ISSN XXXX XXXX © 2019 IJESC

Research Article Volume 9 Issue No.2

Online Ticket Booking using Block Chain

A.Mounika[1], G.Teja[2], S.Alekhya[3], M. Divyajoythi[4], M. Jeevanbabu[5]
Student[1, 2, 3, 4], Assistant Professor[5]
Department of Computer Science & Engineering
Vasireddy venkatadri Institute of Technology Andhra Pradesh, India

Abstract:
Airlines, event usually has to go through a middle man ticketing service, which facilitates the sale of tickets. Likewise, event attendees can only purchase tickets through this middleman, who takes roughly 5-10% of ticket revenues as commission. Another issue is ticketing fraud- tickets can be duplicated, which aids unauthorised entries and loss of revenue for hosts. A ticketing DApp using ethereum would solve all the problems mentioned above. Any Event holders can directly sell their tickets through the DApp with ease and Convenience. We will have fixed number of tickets and each ticket will have the ownership of concert holders. When a customer had done the payment through ethereum wallet then the ownership of the tickets will be changed to the customer. Once the ownership is changed there will be no chance of changing the ownership of tickets there by ticket fraud can be avoided. Once tickets are bought, the ownership of these tickets would be transferred to the buyers. Developing the DApp can prevents ticket fraud as well and prevents external hacks to manipulate the tickets.

Keywords: cryptography, Smartcontracts, consensus, DApp.

1. INTRODUCTION TO BLOCKCHAIN

Block chains rely on public key cryptography to protect user from having unauthorized access. Blockchain uses the hash functions, this uses hash code, hash value, hash sum for efficient mechanism to perform searches. The combinations of hash functions and hash tables with cryptographic techniques, the resulting cryptographic hash function is directly applicable to establishing security and privacy protocols required for blockchain ledger technologies. Blockchain uses cryptographic hash functions is like a signature of a text used to verify and uses SHA256 hash functions algorithm. A generic hash function maps arbitrary size inputs or messages to fixed size hash values or tags[10]. Block in block chain contains the information related to the digital time stamp. A digital time stamp contains the information related to the hash created from the activity of securing the data entered into the ledger.

2. PERMISSION LESS AND PERMISSIONED BLOCK CHAINS

2.1 Permissionless blockchain or public blockchain:

In permissionless blockchain every user is allowed to create a personal address and begin to interact with the network, by submitting transactions and adding entries to the ledger. Any node in the network can employ the mining protocols to verify the transactions by mining operations, in exchange of mining fees and block rewards. Permissionless blockchain uses proof of work which means mining is done by solving complex mathematical equations which in return validate the transactions that to be added to ledger. Digital currencies such as Ethereum, the blockchain network also support smart contracts, which are automated transactions that self-execute when some criteria is met[1].

2.2 Permissioned Blockchain:

Permissioned blockchains have a set of trusted parties to carry out verification, and additional verifiers can be added with the agreement of the current members or a central authority. Permissioned blockchains are intended to compatibility with existing applications (financial or otherwise). They can be fully private (i.e. where write permissions are kept within an organisation), or consortium blockchains (where the consensus process is controlled by a pre-selected set of nodes). Because the actors on the network are named, the intention is that they are also legally accountable for their activity. An advantage of a permissioned blockchain is scalability.

In a permissionless blockchain, the data is stored on every computer in the network, and all nodes verify all transactions. It is obvious that once the number of transactions increases substantially, the users that are able to perform this type of processing and verification will decrease, leading to more centralisation. In a permissioned blockchain, only a smaller number of preselected participants will need to operate, and if these come from large institutions they will be able to scale their computing power in line with the increase in the number of transactions. As there will be smaller number of selected participants it will be easy to alter the results and can reject the transaction easily[1].

3. SMART CONTRACTS

Smart contracts help you exchange money, property, shares or anything of value in a transparent, conflict-free way while avoiding the services of a middleman. In smart contact approach, an asset or currency is transferred into a program and program runs this code to validate automatically to determine whether the asset should go to one person or back to the other person or to be refunded. Ethereum is a platform for deployment of internet services, for which the smart contracts are building blocks[1].

4. CONSENSUS MECHANISMS

There are different consensus mechanisms, e.g., “proof-of-work” or “proof-of-stake”. Depending on the consensus mechanism and the required guarantees, there can be different

notions of when a transaction is taken to be committed or confirmed and thus immutable.

4.1 Proof of work: Proof of work is a requirement to define an expensive computer calculation called mining. A reward is given to first miner who solves each blocks problem. Network miners compete to be the first to find solution for mathematical problem[2].

4.2 Proof of stake: The creator of a new block is chosen in a deterministic way, depending on its wealth defined as stake. The pos system there is no block reward, the miners take the transaction fees[2].

5. DESIGN PROCESS OF BLOCKCHAIN BASED SYSTEM

The design process of blockchain based system starts from the decision to decentralise trust (authority) – or not. A blockchain is used in scenarios where no single trusted authority is required and the trusted authority can be decentralised or partially decentralised [3].

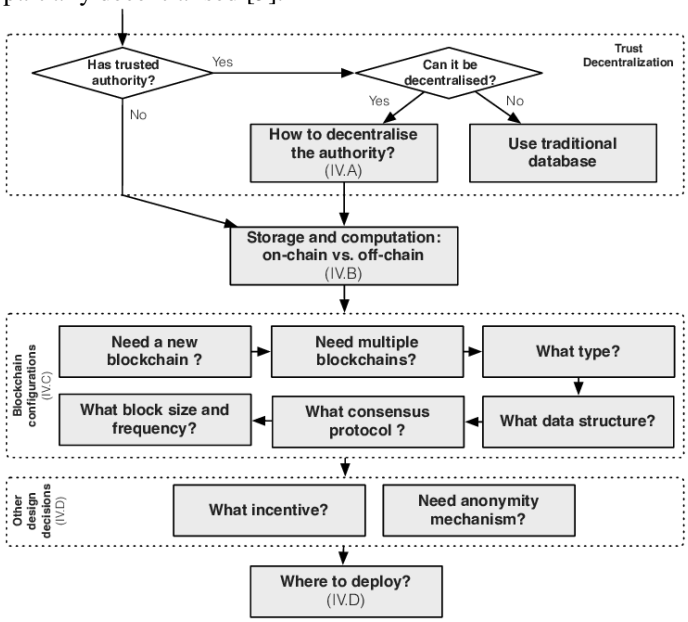


Figure.1. Design Process of Blockchain based applications

5.1 Need of multiple blockchains: In block chain rather than using single chain to record all the transactions , multiple blockchains can be used to isolate information of separate concerns and with different characteristics, and to improve scalability. The first option is to use a sidechain [8]. Side-chaining is a mechanism that allows tokens of one blockchain to be securely transferred and used in another blockchain and still can be securely moved back to the original chain. The original chain is called main chain, and the one that accepts the tokens from the original chain is called side-chain. Multiple private chains could be used to separate concerns, where each of the private chains could link with a public blockchain. Side-chains can help to build a blockchain ecosystem based on a popular main blockchain, without significantly increasing the load on the main chain[3].

5.2 Consensus: Blockchain uses consensus mechanism to achieve a necessary agreement on a single data value or a single state of the network among distributes nodes or systems. The principles of these consensus algorithms are proof of work, proof of Stake, Practical Byzantine fault Tolerance and Delegated proof of work[5].

5.3 Incentive: Blockchains and their applications (especially on public blockchains) introduce financial incentives (or reputation and rating mechanisms) for miners to join the network, validate transactions and generate blocks correctly[3].

5.4 Anonymity: As the Blockchain uses the shared global ledger which is public to all the nodes available on the network. . Therefore, large changes are needed to existing blockchain technologies in order to preserve privacy. We have seen two approaches to the problem. One is to add anonymization (or at least, some greater privacy) to the existing blockchain by techniques such as Confidential Transfers. The other possible method is to create new blockchains that are incompatible with Bitcoin, such as Zerocash that offer guarantees around anonymity built-in by the use of new primitives in their blockchain[5].

5.5 Deployment: Deployment of blockchain also has impact on the quality attributes of the system. For example, deploying a blockchain on a cloud provided by third-party, or using a blockchain-as-a-service model directly introduces the uncertainty of cloud infrastructure into the system. Here the cloud provider becomes a trusted third-party and a potential single point of failure for the system. Deploying a public blockchain system on a virtual private network can make it a private blockchain, with permissioned access controls provided at the network level. However the virtual private network will introduce its own additional latency overhead [3].

6. BLOCKCHAIN ARCHITECTURE

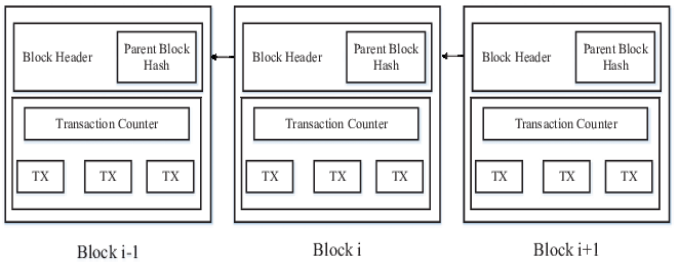


Figure.2. Block chain structure which contains continuous blocks[5].

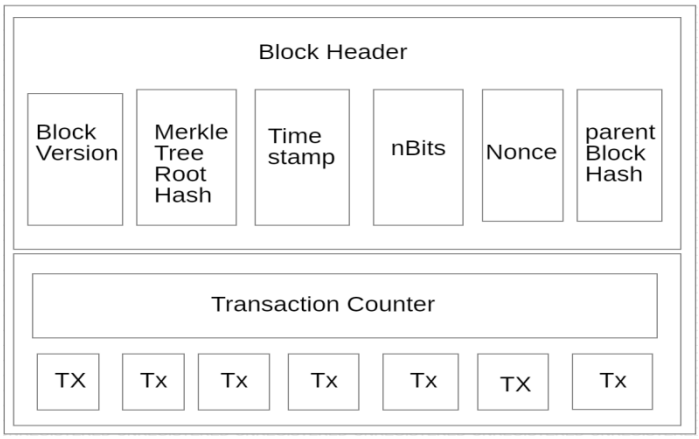


Figure.3. block structure [5].

Blockchain is a sequence of blocks, which holds a complete list of transaction records like conventional public ledger. A block contains only one parent block, with the block hash contained in block header. The first block in the block chain is called genesis block.

- **Block:** A block contains the block header and block body

Block header contains the following.

- **Block version**: indicates which set of block validation rules to follow.

- **Merkle tree root hash**: the hash value of all the transactions in the block.

- **Timestamp:** current time in seconds in universal time since January 1, 1970.

- **nbit**: target threshold of a valid block hash.

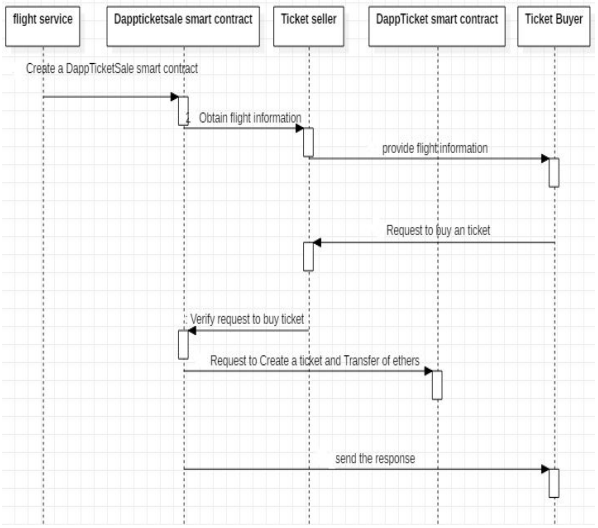
- **Nonce**: an 4-byte field, which usually start with 0 and increase for every hash calculation.

- **Parent block hash:**256-bit hashes valuethose points to previous block.

- **Block Body**: The block body is composed of transaction counter and transactions. The maximum number of transactions that a block contains depends on the block size and the size of transaction. Blockchain uses asymmetric key cryptography mechanisms to validate the authentication of transactions. Digital signature based on asymmetric cryptography is used in an untrustworthy environment [5].

7. PROPOSED BLOCKCHAIN TICKETING SERVICE

- The tickets service will have two smart contracts the first one is DappTicketSale smart contract, which provide information about the ticket and deals with the requests of ticket purchasing and validating the request, the associated smart contract DappToken is used to handle the transfer of ownership. After the successful transfer of money a ticket will be generated with the address of account from which the transfer has been made. Personal details of the person will not be used to generate the ticket to protect the identity and security to the person.
- Airlines first create anDappticketsale smart contract. Ticket seller obtains the information about the flight, also provides flight information to the ticket buyer. When ticket buyer request a ticket then the request will be sent to the ticket seller and then Dappticketsale smart contract verifies the request. If the request is valid then Dappticketsale will call the Dappticket smart contract to create a ticket and transfer the ethers, after that the response is sent from Dappticketsale smart contract to ticket buyers. Dapp will generate an ticket with the account address of metamask. In generation of the ticket we will not use any personal information of the user to provide security to the users.
- Dappticketsale smart contract will fixed number of tickets and each ticket will have the ownership of Airlines. When a ticket buyer had done the payment through ethereum wallet then the ownership of the tickets will be changed to the ticket buyers. Once the ownership is changed there will be no chance of changing the ownership of tickets, there by ticket fraud can be avoided. Once tickets are bought, the ownership of these tickets would be transferred to the buyers.
- The Dapp follows the following security and privacy requirements
  - Only ticket buyers or owners can perform operation about the tickets.
  - People cannot obtain personally identifiable information from data in blockchain.
  - People cannot use the information of ticket to identify other tickets bought by the same user[9].



8. CONCLUSION

To solve the problem of ticket fraud, this study proposed the blockchain ticket service, which can store information about the flight and the tickets in blockchain network. As the ownership of the ticket can be only once change and the transfer of ownership is permanent. Blockchain technology can ensure data integrity; the information of the ticket will be stored to verify authenticity.

9. REFERENCES

[1]. GarethW.Petersz, Efstathios Panayiy Understanding Modern Banking Ledgers through Blockchain Technologies: Future of Transaction Processing and Smart Contracts on the Internet of Money.

[2]. Du Mingxiao, Ma Xiaofeng, Zhang Zhe, Wang Xiangwei, Chen Qijun,A Review on Consensus Algorithm of Blockchain.

[3]. XiweiXu, Ingo Weber, Mark Staples, Liming Zhu, Jan Bosch, Len Bass, Cesare Pautasso, Paul Rimba : A Taxonomy of Blockchain-Based Systems for Architecture Design
Design process of Blockchain based system

[4].Pinyaphat Tasatanattakool, Chian Techapanupreeda: Blockchain: Challenges and Applications

[5].Zibin Zheng1, Shaoan Xie1, Hongning Dai2, Xiangping Chen4, and HuaiminWang3: An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends.

[6]. Harry Halpin*Inria* , Marta Piekarska*Blockstream Montral* Introduction to Security and Privacy on the Blockchain

[7].Blockchain Technology: An Efficient Approach for Agriculture Problems.

[8]. A. Back, G. Maxwell, M. Corallo, M. Friedenbach, and L. Dashjr. Enabling block chain innovations with pegged sidechains. 2014.

[9]. Shi-Cho Cha, Wei-ChingPeng,Tzu-Yang Hsu, Chu-Lin Chang,Shang-Wei Li:ABlockchain-based Privacy Preserving Ticketing Service.

[10]. Buterin, Vitalik. 2014b. A next-generation smart contract and decentralized application platform. White Paper.