International Journal of Scientific Engineering and Research (IJSER)
ISSN (Online): 2347-3878
Impact Factor (2018): 5.426

BitCoin and Blockchain Technology

Ayman Ahmad Omar Omar

Amman-Jordan, Arab Academy For Banking & Financial Sciences – AABFS

Abstract: ***The present paper seeks to effectively address the following question: What Bitcoin looks like? What is blockchain technology, overview of bitcoins, What are the main elements of bitcoins and what are the steps of blockcahin, and the main steps for creating the private and public Key.***

Keywords: Bitcoins, blockchain

1. Introduction

1.1 What is Bitcoin

Bitcoin is a digital currency system based on peer-to-peer virtual data. The concept has grown since in 2009 by Sotashi Nakamoto, and bitcoin values have fluctuated from as low as US$2.95 to nearly $1, 200 per bitcoin. Bitcoin is a crypto currency that records all transactions in a distributed append-only public ledger called blockchain. The security of Bitcoin heavily relies on the compatible proof-of-work (PoW) based distributed consensus protocol, which is run by the network nodes called miners [1]. To use bitcoins, individuals must establish a bitcoin "wallet" on a computer.

The wallet contains nothing more than a regularly updated file, listing all bitcoin transactions ever made. Bitcoins can be transmitted to other user wallets using a combination of public and private key cryptology. The transaction contains the amount of bitcoins, including fractions, and digital signature, protected by a private key. The receiver provides a public key, which serves as the sending address. The transactions' public keys ensure that everyone in the Bitcoin network receives and can validate new exchanges via their wallets. Transactional private keys preserve both the integrity and anonymity of each sender's digital signature [2] [3].

When we use bitcoin there is no need for an administrator, no need for intermediaries, can be sent from any one from peer to peer, user to use. Bitcoin is a decentralized digital currency.

1.2 Bitcoin Technical Overview

1) Decentralization

Bitcoin is distributed crypto-currency system and it is a fully decentralized digital currency system wherethe monetary power is not controlled by any party [2, 4].

2) Transactions

Bitcoin transactions are used to transfer digital coins between different client wallets, these coins are transferred in form of a transaction or consecutive series of transactions, the list of transactions is continuously increasing and there are no builtin higher-level concepts in the system to manage the balances of active accounts or even the identities of clients. The transaction defined by forth language.

Transaction consists of one or more inputs and one or more outputs, the transaction steps as the following:-

a) The user sends bitcoins and designates each address and amount of bitcoins being sent to all address in an output.
b) Each input must refer to previous unspent output in the blockchain.

1.3 Transaction format

Each Bitcoin transaction has a multi-dimensional list or an array of input entries and an array of outputs entries. The transaction is entirely hashed by the SHA-256, and the produced hash value basically serves as a unique global identifier of the transaction. Next, the transaction is advertised by an ad-hoc-based binary format. Moreover, the output entries constitute a set of integers which reflect the amount of Bitcoin currencies. These output entries also constitute a concise code in the form of a particular scripting language named a ScriptPubKey, which reflects the parameters required to validate the redemption of transactions, which will be appended to a later transaction input.

1.4 Transaction Script

The ScriptPubKey appoints the hash of a public key using an Elliptic Curve Digital Signature Algorithm (ECDSA)-based public key along with a signature validation routine.

The transaction can be verified by network node through cryptography and recorded in public distributed ledger called blockchain. The transaction fees are optional and the fees measured by satoshis per byte (Sat/b).

2. Blockchain Technology

Bitcoin is the first application of blockchain, it's based on blockchain technologies, Because the success of Bitcoin, people now can utilize blockchain technologies in many field and service, such as financial market, IOT, supply chain, voting, medical treatment and storage [8]. Its is a public ledger that records all bitcoins transactions, it is implemented as a chain of blocks, each block containing a hash of previous block up to the genesis bloack of the chain. A network of communicating nodes ruining bitcoin software maintains the blockchain, the network can validate transactions and add them to their copy of the ledger and then broadcast these ledger additional to other nodes, and for verification of the blockchain each node in the network stores its own copy of the blockchain because every 10 mints there is a new group of accepted transaction created called Block and added to the

blockchain an published quickly to the all nodes without requiring central servers.

Blockchain contains Cryptography, mathematics, Algorithm and economic model, combining peer-to-peer networks and using distributed consensus algorithm to solve traditional distributed database synchronize problem, it's an integrated multi- field infrastructure construction [8].

2.1 The Blockchain Consist of the Following Elements:

1) **Decentralized: The** basic feature of blockchain, means that blockchain doesn't have to rely on centralized node anymore, the data can be record, store and update distributedly without any need to central node.
2) **Transparent:** The data's record by blockchain system is transparent to each node, it also transparent on update the data that is why blockchain can be trusted.
3) **Open Source:** Most blockchain system is open to everyone, record can be check publicly and people can also use blockchain technologies to create any application they want.
4) **Autonomy:** Because of the base of consensus, every node on the blockchain system can transfer or update data safely, the idea is to trust form single person to the whole system.
5) **Immutable:** Any records will be reserved forever, and can't be changed unless someone can take control more than 51% node in the same time.
6) **Anonymity:** Blockchain technologies solved the trust problem between node to node, so data transfer or even transaction can be anonymous, only need to know the person's blockchain address.

2.2 The Structure of the Blockchain

Generally the block in the block chain is consists of main data, hash of previous block, hash of the current block, timestamp and other information (Figure 1) shows the structure of the blockchain technology:

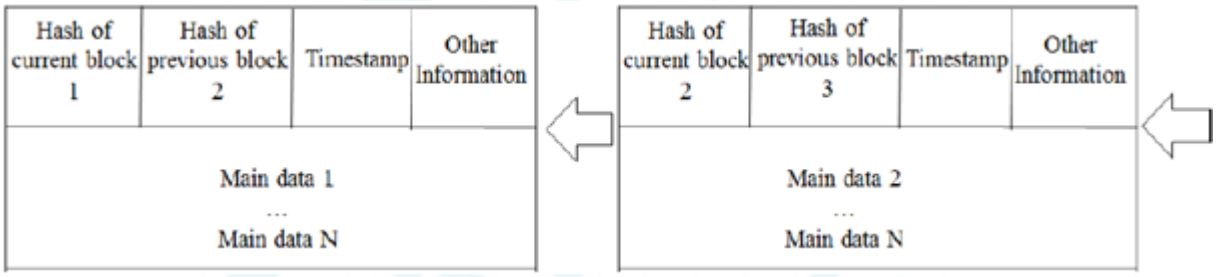

Figure 1: The structure of blockchain

- **Main data**: Depending on what service is this blockchain applicate, for example: transaction records, bank clearing records, contract records or IOT data record.
- **Hash:** When a transaction executed, it had been hash to a code and then broadcast to each node. Because it could be contained thousands of transaction records in each node's block, blockchain used Merkle tree function to generate a final hash value, which is also Merkle tree root. This final hash value will be record in block header (hash of current block), by using Merkle tree function, data transmission and computing resources can be quickly reduced.
- **Timestamp :** Time of block generated.
- **Other information :** Like signature of the block, Nonce value, or other data that user define

Finally, A blockchain is a digital concept to store data. This data comes in blocks, so virtual blocks of digital data. These blocks are chained together, and this makes the data immutable. When a block of data is chained to the other blocks, its data can never be changed again. In the following section we will see the main steps of this technology:-

1) Transaction Data
As we mentioned above bitcoin transactions are used to transfer digital coins between different client wallets, these coins are transferred in form of a transaction or consecutive series of transactions, the list of transactions is continuously increasing and there are no builtin higher-level concepts in the system to manage the balances of active accounts or even the identities of clients. We talk about bitcoins because it is the oldest blockchain in existence. The size of the blocks in the blockchain of the Bitcoin= 1 MB of data each and the transaction size = 250-300Byte

2) Hashing the produced signature in the previous step.
If block one contains of only one transaction. afaf sends 100 Bitcoin to mais. This specific string of data now requires a signature. In blockchain, this signature is created by a cryptographic hash function. A cryptographic hash function is a very complicated formula that takes any string of input and turns it into a unique 64-digit string of output. The SHA (Secure Hash Algorithm) is one of a number of cryptographic hash functions. A cryptographic hash is like a signature for a text or a data file. SHA-256 algorithm generates an almost-unique, fixed size 256-bit (32-byte) hash. Hash is a one way function – it cannot be decrypted back. This makes it suitable for password validation, challenge hash authentication. SHA-256 is one of the successor hash functions to SHA-1, and is one of the strongest hash functions available. In hash function any string input (any size) converted into 64-digit output.
Every message $\rightarrow 2^{64}$ bit (2.3 exabyte or billion g byte).
One digit → 1 byte → 8 bit → 2^8 → 256 bit.

3) The Signature Qualifying
A signature doesn't always qualify. A block will only be accepted on the blockchain if its digital signature starts with a consecutive number of zeroes. For example; only blocks with a signature starting with at least ten consecutive zeroes qualify to be added to the blockchain. as we mentioned before, every string of data has only one unique hash bound

to it. But what if the signature (hash) of a block doesn't start with ten zeroes? In this case, in order to give the block a signature that meets the requirements, the string of data of a block needs to be changed repeatedly until a specific string of data is found that leads to a signature starting with ten zeroes. Because the transaction data and metadata (block number, timestamp, et cetera) need to stay the way they are, a small specific piece of data is added to every block that has no purpose except for being changed repeatedly in order to find an eligible signature. This piece of data is called the nonce of a block. The nonce is completely random and could literally form any set of digits, ranging from spaces to question marks to numbers, periods, capital letters and other digits. To summarize, a block now contains:

- Transaction data.
- The signature of the previous block.
- A nonce.

4) The Mining Process.

Mining is the mechanism that allows the blockchain to be a decencentralized security. It secures the bitcoin system and enables a system without a central authority. Do not confuse the rewards given to miners (new bitcoin) with the process itself.

In this section we will discuss the steps of the mining process :-

- **Step One:** A user signs off on a transaction from their wallet application, attempting to send a certain crypto or transaction from them to someone else.
- **Step Two:** The transaction is broadcasted by the wallet application and waiting to be picked up by a miner on the according blockchain. As long as it is not picked up, it hovers in a 'pool of unconfirmed transactions'. This pool is a collection of unconfirmed transactions on the network that are waiting to be processed. These unconfirmed transactions are usually not collected in one giant pool, but more often in small subdivided local pools.
- **Step Three:** Miners on the network select transactions from these pools and form them into a 'block'. A block is basically a collection of transactions (at this moment in time, still unconfirmed transactions), in addition to some extra metadata. Every miner constructs their own block of transactions. Multiple miners can select the same transaction to be included in their block. But which miner will finish the block first. As shown in (Figure 2).

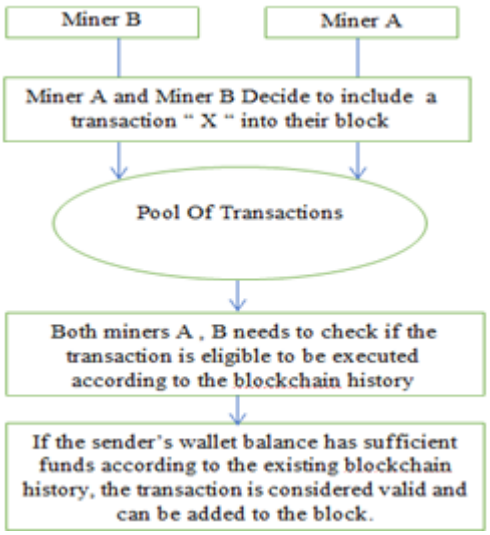

Figure 2: Miner A and B selecting transaction

How to Select Transaction From the Mining Pool

Mining pools are collection of miners that work together as a group in order to collaborate in the proof of work and reduce the variance of their rewards when mining. In order to achieve this, Mining pools distribute amongst the miners the task of finding a block so that each worker works on a different subset of the candidate solutions. Selection of transaction is very important issue. When a transaction is sent from a node in the network, it is broadcast to its peers which in turn will broadcast it to their peers. Miner nodes will keep these unconfirmed transactions in memory and will use this pool of transactions (known as the mempool) to create new blocks. Miners will usually priorities transactions that have a high transaction fee set, because this provides them a higher reward. Many papers discuss transaction selection some of them treat the transaction selection policy performed by miners as a classification problem; for each block they create a dataset, separate them by mining pool and apply feature selection techniques to extract a vector of importance for each feature. The transaction selection policy by default works by selecting transactions from the mempool as follows:

- Transactions are ordered and ranked in descending order by fee-per-kilobyte.
- Transactions which are not selected are left in the mempool for future block attempts.

Step 4: After selecting transactions and adding them to their block, miners create a block of transactions. To add this block of transactions to the blockchain (to have all other miners and nodes register the transactions), the block first needs a signature (as a proof of work). This signature is created by solving a very complex mathematical problem that is unique to each block of transactions. Each block has a different mathematical problem, so every miner will work on a different problem unique to the block they built. All of these problems are equally hard to solve. In order to solve this mathematical problem, a lot of computational power is used.

Step Five: The miner that finds an eligible signature for its block first broadcasts this block and its signature to all the other miners.

Step Six: Other miners now verify the signature's correctness by taking the string of data of the broadcasted block, and hashing it to see if the output hash indeed matches the included signature. If it is valid, the other miners will confirm its validity and agree that the block can be added to the blockchain (they reach consensus, they all agree with each other, hence the term "Proof-of Work"). The signature is the 'proof' of the work performed (the computational power that was spent). The block can now be added to the blockchain, and is spread across all other nodes on the network. The other nodes will accept the block and save it to their transaction data as long as the transactions inside the block correspond correctly with the current wallet balances (transaction history) at that point in time.

Step Seven: After a block has been added to the chain, every other block that is added on top of it counts as a 'confirmation' for that block.

3. The Bitcoin Keys

The concept of ownership on a cryptocurrency system is primarily made of three interconnected elements:

1) Digital keys (Public key and Private key)
2) Cryptocurrency addresses.
3) Digital signatures.

Private Key

In cryptocurrencies, a private key allows a user to gain access to their wallet. The person who holds the private key fully controls the coins in that wallet. For this reason, we should keep it secret. private key for Bitcoin (and many other cryptocurrencies) is a series of 32 bytes. Now, there are many ways to record these bytes. It can be a string of 256 ones and zeros (32 * 8 = 256). It can be a binary string, Base64 string, a WIF key, mnemonic phrase, or finally, a hex string. As showin in (Figure 3). For our purposes, we will use a 64 character long hex string.

Hex: DD5113FEDED638E5500E65779613BDD3BDDBEB8EB5D86CDD3370E629B02E92CD

Base64: 3VET/t7WOOVQDmV3lhO9073b64612GzdM3DmKbAuks0=

WIF: 5KVkpWGfDQGJAUEEDUFbrFxwNPjmXy5kBBmRzzBDf4JkgFXqXTa

Binary:
110111010101000100010011111111110110111101101011000111000111001010101000
000000111001100101011101111001011000010011101111011101001110111101110111
101111101011100011101011010111011000011011001101110100110011011100000011
100110001010011011000000101110100100101011001101

Figure 3: The same private key written in different format

Why 32 bytes?, to create a public key from a private one, Bitcoin uses Elliptic Curve Digital Signature Algorithm (ECDSA). More specifically, it uses one particular curve called secp256k1.This curve has an order of 256 bits, takes 256 bits as input, and outputs 256-bit integers. And 256 bits is exactly 32 bytes. So, to put it another way, we need 32 bytes of data to feed to this curve algorithm. There is an additional requirement for the private key. Because we use ECDSA, the key should be positive and should be less than the order of the curve. The order of secp256k1 is **FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFEBAAEDCE6AF48A03BBFD25E8CD0364141**, which is very big: almost any 32-byte number will be smaller than it.

Generate Private Key

We use the naive method to generate a 32-byte integer, How? The first thing that comes to mind is to just use an RNG library in our programming language of choice. The following example how to generate a random 32-bye in paython:

```
import random
bits = random.getrandbits (256)
#
308488277120212937312084153024565693014993846548772892
4579578647674115537208 2

bits_hex = hex (bits)
#
0x4433d156e8c53bf5b50af07aa95a29436f29a94e0ccc5d58df8e57b
dc8583c32

private_key = bits_hex
#
4433d156e8c53bf5b50af07aa95a29436f29a94e0ccc5d58df8e57bdc
8583c32
```

Along with a standard RNG method, programming languages usually provide a RNG specifically designed for cryptographic operations. Also, there are sites that generate random numbers, such as random.org, a well-known general purpose random number generator. Another one is bitaddress.org, which is designed specifically for Bitcoin private key generation.

Public Key

The important aspect to understand about the incorporation of public key cryptography in cryptocurrency systems. This means that the mathematical functions that constitute public key cryptography are relatively easy to calculate in one direction and are practically impossible to calculate in the opposite direction.

Cryptocurrencies such as Bitcoin utilize elliptic curve multiplication as the foundation for its cryptography. Elliptic curve point multiplication is the operation of successively adding a point along an elliptic curve to itself repeatedly. It is made use of in elliptic curve cryptography as a means of producing a one-way function, which is a function that is easy to compute in one direction. In cryptocurrency systems such as Bitcoin, this one-way function takes the private key as an input to generate the public key, which is the output. Because of this, owners of a private key can confidently distribute their public key knowing that no one is able to reverse the function and calculate the private key from the public key.

The Elliptic Curve protects our privacy and security probably more than anything else on the Internet, especially:
$y^2 = x^3+ax+b$

where $4a^3+27b^2 \neq 0$ (and which is need to avoid singular points). The most popular curve is a Secp256k1 (or Curve 25519), and is defined with a=0 and b=7:

$y^2 = x^3+7$

Elliptic Curves are used in public key cryptograpy to create relatively short encryption keys. They are in the form of $y^2 = x^3 + ax + b$

In this, with ECC (Elliptic Curve Cryptography), we take a random number (*n*), and a point on the elliptic curve (*G*), and then multiply them together to produce P:

P = n G

G will be an (x, y) point on the curve that both afaf and mais will agree to n will then be afaf's private key, and P will be his public key. The challenge is that if n is a 256-bit random value, it will be extremely difficult to find the value, even though we know G and P.

secp256k1: refers to the parameters of the elliptic curve used in Bitcoin's public-key cryptography, and is defined in Standards for Efficient Cryptography (SEC), (Figure 4) shows the parameters :-

```
_p = 0xFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFEFFFFFC2FL
_r = 0xFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFEBAAEDCE6AF48A03BBFD25E8CD0364141L
_b = 0x0000000000000000000000000000000000000000000000000000000000000007L
_a = 0x0000000000000000000000000000000000000000000000000000000000000000L
_Gx = 0x79BE667EF9DCBBAC55A06295CE870B07029BFCDB2DCE28D959F2815B16F81798L
_Gy = 0x483ada7726a3c4655da4fbfc0e1108a8fd17b448a68554199c47d08ffb10d4b8L
curve_secp256k1 = ecdsa.ellipticcurve.CurveFp(_p, _a, _b)
generator_secp256k1 = ecdsa.ellipticcurve.Point(curve_secp256k1, _Gx, _Gy, _r)
oid_secp256k1 = (1, 3, 132, 0, 10)
SECP256k1 = ecdsa.curves.Curve("SECP256k1", curve_secp256k1, generator_secp256k1, oid_
ec_order = _r

curve = curve_secp256k1
generator = generator_secp256k1
```

Figure 4: Secp256k1 parameters

From figure 18 : _a = 0 and _b = 7 ($y^2 = x^3+7$), and that we have a _Gx and a _Gy value. We also have _p which is a prime number in which all the operations are conducted with a (mod _p) function.

In Python we could create two key pairs (one for afaf and one for mais) with:

And where we generate a random 256-bit value for a, and then find the public key (A) by multiply it with G. As shown in (Figure 5). This will give us a point on the elliptic curve. Note that all of the operations are undertaken with (mod _p), and where the mod operator is the remainder of an integer division.

```
a = random.randrange(2**256)
b = random.randrange(2**256)

A =fast_multiply(G, a)
B =fast_multiply(G, b)
```

Figure 5: Random generating for two key pairs

4. Conclusion and Future Work

Bitcoin as a currency has an unclear road ahead of it. Its success or failure really hinges on whether it reaches a critical mass to eliminate wild volatility and reaching this critical mass is by no means a given. One of the main challenges posed to bitcoin is advancement in current payment technology.

References

[1] Conti, Mauro, et al. "A survey on security and privacy issues of bitcoin." *IEEE Communications Surveys & Tutorials* (2018).

[2] Rahouti, Mohamed, KaiqiXiong, and NasirGhani. "Bitcoin Concepts, Threats, and Machine-Learning Security Solutions." IEEE Access 6 (2018): 67189-67205.

[3] Hurlburt, George F., and Irena Bojanova. "Bitcoin: Benefit or curse?." IT Professional 16.3 (2014): 10-15.

[4] Kaushal, Puneet Kumar, AmandeepBagga, and Rajeev Sobti. "Evolution of bitcoin and security risk in bitcoin wallets." Computer, Communications and Electronics (Comptelix), 2017 International Conference on. IEEE, 2017.

[5] Tschorsch, Florian, and BjörnScheuermann. "Bitcoin and beyond: A technical survey on decentralized digital currencies." IEEE Communications Surveys & Tutorials 18.3 (2016): 2084-2123.

[6] Malone, D., and K. J. O'Dwyer. "Bitcoin mining and its energy footprint." (2014).

[7] Luu, Loi, et al. "On power splitting games in distributed computation: The case of bitcoin pooled mining." *Computer Security Foundations Symposium (CSF), 2015 IEEE 28th*. IEEE, 2015.

[8] Lin, Iuon-Chang, and Tzu-Chun Liao. "A Survey of Blockchain Security Issues and Challenges." *IJ Network Security* 19.5 (2017): 653-659.

[9] Casey, Michael J., and Paul Vigna. "In blockchain we trust." MIT Technology Review. Retrieved April 15 (2018): 2018.

[10] Mingxiao, Du, et al. "A review on consensus algorithm of blockchain." Systems, Man, and Cybernetics (SMC), 2017 IEEE International Conference on. IEEE, 2017.

[11] Müller, Paul, et al. "The Bitcoin Universe: An Architectural Overview of the BitcoinBlockchain." 11. DFN-Forum Kommunikationstechnologien. GesellschaftfürInformatikeV, 2018.

[12] Baur, Dirk G., Kihoon Hong, and Adrian D. Lee. "Bitcoin: Medium of exchange or speculative assets?." *Journal of International Financial Markets, Institutions and Money* 54 (2018): 177-189.