Event Management Ticket Booking using BlockChain

Mr. Deepesh Jagdale[1] Mr. Siddhesh Khanvilkar[2] Mr. Swapnil Patil[3] Mr. Lalit Patil[4]
1. Pillai HOC College of Arts, Science & Commerce, Rasayani, Assistant Professor
2. Pillai HOC College Engineering and Technology, Rasayani, Assistant Professor
3. Pillai HOC College of Arts, Science & Commerce, Rasayani, Assistant Professor
4. Pillai HOC College of Arts, Science & Commerce, Rasayani, Assistant Professor

Abstract- Event management usually needs to undergo 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 may be replicated, which aids unauthorised admissions and loss of revenue for hosts. A ticketing Distributed App using ethereum would resolve all the difficulties stated above. Any Event holders can sprightly sell their event tickets through the DistributedApp with easiness and Convenience. We are going to have a hard and fast number of tickets and every ticket will have the ownership of concert holders. When a customer had done the payment through ethereum wallet then the ownership of the tickets are changed to the customer. Once the ownership is modified there'll be no chance of fixing the ownership of tickets thereby ticket deception may be avoided. Once tickets are bought, the ownership of those tickets would be transferred to the buyers. Developing the DistributedApp can avoid ticket fraud furthermore and prevents external hacks to control the tickets.

Index Terms— Cryptography, Smart contracts, consensus, DistributedApp, Block chain.

1 INTRODUCTION

Blockchain is a public distributed database that holds encrypted ledger. Blockchain uses encrypted ledger to keep the details of the people involved in transactions completely anonymous. A block is a collection of recent transactions that are verified and validated. All the verified transactions are collected and hash code is produced to store in a block. Once the block is completed then it is added to the blockchain and a new block is created. When a block is added to the blockchain it goes to a permanent database. Block in the blockchain contains information related to the digital time stamp. A digital timestamp contains the information associated with the hash created from the activity of securing the info entered into the ledger.

Blockchain Overview

Block chain is built on 3 technologies

Public key Cryptography: Blockchain uses public-key cryptography to secure distinctiveness and hash functions to make blockchain absolute, effective searches. Blockchain technology ensures the removal of the double-spend problem, with the help of public-key cryptography, whereby each agent is assigned a private key and a public key shared with all other nodes in the network. A transaction is begun when the future owner of the coins sends her public key to the original owner. The coins are transmitted by the digital signature of a hash. Public keys are cryptographically generated addresses kept in the blockchain. Every coin is connected with an address, and a contract in the crypto-economy is basically a trade of coins from one address to another. The permutations of hash functions and hash tables with cryptographic techniques, the resulting cryptographic hash function is directly applicable to forming security and privacy protocols required for blockchain ledger technologies.

Peer to Peer Network: Blockchain uses peer to peer network to maintain consistency of distributed ledger. When a person tries to make a change in an existing block and tries to add to the

blockchain then the block will not get accepted to add to blockchain because most of the people in the network will have a copy of the blockchain so tampered block gets rejected.

Blockchain Program:
Blockchain programs are developed based on the use cases. Solidity is the most preferred language for writing programs in the blockchain.

Blockchain Types:
Public Blockchain:
Public blockchain have records visible to everybody on the internet and anyone can authenticate and add a block to the blockchain.

Private Blockchain:
Private Blockchain allows only identified people in the organization to verify and add transaction block but everybody on the internet is generally allowed to view.

2 PERMISSION LESS AND PERMISSIONED BLOCK CHAINS

2.1 A permissionless blockchain or public blockchain:

In a permissionless blockchain, every user is allowed to create a personal address and begin to cooperate 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 for 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 the ledger. Digital currencies such as Ethereum, the blockchain network also support smart contracts, which are automated transactions that self-execute when some criteria are met [1].

2.2 Permissioned Blockchain:

Permissioned blockchains have a group of trusted parties to hold out authentication, and extra verifier is added with the agreement of this members or central authority. Permissioned blockchains are intended to compatibility with existing applications (financial or otherwise). They'll 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're also legally in charge of for their activity. An advantage of a permissioned blockchain is scalability. In a permissionless blockchain, the information is stored on every node within the network, and every node verifies all transactions. It's obvious that when the amount of transactions increases substantially, the users that are able to perform this kind of processing and verification will decrease, resulting in more centralisation. In a permissioned blockchain, only a smaller number of preselected members will have to control, and if these come from large organisations they're going to be able to scale their computing power in line with the rise within the number of transactions. As there'll be a smaller number of selected participants it'll be easy to switch the results and may discard 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].

Ethereum Blockchain:
An Ethereum blockchain is similar to the Bitcoin blockchain. The main difference is that Ethereum blocks contain not only the block number, difficulty, nonce, etc. but also the transaction list and the most recent state. For every transaction in the transaction list, the new state is created by applying the previous state. Contracts written in a smart contract-specific programming language are compiled into 'byte code', which a feature called the 'Ethereum Virtual Machine' (EVM) can read and execute. All the nodes execute this contract using their EVMs.

Ethereum Wallet:
This is the place to store the private keys securely. While intermediaries are no longer needed to verify transactions, there's no help desk to turn to for help recovering your secret key in case of any loss of secret keys. Ethereum has plenty of wallets to store crypto-currency like desktop wallets, web wallets, hardware wallets and paper wallets.

Ether:
Ether is a crypto-currency and the currency of Ethereum. The transactions in ethereum are made in ether. Any activity on ethereum that results in change of its current state costs ether as fee and miners who are successful in validating transaction and writing a block in chain will get ether.

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].

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]. Sidechaining 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

Blockchain is a sequence of blocks. Each block holds a complete list of transaction records like a 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 value those 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

1.The tickets service will have two smart contracts the first one is TicketSale smart contract, which provide information about the ticket and deals with the requests of ticket purchasing and validating the request, the associated smart contract Ticketing 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.

2. Event host first create anticketsale smart contract. Ticket seller obtains the information about the event, also provides event information to the ticket buyer. When ticket buyer request a ticket then the request will be sent to the ticket seller and then ticketsale smart contract verifies the request. If the request is valid then ticketsale will call the ticketing smart contract to create a ticket and transfer the ethers, after that the response is sent from ticketsale smart contract to ticket buyers. Dapp will generate a 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.

3. Ticketsale smart contract will fixed number of tickets and each ticket will have the ownership of Event host. 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.

4. The Dapp follows the following security and privacy requirements
   a. Only ticket buyers or owners can perform operation about the tickets.
   b. People cannot obtain personally identifiable information from data in blockchain.
   c. 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 event 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.

REFERENCES

[1] Gareth W. Petersz ,EfstathiosPanayiy 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, CesarePautasso, Paul Rimba : A Taxonomy of Blockchain-Based Systems for Architecture Design Design process of Blockchain based system
[4] PinyaphatTasatanattakool,ChianTechapanupreeda :Blockchain: Challenges and Applications
[5] Zibin Zheng1, Shaoan Xie1, Hongning Dai2, Xiangping Chen4, and Huaimin Wang3 :An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends.
[6] Harry HalpinInria , Marta PiekarskaBlockstream 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 blockchain innovations with pegged sidechains. 2014.
[9] Shi-Cho Cha, Wei-ChingPeng,Tzu-Yang Hsu, Chu-Lin Chang,Shang-Wei Li:ABlockchainbased Privacy Preserving Ticketing Service.
[10] Buterin, Vitalik. 2014b. A next-generation smart contract and decentralized application platform.
[11] White Paper. https://medium.com/coinmonks/https-mediumcom-ritesh-modi-solidity-chapter1-63dfaff08a11