International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.177
Volume 7 Issue V, May 2019- Available at www.ijraset.com

A Meta-Analysis on Blockchain Technology and Bitcoins

Mrs. Divya K V [1], T Gayathri[2], Soumya B Sunny[3], Priyanka Kumari[4], Malli Venkatesh Vardhan P[5]
[1]*Assistant Professor,* [2, 3, 4, 5]*Students, Department of Information Science, New Horizon College of Engineering, Bangalore, Karnataka 560103, India*

Abstract: ***A blockchain is one type of a distributed ledger that consists of replicated, shared, and synchronized data over the Internet. It is a distributed database of records of all transactions or digital event that have been executed and shared among participating parties. Blockchain is the backbone Technology of Digital CryptoCurrency, BitCoin. The bitcoin is a cryptocurrency and is used to exchange digital assets online. Bitcoin uses cryptographic proof instead of third-party trust for two parties to execute transactions over the internet. Each transaction protects through digital signature. As one of its first implementations, bitcoin as a cryptocurrency has gained a lot of attention. In this paper, we presented a organized investigation of blockchain and bitcoins***

Keywords: Blockchain, Bitcoin, CryptoCurrency

I. INTODUCTION

Blockchain technology was first introduced as Bitcoin's underlying technology but soon later its extendable capabilities have been recognized. The peer-to-peer cryptocurrency, Bitcoin, is a core innovation in the financial sector nowadays. Its underlying technology, blockchain, is a type of a distributed ledger especially suitable for processing time ordered data. In addition, embedded cryptography functions of blockchain technology enable integrity of ledgers, authenticity of transactions, and privacy of transactions without a centralized control actor. Those make the blockchain different from traditional distributed database systems being used in the financial sector, e.g., it is practically impossible to modify or delete records of a ledger in the blockchain. This distributed and decentralized nature of the blockchain has attracteded financial institutions over the world to replace existing backbone technologies with blockchain technology.

Blockchain keeps a record of all data exchanges — this record is referred to as a "ledger" in the cryptocurrency world, and each data exchange is a "transaction". Every verified transaction is added to the ledger as a "block" It utilizes a distributed system to verify each transaction — a peer-to-peer network of nodes. Once signed and verified, the new transaction is added to the blockchain and cannot be altered In the cryptocurrency world, your wallet address represents public key and your private key is what let's you authorize transfers, withdrawals, and other actions with your digital property like cryptocurrencies. As an aside, this is why it's so important to keep your private key safe — anyone who has your private key can use it to access any of your digital assets associated with your public key and do what they want with it! Each transaction in that ledger will have the same data: a digital signature, a public key, a timestamp, and a unique ID. For instance, the logistics sector considers blockchain technology for real-time visibility, improved efficiency, transparency, verifiability, and cost reduction for logistics. The property sector is adopting blockchain technology as well for digital but unforgeable property records, few disputes, transparency, verifiability, and lower transfer fees. The food sector is also investing blockchain technology to trace the movements of foods and tackle contamination faster.

II. HYPERLEDGER BLOCKCHAIN FABRIC

A Blockchain is better understood in the state model: replication of the machine, in which a service maintains a state and clients recall operations that transform the state and generate an output. A blockchain emulates a "trusted" processing service via a distributed protocol managed by nodes connected to the Internet. The service represents or creates a resource in which all nodes have an interest. The nodes share the common goal of providing the service but do not trust each other. In an "unlicensed" blockchain like the one beneath the bitcoincryptocurrency, anyone can manage a node and participate through CPU and demonstration spending cycles to a "work demonstration". On the other hand, blockchain of the "authorized" control model participating in the validation and in the protocol: these nodes usually have an established identity and form a consortium.

A Swanson report compares the two models. Hyperledger [1] aims to advance blockchain technology by identifying and implementing the open standard platform for all distributed recordings, which can transform the way business deals are done

globally. Hyperledger fabric is an implementation of a distributed accounting platform for the execution of smart contracts, exploiting known and proven technologies, with a modular architecture allowing the implementation of various functions. Distributed structure accounting protocol is managed by colleagues. The tissue distinguishes two types of pears: the validation homologue and the non-validation homologue. A validation peer is a network node responsible for executing consent, validating the transaction, and managing a ledger. Non-validating peer is a node that acts as a proxy to connect clients to peer validation. A non-invalid peer does not execute transactions, but can verify them. There are three types of transactions that distribute the transaction, invoke the transaction and the transaction querry. Hyperledger Fabric is a blockchain platform licensed for business purposes. It is open source and standards-based, manages user-defined smart contracts, supports strong security, and identifies features and uses of a modular architecture with connectable consent protocols.

The advantages are as it creates an enterprise-grade , open-source distributed ledger framework and code base.It helps in identifying and realizing a cross-industry open standard platform for distributed ledgers .the disadvantage is that it is not trust worthy

III. BITCOIN CRYPTOCURRENCY

Bitcoin has achieved results in terms of widespread acceptance and has spread by promising its users a completely decentralized and inexpensive virtual currency system. It show that Bitcoin vital operations and decisions are not decentralized [4]. A limited set of entities that control the service, decision-making, extraction, and resolution processes. It provide more information on how third parties can unilaterally decide to "devalue" a specific set of bitcoinaddressess belonging to any entity participating in the system. Ultimately, it explore ways to improve decentralization in the Bitcoin system. Bitcoin users may, for example, decide not to accept coins that appear to come from a particular address, as the use of any currency can be traced back to its origin; this disavowal on the part of the users will have the effect of deflating practically the value of these parts, because the other users are reluctant to accept these pieces as payment. It call this effect the contamination and the postulate of the currency which can have a negative effect on the use of the pectoral currency as currency.

While Bitcoin's original design indicates a completely decentralized bitcoin, recent Bitcoin events reveal the true limits of decentralization in this system. A large number of centralized services currently host bitcoin and control a significant share in the bitcoin market. Bitcoin developers retain privileged rights in conflict resolution and formal client maintenance. These entities can decide the fate of the entire bitcoin system, ignoring the will, rights and computing power of the multitude of users that populate the network. At present, almost all financial services are controlled by governments and banks; Bitcoin replaces these powerful entities with other entities such as IT developers and exploration pool owners. Although current systems are governed by transparent and widely studied laws, crucial bitcoin decisions are made through the exchange of opinions among developers and owners of mineral pools on mailing lists. In this sense, Bitcoin is now in an unknown territory; on the one hand, the bitcoin ecosystem is far from being decentralized, on the other hand, the increasing centralization of the system does not adhere to transparent laws / regulations. This could have serious consequences on the fate and reputation of the system.

The advantages are that it fully decentralized and low-cost virtual currency system. It enhance the decentralization in the bitcoin system It increase the transparency of the client development process. The disadvantages are that the existence of public logs in the bitcoin have some negative effects on this currency which extend beyond known privacy and anonymity concern.

IV. ANONYMITY IN THE BITCOIN SYSTEM

A peer-to-peer electronic money system is a complex problem in the system , users are identified only by public keys. An attacker who wishes to remove the issue from his user will try to create one-to-many mapping between users and public key and association information external to the system with users. Bitcoin frustrates this attack in storing a user's card on their public keys only on that user node and allowing each user to generate all required public keys. It was considered as the topological structure of two networks derived from the public transaction of bitcoin history [3]. It shows that both networks have a non trivial topological structure that provides implications for anonymity.

Combine these structures with external information and techniques such as context discovery and flow analysis to investigate a so-called bitcointheft . Before performing the analysis, it expect the user network to be larger and consist of trees representing bitcoin flows between public keys as long as they are not connected to other public keys .However, the analysis reveals that the user network has a considerable cyclical structure and now considers the involvement of this structure with other aspects of the bitcoin system for anonymity. The network can be used in several ways to derive information about Bitcoin users who can use global network properties such as degree distribution to identify outliers that can use local network properties to examine the context a user works by observing the user with whom they interact directly or indirectly. The dynamic nature of the user network also allows us to

perform flow and time analyzes that it can examine in a meaningful way. Bitcoin runs over time between user groups. Bitcoin is an electronic analog of cash in the online world is decentralized, there is no central authority responsible for issuing Bitcoin and there is no need to involve trusted third parties during transfers online. However, this flexibility is so expensive that the entire Bitcoin transaction history is publicly available. In this paper, we have studied the structure of two derived networks in this dataset and their implications for user anonymity. By using an appropriate network representation, it is possible to associate many public keys with each other and the external identification information with the appropriate tools, the activities of the known users can be observed in detail. Active analytics in which an interested party can potentially distribute marked bitcoin and collaborating users discover more information. It also believe that large centralized services such as exchange and portfolio services are able to identify and track a significant portion of the technical members of Bitcoin community user activities warned that high anonymity was not a primary goal of the bitcoin system design. However, occasional users need to be aware of this especially when sending Bitcoin to users and organizations they would prefer not to be publicly associated.

The advantages are that the large centralized services such as the exchanges and wallet services are capable of identifying and tracking considerable portions of user activity.Possible to associate many public-keys with each other, and with external identifying information by using an appropriate network representation.The disadvantage is that anonymity in bitcoin, a peer-to-peer electronic currency system, is a complicated issue.

V. INFORMATION TRANSMISSION IN THE BITCOIN NETWORK

Bitcoin is a digital currency that unlike traditional currencies does not rely on centralized authority. But on a network of volunteers who collectively implement a left-handed register and check the transactions , it analyze how Bitcoin uses a multi-hop transmission to propagate transactions and blocks to the network to update general ledger responses [3]. It can use the information collected to test the hypothesis that propagation delay in the network is the main cause of multi-range forks.

Block chain forks should be avoided because they are symptomatic of the coherence between the replicas of the network. Bitcoin has experienced rapid growth in both value and number of transactions, mainly due to the innovative use of a peer-to-peer network for user-to-user transfer.

This is the fundamental difference from previous research that focused on building systems based on a centralized issuer to create credit between users.

These systems forced users to trust the original sender, which was always used to permanently delete transactions. The main problem among the solutions to be solved is distributed monitoring and transaction validation. For this reason, the network must reach a consensus on the account balances it tracks and valid transactions.

Bitcoin achieves this with the best guarantees described as a final consistency: the different replicas may be temporarily inconsistent, but will eventually be synchronized to reflect the current transaction history Since the transactions are validated against the replication states, any inconsistency introduces uncertainty as to the validity of a given transaction. In addition, an inconsistency can make it easier for an attacker to rewrite the transaction history. In this work, it analyzed Bitcoin from the point of view of the network, that is, when the information is disseminated or propagated in the Bitcoin network. It identify the main weaknesses and the resulting problems.

It analyzed the synchronization mechanism that fails to synchronize the information stored in the general ledger with a not insignificant probability.

It make changes to the Bitcoin protocol that reduce the risk of blockchain fork. Our measurements show that a single node implementing these changes reduces the number of chain forks in the network by more than 50%.

However, the root cause of the problem is intrinsic to the way information is propagated on the network.The advantages are that it reduces the risk of a blockchain fork and it reduces the number of blockchain forks in the network by over 50%.the disadvantages are that it delays the clearing of transactions and also poses threat to the network itself.

VI. CONCLUSIONS

Bitcoin and related cryptocurrencies have became amazingly popular. The blockchain technology provides a de-centralized, open, Byzantine fault-tolerant transaction mechanism, and promises to become the infrastructure for a new generation of Internet interaction, including anonymous online payments remittance, and trans-action of digital assets. Ongoing work explores smart digital contracts, enabling anonymous parties to programmatically enforce complex agreements.

REFERENCES

[1] C. Cachin, "Architecture of the HyperledgerBlockchain Fabric," July 2016
[2] A. Gervais, G. Karame, V. Capkun, and S. Capkun, "Is Bitcoin a Decentralized Currency?," IEEE Security & Privacy, vol. 12, no. xx, pp. 54–60, May-June 2014.
[3] Fergal Reid, Martin HarriganAn Analysis of Anonymity in the Bitcoin System, 2011 IEEE International Conference on Privacy, Security, Risk, and Trust, and IEEE International Conference on Social Computing.
[4] Christian Decker,RogerWattenhoferInformation Propagation in the Bitcoin Network, 13-th IEEE International Conference on Peer-to-Peer Computing, 2013.
[5] B. Lee and J.-H. Lee, "Blockchain-based secure firmware update for embedded devices in an Internet of Things environment," Journal of Supercomputing, vol. 73, no. 3, pp. 1152–1167, March 2017.
[6] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008.
[7] PwC, "Top financial services issues of 2017 ", December 2016.
[8] G. Wood, "Ethereum: A Secure Decentralised Generalized Transaction Ledger," 2014
[9] R. C. Merkle, "A digital signature based on a conventional encryption function," in Proc. of the Advances in Cryptology, pp. 369–378, 1987.
[10] M. Castro and B. Liskov, "Practical Byzantine Fault Tolerance and Proactive Recovery," ACM Transactions on Computer Systems, vol. 20, no. 4, pp. 398–461, November 2002.
[11] A. Clement, E. Wong, L. Alvisi, M. Dahlin, and M. Marchetti, "Making Byzantine Fault Tolerant Systems Tolerate Byzantine Faults," in Proc. of the 6th USENIX Symposium on Networked Systems Design and Implementation, pp. 153–168, 2009.
[12] F. Brezo and P. Bringas, "Issues and Risks Associated with Cryptocurrencies such as Bitcoin," in Proc. of the 2nd International Conference on Social Eco-Informatics, 2012.
[13] J.-H. Lee and M. Pilkington, "How the Blockchain Revolution Will Reshape the Consumer Electronics Industry," IEEE Consumer Electronics Magazine, vol. 6, no. 3, pp. 19–23, July 2017.
[14] M. Pilkington, R. Crudu, and L. Grant, "Blockchain and bitcoin as a way to lift a country out of poverty – tourism 2.0 and e-governance in the Republic of Moldova," International Journal of Internet Technology and Secured Transactions, vol. 7, no. 2, pp. 115–143, October 2017.