SECURITY DATA SYSTEM OF BALLOTS CALCULATION BY USING THE MULTILEVEL BLOCKCHAIN STORAGE METHOD

1st Wahyu Santoso
Computer Engineering - ITS
Surabaya, Indonesia
wahyusantoso1997@gmail.com

2nd Dr. Reza Fuad Rachmadi, ST., MT.
Computer Engineering - ITS
Surabaya, Indonesia
fuad@its.ac.id

3rd Arief Kurniawan, ST., MT.
Computer Engineering - ITS
Surabaya, Indonesia
arifku@ee.its.ac.id

***Abstract*—Voting is a process to expressing the people's opinions to choosing the leaders or in making decisions. The conventional voting system is not efficient by cost and time, the solution is e-voting. However, most e-voting systems are still using the centralized server, they are able be down if the main server is damaged or hacked. So in this final project, the solution is using the distributed system with blockchain data storage. The system will be designed using multilevel blockchain storage method for ballots in the TPS (client) of the village, city, province, and country to reduce the validation time of blockchain when there is a new data. In this project, the system can validate the blockchain. If the blockchain is approved by more than 50% of nodes in the network, so the blockchain is valid. Then system can validate the registered user to submit the ballot once. And the system is able to recapitulate the election ballots well. Hoped this system can secure the data of election.**

***Index Terms*—e-voting, blockchain, distributed system**

I. Introduction

The e-voting technology can save money and time than conventional voting, but it is still have some security issues, the one is the centralized and decentralized network system, which if the server of network is hacked by someone, so the ballots or data can be manipulated.

Blockchain is a distributed system model, which can maintain the security and integrity of the election ballots. The concept is each computer or node in the network is connected to other. Ballots are saved to the blockchain each node in the network, the data is identical to each other. In other words, each node in the network have the copy of data. If one of the nodes in the network want to change the data, so it is must be verified by more 50% of nodes in the network, if it is pass verification, all copies of data in the network will be updated so no data different.

National level of election is followed by a large number of voters so it need the multilevel blockchain storage method to reduce the duration of blockchain validation when there is a new data. The levels are village, city, province, and country.

Hoped this system can be a solution to maintaining the security and integrity of the election ballots, because changing the data in the blockchain network is impractical, and guarantee the availability of data if main server or node is down.

II. Basic Theory

A. Peer-to-Peer Distributed Network

A peer-to-peer distributed network (P2P) is a network which every computer (can be called peer or node) that is in a network are connected to each other and no central node, or in other words each computer have the same functions to receiving, sending, and processing data. P2P network can develop widely by joining peers or new nodes in the network. The path of data communication on P2P network is not easy to be disabled because the type of network can transmit data through many paths among many nodes available in the network.

This network don't require centralized control or even centralized service. In this network, data communication can pass through any node path getting to the destination, in other words if one node is down, the data can pass through another path and still reach the destination. This greatly distinguishes distributed networks with centralized and decentralized networks which if one gateway from one node is disabled, so the data will not reach the destination, as can be seen in Figure 1

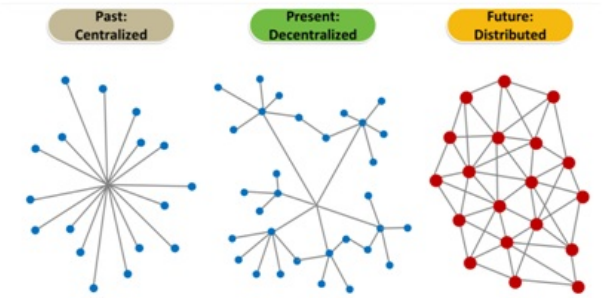

Fig. 1: Different of 3 Networks

B. Blockchain

Blockchain is a distributed database that is used to handle data records that continue to increase, the data record is called block. Each block have a time marker and a unique code that is connected to the previous block, so that each block is

connected to each other and cannot be changed. Blockchains are usually managed by peer-to-peer network that collectively follow protocols to validate new block. If there is an order to add a new block, so each node in the peer-to-peer network will first validate the block and then all nodes will update their data record, as shown in Figure 2

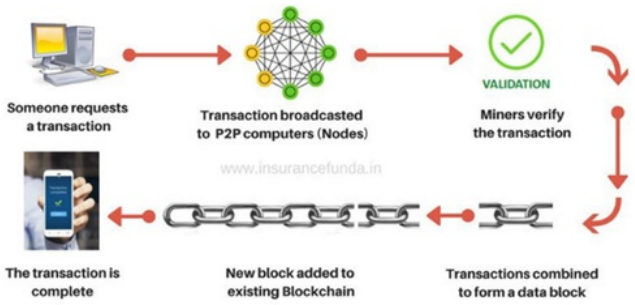

Fig. 2: How Blockchain Work

Blockchain have several types [1], they are Public Block that can accessed by everyone like Bitcoin [3], then Permissioned Blockchain is controlled by an organization but can be used by the public, and the last is the Private Blockchain can only be used by certain organizations. The type of blockchain that will be used in this Final Project is a combination of the Permissioned Blockchain and the Private Blockchain.

III. Design and Implementation

A. System Design

The system is built using a multilevel blockchain concept, voter's ballots are stored in the blockchain in each village where voters are registered. After the election is done, the blockchains in the village level are saved to the blockchain network in the city level, then from the city level, blockchains are saved to the provincial level and then to national level. This multilevel system is created to deal with the high traffic when the election is going on. So by this system, the blockchain network only need to handle the transactions in the village level. Figure 3 is a design that describe the concept and working of the system.

B. Workflow Design

Figure 4 is the finite state machine (FSM) process of ballot blockchain in the village level. The node as the host will be listening. If the host receive ballot from the voter (client), then the host will check the ballot status in the network, if it is valid, so the ballot is pushed into the pool, the container to hold all incoming ballots before they are saved in the blockchain. Every certain duration or if the pool have exceeded the specified capacity, then the ballots in the pool are broadcast to all nodes in the network for mining, the process of completing the challenge determined by the network. Ballots will be saved in a new block with hashing obtained from completing the challenge, then the block is pushed into the blockchain.

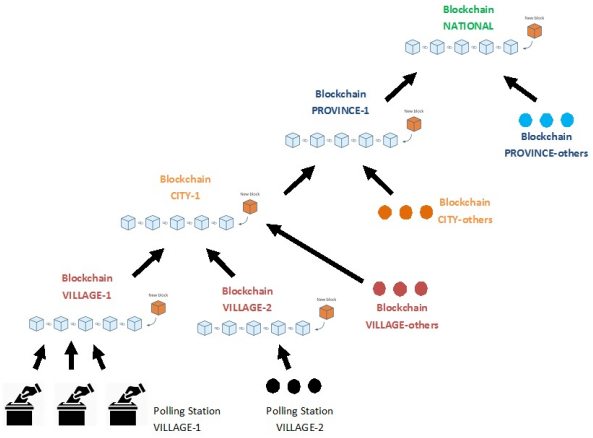

Fig. 3: How System Work

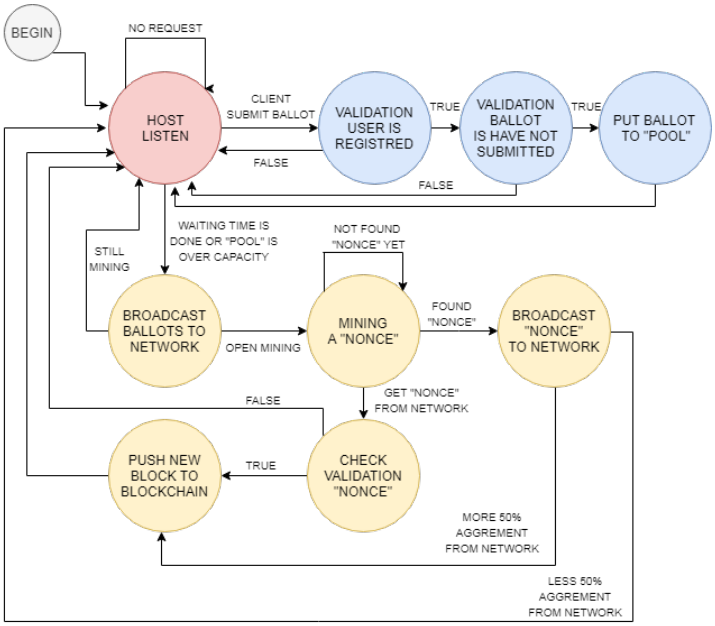

Fig. 4: FSM of System

Before push a new block into the blockchain, the block must be agreed that the block is valid by more than a half (50%) of the nodes in the network, because the blockchain remain valid through the most decision making in the network to determine the addition of the new block which is valid. Therefore, the nodes in a network is at least 3 nodes or more (must be odd), to avoid conflict because the decision to validate the block is balance.

After the election is done, the bottom network, village level recapitulate the ballots and send the result to the top network, it is the city level. Then the network in the city level recapitulate the result of recapitulation from each network in the village level. also at the provincial and national levels.

Figure 5 describe the flow of the ballots recapitulation pro-

cess in the village level (type ”data”) or top level (type ”file”). In the village level, ballots in the blockchain are recapitulated, then the hashing of the blockchain have been hammered with recapitulation data, the hashing of the recapitulation is used as the file name to store recapitulation data in the village level. As for the top level, it is necessary to check first that the blockchain in the lower level is valid before recapitulating. The top level only combine all recapitulation data from the lower level, then the next process is the same as village level.

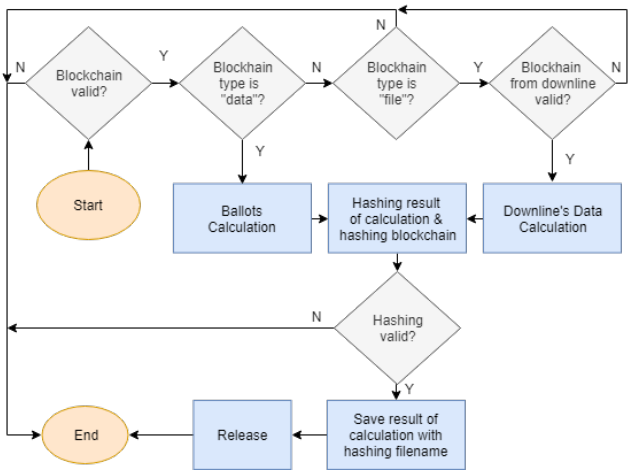

Fig. 5: Workflow of Ballot Calculation

C. Release the Result of Ballots Calculation

Blockchain is hashed, so the hashing blockchain is obtained. Then the blockchain is recapitulated so the result of votes for each candidate is obtained. Then it is hashed with the hashing blockchain so the hashing recapitulation is obtained. Hashing blockchain and hashing recapitulation are send (release) to the top network without send the original master data, just send the file name of hashing. It can save the memory space in the node, if the master data is changed 1 bit only, then the recapitulation result are invalid due to difference in hashing. Figure 6 describe the ballots recapitulation flow.

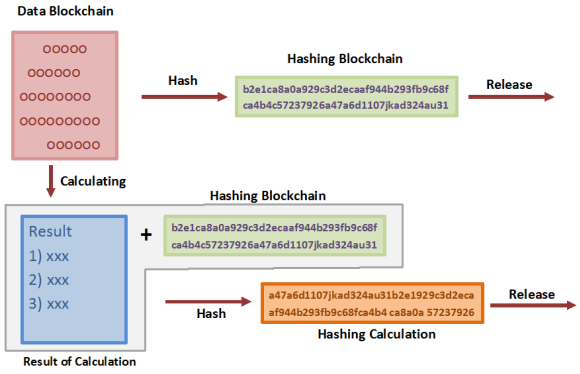

Fig. 6: Release the Result of Ballots Calculation

IV. Testing

The Tests in this Final Project are testing functions of the blockchain system at the village level and at the top level, as well as testing the performance and efficiency of the system.

A. Devices

There are 3 computers with difference specification.

1) PC1 - RAM 4 GB - CPU 2 core 1.8 GHz
2) PC2 - RAM 8 GB - CPU i5 4 core 1.8 GHz
3) PC3 - RAM 16 GB - CPU i7 4 core 3.5 GHz

B. Simulation Data

There are 100000 data (ballots) with registered voter's identity number from 2000001 to 2100000 and password is ”*secret*”.

C. Blockchain Validation

The test was manipulate the data with 3 different nodes combination. Look for Table I.

TABLE I: Blockchain Validation

Manipulate Node	Blockchain Status in Node			Blockchain Status in Network
	1	2	3	
None	Valid	Valid	Valid	Valid
1	Not Valid	Valid	Valid	Valid
2	Valid	Not Valid	Valid	Valid
3	Valid	Valid	Not Valid	Valid
1,2	Not Valid	Not Valid	Not Valid	Not Valid
1,3	Not Valid	Not Valid	Not Valid	Not Valid
2,3	Not Valid	Not Valid	Not Valid	Not Valid
1,2,3	Not Valid	Not Valid	Not Valid	Not Valid

According in this test, the system can validating the blockchain well, the blockchain is valid if in each node is similar. In the case of manipulating data in one node, only in that node, the blockchain is invalid, and the other are valid. In the case of manipulating data in more than one node, so the blockchain in all nodes become be invalid, because the blockchain validation is less than 50% of nodes in the network.

D. Duration of Ballot Submission

Test was use 10, 20, and 40 of concurrent clients on each computer, with mining difficulty levels are 3 and 4.

Look Table II and Table III for the result.

According the tests shown in Table II and Table III, if more clients were submit ballot at the same time, so the average duration needed by the voters to submit ballot became longer, but the total duration needed for the election become faster. From that, the duration required by PC1 is at least 5 times more than PC2, because PC2's specification is better than PC1. PC2 only take about 6 hours for the election, so the system with PC2's specification is minimal the specification needed

TABLE II: Duration of Ballot Submission (Mining Difficulty Level is 3)

Con. Client	Total Duration (seconds)			Average Duration (seconds)		
	PC1	PC2	PC3	PC1	PC2	PC3
10	111987.56	36191.25	24637.67	11.19	3.61	2.46
20	101139.68	34916.06	23684.91	20.22	6.98	4.73
40	98780.30	31229.17	21924.27	39.51	12.49	8.76

TABLE III: Duration of Ballot Submission (Mining Difficulty Level is 4)

Con. Client	Total Duration (seconds)			Average Duration (seconds)		
	PC1	PC2	PC3	PC1	PC2	PC3
10	149941.15	36043.26	25161.47	14.99	3.60	2.51
20	135709.54	31476.08	18467.56	27.14	6.29	3.69
40	122378.66	26039.48	14160.79	48.95	10.41	5.66

to fit the time required by conventional elections (for 100.000 registered voters).

E. Duration to Create New Block

Test was use 10, 20, and 40 of concurrent clients on each computer, with mining difficulty levels are 3 and 4. New block was created if the pool have more than 50 ballots or every 2 minutes.

According the tests shown in Table IV and Table V, if concurrent clients were very much, so very little blocks were generated, because the average duration needed to validated and created the new block very long, so the ballots in each block were very much too.

TABLE IV: Duration to Create New Block (Mining Difficulty Level is 3)

Con. Client	Block Created Total			Average Duration (seconds/block)			Average Ballot (ballots/block)		
	PC1	PC2	PC3	PC1	PC2	PC3	PC1	PC2	PC3
10	1067	2113	2074	104.12	5.47	3.65	93.72	47.32	48.21
20	521	2096	2046	193.96	9.42	6.47	191.93	47.70	48.87
40	275	1961	1684	359.56	14.45	11.52	363.63	50.99	59.38

TABLE V: Duration to Create New Block (Mining Difficulty Level is 4)

Con. Client	Block Created Total			Average Duration (seconds/block)			Average Ballot (ballots/block)		
	PC1	PC2	PC3	PC1	PC2	PC3	PC1	PC2	PC3
10	968	1725	1820	154.15	15.75	9.26	103.30	57.97	54.94
20	499	1012	738	271.48	31.29	24.00	200.40	98.81	135.50
40	248	725	140	494.04	42.36	92.05	403.22	137.93	714.28

F. Ballots Calculation

In this tests, from village to national level. And 3 candidates are selected by randomly with numbers 1, 2 and 3.

This is ballot calculation in village level. Look for Table VI

TABLE VI: Ballots Calculation in Village Level

Village Name	City Name	Ballots Total	Vote Total		
			1	2	3
Village-A	City-A	40000	19034	19044	1922
Village-B	City-A	100000	47770	47158	5072

This is ballot calculation in city level. Look for Table VII

TABLE VII: Ballots Calculation in City Level

City Name	Province Name	Ballots Total	Vote Total		
			1	2	3
City-A	Province-A	140000	66804	66202	6994
City-Others	Province-A	1000	339	633	28

This is ballot calculation in province level. Look for Table VIII

TABLE VIII: Ballots Calculation in Province Level

Province Name	Country Name	Ballots Total	Vote Total		
			1	2	3
Province-A	Indonesia	141000	67143	66835	7022
Province-Others	Indonesia	1000	614	195	191

This is ballot calculation in national level. Look for Table IX

TABLE IX: Ballots Calculation in National Level

Country Name	Ballots Total	Vote Total		
		1	2	3
Indonesia	142000	67757	67030	7213

According in this test, the system can calculating the ballots from blockchain well. Ballots are grouped and calculated so obtaining the result of votes for each candidate.

V. Conclusion

1) The system can validate the blockchain. If the blockchain is approved by more than 50% of nodes in the network, so the blockchain is valid, if it is not more than 50%, so the blockchain is invalid.

2) The average duration total of ballot submission in PC1 is 33 hours, PC2 is 9 hours, and PC3 is just 6 hours.
3) The average duration needed to create new block in PC1 is 262.89 seconds/block, PC2 is 19.47 seconds/block, and PC3 is 24.49 seconds/block.
4) And the system is able to recapitulate the election ballots well.

REFERENCES

[1] M. Gupta, Blockchain For Dummies. United States of America: John Wiley and Sons Inc, 2017.
[2] A. Rayendra, RANCANG BANGUN SISTEM E-VOTING DENGAN MENGGUNAKAN TEKNOLOGI BLOCKCHAIN. Padang: Politeknik Negeri Padang, 2017.
[3] S. Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System. Bitcoin org, 2009.
[4] a. e. M. Hajjar, "An e-voting system for lebanese elections," Journal of Theoretical and Applied Information Technology, 2006.
[5] a. e. Zamora C.G., "Seles: An e-voting system for medium scale online elections," Proceedings of the 6th Mexican International Conference on Computer Science (ENC'05), 2005.
[6] C. Z. dan A. Pilkjaer, "E-voting in pakistan," Master Thesis, Departement of Business Administration and Social Sciences, Lulea University of Technology, 2007.
[7] L. H. dan Varida Megawati Simarmata, "E-voting: Kebutuhan vs. kesiapan (menyongsong) e-demokrasi," Fakultas Hukum Universitas Indonesia Depok, Jawa Barat, 2011.