International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 07 Issue: 09 | Sep 2020 www.irjet.net p-ISSN: 2395-0072

ETHEREUM CONCEPTS AND DIGITAL VOTING USING BLOCKCHAIN

Adhitya Nair[1]

[1]*PG Student, Vivekanand Education Society's Institute of Technology, Dept. of MCA, Mumbai, India.*

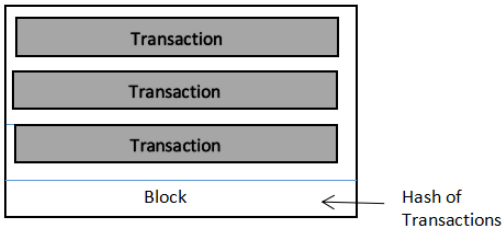
Abstract - *With ubiquitous internet connections in most places of the world, global information transmission has become incredibly cheap. Technology-rooted movements like Bitcoin have demonstrated, through the power of the default, consensus mechanisms and voluntary respect of the social contract that it is possible to use the internet to make a decentralized value-transfer system, shared across the world and virtually free to use. This system can be said to be a very specialized version of a cryptographically secure, transaction-based state machine.*

Ethereum is a project which attempts to build the generalized technology; technology on which all transaction-based state machine concepts may be built. Moreover, it aims to provide to the end-developer a tightly integrated end-to-end system for building software on a hitherto unexplored compute paradigm in the mainstream: a trustful object messaging compute framework.

Keywords: Smart Contracts, Dapps, Blockchain, Datestamping, Serpent

I. Introduction

Blockchain is a distributed database. It is an incorruptible digital ledger of economic transactions that can be programmed to record. It's not just a financial transaction but virtually everything of value. Data stored in a blockchain is designed in a way that it is impossible to change once it is in the blockchain without it being detected by other users.



Each block address knows the previous block address → chain of blocks. For a person to enter the chain, solve a mathematical puzzle (mining technique) which is a proof of work. When a block is added to a chain, a copy is sent to everyone and therefore a trust is established as so many people have copies.

II. Understanding the Problem

The main problem is to facilitate transactions between consenting individuals who would otherwise have no means to trust one another. This may be due to geographical separation, interfacing difficulty, or perhaps the incompatibility, incompetence, unwillingness, expense, uncertainty, inconvenience or corruption of existing legal systems. By specifying a state-change system through a rich and unambiguous language, and furthermore architecting a system such that we can reasonably expect that an agreement will be thus enforced autonomously, we can provide a means to this end. Dealings in this proposed system would have several attributes not often found in the real world. The incorruptibility of judgement, often difficult to find, comes naturally from a disinterested algorithmic interpreter. Transparency, or being able to see exactly how a state or judgement came about through the transaction log and rules or instructional codes, never happens perfectly in human based systems since natural language is necessarily vague information is often lacking, and plain old prejudices are difficult to shake.

III. Ethereum

Ethereum is a decentralized platform that runs smart contracts without any downtime, fraud and third-party interference and has its own cryptocurrency called Ether. The main characteristics of Ethereum include:

Open Source: Ethereum is an open source application which can be developed by anyone with high-end computational systems thus providing transparency.

Fast Transactions: Ethereum is capable of processing the transactions very fast.

Funded Transactions: Many corporate organizations are coming forward to fund and test Ethereum to make it a source of transaction in future.

Proof of Work: One of the important characteristics where the proof of work i.e transaction details are all highly proofed to tamper with.

The reason why Ethereum is gaining popularity is as follows:

Community Support: Ethereum has drawn the attention of a lot of people from all over the world.

Evolved: The main advantage of ethereum is the evolution of blockchain from the shortcomings of bitcoin.

Secured: It is almost impossible to tamper with the transactions of the block.

IV. Gas in Ethereum

Gas is the fundamental block of the Ethereum ecosystem that is paid for every operation performed on the Ethereum blockchain. It is the crypto fuel for Ethereum. It can be considered as a transaction fee which has to be paid when one party sends Ether to another party. This fee has to be paid regardless of whether the transaction succeeds or fails. Gas price is referred to as the total number of gas required for a transaction and Gas limit is the amount of gas the user is willing to pay for a transaction. Therefore, if the gas price exceeds the limit the transaction is not proceeded with a message 'Out of gas'.

V. Ether

Ether is an incentive that the client of the platform pays to execute requested operations. It is a necessary element required to operate the Ethereum platform. It ensures that the developers write error free codes because unnecessary codes will increase the cost. A place to securely store the ether is called Ethereum wallets. It can be hardware wallets, paper wallets, desktop wallets, mobile wallets etc.

Currency Symbol = ETH

1 ETH = 1 Quintillion WEI (Smallest)

1ETH = 1000 Finney

1ETH = 1 million Szabo

Other currencies include Kether, Mether, Gether, Tether.

VI. Ethereum Virtual Machine

Ethereum Virtual Machine (EVM) is an engine which executes translation code. Smart contracts are compiled into bytecode which an EVM can read and execute. Ethereum possesses its own programming language known as the EVM bytecode. The Ethereum Virtual Machine (EVM) uses a set of instructions called opcodes to execute specific tasks. The languages used in Ethereum are Solidity, LLL, Vyper, Serpent, Mutan, Julia.

VII. Smart Contract

A smart contract is a code running on top of the blockchain. It contains the set of rules for the nodes to agree upon so that they interact with each other. It has an Ether balance, an associated code, is triggered by transactions or messages and performs operations of arbitrary complexity. The characteristics of smart contract includes:

Self-verifying

Tamper-resistant

Cost saving

Self-executing

Process of Smart Contracts

An optional contract is written between the parties as a code in blockchain. The individuals involved are anonymous but the contract is made through a public ledger.

A trigger event like an expiration date or a strike price is hit, and the contract executes itself according to the coded terms.

Regulators can use the Blockchain to understand the activities in the market while maintaining the privacy of an individual's position.

VIII. Ethereum Tools

The types of Ethereum tools include:

Geth: Geth is a multipurpose command line tool that runs on Ethereum node implemented in Go. It is the official go line implementation of the Ethereum protocol and is commonly used to interact with the Ethereum network.

Ganache CLI: Ganache CLI is a fast and customizable blockchain emulator which allows to make calls to Blockchain without running the actual Ethereum node. The transactions are mined instantly with no transaction cost. Accounts can be recycled, reset and instantiated with a fixed amount of Ether without the need for faucets or mining. Gas price and Gas limit can be modified. A convenient GUI gives you an overview of your test chain events.

Parity: Parity is the most secure, lightweight Ethereum client that provides the core infrastructure essential for quick and reliable services. It is written in Rust language and is incorporated directly into your web browser. It serves as an Ethereum GUI browser and provides access to a diverse range of Ethereum features including dApps.

MetaMask: MetaMask turns Google Chrome into a browser that allows the users to send and receive transactions and also to fetch data from blockchain.

Mist Wallet: Mist Wallet is an end user interface used for browsing and using DApps. It is an official Ethereum wallet and was developed and distributed by the team which is responsible for the management of the Ethereum ecosystem. It is used by the developers who want to create, deploy and use smart contracts. It is a full node wallet which means you will have to download the entire Ethereum blockchain onto your computer.

IX. Digital Voting

Democratic voting is a crucial and serious event in any country. The most common way in which a country votes is through a paper-based system, but is it not time to bring voting into the 21st century of modern technology? Digital voting is the use of electronic devices, such as voting machines or an internet browser, to cast votes. These are sometimes referred to as e-voting when voting using a machine in a polling station, and i-voting when using a web browser. Security of digital voting is always the biggest concern when considering implementing a digital voting system. With such monumental decisions at stake, there can be no doubt about the system's ability to secure data and defend against potential attacks. One way the security issues can be potentially solved is through the technology of blockchains. Blockchain technology originates from the underlying architectural design of the cryptocurrency bitcoin. It is a form of distributed database where records take the form of transactions, a block is a collection of these transactions. With the use of blockchains a secure and robust system for 4 digital voting can be devised. This report outlines our idea of how blockchain technology could be used to implement a secure digital voting system.

X. Proposed Digital Voting Steps

Registration: The first aspect of the design is the registration process, verifying a voter is essential in establishing security within the system. Making sure that someone's identity isn't being misused for fraudulent purposes is important, especially when voting is considered, where every vote matters**.** To allow users to register to vote our proposed service utilizes both postal based forms as well as web forms requiring the same information to ensure we cater for those without a direct internet connection. This information includes their national identity number (an example would be a Indian citizen's Aadhar card number or PAN Card number), postal address, optional email address and a password. All of this information then forms a transaction for the user agreeing with the government that they are asking to vote; this transaction is then created on the voter blockchain which is distinctly different from the vote blockchain. Once someone has registered an automated government miner analyses the transaction and if they haven't been awarded or denied a vote the miner will make the decision as to whether to verify the user or not. If the user is verified, they will be sent a ballot card with their information on it to both their home address and email address if provided. They will also be sent a randomly generated password to use on the polling stations. Once this correspondence has been sent, the 9 miners will create a transaction giving the user a vote from an infinite government pool of votes on the voter blockchain. During this process, a voter blockchain is used to keep a record of both transactions taking place at each stage of this process for each voter: a. Firstly, a transaction is created when a user 'registers. b. The next transaction is created when a government miner authorizes that user's right to vote. After the correspondence is received by the user they can then await voting to open to use their credentials to vote. It is important to note that this voter blockchain will never contain details of the vote cast by the user.

Voting Mechanism and Architecture:

When deciding on the architecture we took strong inspiration from both the distributed and availability of the Bitcoin network and the aggregation process of traditional voting. The network is a multi-tiered, decentralized infrastructure which houses the two distinct blockchains, the network is divided into three abstract tiers, National, Constituency and Local. The local tier contains all the digital polling stations across the country, each of which is associated to a constituency node. A local node is set up to only communicate with the other local nodes under the associated constituency node and the constituency node itself. The constituency tier contains all the nodes that are deemed to be at a constituency level. These nodes would be directly connected to each other and to a subset of polling stations depending on 10 locations. The national tier is a collection of nodes that are not tied to location, their pure purpose is to mine transactions and add blocks to the vote blockchain, all constituency nodes communicate to a national node and national nodes can communicate with each other. Independent bodies will monitor and audit the voting process. These bodies will host or have access to a national node and will be able to verify that the unencrypted results match the encrypted votes. Individuals and organizations can volunteer to be a national node. These applications are processed by the government to ensure that they meet the minimum requirements set by a governing body. These individuals will also act as miners during the counting process. As part of our design we have an encryption method based on public and private keys and have implemented a structure where the data is segregated within the blockchain. This segregation has been achieved by getting the constituency level nodes to generate keys pairs. The public keys are then distributed to the connected polling station nodes, which then use the public key to encrypt

any vote made to that polling station. The data is then stored in an encrypted format within the blockchain and propagates out to the entire network. Due to the fact each constituency will have a different public key means that chunks of data within the block chain will be encrypted differently to a chunk of data next to it. We decided to apply this method to prevent any one person being able to decrypt the voting data before the end of voting deadline. If a hacker manages to get hold of a constituency private key, they would only be able to decrypt certain sections of the blockchain, so would never know the full outcome of the vote. Once the voting deadline has passed, the software within the constituency nodes 11 publishes the private keys to allow the blockchain network to decrypt the data, which in turn means the votes can then be counted.

Voting Process:

When it is time to vote, authentication of a user requires three distinct pieces of evidence; their identification number (e.g. Indian citizens have Aadhar card numbers), the password supplied on registration, their ballot card which contains a QR code. As there are two methods of voting (web browser, physical polling station) the way the user will input the authentication details shall differ; however, in order to vote they are required to provide all three pieces of information. It is also important to note that each user will have been registered at a certain constituency so they will only be able to vote at a local polling station within that constituency or via the internet at the URL provided on the ballot card. (Each constituency is to be equipped with its own web server and URL to ensure votes are aggregated within the right network.) Behind the scenes the polling station will consult the voter blockchain to ensure the voter has not already used up their vote. If the user does have a vote, then the station will then allow the user to continue to the voting screen. If not, then system will respond to the user appropriately.

After selecting their vote (from the selection of options including abstention) and then confirming the submission, the vote will become a transaction, it will be encrypted with the relevant constituency's public key. This transaction is then passed to the constituency node where it is added to a block and the update is then pushed to all other nodes connected to that particular constituency node. The connected nodes then pass the data on to their peers until the whole network is updated. Once the vote has been confirmed the polling station will then 12 generate a transaction to remove the user's vote within the voter blockchain. It is important to note that there are two distinct blockchains being held; one which contains transactions relating to which users have registered and which users still have a vote, the second containing the contents of the vote (such as what party was voted for.). Through the use of these two distinct blockchains we ensure voter anonymity when selecting their vote

XI. Cons of the System

One risk is if a voter were to forget their ID, password or polling card on the day of voting. In this case the voter will be unable to cast their vote as they cannot enter the system. Possible risk mitigations include the voter returning later that day with the correct information or the implementation of a backup authentication service such as by phone. Alternatively, a forgotten password system could be added to the voter registration website; this could work in much the same way as recovering a password works on other websites. However, this increases the risk of a hacker attempting to change a voter's password without their knowing

The basis of the attack being that someone could theoretically control a majority of the digital voting mining hash-rate, leading to them being able to manipulate the public ledger. The chances of this type of attack occurring are slim due to the immense cost needed to purchase hardware capable of this scale of processing.

The online aspect of the voting within our system is the largest attack vector for hackers as they could potentially exploit voters through their own devices in a host of ways. To combat this software could be developed that could be downloaded onto the client's device to establish a secure connection to the polling station.

XII. Conclusions

The Ethereum protocol was originally conceived as an upgraded version of a cryptocurrency, providing advanced features such as on-blockchain escrow, withdrawal limits and financial contracts, gambling markets and the like via a highly generalized programming language. The Ethereum protocol would not "support" any of the applications directly, but the existence of a Turing-complete programming language means that arbitrary contracts can theoretically be created for any transaction type or application. What is more interesting about Ethereum, however, is that the Ethereum protocol moves far beyond just currency.

Protocols and decentralized applications around decentralized file storage, decentralized computation and decentralized prediction markets, among dozens of other such concepts, have the potential to substantially increase the efficiency of the computational industry, and provide a massive boost to other peer-to-peer protocols by adding for the first time an economic layer.

Finally, there is also a substantial array of applications that have nothing to do with money at all. The concept of an arbitrary state transition function as implemented by the Ethereum protocol provides for a platform with unique potential; rather than being a closed-ended, single-purpose protocol intended for a specific array of applications in data storage, gambling or finance, Ethereum is open-ended by design, and we believe that it is extremely well-suited to serving as a foundational layer for a very large number of both financial and non-financial protocols in the years to come.

The idea of adapting digital voting systems to make the public electoral process cheaper, faster and easier, is a compelling one in modern society. Making the electoral process cheap and quick, normalizes it in the eyes of the voters, removes a certain power barrier between the voter and the elected official and puts a certain amount of pressure on the elected official. It also opens the door for a more direct form of democracy, allowing voters to express their will on individual bills and propositions. In this paper, we introduced a unique, blockchain-based electronic voting system that utilizes smart contracts to enable secure and cost-efficient election while guaranteeing voters privacy. By comparison to previous work, we have shown that the blockchain technology offers a new possibility for democratic countries to advance from the pen and paper election scheme, to a more cost- and time-efficient election scheme, while increasing the security measures of the todays scheme and offer new possibilities of transparency. Using an Ethereum private blockchain, it is possible to send hundreds of transactions per second onto the blockchain, utilizing every aspect of the smart contract to ease the load on the blockchain.

References:

[1] Intrinsic value: https://tinyurl.com/BitcoinMag-IntrinsicValue

[2] Smart property: https://en.bitcoin.it/wiki/Smart_Property

[3] Smart contracts: https://en.bitcoin.it/wiki/Contracts

[4] B-money: http://www.weidai.com/bmoney.txt

[5] Reusable proofs of work: http://www.finney.org/~hal/rpow/

[6] Secure property titles with owner authority: http://szabo.best.vwh.net/securetitle.html

[7] Bitcoin whitepaper: http://bitcoin.org/bitcoin.pdf

[8] Name coin: https://namecoin.org/

[9] Electronic ID Card : https://e-estonia.com/component/electronic-id-card/

[10] Genesis block : https://en.bitcoin.it/wiki/Genesis_block