Bitcoin Mining: A Case Study

Prashant Ankalkoti
Department of Computer Applications,
J N N College of Engineering, Shimoga, Karnataka, India
prashantsa@jnnce.ac.in

Abstract – This paper is a study on Bitcoin Mining practice. Bitcoin mining is the technique of adding transaction records to Bitcoin's community ledger of former period transactions or blockchain. The mining practice is used to validate and make safe transactions. This process is organized as a speed game among persons or firms – the miners – with diverse computational powers to solve a mathematical difficulty, bring a proof of work, extend their solution and attain agreement among the Bitcoin network nodes with it.

Keywords: Network, Blockchain, Nodes, Wallets.

1. **Introduction**

A merely end-to-end version of electronic cash would allow online payments to be sent straight from one person to another without going through an economic body. Bitcoin was shaped by **Satoshi Nakamoto [1]**, who published the invention and later it was implemented as open source code. Bitcoin is a network practice that enables folks to transfer assets rights on account units called "bitcoins", created in limited quantity. When a person sends a few bitcoins to another individual, this information is broadcast to the peer-to-peer Bitcoin network. Well, the technology remains similar to buying something with virtual currency, but one benefit of Bitcoins is that the contract remains unidentified. The identity of the sender and the beneficiary remains encrypted [2]. And that's why it has become a trusted form of sending money online. By tradition, the complexity in creating distributed money is the need for a proposal to prevent double spending.

One individual might concurrently transmit two transactions, sending the similar coins to two separate parties on the network; but lacking a central server to sort out both transactions and come to a decision which is legal [2,3], divergence arises over the true history and ownership of a given coin (see Fig. 1).

Bitcoin resolves this difficulty and guarantees agreement of rights by maintaining a community ledger of all transactions, called the blockchain. Fresh transactions are grouped mutually and are checked against the existing record to ensure all new communications are valid. Bitcoin's accuracy is guaranteed by those who give computation authority to its network known as miners to authenticate and affix transactions to a public ledger [4]. Miners' readiness to loan their computation power to the network, typically in the form of ASICs committed to mining, in exchange for incentive is key to survival of Bitcoin.

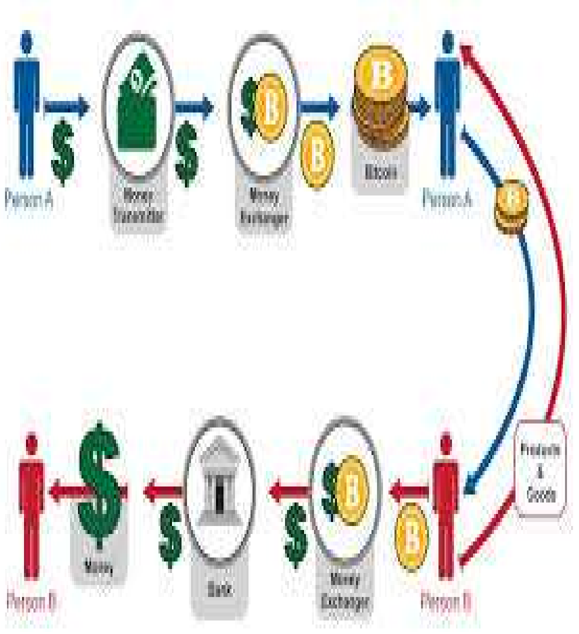

FIG 1.1 BITCOIN EXAMPLE
(Source: https://kingdomecon.wordpress.com)

2. Overview Of Bitcoin Mining

Bitcoins don't exist physically and are merely a sequence of virtual data. It can be exchanged for genuine money though, and are largely permissible in most countries around the world. There's no central authority for Bitcoins, similar to a central bank which controls currencies. Instead, programmers solve complex puzzles to endorse Bitcoin transactions and get Bitcoins as a reward [4,5]. This activity is called Bitcoin mining, and with some knowledge of encoding codes and dollops of desire for capital, anybody can get cracking.

2.1 How to Mine Bitcoins

This is somewhat complex. But if you want to take it head on, here's how it works: Get a dominant CPU with the best processing power. A blazing speedy internet link. Next step, there are many online networks which list out the newest Bitcoin transactions taking place in real time. Log on with a Bitcoin client and attempt to validate those transactions by evaluating blocks of data, called hash [5]. The communication travel through several systems, called nodes, which are just blocks of data. And since the information is encoded, a miner is required to check if his solutions are exact.

Once the nodes get confirmed, a transaction becomes successful and the miner is rewarded with some Bitcoins. In short, you're acting as a bank clerk, along with many other bank clerks meeting online. Whosoever verifies the deal gets rich. Miners from all over the planet try to be the first to match their hash with the solution, and it takes an average of 10 minutes for the correct solution to appear. The mathematical brainteaser is designed so as to alter the difficulty level automatically. If the average time to guess the right answer falls less than 10 minutes [8,9], the puzzle becomes harder to crack, and vice versa. Also, after fixed intervals, the incentives keep getting halved until it reaches nil. After that the programmers who crack the right solutions are rewarded with just a transaction fee for their approval (see Fig. 2).

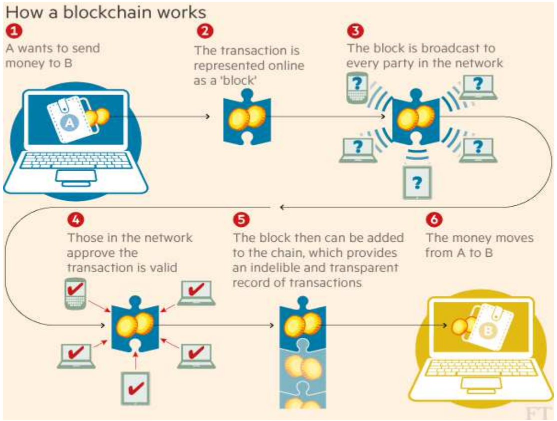
How a blockchain works
1
A wants to send money to B
2
The transaction is represented online as a 'block'
3
The block is broadcast to every party in the network
4
Those in the network approve the transaction is valid
5
The block then can be added to the chain, which provides an indelible and transparent record of transactions
6
The money moves from A to B
A
B
FT

FIG 2.1 BITCOIN BLOCKCHAIN WORKING

(Source: https://www.weforum.org)

2.2 How mining works

Mining requires a task that is very tricky to perform, but easy to verify. Bitcoin mining uses cryptography, with a hash function called double SHA-256. A hash takes a portion of data as input and shrinks it down into a smaller hash value (in these case 256 bits). With a cryptographic hash, there's no way to get a hash value you want without trying a whole lot of inputs [7]. But once you find an input that gives the value you want, it's easy for anyone to authenticate the hash. Thus, cryptographic hashing becomes a good way to apply the Bitcoin "proof-of-work".

In more detail, to mine a block, you first collect the new transactions into a block. Then you hash the block to form a 256-bit block hash value. If the hash starts with sufficient zeros, the block has been successfully mined and is sent into the Bitcoin network and the hash becomes the identifier for the block [11]. Most of the time the hash isn't successful, so you alter the block to some extent and try again, over and over billions of times.

About each 10 minutes somebody will successfully mine a block, and the procedure starts over. The fig below shows the structure of a precise block, and how it is hashed. The yellow part is the block header, and it is followed by the transactions that go into the block. The first transaction is the special coinbase transaction that grants the mining reward to the miner. The remaining transactions are normal Bitcoin transactions moving bitcoins around. If the hash of the header starts with enough zeros, the block is successfully mined [13]. For the block below, the hash is successful: 0000000000000000e067a478024addfecdc93628978aa52d91fabd4292982a50 and the block became block #286819 in the blockchain (see Fig 2.2).

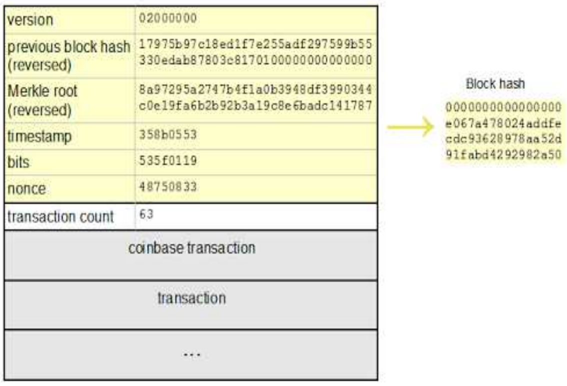

FIG 2.2 STRUCTURE OF BITCOIN BLOCK

(Source: http://www.righto.com)

The block header contains a handful of fields that illustrate the block. The first field in the block is the protocol version. It is followed by the hash of the preceding block in the blockchain, which ensures all the blocks form a continuous sequence in the blockchain. The next field is the Merkle root, a special hash of all the transactions in the block. This is also a key part of Bitcoin security, since it ensures that transactions cannot be altered once they are component of a block. Next is a timestamp of the block, followed by the mining complexity value bits. Finally, the nonce is a random value that is incremented on each hash attempt to give a new hash value [12]. The difficult part of mining is finding a nonce that works.

3. Bitcoin Transaction

A Bitcoin transaction is a signed section of data that is transmitted to the network and, if valid, ends up in a block in the blockchain. The idea of a Bitcoin transaction is to transfer ownership of an amount of Bitcoin to a Bitcoin address [14]. When you send Bitcoin, a single data structure, namely a Bitcoin transaction, is created by your wallet client and then broadcast to the network. Bitcoin nodes on the network will communicate and rebroadcast the transaction, and if the operation is valid, nodes will include it in the block they are mining. Usually, within 10-20 mins, the transaction will be included, along with other transactions, in a block in the blockchain. At this position the receiver is able to see the transaction amount in their wallet (see Fig 3.).

The main components of this standard transaction are color-coded:

✓Transaction ID
✓Descriptors and meta-data
✓Inputs
✓Outputs

Four obvious truths about transactions:

- Bitcoin amount that we send is always sent to an address.
- Bitcoin amount we receive is locked to the receiving address – which is connected with our wallet.
- Every time we spend Bitcoin, the amount we spend will always come from funds earlier received and currently present in our wallet.
- Addresses receive Bitcoin, but they do not send Bitcoin – Bitcoin is sent from a wallet.

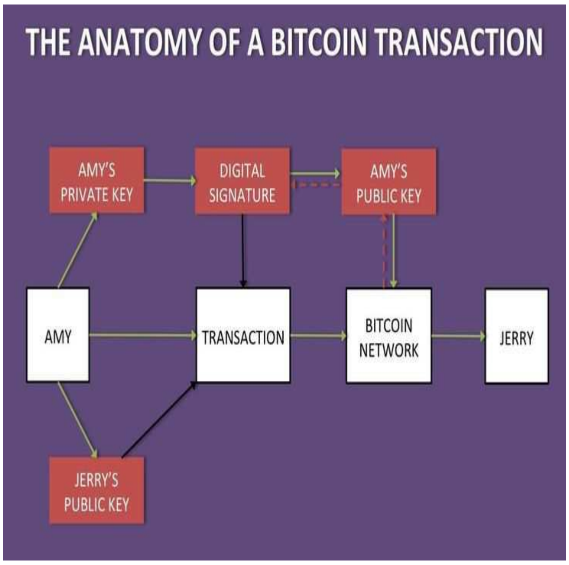

Fig 3. Anatomy of bitcoin transaction

(Source: https://www.pinterest.com/explore/bitcoin-transaction/)

4. Bitcoin Wallets

Bitcoin wallets accumulate the private keys that you want to access a bitcoin address and pay out your funds. They emerge in different forms, intended for special types of device [10,15]. You can even use paper storage to avoid having them on a computer at all. It is very essential to secure and backup your bitcoin wallet. Bitcoins are a fresh correspondent of cash and, every day, another merchant starts accepting them as payment (see Fig 4.).

We know how they are generated and how a bitcoin transaction mechanism works, but how are they stored? We store cash in a physical wallet, and bitcoin works in a similar way, except its usually digital. Well, to be completely precise, you don't technically stock up bitcoins anywhere. What you store are the protected digital keys used to access your public bitcoin addresses and sign transactions. There are five main types of wallet: desktop, mobile, web, paper and hardware.

4.1 Desktop wallets

If we have already installed the original bitcoin client (Bitcoin Core), then you are running a wallet, but may not even know it. In addition to relaying transactions on the network, this software also enables you to create a bitcoin address for transfer and getting the virtual currency [16,18], and to accumulate the private key for it. MultiBit runs on Windows, Mac OSX, and Linux. Hive is an OS X-based wallet with some distinctive features, including an app store that connects straightforwardly to bitcoin services. Some desktop wallets are customized for enhanced security: Armory falls into this group. DarkWallet – uses a lightweight browser plug-in to offer services including coin mixing in which users coins are exchanged for others, to prevent natives tracking them.

4.2 Mobile wallets

An app on your smartphone, the wallet can store up the private keys for your bitcoin addresses, and allow you to pay for things directly with your phone. In some cases, a bitcoin wallet will even take benefit of a smartphone's near-field communication (NFC) aspect, enabling you to tap the cell phone against a reader and pay with bitcoins without having to enter any information at all.

One general feature of mobile wallets is that they are not complete bitcoin clients. A full bitcoin client has to download the entire bitcoin blockchain [16,18], which is constantly growing and is multiple gigabytes in size. A lot of phones wouldn't be able to hold the blockchain in their memory, in any case. As an alternative, these mobile clients are repeatedly designed with simplified payment verification (SPV) in mind. They download a very small subset of the blockchain, and rely on other, trusted nodes in the bitcoin system to make sure that they have the exact information. Examples of mobile wallets comprise the Android based Bitcoin wallet, Mycelium.

4.3 Online wallets

Web-based wallets store your private keys online, on a computer restricted by someone else and coupled to the Internet. numerous such online services are available, and some of them bond to mobile and desktop wallets [17], replicating your addresses among different devices that you own. One gain of web-based wallets is that you can contact them from anywhere, in spite of of which device you are using. though, they also have one major drawback: unless implemented appropriately, they can put the organisation running the website in charge of your private keys – basically taking your bitcoins out of your power. That's a forbidding idea, particularly if you commence to add lots of bitcoins. Coinbase, an integrated wallet/bitcoin exchange operates its online wallet globally. Users in the US and Europe can buy bitcoin through its exchange services. Circle offers users worldwide the ability to store, send, receive and buy bitcoins. Blockchain also hosts an accepted web-based wallet, and Strongcoin offers a fusion wallet, which lets you encrypt your private address keys prior to sending them to its servers – encryption is passed out in the browser.

4.4 Hardware wallets

Hardware wallets are now very partial in number. These are keen devices that can grasp private keys electronically and make easy payments. The Trezor hardware wallet is targeted at bitcoiners who wish to preserve a substantial stash of coins [14], but do not want to rely on intermediary bitcoin storage services or not practical forms of cold storage. The compact Ledger USB Bitcoin Wallet uses smartcard protection and is available for a sensible price. KeepKey launched a hardware wallet in September 2015, which is priced at $239 a unit. The KeepKey wallet software was originally a branch of Trezor's code.

4.5 Paper wallets

One of the mainly admired and cheapest options for keeping your bitcoins safe and sound is somewhat called a paper wallet. There are numerous sites offering paper bitcoin wallet services. They will produce a bitcoin address for you and generate an image containing two QR codes: one is the public address that you can use to receive bitcoins; the other is the private key [14], which you can use to pay out bitcoins stored at that address. The profit of a paper wallet that is made suitably is that the private keys are not stored digitally anyplace, and are therefore not subject to typical cyber-attacks or hardware failures.

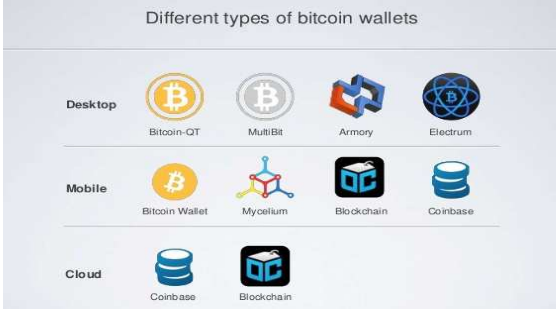

Fig 4. Bitcoin wallets
(Source: https://www.slideshare.net/CoinDesk/)

5. CONCLUSION

Bitcoin is the foremost broadly popular crypto-currency with a big user base and a wealthy network, all hinging on the incentives in place to retain the important Bitcoin blockchain. Bitcoin is a latest Internet currency that anybody can get started pulling out. There are a number of reasons you may mine: for revenue, to help secure the network, to help set up a new Internet currency, or just to gain practical experience. bitcoin mining is the tentatively decentralised method where anyone can affix a block of transactions to the bitcoin blockchain, without needing consent from any authority, and get rewarded in bitcoins for it. It is made purposely difficult, using proof of work as a defence against Sybil attacks.

The mining complexity increases with the network hashing power, so the additional processing influence of the whole network there is, the the more power somebody needs to emphasize control over the network. It works well in anticipation of any individual or coordinated group controls too much of the hashing power, at which point they can control a variety of aspects of the system. Currently 90% of blocks are mined by known pools or syndicates of miners, and if a little pool joins together, they could cause changes and affirm control over the network.

REFERENCES

[1] S. Nakamoto. Bitcoin: A peer-to-peer electronic cash system. https://bitcoin.org/bitcoin.pdf

[2] Andes: Bitcoin's kryptonite: The 51% attack. https://bitcointalk.org/index.php?topic=12435

[3] Andresen, G.: March 2013 chain fork post-mortem. BIP 50, https://en.bitcoin.it/wiki/BIP_50,

[4] Barber, S., Boyen, X., Shi, E., Uzun, E.: Bitter to better, how to make Bitcoin a better currency. In: Financial Cryptography and Data Security.

[5] Bitcoin community: Bitcoin source. https://github.com/bitcoin/bitcoin,

[6] Bitcoin community: Protocol rules. https://en.bitcoin.it/wiki/Protocol_rules.

[7] Bitcoin community: Protocol specification. https://en.bitcoin.it/wiki/Protocol_ specification.

[8] bitcoincharts.com: Bitcoin network. http://bitcoincharts.com/bitcoin/,

[9] blockchain.info: Bitcoin market capitalization. http://blockchain.info/charts/market-cap,

[10] Eyal, I., Sirer, E.G.: Majority is not enough: Bitcoin mining is vulnerable.

[11] Kroll, J.A., Davey, I.C., Felten, E.W.: The economics of Bitcoin mining or, Bitcoin in the presence of adversaries.

[12] Lee, T.B.: Four reasons Bitcoin is worth studying. http://www.forbes.com/sites/timothylee/ 2013/04/07/four-reasons-bitcoin-is-worth-studying/2/

[13] CoinDesk, "CoinDesk State of Bitcoin Q2 2014," Technical Report, CoinDesk July 2014. available at http://www.coindesk.com/state-of-bitcoin-q2-2014-report-expanding-bitcoin-economy/

[14] Wikipedia: List of crypto currencies. https://en.wikipedia.org/wiki/List_of_cryptocurrencies

[15] https://www.quora.com/What-is-Bitcoin-how-does-it-work-in-Ransomware

[16] http://seotechfeed.com/2017/03/20/how-does-bitcoin-work/

[17] http://www.righto.com/2014/02/bitcoin-mining-hard-way-algorithms.html

[18] https://www.pinterest.com/explore/bitcoin-transaction/