International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 06 Issue: 01 | Jan 2019 www.irjet.net p-ISSN: 2395-0072

Bitcoin Technology: Review

Swati S. Tawade[1]

[1]*Lecturer, Department of Computer Engineering, V.P.M's Polytechnic, Thane, Maharashtra, India*

Abstract - *Bitcoin is either virtual currency or reference to the technology. Bitcoin is a cryptocurrency created in 2009. Marketplaces called "bitcoin exchanges" allow people to buy or sell bitcoins using different currencies. Bitcoin the platform is built on the concept of "proof of work" data that is expensive and time-intensive to produce but can be easily verified. Bitcoin is a platform that hosts a digital ledger on which people can mine, store and trade bitcoins, a digital form of currency earned through a computer algorithm and tied to no central authority.*

KeyWords*: *Bitcoin, Blockchain, Bitcoin Protocol, Digital Currancy, Mining.

1. INTRODUCTION

Bitcoin has been with us since 2009, when a person (or group) under the pseudonym Satoshi Nakamoto[1][2] introduced a platform (Bitcoin, uppercase) that hosts a digital currency (bitcoin, lowercase).

1.1. How Bitcoin Works

The Bitcoin system maintains a global, distributed cryptographic ledger of transactions, or blockchain, through a consensus algorithm running on hardware scattered across the world. These machines performa computationally intense proof-of-work function called mining, which integrates BTC transactions into the blockchain. Each transaction debiting a sender's account and crediting a receiver's account is aggregated with other pending transactions into a block by a single machine and posted to the blockchain's head. A block also contains a hash of the previous head block, creating a total order. Upon receiving notice of a block's posting, other nodes in the system will verify that the transaction is in order—for instance, not improperly creating, moving, or destroying BTCs and then use the new block as the head block for future blockchain updates.[3]

In Bitcoin's case, proof of work is created through the process of "mining." To mine a bitcoin, a computer must complete a complicated algorithm, essentially going through the work of an extensive calculation in exchange for some newly minted currency. [4][5]That piece of digital currency is worth whatever the market decides through supply and demand. A key component of Bitcoin's blockchain is the fact that it is an open, distributed ledger. Through the distributed nature of this ledger, the transactions on the blockchain are verified by the consensus of every member, offering security and trust without a third-party overseer.[6]

2. BITCOIN PROTOCOL

Here, we adopt the specification of the synchronous Bitcoin protocol [7], which has the following steps for each miner m:

1) m starts a round with a local chain C.
2) m retrieves all the chains broadcast by other miners in the previous round from its receive buffer.
3) Based on some criteria, m chooses the "best" chain ˜ C.
4) m attempts to include a transaction (or a batch of transactions) into ˜ C by executing the POW algorithm.
This step may be preempted if m does not successfully solve the puzzle.
5) If m finds a new block, it broadcasts the block to the Bitcoin network. The block would be transfered to every other miner's receive buffer by the underlying communication network.
6) m continues to the next round.

The blockchain is a public, append-only, link-list based data structure which stores the entire network's transaction history in form of blocks. In each block, the transactions are stored using Merkle Tree [8], and a relatively secure time-stamp and a hash of the previous block is also stored. Figure 2 shows the working methodology that is used for creating and maintaining the blockchain. To successfully add a new block in the blockchain, the miners need to verify (mine) a block by solving a computationally difficult PoW puzzle. One can traverse the blockchain to determine the ownership of each bitcoin because the blocks are stored in an ordered fashion. However, tempering within a block is not possible as it would change the hash of the block. If a transaction in a block is tampered, the hash value of that block will change, and it will change the subsequent blocks because each block contains the hash of the previous block. The

blockchain continually grows in length due to the continuous mining process in the network.[9]

3. THE PROCESS OF ADDING A NEW BLOCK

(i) once a miner determines a valid hash value (i.e., a hash equal or lower than target) for a block, it adds the block in her local blockchain and broadcast the solution.

(ii) upon receiving a solution for a valid block, the miners will quickly check for its validity, if the solution is correct the miners update theirlocal copy of blockchain else discard the block.[10][11]

In general, the security in Bitcoin is on the assumption that the honest players control a majority of the computing resources. The primary driving factor for miners to honestly verify a block is the reward (i.e., 12.5 BTCs) that they receive upon every successful block addition in the blockchain. [12]As mentioned before that to verify a block the miners need to solve the associated hard crypto-puzzle. The probability of solving the crypto-puzzle is proportional to the number of computing resources used. As per [13], a single home miner who uses a dedicated Application-Specific Integrated Circuit (ASIC) for mining will unlikely verify a single block in years.For this reason, miners mine in the form of the so-called mining pools. All miners that are associated with a pool works collectively to mine a particular block under the control of a pool manager. Upon successful mining, the manager distributes the reward among all the associated miners proportional to the resources expended by each miner. A detailed discussion of different pooled mining approaches and their reward systems is given in [14] [15].

4. BENEFITS –

_ No Third-Party Seizure: No central authority can manipulate or seize the currency since every currency transfer happens peer-to-peer just like hard cash. In particular, bitcoins are yours and only yours, and the central authority cant take your cryptocurrency, because it does not print it, own it, and control it correspondingly.

_ Anonymity and transparency: Unless Bitcoin users publicize their wallet addresses publicly, it is tough to trace transactions back to them. However, even if the wallet addresses are publicized, a new wallet address can be easily generated. Bitcoin system dramatically increases privacy when compared to traditional currency systems where third parties potentially have access to personal financial data. Moreover, this pseudonymity is achieved without sacrificing the system transparency as all the bitcoin transactions are documented in a public ledger.

Unfortunately, numerous research works have shown that the practical technologies of clustering and flow analysis are much effective for tracing Bitcoin transaction and thereby revealing the owner involved [9] [10].

However, to fix the privacy and anonymity flaws in Bitcoin, much work has been done and many schemes proposed in the research community manage to enhance the property of anonymity [7] [6] [8].

_ No taxes and lower transaction fees: Due to its decentralized nature and pseudonymity, there is no viable way to implement a Bitcoin taxation system. In the past, Bitcoin provided instant transactions at nearly no cost.
Even now, Bitcoin has lower transaction costs than a credit card, Paypal, and bank transfers. However, the lower transaction fee is only beneficial in situations where the user performs a substantial value international transactions. This is because the average transaction fee in Bitcoin becomes higher for minimal value transfers or purchases such as paying for regular household commodities.

_ Theft resistance: Stealing of bitcoins is not possible until the adversary has the private keys (usually kept offline) that are associated with the user wallet. In particular, Bitcoin provides security by design, for instance, unlike with credit cards you dont expose your secret (private key) whenever you make a transaction. Moreover, bitcoins are free from Charge-backs, i.e., once bitcoins are sent, the transaction cannot be reversed. Since the ownership address of the sent bitcoins will be changed to the new owner, and it is impossible to revert. This ensures that there is no risk involved when receiving bitcoins.

5. Challenges:

- **High energy consumption**: Bitcoin blockchain uses PoW model to achieve distributed consensus in the network. Although the use of PoW makes the mining process more resistant to various security threats such as Sybil and double spending, it consumes a ridiculous amount of energy and computing resources [3] [4]. The miners bundle a set of transactions to create a block and to mine the block, it is hashed by varying the nonce. However, the hashing is not inherently computationally intensive, but to get

the required hash that starts with the required number of zeros, a miner has to repeat the hashing process, until the result has the proper number of zeros. This process of hashing and rehashing usually goes on thousands of times, and it is done in parallel in the Bitcoin network by all the miners. Hence it consumes lots of energy. Due to the reason mentioned above, the energy cost for Bitcoin is high in comparison to the conventional financial transactions. For instance, processing a bitcoin transaction consumes more than 5000 times as much energy as using a Visa credit card. Therefore, innovative technologies that reduce the energy consumption are required to ensure a sustainable future of Bitcoin. Furthermore, due to the continuous increase in network load and energy consumption, the time needed for bitcoin transaction processing is increasing. Wallets can be lost: Since there is no trusted third party if uses lost the private key associated with her wallet due to a hard drive crash or a virus corrupts data or lost the device carrying the key, all the bitcoins in the wallet has been considered lost for forever. There is nothing that can be done to recover the bitcoins, and these will be forever orphaned in the system. It can bankrupt a wealthy Bitcoin investor within seconds.

- **Facilitate Criminal activity:** The pseudonymity provided by the Bitcoin system helps the would-be cybercriminals to perform various illicit activities such as ransomware [70], tax evasion, underground market, and money laundering. However, the law enforcement could catch the criminals with careful analysis of blockchain data because the transactions are only pseudonymous and the whole history is public. Hence, criminals are starting to use other digital currencies such as Monero or ZCash, which is built specifically for increased user privacy.

REFERENCES

[1] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," Available: http:// bitcoin.org/ bitcoin.pdf , 2008.

[2] G. O. Karame, E. Androulaki, and S. Capkun, "Double-spending fast payments in bitcoin," in Proceedings of the 2012 ACM Conference on Computer and Communications Security, ser. CCS '12. New York, NY, USA: ACM, 2012, pp. 906–917.

[3] E. Heilman, A. Kendler, A. Zohar, and S. Goldberg, "Eclipse attacks on bitcoin's peer-to-peer network," in Proceedings of the 24th USENIX Conference on Security Symposium, ser. SEC'15. USENIX Association, 2015, pp. 129–144.

[4] C. Decker and R. Wattenhofer, "Bitcoin transaction malleability and mtgox," in ESORICS 2014: 19th European Symposium on Research in Computer Security. Springer International Publishing, 2014, pp. 313–326.

[5] A. Maria, Z. Aviv, and V. Laurent, "Hijacking bitcoin: Routing attacks on cryptocurrencies," in Security and Privacy (SP), 2017 IEEE Symposium on. IEEE, 2017.

[6] I. Eyal and E. G. Sirer, "Majority is not enough: Bitcoin mining is vulnerable," in Financial Cryptography and Data Security: 18th International Conference. Springer Berlin Heidelberg, 2014, pp. 436– 454.

[7] A. Sapirshtein, Y. Sompolinsky, and A. Zohar, "Optimal selfish mining strategies in bitcoin," in Financial Cryptography and Data Security: 20th International Conference, FC 2016, Christ Church, Barbados,February 22–26, 2016. Springer Berlin Heidelberg, 2017, pp. 515–532.

[8] K. Nayak, S. Kumar, A. Miller, and E. Shi, "Stubborn mining:Generalizing selfish mining and combining with an eclipse attack," in 2016 IEEE European Symposium on Security and Privacy (EuroS P), 2016, pp. 305–320.

[9] I. Eyal, "The miner's dilemma," in Proceedings of the 2015 IEEE Symposium on Security and Privacy, ser. SP '15. Washington, DC, USA: IEEE Computer Society, 2015, pp. 89–103. [10] J. Bonneau, A. Miller, J. Clark, A. Narayanan, J. A. Kroll, and E. W. Felten, "Sok: Research perspectives and challenges for bitcoin and cryptocurrencies," in 2015 IEEE Symposium on Security and Privacy, May 2015, pp. 104–121.

[10] WikiLeaks, "Donation request via cyrptocurriencies," Available: https: // shop.wikileaks.org/donate.

[11] W. F. Slater, "Bitcoin: A current look at the worlds most popular, enigmatic and controversial digital cryptocurrency," in A Presentation for Forensecure 2014, April 2014.

[12] "Status about bitcoin technoogy was obtained from-what 2016 holds for bitcoin business," Available: http://www.coindesk.com/ what-2016-holds-for-bitcoin-businesses/.

[13] M. T. Alam, H. Li, and A. Patidar, "Bitcoin for smart trading in smart grid," in The 21st IEEE International

Workshop on Local and Metropolitan Area Networks, April 2015, pp. 1–2.

[14] Y. Zhang and J. Wen, "An iot electric business model based on the protocol of bitcoin," in 2015 18th International Conference on Intelligence in Next Generation Networks, Feb 2015, pp. 184–191.