CRYPTOCURRENCY MINING THROUGH BLOCKCHAIN USING PYTHON

Conference Paper · June 2020

1 author:

Paras Khandelwal
Rashtrasant Tukadoji Maharaj Nagpur University
3 PUBLICATIONS **23** CITATIONS

SEE PROFILE

CRYPTOCURRENCY MINING THROUGH BLOCKCHAIN USING PYTHON

Paras Manish khandelwal, Student**, Shriram Hanmantrao Patil,** Student**, Dasari Anantha Reddy,** Assistant Professor
Department of Information Technology, KITS, Ramtek, Nagpur-441106.

Abstract: Block chain, the foundation of crypto currency has received extensive attention in last five years. It serves as an immutable ledger which allows transactions take place in a decentralized manner. Basically block chain is a distributed data storage consisting of containers (blocks) which are connected and crypto currency uses the block chain technology. If the data we store on a block is a list of transactions, the coins transferred in transactions form the crypto currency. The security mechanism through hashing used in block chain keeps the transactions safe. We use a typical consensus algorithm which is designed to achieve reliability in a network involving multiple nodes in the block chain. We also create a user interface and a wallet for convenience of the users. Block chain based applications are springing up, covering numerous fields including financial services, reputation system and IOT, and so on.

KEYWORDS: *Block chain, Decentralization, Consensus, Nodes, and Crypto currency*

Introduction: Blockchain, the foundation of cryptocurrency has received extensive attention in last five years. It serves as an immutable ledger which allows transactions take place in a decentralized manner. Basically blockchain is a distributed data storage consisting of containers (blocks) which are connected and cryptocurrency uses the blockchain technology. Blockchain is nothing but one big ledger on the cloud which decentralizes complex management systems into distributed and simpler management technology. The current currency trends contains a huge risk and very complicated finance management system, similarly there are various centralized systems in healthcare, supply chain, Internet of things where there is an enormous need of decentralization.

Blockchain provides a decentralized approach as a solution. If the data we store on a block is a list of transactions, the coins transferred in transactions form the crypto currency. The security mechanism through hashing used in block chain keeps the transactions safe. We use a typical consensus algorithm which is designed to achieve reliability in a network involving multiple nodes in the blockchain. We also create a user interface and a wallet for convenience of the users. The initial objective is to create a live and working blockchain environment. The blockchain has the capability to disrupt various sectors such as agriculture, banking & finance, healthcare management, IOT, governance and many more.

Blockchain is the technology of tomorrow and the implementation of which has already begun, countries such as Japan, Germany, and France have welcomed blockchain and cryptocurrency in every sector. In India, the state of Andhra Pradesh has already started the implementation of block chain in agriculture. To manage the block chain a lot of computing power and various other resources are required, and a crypto currency plays as an incentive system for the people and organizations (miners) who manage the block chain environment. Block chain is today what internet was in 1990, unlike social media and mail, it is not one of the use cases of internet but rather a newer and upcoming dawn in the era of technological advancements.

Review of Literature: Christian Decker, et.al.,(2014)[1]The Bit coin system only provides eventual consistency. For everyday life, the time to confirm a Bit coin transaction is prohibitively slow. In this paper we propose a new system, built on the Bit coin block chain, which enables strong consistency. Our system, Peer Census, acts as a certification authority, manages peer identities in a peer-to-peer network, and ultimately enhances Bit coin and similar systems with strong consistency. Our extensive analysis shows that Peer Census is in a secure state with high probability. We also show how Discoin, a Bit coin variant that decouples block creation and transaction confirmation, can be built on top of Peer Census, enabling real-time payments. Unlike Bit coin, once transactions in Discoin are committed, they stay committed**.**

Satoshi Nakamoto,et al., (2015) [2] a purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network.

Ittay Eyal et.al., (2016) [3] the Bit coin crypto currency records its transactions in a pub-lic log called the block chain. Its security rests critically on the distributed protocol that maintains the block chain, run by participants called miners. Conventional wisdom asserts that the mining protocol is incentive-compatible and secure against colluding minority groups, that is, it incentivizes miners to follow the protocol as prescribed.

Stephen Chan, et.al.,(2015)[4] analyzed statistical properties of the largest crypto currencies (determined by market capitalization), of which Bit coin is the most prominent example.

Quan-Lin Li1, et.al., (2018)[5] In this paper, they have developed queuing theory of block chain systems and provide system performance evaluation. To do this, we design a Markovian batch-service queueing system with two different service stages, which are suitable to well express the mining process in the miners pool and the building of a new block chain. By using the matrix-geometric solution, we obtain a system stable condition and express three key performance measures: (a) The average number of transactions in the queue, (b) the average number of transactions in a block, and (c) the average transaction-confirmation time. Finally, they used numerical examples to verify computability of our theoretical results. Although our queueing model here is simple only under exponential or Poisson assumptions, our analytic method will open a series of potentially. Promising research in queueing theory of block chain systems.

Harsha Patil et.al.,(2019)[6] the objective of this research paper is to focuses on working framework of Block chain Technology and enlightens the security of Block chain technology through vulnerability

Naseema Shaik, et al.,(201)[7] Block chain is a decentralized and distributed log of records, where, blocks containing a set of transactions are chained together by cryptographic hash value. Transactions originating from a node are validated by participating nodes and a set of transactions are added into a block by a "mining" node. Any mining node with sufficient compute power that solves a cryptographic problem can generate and broadcast a new block containing the set of validated transactions.

Block chain is a technology that allows data to be stored and exchanged on a peer-to-peer1 (P2P) basis. Structurally, block chain data can be consulted, shared and secured thanks to consensus-based algorithms2. It is used in a decentralized manner and removes the need for intermediaries, or "trusted third parties". In this paper we are discussed on Bloch chain technology instead of digital currency.

Block chain Approach: Block chain is a decentralized, distributed, and oftentimes public, digital ledger that is used to record transactions across many computers so that any involved record cannot be altered retroactively, without the alteration of all subsequent blocks. This allows the participants to verify and audit transactions independently and relatively inexpensively. A block chain database is managed autonomously using a peer-to-peer network and a distributed time stamping server. They are authenticated by mass collaboration powered by collective self-interests such a design facilitates robust workflow where participants' uncertainty regarding data security is marginal. The use of a block chain removes the characteristic of infinite reproducibility from a digital asset. It confirms that each unit of value was transferred only once, solving the long-standing problem of double spending. A block chain has been described as a value-exchange protocol. A block chain can maintain title rights because, when properly set up to detail the exchange agreement, it provides a record that compels offer and acceptance.

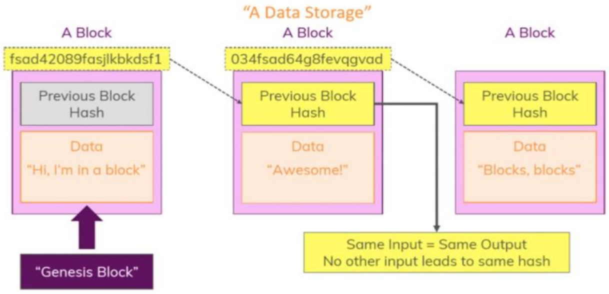


Fig:1 Blockchain

Blocks hold batches of valid transactions that are hashed and encoded into a Merkle tree. Each block includes the cryptographic hash of the prior block in the block chain, linking the two. The linked blocks form a chain. This iterative process confirms the integrity of the previous block; all the way back to the original genesis block.

The block time is the average time it takes for the network to generate one extra block in the block chain. Some block chains create a new block as frequently as every five seconds. By the time of block completion, the included data becomes verifiable. In crypto currency, this is practically when the transaction takes place, so a shorter block time means faster transactions. The block time for Ethereum is set to between 14 and 15 seconds, while for bit coin it is 10 minute

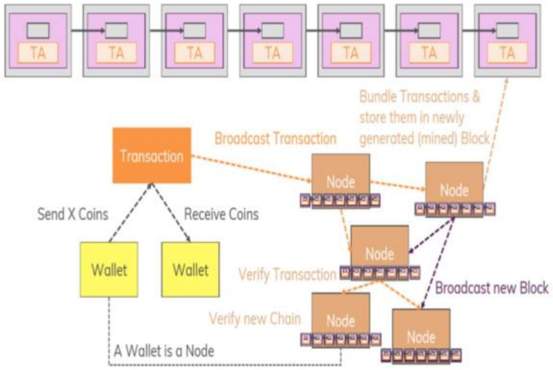
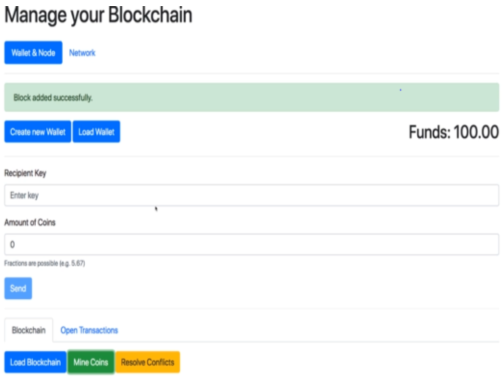


Fig. 3.2 System Architecture of Crypto currency mining through block chain

Stem Architecture shows how the whole system works from both the block chain management point of view, miner point of view and user point of view. It gives the basic idea of how the transactions are stored in the form of data and how the nodes are interconnected in peer to peer network, and how the user can send and receive funds using the GUI provided in the wallet.

Results: The implementation details are provided in the form of results which appear in the different modules.



Manage your Blockchain

Block added successfully.

Funds: 100.00

Recipient Key

Enter key

Amount of Coins

0

Fractions are possible (e.g. 5.67)

Fig3: Home Screen

Above figure present the wallet of the project with wallet and nodes. It also consists of creating new wallet, loading a wallet with the recipent key, amount of coins that wants to be send. It also gives option like open transaction and load blockchain. At the top of right corner it shows available funds.After making a transaction successful it creats a one block.

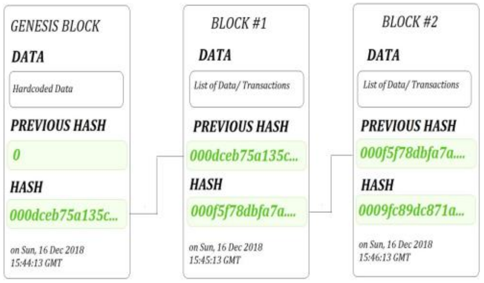
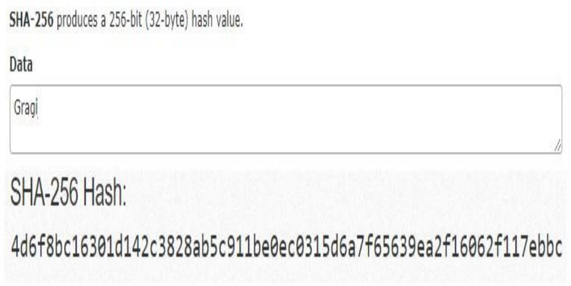


Fig4:Block chain

After making a successful transaction it creates a block and that bock is added in distributed network called as block chain. It is collection of 'n' number of blocks, which are connected to each other and form a block chain which is distributed. They are connected to each other by using hash values of next block. Each new block stores the previous blocks. That makes block chain is distributed.

Bit coin uses SHA 256 while Ethereal uses Keccak-256 algorithms respectively. The only important thing to take away is that this generated hash key is the one that stores data of current block and address of the next block, hence linking both the blocks and keeping track of the previous block. In given diagram below, I have generated hash of a string using SHA 256 algorithm, you too can generate hash values from here.



SHA-256 produces a 256-bit (32-byte) hash value.

Data

Gragi

SHA-256 Hash:

4d6f8bc16301d142c3828ab5c911be0ec0315d6a7f65639ea2f16062f117ebbc

Fig5: SHA-256 Conversion

Conclusion: Same as paypal or bank credits the crypto currencies could be considered as a digital currency used for online transactions. A digital ledger is the responsible item over recording the digital transactions and balances which is in term called as block chain. Wallets are the software's used to access the crypto currencies.

The transactions are created within the wallets which are broadcasted to the whole network which in turn is added onto the block chain. Through the online exchanges of crypto currency or with the help of a broker the crypto currencies could be bought. There are many other crypto currencies beyond Bit coin. The digital currency like bit coin which implement cryptography over block chain are decentralized and hence is entirely different from flat currencies provided by banks and other government organizations. An algorithm and the miners are the personals who have the sole control over the digital currency rather than a centralized power.

References

1. C.Decker , J. Seidel and R. Wattenhofer, "Bitcoin meets Strong Consistency" , in proceedings of the 17th International conference on Distributed computing and Networking (ICDCN). Singapore,Singapore : ACM , 2016, p. 13.

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

3. I. Eyal, A. E. Gencer, E. G. Sirer and R. Van Renesse, "Bitcoing : A Scalable blockchain protocol" , in proceedings of 13th USENIX Symposium on Networked Systems Design and Implementation(NSDI16) , Santo Clara, CA , USA ,2016, pp.45-59.

4. Chu , Jeffrey, Saraless Nadarajah , and Stephen chan. 2015. Statistical analysis of the exchange rate of Bitcoin. PLoS ONE10:e0133678 ,doi : 10.1371 / joural.pone.0133678.

5. S. Haber, W.S. Stornatta, "How to time stap a digital document," In Journal of cryptology, Vol. 3, no .2 pages 99-111, 1991.

6. H. Marsias, X.S. Avila, and J.J .Quisquator, "Design of a secure time stamping service with minimal trust requirements ,"In 20th Symposium on Information Theory in the Benelux, May 1999.

7. M. Moser, "Anonymity of bitcoin transactions: An Analysis of mixing services," in proceedings of Miinster Bitcoin

conference, Miinster, Germany, 2013, pp.17-18.

8. G. Maxwell, “coinjoin: Bitcoin privacy for the real World,” in Post on Bitcoin forum, 2013.

9. E. Swans: Bitcoin mining calculator, http://www.alloscomp.com/bitcoin/calculator,retrived Sep. 2013

10. J. A. Kroll, I. C. Davey, E. W. Felten: The economics of Bit coin Mining or, Bit coin in the presence of adversaries. In : Workshop on the Economics of Information Security (2013).

11. A. Biryukuv, D. Khovratovich, and I. Pustogarov, “Deononymisation of clients in bit coin P2P network”, in proceedings of the 2014 ACM SIGSAG conference on computer and communications security NewYork , NY , USA ,pp. 15-29.

12. S.King and S.Nadal, “Ppcoin : Peer-to-peer Cryptocurrency with proof-of-Stake”,self.published paper,August , Vol. 19, 2012. [12].

13. J. Baralo , “User privacy in the public bitcoin blockchain” ,2014. [13]. G. Wood , “Ethereum : A Secure decentralized generalized transaction ledger” , Ethereum Project Yellow paper, 2014.

14. Eli Ben-Sarson, Alessandro chiesay ,etc. , Zerocash : Decentralized Anonymous payments from Bitcoin , IEEE Sysposium on security and privacy , 2014.

15. R. Dennis and G. Owen , “Rep on the block : A next generation reputation system based on the block chain” , in 2015 10th International conference for Internet Technology and secured Transactions (ICTST) Dec 2015 ,pp-131 – 138.

16. V.Buterin, “On Public and Private Block chains”, 2015 accessed: 2017-07-01[Online].Available: https://blog.ethercum.org/2015/08/07/on -public- and-private-block chains.

17. M.Mettler, “Block chain technology in healthcare : The revolution Starts here” in 2016 IEEE 18th International conference on e-Health Networking Applications and services (Healthcom) Sept-2016,pp.1-3.

18. F.Tscharsch and B. Schecurmann, “ Bitcoin and beyond : A technical survey on decentralized digital currencies” ,IEEE communications surveys Tutorials,vol.18 ,no.3 pp. 2084-2123, 2016.

19. Briere Marie,k :m Oosterlinck and Ariane Szafarz , 2015 . Virtual Currency , tangible return : portfolio diversification with Bitcoins, Journal of Asset management