International Journal of Computer Applications Technology and Research
Volume 9–Issue 09, 254-256, 2020, ISSN:-2319–8656

Survey on Blockchain -Future of Security for Cryptocurrency- Bitcoin and Ethereum

Urvashi M. Chaudhari
Asst. Professor
Dept. of Computer Engineering
Sardar Patel College of Engineering,
Bakrol- Anand, Gujarat, India.

Brijesh Y. Panchal
M.Tech Scholar
Dept. of Computer Engineering
Dharmsinh Desai University,
Nadiad, Gujarat, India.

Abstract: As the use of online transaction is increasing day by day, security measure parameter is difficult to manage. In that case Blockchain enables peer-to-peer transfer of digital assets without any intermediaries in a secure manner with use of verification and validation operation by different miner nodes of decentralized network. Blockchain technology also supports the cryptocurrencies like bitcoin and ethereum for amount transfer digitally with secure communication.

Keyword: Blockchain, Block, Transaction, Bitcoin, Ethereum.

1. INTRODUCTION

Unlike traditional methods, blockchain enables peer-to-peer transfer of digital assets without any intermediaries [1]. Blockchain is a chain of sequential blocks, these blocks store all transactions of public ledger. The chain of Blocks extending continuously whenever new block append on it. Blockchain works in a decentralized network with the use of cryptographic hash functions, digital signatures and distributed consensus algorithms. All the transactions occur in a decentralized manner that eliminates the requirement for any intermediaries to validate and verify the transactions [3]. Blockchain has some key characteristics, such as decentralization, transparency, immutability, and auditability [3]. A Blockchain transactions are the a tasks that are stored in public records. These records referred as Block. As mentioned earlier blocks are executed, implemented and stored in blockchain for validation by all miners of the blockchain network. Each previous transaction can be reviewed at any time but it cannot be updated by miners [6].

2. BLOCKCHAIN ARCHITECTURE

A node initiates a transaction in a decentralized blockchain network with digital signature using private key cryptography. A transaction can be considered as a data structure which, represents transmission of digital assets between peers on the blockchain network. All the transactions are stored in an unconfirmed transaction pool and propagated in the network by using a flooding protocol known as Gossip protocol [3].In the case of transactions, it is the responsibility of the peers to select and validate these transactions based on preset criteria. After the verification and validation of transaction based on preset criteria by the miners, who use their computational power for the verification and validation of the blocks of their peers to know whether their peers have sufficient balance for the transaction or not. Once the verification and validation is completed, transaction is included in a block. Miner nodes need to solve a computational puzzle and spent a sufficient amount of their computing resources to publish a block [3]. The miner node who solves the puzzle first will become a winner node and it grabs the chance to create a new block. A small amount of incentive is given to the winner node on the successful creation of a new block. All the peers in the network, verify the newly created block using a consensus mechanism, which is a technique that assist a decentralized network to come on some agreement for certain matters. Once it is completed, the newly generated block will be added to the existing chain and the local copy of each peer's immutable ledger. At this point of time, the transaction is confirmed. The next block links itself with the newly created block with the use of cryptographic hash pointer. Now the block obtains its

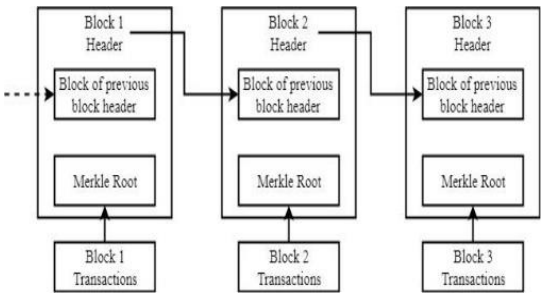

Fig.1 The structure of the Blockchain [4]

first confirmation while the transaction obtains the second confirmation [3]. Whenever a new block is appended to the existing chain, the transaction will be reconfirmed. In general, a transaction needs six confirmations in the network to be considered final [2].

Blockchain Structure has two parts block header and block body. The block is a collection of related information and record data. The data structure of the blockchain is composed of a block header and a block body. Block header contains metadata, which

are of size 80 bytes. Block header contains the hash value of the previous block, to connect the previous block for integrity ensurance of the blockchain. Block body contains business data of variable size. Markle tree is a hash of binary tree which is used for validation of the integrity of the data structure. It is mandatory that a hash node pair as a leaf node, for making node pair hash and inserting a new hash node in a hash binary tree. The hash process generates a unique Markle root, which is used for business record[5].

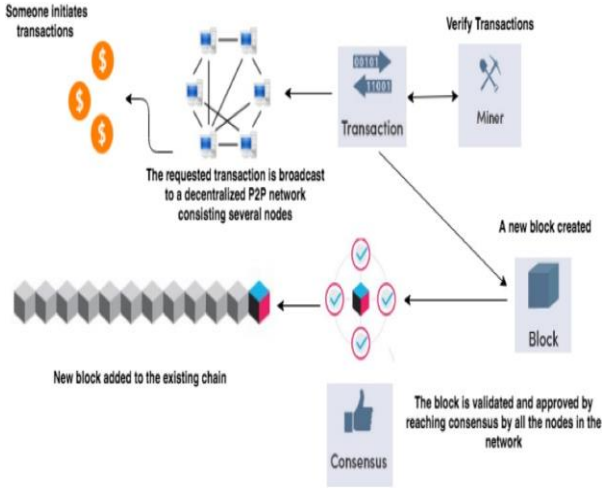

Fig.2 Functional Diagram of Blockchain [3]

3. BLOCKCHAIN TRANSCATION PROCESS

The first step of the blockchain transaction process is the identity verification of the sender, to know that the transaction is requested by the authorized sender and not by anyone else. For this verification, Blockchain uses digital signatures (public and private keys).

Transaction validation is done independently by all miners based on differ- ent criteria. Elliptic curve digital signature algorithm (ECDSA) is used by blockchain [3]. It ensures that the funds can only be spent by their true possessors. The signature in each transaction contains 256 bits.

After completion of validation by miners, new block is generated and ap- pended to blockchain with use of consensus mechanism.

4. BITCOIN

According to the original Bitcoin whitepaper, the main purpose of this digital cryptocurrency was to allow a decentralized electronic cash payment system between different parties by eliminating central intermediaries [3].A Bitcoin transaction refer to transfer the ownership of some bitcoin amount to another bitcoin address(Receiver bitcoin address). For the transaction initiation which is done by bitcoin wallet of a client and later it broadcasts to the network. The nodes on the network will further rebroadcast the transaction and include that transac- tion in the block ,nodes are mining only when if the transaction is valid. It takes approximately 10 minutes to include the transaction along with other transactions in a block [3]. The receiver should see the amount of transaction in their wallet after validation. The major element of structure of a bitcoin is unspent transaction output (UTXO), it refers to the output amount of a transaction, which is received by a user and it also refers to the the capability of spending in the future. All the received amount in a Bitcoin wallet maintained as a separate entity.

$$Inputsoutputs = Transactionfees \quad (1)$$

Miners include their individual coinbase transaction with the transaction data, which miners are trying to verify and validate during block mining. A coinbase transaction is a unique type of bitcoin transaction which can created by only miner. This type of transaction has outputs. The coinbase transaction will send the block reward and the sum of the transaction fees to the miner on given address. It shows that a miner has to assign his reward only when it is creating a block. It can be defined as equation (2).

$$sum(BlockOutputs)sum(BlockInputs) + BlockReward \quad (2)$$

5. ETHEREUM

Ethereum introduced a new concept of an account as a part of the protocol which is the initiator and target of a transaction.Here transactions directly updated to the account balances rather than maintaining the state information. Ethereum has two types of account, Externally Owned Account (EOA) and Contract Ac- count (CA).Externally Owned Account is owned using private keys, where in the case of Contract Account,it is controlled by the code and activated by an EOA only. Externally Owned Account is needed to participate in the Ethereum network , it interacts with the blockchain with the use of transactions. Con- tract Account represents a smart contract, which is piece of code deployed in the blockchains node. It adds a logic and computation to the trust infrastruc- ture [3]. Execution of an smart contract is initiated by a message, which is em- bedded in the transactions. In Ethreum transaction amount is refered as ether. An Ethereum transaction has fields for ether and messages to trigger smart con- tracts. For any action in Ethereum , crypto fuel or gas is required.Where Gas is used as a fees instead . Gas is a cryptocurrency independent of valuation for the transaction fee and computation fee [3].

6. CONCLUSION

Today Blockchain technology is rapidly growing because of its security con- straints. This paper provides information about the blockchain technology, its characteristics, block structure and cryptocurrencies like Bitcoin and Ethereum. For security constraints, it uses cryptographic hash functions and consensus al- gorithms like proof of work.

7. REFERENCES

[1] Aste, T., Tasca, P., Di Matteo, T.: Blockchain technologies: The foreseeable impact on society and industry. computer **50**(9), 18–28 (2017)
[2] del Castillo, M.: Chain is now working on six ‘citi- sized’blockchain networks (2017)

[3] Monrat, A.A., Schelén, O., Andersson, K.: A survey of blockchain from the perspec- tives of applications, challenges, and opportunities. IEEE Access **7**, 117134–117151 (2019)

[4] Sukheja, D., Indira, L., Sharma, P., Chirgaiya, S.: Blockchain technology: A compre- hensive survey. Journal of Advanced Research in Dynamical and Control Systems **11**,1187–1203(092019). https://doi.org/10.5373/JARDCS/V11/20192690

[5] Zheng, Z., Xie, S., Dai, H.N., Chen, X., Wang, H.: Blockchain challenges and oppor- tunities: A survey. International Journal of Web and Grid Services **14**(4), 352 375 (2018).

[6] Zheng, Z., Xie, S., Dai, H., Chen, X., Wang, H.: An Overview of blockchain tech- nology: Architecture, consensus, and future trends. In: 2017. pp. 557-564. IEEE(2017).