ElectionChain—a Decentralized, Fair, Open, Just Blockchain Voting System V1.35

ElectionChain Team

Election, in a narrow sense, refers to activities in which social members select or elect, depending on their own wills, representatives or principals in accordance with certain voting procedures and methods; in a broad sense, refers to voting by social members depending on their own wills, to elect principals and determine the directions of democratic affairs and democratic decisions based on the principle that minority is subordinate to the majority, which can be understood as a voting process.

Application scenarios of election and voting include: U.S. governor and presidential election, NPC member election of the P. R. C., voting and decision making by shareholders of listed companies, intra-company election of excellent employees and lottery voting. Democratic decision-making and public opinion poll can be seen as extension of voting, while the election object is a decision or an answer other than a candidate. Likewise, lotteries are in fact combinations of numbers cast within certain scope of digits.

At present, voting methods include: voting by raising hands, paper ballots, electronic voting and network voting, in which there are problems such as low openness degree, low transparency, ballot fraud and manipulation of election results.

The main purpose of ElectionChain is to solve the problems related to openness and transparency of democratic election, democratic decision-making, public opinion poll and lottery vote by adopting technical means, to avoid man-made interference to election results, to ensure the fairness of results of election and voting, and Make the election more credible.

1 Project Background and Meaning

Current voting methods include voting by raising hands, paper ballots, electronic voting and network voting.

1.1 Voting by Raising Hands

Voting by raising hands is usually adopted in face-to-face voting by small group of people, where voters raise their hands to show their approvals or rejections to a proposal or candidate. The method applies to voting by voters with trust foundation and the result shall be clear at a glance, for example, voting by board members, class leader election. This method is not suitable for large-scale elections.

1.2 Paper Ballots

Voting by paper ballots means to record or specify vote goals on specially-made or ordinary, anonymous (usually) or nominative ballots. This method is widely used today, and is commonly used in most democratic elections in China and the U.S.

However, the distribution and collection processes are inconvenient. In case of nonlocal voting, the ballots need to be mailed to the polling station, during which the ballots are easy to be tampered, thus affecting the voting result.

1.3 Electronic Voting

Electronic voting refers to voting via official electronic voting devices in a certain place with the electronic signals of votes collected by electronic technology, so the voting result can be obtained without manual counting. With advantages such as low cost, low error and high efficiency, this voting method is adopted by at least 30 countries to different extents. However, the disadvantages are obvious:

(1) Due to the concern for security of data transmission, this method is not widely applied in international polling, in case the voting result is falsified by hackers invading in an electronic voting system, the consequence will be unimaginable.

(2) Personal data of voters, such as names and ID card numbers input in the electronic system to confirm their identities are subject to leakage.

(3) Scandals relating to electronic voting system data loss, file corruption, bribe-taking by officials, may exaggerate the defects of electronic voting, while these make people worry about electronic voting;

(4) The result of electronic voting is under the centralized control of an electronic voting device, so it is impossible for voters to check their votes.

Lottery ballot is another form of electronic voting, because a random No. device is a specially made device, and it is impossible to verify its authenticity.

1.4 Network Voting

Network voting refers to Tele-voting via Internet, with voting results recorded and collected in a centralized database. In the past few years, network voting is very common in life, and many election / voting processes are Internet based, greatly improving voting efficiency and lowering the cost.

Problems of network voting are as follows:

(1) Network voting is managed and operated by a centralized agency, and the data is not open and not transparent, and the matter could be worse in case of data falsification, so there is no guarantee for credibility of vote results.

(2) The network voting system, as not supported by high technology, is weak in identifying successive ballots. Currently, ordinary validation techniques include registered user verification, Session validation, Cookies validation and IP address validation, are easy to be cracked by those with little knowledge on computer software, resulting in continuous ticket brushing affecting voting results, and giving rise to various ticket-brushing software and companies.

(3) Data of a network voting system is usually stored in the database. Once the voting result is falsified by a hacker after cracking the database server to reach the goal of some people, the voting result will be unfair and unjust.

1.5 Voting by Blockchain

The birth of Bitcoin at early 2009 aroused a new wave of technology. The underlying technology—Blockchain—drew more and more attention since 2015, and became popular and widely known in the world since March or April 2016. At present, Blockchain has been well developed with many of its applications practiced at home and abroad.

“Blockchain” is a decentralized distributed ledger in nature. Decentralization means that all

transactions are point-to-point transactions, with no need for any credit intermediary or centralized liquidation agency; distributed ledger means that when transactions take place, all participants on the Blockchain will receive information about the transactions which are displayed on the ledger. Those transactions are completely open, encrypted and tamper-resistant.

Based on the technical features of Blockchain, in view of the disadvantages of current election technologies, we will build an open-source Blockchain application for election, voting and lottery, and name it as ElectionChain. We want to optimize the election and voting technology, so as to make election more open and transparent with less artificial manipulation and verifiable voting results.

2. Content of Project Development

2.1 Current Application at Home and Abroad

At present, there are application projects for Blockchain voting, which are necessary to be studied intensively, to learn the advantages so as to realize the project goal.

2.1.1 Nasdaq shareholder voting system

Nasdaq is in cooperation with Chain—a newly established enterprise of Blockchain, and they jointly developed a digital asset voting system. Tokens can be used to vote, and the tokens will be distributed to shareholders, enabling shareholders to participate in voting on the annual meeting of the Company without attending the annual general meeting. They hope to reduce the complexity of and cost on organizing shareholders for voting, to promote overall participation.

The project was tested in Nasdaq Market, Estonia in 2016. By placing the voting process on the open ledger of Blockchain, voting by mobile phones was realized and the records could be saved permanently. The test result was satisfying, and the achievement was planned to be applied to other customer solutions and internal processes.

This voting system is the first shareholder voting system adopting Blockchain technology around the world, and the system was tested in the market. The advantage is that voting data are recorded on Blockchain, so the data are tamper-resistant against hacker attack on the system,

whilst the openness and transparency of the data can improve the credibility of voting results, reducing manual intervention and lowering cost. So the benefits are numerous.

The voting system is limited in terms of application scenarios. That is to say, it is applicable to certain scenarios such as shareholder voting, excluding scenarios such as public opinion poll and democratic election. In addition, the system cannot be commercialized, so it needs to be further optimized to meet market requirements.

2.1.2 Republican presidential candidate election in Utah, the U. S.

In 2015, Blockchain technology was adopted in Utah for election of Republican Party candidates participating in the U. S. Presidential Election. Voters of Utah voted via network at home (but a polling station) or elsewhere in or out of Utah, in or out of the U. S.

Voters have to visit the Republican Website of Utah to get registered. Once an identity is validated, the voter will receive a secret key which is the ballot ticket to be input by the voter for network voting.

Americans working abroad will not have to worry about their votes to be tampered, because the data security is guaranteed, encouraging more people to participate in voting.

Besides, the voting system is limited to use only for election of Republican Party candidates in Utah, because it is not a general-purpose voting system.

2.1.3 Other Blockchain election systems

There are also some newly established companies using blockchain technology for election, and they developed some product prototypes. On the whole, blockchain voting systems are not perfect, for the following problems: (1) the overstress on anonymity undermines identity validation; (2) deviation from practical applications of enterprises and public institutions, and inadequate technology interconnection; (3) the systems are based on Bitcoin or Ethereum, which not meet the high-performance demands of large-scale voting; (4) poor universality for polling; (5) the systems cannot be employed for public opinion poll and election quizzes.

2.2 Profile of ElectionChain

ElectionChain is aimed to research and develop a blockchain exclusive to election, voting

and lottery, which supports American Presidential Election as well as entertaining applications such as election donation, election quizzes, campaign speeches and live broadcast, and election games. In ElectionChain, each voter performs a real-name vote or anonymous vote with a real identity or virtual identity according to one's own wish, and the vote can be validated to see whether it is included in the final result. By technology, ElectionChain avoids disadvantages of paper ballots, electronic voting and network voting, making election, voting for decision-making and public opinion poll more open and transparent, preventing man-made interference to make the election more creditable .

2.2.1 Application Scenarios

Application scenarios that ElectionChain supports include democratic election, democratic decision-making, public opinion poll, voting quizzes, lottery, voting donation, etc., as well as some related entertaining applications including election campaign live broadcast and campaign games.

(1) Election: all voting and elections around the world can be conducted on ElectionChain, such as U.S. governor and presidential election, NPC member election of the P. R. C., voting by shareholders of listed companies and various network voting activities;

(2) Democratic decision-making: public voting by members on certain decisions or matters such as Brexit, force use and commence of infrastructural projects. This method is simple for the voters to show their attitudes by choosing from yes, no or abstention.

(3) Public opinion poll: seeking for opinions of citizens on certain themes such as presidential support rate and views towards something, usually performed in the form of questionnaire survey on Blockchain;

(4) Voting quizzes: themes for voting quizzes are usually about popular and important matters such as presidential election and Brexit. People can guess which candidate or decision will win at last;

(5) Voting donation: people can donate for candidates on Blockchain. Blockchain can record the donation to a candidate by voters or non-voters, making the donation more transparent.

(

(6) Entertaining election: with campaign speeches, live broadcast and rewards, campaign games and other entertaining applications introduced in, ElectionChain is a more interesting

program, but a politicized one.

(7) Lottery: In China only approved lottery agencies are allowed for lottery issuance. To avoid conflict with national laws, ElectionChain will not issue lotteries by itself, and the lottery scenarios are realized by cooperating with lottery agencies at home and abroad.

2.2.2 Voting processes

The most critical part of a vote can be carried out in two modes:

(1) Voting by virtual identity

- Election processes: An elector initiating election => designating voters' addresses (optional) => determining the candidate, preparing the election scheme and survey questions => starting and ending times of the election => generating ballot tickets => issuing ballot tickets to voters => voting (voters send their votes and answers to the candidate) and real-time statistics => end of election at the ending time => publishing the voting result
- Quiz process: an initiator (anyone) initiating a voting quiz on certain election open to everyone => stake offering => end of stake offering and start of election => voting result => distribution of bonus in the quiz pool;

(2) Voting by real identity

For voting by real identity, two procedures, identity authentication and registration of voters, shall be finished before other procedures:

- Identity authentication: voters issuing applications for identity authentication => replies by a relevant party;
- Registration of voters: Registration of voters for certain voting => identity authentication of voters by the elector => identity authentication by an authority => obtaining the authentication result => result feedbacks to voters;
- Election processes: An elector initiating election => determining the candidate, preparing the election scheme and survey questions => starting and ending times of the election => registration of voters=> generating ballot tickets => issuing ballot tickets to voters => voting (voters send their votes and answers to the candidate) and real-time statistics => end of election at the ending time => publishing the voting result;

The above two voting modes differentiate on whether the real identity authentication is

needed.

2.2.3 Tokens of ElectionChain

ElectionCoins (ELT) refers to tokens on ElectionChain for the following purposes:

(1) The elector, upon initiating an election, voting for decision making or public opinion poll, uses ELTs to generate ballot tickets, with certain amount (adjustable) of ELTs corresponding to one ballot ticket. After binding, these ELTs are locked on the Blockchain until the end of this election or voting when these ELTs are released.

(2) ELTs are required for payment on ElectionChain, which is similar to a Bitcoin payment system;

(3) ELTs are required for quizzes, campaign cash, rewards, lottery, games, etc.

Ways to acquire ELTs:

(1) ELTs can be acquired by earlier-stage ICO investments in bitcoin or ETH. See the next chapter for the issuing mechanism of ELTs;

(2) ELTs can be purchased at an exchange supporting ELT exchange;

(3) ELTs can be acquired by establishing accounting nodes to serve the whole network;

(4) New ELTs can be acquired with interests incurred from ELTlocking;

(5) Free ELTs can be applied from an ElectionChain development team by the government and non-profit organizations to carry out elections. These ELTs will return to the wallet of the development team after use;

(6) ELTs can be rented from the decentralized leasing market built in ElectionChain. The decentralized ELTleasing market is detailed in the following chapters.

It is necessary to note that a raise in ELTprice may lead to surge of cost on election, The problem can be solved by the above items (5) and (6).

2.2.4 Participants

ElectionChain creates an electoral ecosystem as bigger as possible, to involve in as many participants as possible. At present, the participants include election initiators, voters, candidates, representatives of voters, authoritative identity authentication agencies, peripheral developers of ElectionChain, development teams of ElectionChain, providers of quizzes, lottery providers,

agencies for public opinion poll, game providers, live broadcast providers and advertisers.

(1) Election initiators: individuals or organizations initiating an election or decision-making, who shall pass identity authentication for voting by real identities. Initiating of some elections shall only be performed by legal institutions to avoid conflict of laws among different countries.

(2) Voters: election initiators with right to limit the conditions and identities of voters for certain election or decision-making. The conditions and identities of voters for real-world voting shall be real. Voters are those with ballot tickets, and can vote only via the ballot tickets.

(3) Candidates: those to be voted by others in election, whose real addresses and names shall be shown on the Blockchain.

(4) Representatives of voters: voting in some elections shall be further performed by selected representatives, such as the electoral system for the U. S. presidential election.

(5) Authoritative identity authentication agencies: agencies to verify real identities of voters. There are many of those agencies participating in ElectionChains in many countries. We can avoid frauds of some organizations via validations by more than two thirds of the above agencies.

(6) Peripheral developers of ElectionChain: ElectionChain provides open-source underlying systems, which need secondary development so as to integrate with information management systems of enterprises and public institutions. These works, as an important part of ecological construction, are performed by peripheral developers of ElectionChain.

(7) Development teams of ElectionChain: the original development and operation teams of ElectionChain.

(8) Providers of quizzes: the quizzes are similar to a gambling game, in which a real-world banker may involve to provide guarantees and compensation via a smart contract, which is safe and reliable.

(9) Agencies for public opinion poll: introducing professional agencies for public opinion poll improves credibility and influence of data.

(10) Game providers: Game providers provide campaign games requiring payment in ELT and

item purchase.

(11) Live broadcast providers: introducing live broadcast providers for campaigns is convenient for voters to know about the situation and reward with ELT, promoting the entertainment.

(12) Advertisers: a program drawing much attention can be advertised by payment in ELT.

(13) Lottery providers: introducing lottery providers approved by the national government to provide lottery service.

ElectionChain, with strong social influence, attracts many people around the world to join in, and this is extremely beneficial to the development of ElectionChain.

2.2.5 Ultimate goal of ElectionChain

The ultimate goal of ElectionChain is to support the U. S. presidential election. American voters elect presidential candidates and electors by direct voting, and the electors form an "electoral college" to vote in the presidential election, forming the Electoral College System unique to the U. S. On the U.S. Election Day, 240 million citizens will elect 538 electors and a president within 12 hours. This means that the election system will be under the pressure of a transactional throughput of 5555TPS within 12 hours, which is a great challenge to ElectionChain.

The following chapters detail the ways to realize the ultimate goal of ElectionChain.

2.3 Relevant Legal Issues of Countries

ElectionChain has no intention to oppose the laws of countries, and its aim is just to provide an open-source, legal, open and transparent voting technical means, thus how to use such a technical means and what kind of election and lottery will be initiated are the concerns of electors and voters.

However, ElectionChain shall conform to the laws of countries, when involving the corresponding election and lottery in reality, electors and voters shall provide real identity certificates respectively, so as to conduct KYC well as far as possible.

Any votes or lotteries on ElectionChain shall not offend against the laws of countries where electors and voters are located, otherwise, ElectionChain team has the right to suspend the election action that may rise legal dispute and affect the normal operation of ElectionChain.

3. Technical Scheme

This part is focusing on the preliminary technical scheme of ElectionChain, including identity authentication, multi-chain system, flash voting protocol, consensus algorithm EDPOS, privacy protection, design of voting mechanism, decentralized ELT leasing market, storage scheme and smart contract. In the above technical scheme, some techniques have a strong confirmation, because they have been designed and tested; some are just preliminary ideas, with certain feasibility but uncertainty. It is normal that the final design scheme might be inconsistent with, even opposite to the existing scheme.

3.1 Identity Authentication

According to the above context, there are two voting patterns for voters, real-identity voting pattern and virtual-identity one, which are determined by election initiators when conducting election.

Under the virtual-identity voting pattern, lottery players and voters can directly vote in the way of Blockchain address, with no need of identity authentication by an authoritative identity authentication agency.

Under the real-identity voting pattern, each voter, elector or representative must conduct identity authentication through an authoritative identity authentication agency. Each participant shall disclose his/her identity to the authoritative identity authentication agency, which will return a BID (Blockchain Identity Card) to the participant after validating his/her identity through identity library, including the abstract value of real identity, publicly available information of the user and signature for the user, which shall be observable to everyone.

Authentication of some Blockchains has combined with biological recognition data, such as Case and ShoCard. To apply the Netki, OneName, BitID and Identify authentications, identity information shall be firstly registered on the Blockchain, and then linked to the account of social media. Moreover, Cambridge Blockchain, Trunomi, uPort, Tradle and Ripple emphasize on the integration with the existing enterprise solutions. ElectionChain will refer to these Blockchain authentication techniques and widen authentication channels, to make the identity authentication more convenient and efficient.

Centralized issue of authoritative identity authentication agency—we believe that there must be some trustworthy agencies to participate in when Blockchain is confronting with real world,

which can conduct identity authentication, asset acceptance and other operations, called ORACLES. To prevent the fabrication by one authoritative identity authentication agency, user identity shall be confirmed by introducing a mechanism of agreement by multiple or 2/3 agencies In the global scope, each country has its own authoritative identity authentication agency, each user shall conduct identity authentication in the multiple authoritative identity authentication agencies of the country where the nationality of the user belongs to, therefore, each country on the ElectionChain also has multiple authoritative identity authentication agencies.

The upper chain of authoritative identity authentication agency needs special verification procedures, such as governmental certificate, industrial certificate, license certificate and business certificate, which shall be initially examined and approved by development team, with subsequent scheme determined by ballot.

3.2 Multi-chain System

ElectionChain, a multi-chain system, consists of three sub-chains, namely identity chain, tickets chain and payment chain, each of which has its own responsibility. Identity chain is used for storage of identity authentication information of users, and transfer of identity information; tickets chain is used for management of the voting process and transfer of votes; payment chain, a payment system of digital currency, similar to bitcoin, is mainly for carrying ELT. Each user has the same address in these three sub-chains, which is routed through IDs of sub-chains.

Such design can flexibly meet the requirements of participants, for example, authoritative identity authentication agency only needs to read the information in identity chain, with no need of concerning tickets chain and payment chain; users who are only interested in digital currencies just need to visit payment chain without participating in the other two chains; users who have no ELTs and don't want to use them as well just need to join in identity chain and tickets chain for identity verification and vote; even don't take part in the identity verification, just vote with accepting votes. The above requirements of such participants can all be met.

Each sub-chain uses the same consensus algorithm in the same time interval through the same accounting, to produce a new block. For the sake of correlation, IDs of new blocks of identity chain and tickets chain need to be written into the block head structure of payment chain, by which other nodes will be updated.

ElectionChain will build a global Blockchain for election, but each country is allowed to possess its

own independent ElectionChain, because (1) there are a huge number of users in the world, and each country has different authoritative identity authentication agencies, (2) throughput shall be increased, (3) storage requirement of nodes shall be reduced. In order to differentiate these ElectionChains, we take global chain as the main ElectionChain, ElectionChains in countries are regarded as election side chains. All countries are not required to establish side chains, but an independent side chain can be established for a larger country with more elections; moreover most of small countries can launch elections on the main ElectionChain.

Interaction between the main chain and side chain includes ELTexchange, mutual recognition of identity and mutual acknowledge of votes, which shall be completed through ChainGate crossing the main chain and side chain. Any nodes can become a ChainGate, just by configuring a side chain that is required to be connected.

Interaction between side chains is similar to that between main chain and side chain, however, interaction between side chains is conducted through main chain, i. e. interaction between side chains is completed through two ChainGates.

Because the resources are greatly consumed by interactions between the main chain and side chain, as well as between side chains, (for example, the same transaction is transmitted in several Blockchain networks), such cross-chain transactions need extra expenses.

3.3 Consensus Algorithm EDPOS

Consensus algorithm is an effective method to guarantee the data consistency in distributed calculation system. At present, there are four types of consensus mechanisms, which are POW, POS, DPOS and traditional distributed data consistency algorithm.

(1) POW, Proof of Work, i. e. bitcoin mining is calculated by HASH operation to obtain an appropriate random number, then a new block is produced, which contains all transactions, and such a block shall be stored after verifying nodes in the whole network; however, this way is consuming energy greatly, so that resources are wasted greatly and the mining is centralized.

(2) POS, Proof of Stake, reduces the difficulty of block generation and accelerates the speed to look for random number, without consuming energy, according to the number and ownership duration of tokens occupied by each node;

(3) DPOS, Delegated Proof of Stake, similar to the votes of board of directors, i. e. coin holders

launch a certain number of voting nodes to conduct verification and bookkeeping on behalf of them. This way greatly reduces the number of nodes participating in validations and bookkeeping, and enhances the speed of confirming transactions.

(4) Traditional distributed consistency algorithms, such as PBFT, Paxos and Raft, together with data verification mechanism, can realize second-level consensus with no need of tokens, and is applicable to the Blockchain of alliance operation.

From the analysis of the above consensus algorithms, DPOS is suitable for public chain with higher performance requirement, similar to ElectionChain, and its confirmation time of transaction is two to three seconds, which is very fast.

Electrionchain is planning to enhance stimulation on the basis of DPOS, to make network much faster and more robust. Consensus algorithm adopted by ElectionChain is called VDPOS (VDPOS). According to improvement of application scenarios of multi-chain system, the time of producing block is three seconds with the size of 1M, and the main improvement is (1) to introduce Coinbase transaction in blocks of payment chain, and averagely distribute the annually increased coin quantity of 5 percent to each block, (2) that bookkeeping nodes send the remaining bookkeeping revenue after retaining 25 percent to backers in the period of every other 28,800 blocks. More stimulation makes the network faster and more robust, (3) that bookkeeping nodes firstly package blocks of identity chain and tickets chain, finally blocks of payment chain, and then put IDs of the latest Blockchains of identity chain and voting chain into the latest block of payment chain, to keep the consistency.

However, the number of nodes required by VDPOS is 101, with higher participation, thus VDPOS algorithm is used in advance, and then EDPOS at the appropriate time. The time for producing block of POS algorithm is one minute, with the size of 2M and annual rate of 5 percent.

The election side chain of countries constitutes ElectionChain network by independent VDPOS nodes, the number of consensus nodes can be reduced to 51, and such consensus nodes undertake the role of communication with the main chain as ChainGate.

3.4 Flash Voting Protocol

Lightning network is a kind of payment technique by using bitcoin script to ensure the safety of funds and accelerate the micropayment speed to second, with the aim of taking away the

micropayment from bitcoin Blockchain to conduct initial and final settlement just on the bitcoin Blockchain, during which, multiple payment processes are safely completed through establishing payment channel by lightning network.

ElectionChain will establish a kind of fast voting network similar to lightning network, which is called Flash Voting Protocal (FVP), to support explosive voting transactions, with the aim of (1) accelerating the voting process to make the vote successful, with no need of block confirmation, (2) being unable to change voters, candidates in ballot, and abandon the votes, (3) verifying whether their own votes of voters are recorded correctly, as the voting outcome is recorded on the Blockchain.

Specific thoughts are as follows:

(1) Establish independent or co-existing Flash Voting Node, to deal with real-time voting. Flash Voting Node can incorporate ElectionChain node, or be independent. i. e. every node has two patterns, one is election pattern (common ElectionChain node pattern), the other is flash voting pattern, both patterns can operate at the same time, but requirement on configuring nodes is high.

(2) Under the flash voting pattern, node can accept and collect flash voting requests, then condense them to a transaction, and record it on the voting chain, whilst the safety, verifiability and performance of flash voting transaction hereby shall be guaranteed.

(3) Lightning network guarantees the safety of funds by signature addresses of two public keys and zero-knowledge proof, whilst Flash Voting Protocol shall need such means to guarantee the votes not to be abandoned and changed.

The confirmation time of transaction in VDPOS algorithm is short with higher performance, thus it is not urgent for Flash Voting Protocol in terms of time, and there is a lot of time to consider and perfect the Flash Voting Protocol, therefore, we hope more technicians to provide better thoughts.

3.5 Privacy Protection

Privacy protection of ElectionChain is mainly reflected in privacy protection of identity and privacy protection of voted ballots.

(1) Privacy protection of identity

- The information shall be encrypted when initiating identity authentication, which is only

observable by authoritative identity authentication agencies.

• Identity information HASH (i.e. ID and signature) can be only appeared when issuing BID (Blockchain ID)

• When voters register, electors can require authoritative identity authentication agencies to conduct identity authentication to voters, so as to obtain the real identities of voters.

(2) Privacy protection of voted ballot.

•The vote is conducted as a virtual identity under the virtual identity voting pattern: Others know that this address has been voted, and that which candidate is voted by this address, which embodies the openness and transparency of Blockchain;

• The vote is conducted as a real identity under the real identity voting pattern

* Real-name vote: electors know who the voters are and which candidate is voted by them, but others have no idea of real identities of these voters, but their virtue identities.
* Anonymous vote: electors know who the voters are, and know the fact that they have already voted, but have no idea which candidate is voted by these voters, only the voted candidate knows the voter.

3.6 Design of Vote Mechanism

When launching a ballot by elector, abundant ballot tickets should be distributed to the voters, voters who have tickets can vote in this election. Ballot ticket is a kind of digital asset locking multiple ELTs (100 ELTs at the beginning, this number can be changed after voting), therefore electors shall calculate the number of voters when launching a ballot, the number of ELTs shall be the same as that of voters. These ELTs will be locked during election, shall not be used for payment, and these locked ELTs will come back to the electors until the ballot tickets are released when the election is finished.

Management of life cycle of election includes initiating election, (leasing ELT), distributing votes, starting votes, finishing votes and so on, while there is real-time statistics and outcome disclosure around this process.

Life cycle of ballot tickets includes four processes—generation, distribution, vote and release, among which generation means electors produce abundant ballot tickets according to election scenarios; distribution means that electors distribute the ballot tickets to each voter; vote means

the process of voters' voting candidate; release means the process of electors' destroying the ballot tickets and unlocking the ELTs after election.

Binding of ELTand ballot tickets is realized by locking ELTs of elector on the payment chain. When an elector produces certain number of ballot tickets, the corresponding number of ELTs will be locked on the payment chain; distribution and voting process of ballot tickets have nothing to do with payment chain; when releasing ballot tickets, they shall be destroyed on tickets chain, and the locked ELTs will be unlocked and returned at the same time.

3.7 Decentralized Leasing Market

With the price growth of ELT, some electors can't afford to buy ELTs that the election needs, which is unfavorable to the promotion of ElectionChain. Thus we introduced a decentralized leasing market, in which there are leaser and leasee, the leaser with ELTcan rent these ELTs for profits; because the ELTs are required for election, the leasee is willing to rent them by paying daily interests.

Before selling by the leaser, the leaser must have ELTs, and the system will lock some ELTs; before buying by the leasee, the leasee must possess enough ELTs to pay the interests for the leasing period, and the system will lock some ELTs as well. The system realizes the purchase and sales at the price of daily interest rate, taking account into the leasing duration and the number of coins. When achieving an order successfully, the interests shall be paid daily, and the leasing time shall be calculated by the hour.

Meanwhile, the development team will accept the applications of leasing ELTfor free from some governments and non-profit organizations, as long as these organizations pass the identity authentication, the team will lend the required ELTs to the elector for free, while these ELTs will return to the account of the development team after election.

3.8 Storage Mechanism

Storage requirement: it assumes that each vote needs 100 bytes, there are 240 million people, and one presidential election consumes 22.34GB storage space, so that the storage pressure is huge. With the characteristic of co-sharing accounting book in Blockchain network, each node keeps the same accounting book, the storage cost is huge. Both bitcoin Blockchain and Ethereum need 160GB capacity respectively, however, BitShares just needs no more than 10GB capacity, that is because BitShares adopts lots of measures to compress the storage, such as replacing long

ID with short index, and only keeping raw data.

Because the tickets chain is separated with other chains, it can conduct storage independently, if there is no interest in the votes unrelated to oneself, the relevant election and voting process can just be kept, so as to reduce storage demand.

3.9 Smart Contract

Ethereum is the first smart contract platform based on Blockchain, the preparation of smart contract can realize the business scenario more easily, with no need of considering the low-level design and its realization. However, there is a performance issue in Ethereum, EVM is a major smart contract system. When verifying each smart contract transaction, it is necessary to start EVM, conduct smart contract call and store the updated data, so it takes time for the verification process. Compare the testing results of the following four Blockchains (with configuration of eight cores CPU/16G memory/VPS with 5Mbps flow)

(1) Ethereum. During our experimental test, Ethereum can only support 100TPS, far from meeting the requirement of ElectionChain.

(2) The test outcome of 4 nodes of Fabric alliance chain is similar to that of Ethereum test, i.e. transaction throughput is around 100TPS as well.

(3) Bitcoin private chain based on PBFT consensus algorithm can almost reach 1000TPS in our actual test.

(4) We don't test BitShares, but it can support 3300TPS in real environment, according to the official test results.

Therefore, we have to reconsider the smart contract. For the big impact of smart contract system, bitcoin script and BitShares operation on performance, we believe: the general smart contract platforms, such as Ethereum and Fabric, can greatly facilitate the application and development of Blockchain, but reduce the performance of Blockchain at the same time; however, it takes shorter time for bitcoin script and BitShares operational Blockchain to verify the transactions, whilst the throughput capacity can be improved.

ElectionChain, a Blockchain application system, focuses on the application scenarios of election, therefore, it will select a Blockchain that is the most suitable for such application scenarios, and BitShares seems appropriate for now.

3.10 Transaction Throughput

For Blockchain, transaction throughput is a bottleneck. Election has a higher requirement to the timeliness and throughput. Once the election is started, business volume is greatly increased, and the Blockchain network will bear a great pressure. Taking the U. S. Presidential Election Day as an example, 240 million Americans elect a president and 538 electors within 12 hours, i.e. the Blockchain has to support 5555TPS within 12 hours, which is a big challenge to a Blockchain system. At present, none of Bitcoin public chain, Ethereum private chain and Fabric alliance chain can meet this requirement, even though BitShares public chain can support 3300TPS, there is no Blockchain system that can reach 5555TPS in practical use for now.

The ultimate aim of transaction throughput design in this project is to support the U. S. presidential election. There are lots of factors in correlation with throughput, including consensus algorithm, flash voting protocol, multi-chain system, size of Blockchain, time of block production, verification time of transaction, use of smart contract, node configuration and size of broadband, and we will verify the optimization one by one, to achieve the best performance effect.

4 Project Team and Plan

4.1 Project Team

4.1.1 Project leader: Shentu Qingchun

Bankledger CEO, member of Shenzhen Financial Standards Board, doctor of Shenzhen University, senior engineer, high-level talents in Shenzhen, appraisal expert in Shenzhen government procurement. Shentu Qingchun ever obtained Shenzhen Science and Technology Innovation Award in 2008, the third prize of Guangdong S&T Progress Award in 2009, Shenzhen Invention Award in 2012 and his four inventions have obtained patents. He set up the Bankledger in 2012, and started to study Blockchain in 2013, then went into financial industry in 2016. He ever

published more than 20 technical articles about Blockchain. See details in 8btc column: http://www.8btc.com/author/14523

He also published several academic articles, see details on the websites of arxiv.org:

(1) Research on Anonymization and De-anonymization in the Bitcoin System

https://arxiv.org/abs/1510.07782

(2) A Blind-Mixing Scheme for Bitcoin based on an Elliptic Curve Cryptography Blind Digital Signature Algorithm

https://arxiv.org/abs/1510.05833

(3) Transaction Remote Release (TRR): A New Anonymization Technology for Bitcoin

https://arxiv.org/abs/1509.06160

4.1.2 Leader of project research and development: Tu Xiaoqiang

- Tu was born in 1984 and graduated from computer department, Wuhan University.
- Senior software developer and programmer, 10 years experience of C++ development; IOS development engineer
- Tu successively held the post of Project Manager and Department Manager in Foxconn, Donson Network and Hua Yang Xintong, and was involved in R&D of financial technology.

•Tu have three years experience of Blockchain R&D and is familiar with varies of underlying technologies of Blockchain. He was appointed CTO of Bankledger in 2016.

4.1.3 Director of project operation: Zhou Ting

•Zhou was born in 1985 and is a graduation of Shenzhen University in English.

•Zhou worked in customer engineering dept of HUAWEI in 2019-2012 and took charge of overseas client reception.

•Zhou successively held the post of deputy general manager of Bitcoin International Exchange in 2013-2015 and operation director of POW8, who commits to marketing, administration and financial affairs.

•Zhou was appointed COO of Bankledger in 2016.

4.1.4 Overseas technical specialist: Steven Li

•Mr. Li is a Chinese American, and an entrepreneur with successive success.

•He graduated from special class for the gifted young belonged to University of Science and Technology of China, and devoted himself to research and innovation of software and Internet since early 1990s and become senior specialist in technology and management in Silicon Valley.

•For the first time, under his leadership, pre-technical team developed video conference product —WebEx, which is pioneering in market. The company was sold out at a price of $3.2 billion.

•For the second time, he set up Sumilux, a technology company devoting to application service for Internet enterprise. He successfully withdrew after the company was bought out.

•Mr. Li ever held post of vice president of Amazon global website platform, taking charge of 80% of its global traffic.

•As a business angel, he invested several startups, and made a profit of 200 million from one program among which in period of two and a half years, then he withdrew from it.

•He entered Bitcoin industry in 2013, and became one of business angels of DarkNetSpace DNC program developed by Doctor Shentu.

•In 2017, Mr. Li became business angel and overseas technical specialist of ElectionChain responsible by Doctor Shentu again.

4.1.5 Other members

•A project team of nearly 20 members;

•14 members for C++ and JAVA development

•Two members for operation, maintenance and graphic design;

•Four members for promotion, operation, maintenance and logistics.

4.2 Senior consultant

Guo Hongcai, Founder of BitAngel

He is a business angel of Blockchain and actively involved in Blockchain field. He has unique understanding about global digital currency transaction and rich resources of it.

Mr. Guo Hongcai is appointed senior consultant of ElectionChain.

4.3R&Dand Promotion Plans

VoteChain R&D program is as follows:

(1) Based on POS consensus algorithm, the ELT1.0 PC wallet, which will be launched in early November 2017, supports WINDOWS, LINUX and Mac OS, as well as blockchain browser and Android mobile wallet.

(2) Blockchain voting can be conducted by WeChat public account of VoteChain which will be launched in mid-November 2017;

(3) Blockchain voting can be conducted by VoteChain APP which will be launched in mid-December 2017;

(4) The second version, namely the VoteChain test chain based on VDPOS consensus algorithm, will be launched in March 2018. However, the first version will be still the official one. To implement VDPOS algorithm, voting and decision-making process;

(5) The third VoteChain version, which will be launched in September 2018, will be used as the

formal running version for voting, decision making and other business. Besides, a snapshot of the first version will be taken, so that ELT can be transferred to this version.
The promotion plan of VoteChain is shown below:
(1) VoteChain will be launched at foreign exchanges in mid-November 2017 and start transaction;
(2) VoteChain will start overseas promotion in June 2018;

5 Contacts

Official website of project: http://electionchain.com

Email: marketing@electionchain.com

Wechat: elcoin666

qq group; 428387783