12; 2)

The first announcement for a valid block that has the computational puzzle solution which is correct got to be the new block. So, the rest of participants will start working on finding the following block. If the announcement of the solution was invalid, the participant should keep working on the search for the right solution for a valid block. As we mentioned before the longest version is the consensus block chain. Usually, the concept just means the most blocks branch. However, the difficulty of mining process can differ among long forks. Therefore, the chain with the greatest difficulty for production considered the longest. Depending on the network latency, there is a possibility that two valid solutions are found at the same time, which could cause a temporary fork when there are two chains with equal length. Wither fork can be chosen by the miners, but one block chain will extend further eventually and must adopt by the miners. (9; 20; 2; 8)

The emerging of the eventual consensus was provided as an informal argument in the original Bitcoin specification. The following research proved that the assumption of an effective on time broadcast channel where the miners control the computation power majority up to protocol which they are robust and the consensus would be reached in the

Fig. 4. Transactions and Scripts concept
network gradually. The consensus mechanism gradual nature implies that to gain high confidence of a transaction included permanently in the block chain, the users should wait for the blocks to be found. One of the branches during a fork eventually will be discarded after miners converging the other. Mostly the same transactions would be included typically in both branches. However, if there is a transactions that conflicting in competing branches then it is most likely to be in the longest chain, but if the other branch surpasses it, it will be revoked. Double spending will enable effectively in the worst case. (5; 14; 11; 9)

The consensus algorithm depend on miners getting monetary rewards, therefore it is not easy be utilized in systems that does not require transferable value. In Bitcoin there is no other mechanism allowed to create money other than what the miners received initially. The miners will have no motivation to find valid block or solve a difficult puzzle without this reward, thus the consensus protocol will issue these rewards for them. The reward size for the block is determined a fixed amount, so the miner earns 50 Bitcoins for each block. Then it halves to 25 Bitcoins and halves more every four years by schedule until 2140 roughly at a point where creating new Bitcoins is not possible. The currency creation by enabling this wind-down approach will profit the miners by claiming the net difference in value among the full input and output block transactions. If the input value in a block is greater than the output value, the transaction fee is included and paid to the miner. (22; 23; 2; 9)

The penny flooding primarily uses the transaction fees to depress the network overuse with many small transactions and have a limit of mining revenue with no more than 1-2 percent. Having defaults configured in the reference client to determine the fee values with a small number of users who might choose to pay a higher fee to publish their transactions faster. To lower the miners revenue, they collaborate in mining pools by rewards sharing with other miners groups. Each pool has a manager who collects valid blocks rewards for a small fee then allocates the profit to the pool members in proportion passed on the work amount they contributed to the pool. To prove the work amount the miners performed, the send shares that near blocks with a hash begin with a large number of zeros but still not a valid blocks. Due to the risk sharing, pool members received lower rewards variance that will serve as a small drop in estimated earnings to insurance the fee of the pool manager. (14; 21; 15)

The pools were not designated in the original protocol, but since 2013 most of the mining power has been structured into the pool. To divide pool revenue among its member’s many formulas have been used for loyalty encouragement and moderate pool hopping as long as the new members dont feel intimidating. The communication from pool operators to members also have several standard protocols for law latency, the same in the communication among operators of another pool. The pools mostly are center administered, but there are also ad hoc pools that use p2pools protocol. (22; 13; 21; 9)

III. Comparison criteria

A. Traditional online banking and Bitcoin

The Bitcoin design main concept is to decentralize the online banking model. Both approaches have advantages and disadvantages. In the table 1 we can see some of point criteria that we make comparison based on them and in this section we explore much more about that.

<table>
<thead>
<tr>
<th>Attributes</th>
<th>Online Banking Model</th>
<th>Bitcoin Model</th>
</tr>
</thead>
<tbody>
<tr>
<td>Regulation monitoring</td>
<td>Central</td>
<td>Consensus</td>
</tr>
<tr>
<td>Verification</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Loans</td>
<td></td>
<td>Mining</td>
</tr>
<tr>
<td>Money Creation</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Money Supply</td>
<td></td>
<td>Finite</td>
</tr>
<tr>
<td>Exchange rate</td>
<td></td>
<td>Proof of work, trust, supply and demand</td>
</tr>
<tr>
<td>Mediated, reversible</td>
<td></td>
<td>Direct, non-reversible</td>
</tr>
<tr>
<td>Implementation dependent</td>
<td></td>
<td>Somewhat anonymous</td>
</tr>
<tr>
<td>Privacy</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fees</td>
<td></td>
<td>Virtual constant transaction charge</td>
</tr>
<tr>
<td>Transaction charge</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Transaction Delay</td>
<td>Practically in order of days</td>
<td>In the order of Ten Minutes</td>
</tr>
</tbody>
</table>

Fig. 5. Traditional online banking and Bitcoin

A.1 double spending

In the online centralized bank scenario where the coins are distinguished by using serial numbers, double spending is detected in trivial manner. Nonetheless, the offline scenario was considered in the early digital currency where contacting the bank for transaction authorization was impossible. Therefore, double spending become a major issue, even with existing of the central authority. Although Bitcoin In general has an online setting, the offline transactions is considered also. However, other possibilities for
double spending in Bitcoin even where there is no central back is open up because of the distributed ledger. (2; 11)

To deal with double spending, there are two general conceived approaches. First, after the fraud occurred, detect the double spending and the adversary identified for prosecution. Second, attempt to prevent the double sending before it happened. The first approach was followed by the early digital currency where there is a possibility to double spends to happened and randomized parts of identifiers is required in the transactions. If the bank found a double spending, it could afterward assemble these parts for adversary identification. A help from a third party as witness or quorum mechanisms is used to mitigate double spends in the first approaches. Bitcoins approach is similar to them, however that raise vulnerability to Sybil attacks. (2; 2)

A.2 Scalability

The ability to distribute the information quickly into the whole fragments of the network in Bitcoin is the main objective of the peer-to-peer network. The distributed consensus formation is effected by the propagation mechanisms variation and thereby the Bitcoin security. Generally, inconsistent states are undesirable. For example, block chain forks because they prone to double spending. However, scalability issues raised in the Bitcoin network and the most parts that pose challenges are network bandwidth, network size and storage requirements. (2; 9; 10)

Some studies state that the Bitcoins protocol has more transaction rate than the current values and thereby able to provide more scalability. Bitcoin limit the number of transactions per block using 1 MiB artificial maximum block size which also limit the block chain growth rate. The limitation enforces to prevent the block chain inflating before the Bitcoin protocol can handle more transactions. For example, we have a single input and single output pay-to-PubKey (P2PK) transaction which has one of the smallest standard size of 166 bytes. A theoretical upper bound of 10 transactions per second (tps) is a result of back of the envelope calculation. By considering P2PK transactions with at least two inputs and two outputs we would be more conservative and realistic assumption. Based on that, 4 (tps) is the approximate transaction rate capability in Bitcoin. The alternative approach is to shorten the interval of block generation, which accordingly imply adjustment in the proof of work difficulty. As we mentioned before, what leads to block chain fork is when different miners do close to simultaneous block validation. Thus, getting a higher chance of block chain forks accompany with a shorter block creation intervals. (2; 17; 9)

The scalability in both ways to higher transaction rates would consume more resources eventually. For instance, the size of block should be more than half a gigabyte with 1 MiB/s internet connection is required to handle a transaction rate of 2,000 (tps). As an alternative to the banking model, if Bitcoin wants to achieve higher transaction rate that demand a super peer based overlay structure eventually for load handling. In the Bitcoin network, we can observe some evidence of the super peers which consider necessary. For example, some studies found that 20 connected peers forwarded more than 70 percent of both blocks and transactions first of total of 1300 peers. Therefore a hierarchical network structure introduced explicitly which consists of super peers called miners, full nodes, and wallet nodes. (2; 16; 9)

Full nodes or full chain clients resembled in exchanges responsible for downloading and verifying the genesis block and all other blocks after that which is the most secure operation mode. It also participate in P2P network and not strict only for client but it helps propagate information. On the other hand, wallet node known as online wallets or thin clients which utilized the simplified payment verification (SPV) can be used as an alternative. The block headers the only part that thin client needs to request transaction on demand. As it shown in the figure. 3. Merkle root incorporated in the header block which secure the transaction by construct a hash tree over a particular block transaction IDs that have been paired and hashed. The transaction hashed keep repeated in hierarchical manner until we left with a single hash known as Merkle root. By traversing through the respective leaf to the branches up to the root the clients can verify if the transaction is a part of the block. The transaction should be in the block if the final hash equivalent to the Merkle root. Thin client request an intermediary hashes list for verification purposes from the full nodes without needing the whole transaction data from the complete block. It is hard to fake an intermediate hashes, thus the block headers with the Merkle root provide security. (15? ; 2; 16; 9)

Clients can sample from several nodes to reduce the risk, but that does not eliminate the eclipse attacks. Furthermore, other privacy implications arise when we request a specific transactions form full nodes which infer the coins ownership. Bloom filter used in Bitcoin to obfuscate requests and limit the information leak. Clients requests send to the full node as a bloom filter. The transactions sent to the thin client if they match the bloom filter pattern. For adjusting the privacy level at some additional overhead is to use the inherent false positive of bloom filters. The scalability issues in bitcoin is mitigated by the thin clients and relying on the full nodes data provisioned. Consequently, store the raw transaction data separately and include only the transaction hashes in the block. Making a distinction between the full node and thin client and storing all data in the full nodes are required in this approach. Many techniques used by the thin clients to limit the trust necessity in others, the purpose of subverting the core of Bitcoin is to have rigorous decentralization. Other than that the rest of structure is similar to the banking model. (11? ; 2; 9)
Some scientists disrupt on the design concept of Bitcoin and propose a cryptocurrency system that more agreeable with the traditional banks model. They call the system RSCoin which use the central bank method to control the money supply, but using distributing setting for transaction verification and double spending prevention. Their system eradicate the waste on proof of work and return system based on scalable distributed ledger. (11; 2)

A.3 Privacy

The Bitcoin philosophy is a contrast to the traditional banking regarding privacy consideration. Trusting a third party model limits the trending information accessibility while the block chain in Bitcoin reveals the whole transactions data in public. However, pseudonymity is what provided in the block chain public addresses but in the same time this open transaction history never imply identity directly. For each transaction, a new pair of key with a new address is used. Therefore, for each transaction generate a change addresses which also refer to as shadow addresses by the clients to receive in the output side, the transaction change. (13; 18; 11)

Although hiding behind pseudonyms, privacy and social network research point out that we can reveal identification information by linking them. Thus, many discussed and analysis the availability of public block chain in Bitcoin. The idiom rich get richer can be taken literally in Bitcoin. The wealth of rich user can increased their wealth faster than the users with low balance. Furthermore, if a group of people cooperate under pseudonyms, they can exceed the power of all other small individual miners. Which let us ask is Bitcoin really a decentralized system or it starts to swing towards the centralized banking model! (2; 9; 10)

B. Attack points and weaknesses

The security risks and implications of Bitcoin system and protocol design is significate part. We already mentioned some of the potential vulnerability and attacks that encounter the Bitcoin structure, the figure. 6. is a summarization of most of these attacks and more. In this section we give a short explanation to some of these attack that we did not explore yet.(13; 9; 2; 10)

B.1 Wallet and theft

Because installing Bitcoin client occupies a large disk space and needs to download for multiple hours and to index the block chain. Users are using web wallets which is a centralized services that host the main bitcoin function such as managing, storing and transfer the data on a remote server. However, there are some serious concerns of losing the wallets due to week endpoint security which result in the coins theft. For example, a theft of 923 BTCs occurred in April 2013 to the OzCoin mining pool. (13; 9; 10)

B.2 51 percent attack

Because block verification happen in each hop before forwarding to the network. The delay will cause a slowness in propagation of the new blocks. This leads the nodes to waste CPU cycles mining on the blocks of out-of-date. Therefore reducing the network computation power and make it easy for 51 percent attack which is dishonest of miners majority, to mount on the distributed ledger. (14; 22; 16; 23)

B.3 Block withholding

Block withholding occurs when a miner finds the right answer but does not submitted to the pool or to the Bitcoin network. In contrary, he withhold that answer which undermined the overall earnings for the all miner including himself/herself in the victim pool. When we consider a single pool in the system this attack with the existing protocol are secure against the attack but that not always the case! (7; 15)
B.4 Transaction Malleability

The possibility of changing the transaction ID without questioning the transaction validation or make it invalid that what know as transaction malleability which is a bug in the Bitcoin protocol. From the previous description each transactions input has a reference with the respective redeem script scriptSig which specify one or more multiple destinations output. Therefore, transaction ID identified each transaction uniquely which has the redeem scripts along with the transaction data. (19; 2; 16)

We could discuss more attacks in depth but that might be another further topic for future reading and research.

IV. DISCUSSIONS

Previous this research our understanding of digital cryptocurrency was leaning toward unfavourable side, but reading about Bitcoin make us change this feasible assumptions about the mining process and trusting the existing pools. After many trials the clients can decide which pools and wallets they can invest in. the results depending on the machine that you used and how much you can give to this process in conflict of energy consumption. Are you making money or loosing? Is it an easy money or the peers hard work to be able to make reasonable amount of actual value that could exchange with actual goods? Who knew what is the future of digital crypto-currency and what could achieve!

V. CONCLUSION

In this paper, we are going through different cryptocurrency protocols and design structure. we make a comparison between the online banking model and the Bitcoin model and how the crypto-currency could consider a plausible option for money investment. Moreover, explore many attacks vectors and weaknesses along the survey and provide more details.

VI. ACKNOWLEDGMENT

The writer would like to thank Dr. Xukai Zou for encouraging us to work on such motivating topics. finding a novel and interesting topics in digital currency was very challenging and useful. Thank you for everyone who provide a feedback or a great reference to this survey.

REFERENCES


