Development of the Voting System for Game Show Program Using Blockchain Technology

Sataporn Khaikaew
Technology of Information System Management,
Faculty of Engineering, Mahidol University
Nakhonpathom, Thailand
sataporn.khi@student.mahidol.ac.th

Adisorn Leelasantitham*
Technology of Information System Management,
Faculty of Engineering, Mahidol University
Nakhonpathom, Thailand
*Corresponding author--adisorn.lee@mahidol.ac.th

***Abstract*— At present, it is well known that blockchain technology can be applied in many organizations, whether large or small. The users can adapt the blockchain technology to suit their need. It has become an important technology in a very short time and it begins to play a beneficial role in many disciplines. This research is aimed to develop the voting system for game show program using blockchain technology in order to assess the efficiency and transparency of the system by voting through the application web developed by the researchers. The result revealed that the votes were correct and transparent because recording the votes in blockchain is immutable. Moreover, as the efficiency of proof of work (PoW) and Ganache were compared with each other, the transaction sending speed in Ganache was found to be slightly faster than that in PoW in the order of seconds.**

Keywords—game show, blockchain, smart contract, vote

I. INTRODUCTION

Game Show is a television program for entertainment which may have different forms. Most of them are very popular, because besides being fun and entertained, they also include essential knowledge for everyday life [1]. One of the interesting form is to provide the audiences with feedback or reflection response feature after watching a program. The audiences' feeling satisfication, dissatifaction or opinions are very important to the program producers [2]. Game Show program originated in the United States of America. In Thailand, there are a variety of game show programs that have been created as we have watched them nowadays. The programs consist of several candidates playing game for rewards aiming to give knowledge, entertainment, and fun to the participants and audiences [3]. The market capitalization, in the media category, of game show programs was worth as much as 1,019,163.62 ('000 bath) as of May 1, 2020 [4]. In 2019, in comparison with news programs, game show programs had a higher rating at 4.993 while news programs'rating was at 1.943 because of their popularly among the audiences [5].

However, the SMS has the weak spot of making the audiences sceptical about the transparency of the voting system, since the audiences cannot monitor the votes. The audiences may suspect that the program has already locked the result, and so they lose confidence in the outcome. This research is aimed to develop the voting system for game show program using Blockchain Technology. In order to resolve the transparency problem of the game show program.

II. LITERATURE REVIEW

A. SMS Voting (Short Message Service Voting)

SMS is the technology of receiving and sending information using store and forward method through the device called SMS-C .It is a short message service via mobile. Presently, the SMS is limited to 160 characters per one sending. Nowadays, SMS is used in the voting system called SMS voting [6]. The diagram showing the operation of SMS voting is illustrated in Figure 1.

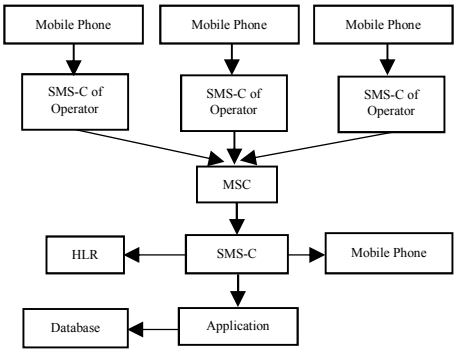

Fig. 1 Operation of SMS Voting

B. Blockchain

Blockchain technology originated in 2008 by the presentation of Satashi Nakamoto. Blockchain is a Shared Database or Distributed Ledger Technology (DLT). It is the way of recording data such that the security of the previously recorded data cannot be changed or modified which all the users will see the same set of recorded data, so increasing the reliability [7].

C. Blockchain Consensus Protocol

Consensus Algorithm is the transaction process that everyone in the blockchain network agreed upon about the status of distributed ledger. Consensus algorithm gains the reliability of the blockchain network. It wants trust among the unacquaintants in distributed computing environment. Basically, consensus protocol ensures that every new blockchain added is the single one truth approved by every node [8].

Proof of Work (PoW): The idea of Proof of Work was published for the first time in 1993 by Cynthia Dwork and Moni Naor. Later, it was used by Satoshi Nakamoto in 2008 [9]. Pow is the most well-known algorithm in Bitcoin system, all the transactions occurring in 10 minutes will be grouped as one block and linked by time chain as a single chain and shared on the entire P2P (peer-to-peer) network without a third party involved [10]. It is the consensus process that

involves complex mathematical solutions and taking time to value problem of every node in the PoW network.

Proof of Stake (PoS): is a new consensus protocol which has been developed to resolve the weak spot of PoW. PoS uses the asset of validations to confirm transactions. If the validators have large guaranteed assets, they have a high opportunity to have write access in the next block. The writer of the data in the next block will get the fee in return [7]. The advantage of PoS is that it is not necessary to operate. Some of the advantages of Proof of Stake are that no Work is required, thus it requires less energy; the 51% attack is theoretically more expensive, and PoS may encourage a more decentralized network of nodes than PoW [11].

Proof of Authority (PoA): Proof of Authority (PoA) uses the ID of the users to create the best verifying tools for the transaction. Proof of Authority was introduced by Gavin Wood who founded Ethereum and Parity Technology. PoA is the process of consensus algorithm which conforms to the licensed blockchain. It is important because of the higher efficiency as compared to Byzantine Fault Tolerant Algorithms (BFT) [12].

D. Ethereum Blockchain

Etherum blockchain was initially developed by Vitalik Buterin, a Russian developer in 2013.

Smart Contract: Nick Szabo was the first to coin the term "Smart Contract" in 1994. Later in 1998, He created the virtual currency called "Bit Gold", 10 years before the creation of Bitcoin [13]. Smart Contract is a digital process determined in advance to automatically process transactions. It can operate to the agreement automatically and immediately when events are compliant with the contract which specifies the conditions in advance. It is immutable and is transparent.

Solidity is the language for creating smart contract on Ethereum. It is derived from the language C++, Python, and JavaScript and developed for EVM. Importantly, it is a statically typed language, i.e. the variables must be defined when they are declared. It is also an Object-Oriental (OO) language due to its property of inheritance and structure, with libraries supported. It can define types of data by programmers, examples of solidity application include fundraising program, bidding program, wallet, voting program [14].

Function is a part of Smart Contract. Function can interact with other Smart Contract in deciding to store data and send Ether coin to others. In this research, we use functions for data entry and configuration.

Variable is used for data storage.

Gas is the fee or setting the prices for successful transactions or making contract on Ethereum blockchain platform. The prices are in the unit of cryptocurrency ether, known as Gwei. Gas is used to manage the resources of Etheruem Virtual Machine (EVM) for safety operation of smart contract. The right price of Gas is determined by network's miners who can deny to process the transactions if the price of Gas is not standard [15].

Ganache is a personal blockchain for development to Ethereum which is capable of contract modification, application development, and test run. It can be used in develop application program and command- line tool (formerly named as TestRPC) Ganache is ready for use on Windows, Mac, and Linux

E. Decentralized Applications (DApps)

Decentralized Application (DApp) is an application that uses Smart Contract as an interface between users and Smart Contract. A typical example of DApp is a cryptocurrency application that runs on the blockchain network. The DApp's application structure consists of front-end interface (Web browser, HTML, CSS) and back-end interface (Web3 JavaScript) as described in Figure 2. DApp interacts with Ethereum (EVM) nodes using JSON RPC, JSON RPC as the protocol. Remote procedure call (RPC) wirelessly weighs The Ethereum clients use to interact with the node Ethereum [16].

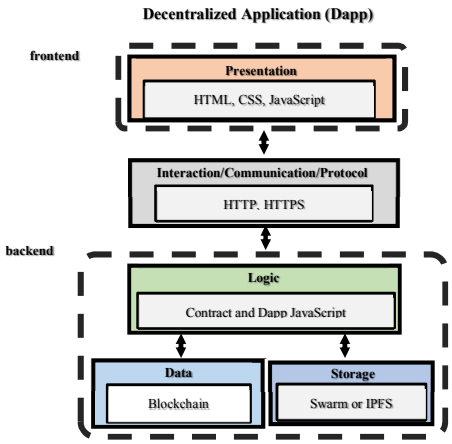

Fig. 2 DApp structure

F. Related Research

Blockchain technology has its influence in banking business, but also in other industries as well, such as automobile industry, contribution and fund raising, medical field, including application in utilities which is a case study of consumers, prosumers and SMEs [17].

One of other application of blockchain technology is in the voting system of an election. The introduction of blockchain system in an election to increase transparency causes Republic of Sierra Leone which is a very small country in West Africa to adopt blockchain system to enhance and develop a digital election as the first country in the world. This country has approved and permitted Agora company from Switzerland to implement the blockchain system in an election in the hope that it will help counting the votes, preventing cheating and creating transparency [18].

Estonia adopts the blockchain technology in an election and is well-known as i-voting. The country has employed digital voting since 2005 AD and has permitted online voting since 2007 AD. Later in 2015 AD the country has adopted the voting system based on blockchain technology. The evidence used in i-voting is the digital ID card which every citizen of the country must possess. Blockchain technology will be used in sending the voting cards. Every voting card must be examined for validity in the process and must be time stamped. The data will be kept in the blockchain system for proof of existence [7].

III. Research Methodology

A. Proposed Method

As previously mentioned about the non-transparency issue in the voting through SMS, this research presents development of voting system for game show program using blockchain technology to resolve the problem as illustrated in Figure 3.

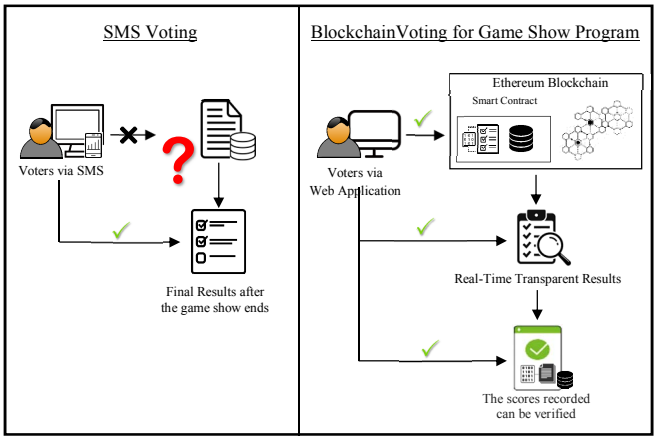

Fig. 3 Proposed voting system Game Show Program using blockchain technology

In each voting, the data will be kept as a transaction on blockchain, and making backup copies which are saved in many distributed places in a node. Each voter votes by using account address for verification and confirmation of voting. When a voter votes for his or her favorite candidates, the wallet will decrease (meaning that if you have a lot of wallet, you can vote for your favorite candidates as many times as you want within a time limit set by game show programs) so the voting in game show programs is different from an election voting which the elligible can vote only once and is also different from SMS voting which voters cannot see the scores in real time and cannot verify the data. The application consists of smart contract which written using Etheruem's solidity language, scripts written in JavaScript, and HTML page. In this research, a game show program has been simulated by letting voters vote for their favorite singers within a time limit. If duplicate votings occur at the same time (known as double spending) , the transactions will be examined by miner who is elected by the blockchain network to perform the verification and confirmation of the data. Double spending is the attempt to use the same digital currency twice by making duplicate transactions. This problem is one of important drawbacks in digital currency which must be solved to ensure that it will not be used in the wrong way. So the blockchain must have an examiner of duplicate transactions, known as Miner. In a blockchain, only the first transaction of double spending will be verified and confirmed by miner, the second one will be ignored since it is considered incorrect.

B. System Model

The application web is designed as shown in Figure 4 to model the voting system for game show program using blockchain technology and smart contract. It operates on the distributed network, i.e. ethereum blockchain. The research method includes writing smart contract using ethereum's solidity language to set the voting rules. The data are kept in Variable. The application web using JavaScript, HTML, and CSS as detailed in the following.

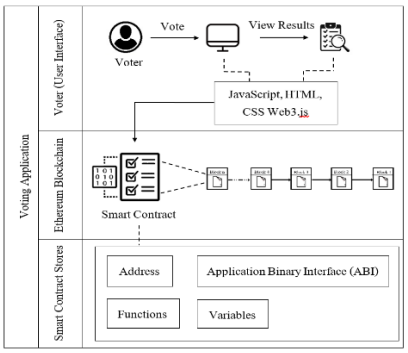

Fig. 4 Overview of Voting steps using Blockchain

Ethereum's Web3 Framework will help the voters to manage the correspondence with Ethereum blockchain easily. The voters need not download full or part Ethereum. When the voters vote, the correspondence will be safe and can be verified. The voters will receive a node on his or her mobile and is synchronized with blockchain for corresponding with the system through Web3. The processings are as follows:

1) Smart Contract Stores Phase: keeps the data of Private Key (Wallet Address), Function and Variable

2) Ethereum Blockchain Phase: creates Accounts, run miner, confirms transaction and keeps smart contract.

3) Voter Phase: votes through application web .html, links the voters with the system, votes for his or her favorite candidate, clicking the related pushbutton will call the commands (in JavaScript).

C. Steps of Smart Contract

In this research, there are 2 steps of smart contract as shown in Figure 5. It can be seen that the functions Vote( ) and getWinning( ) are included in all steps to retrieve the database recorded on Ethereum Blockchain. In the final of voting, the function getWinning( ) will return the votes with highest score.

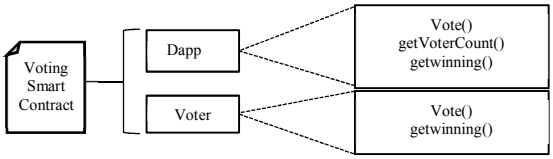

Fig. 5 The content of the proposed voting smart contract

In Figure 6, the first layer, Dapp interface, is for the correspondence with the users. The second layer, Data layer, transforms the input data of the first layer into string data, JSON. The third layer, Smart Contract layer, contains the voting smart contract. The last layer, Web3. js layer, is responsible for connection the voters with Ethereun Blockchain.

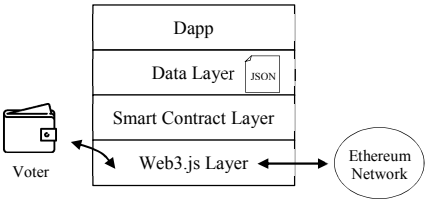

Fig. 6 The structure of decentralized application used in the proposed system

IV. Experimental Results

In this research, the voter can see the real-time score and the system records the score, gas value, and the voting time. The function Voter( ) will receive the data and send eth. calls to voting contract. After that, the selected candidate will be verified and the number of times of the vote will be counted. The system will examine voters' account address. Each new vote will be sent to every node. Each node will keep the data which are collected as a block. Each node will verify each block. If the votes come in at the same time, the one which is verified and confirmed first will be considered a correct block, others will be assigned orphan blocks. The orphan blocks will be sent to the queue in unconfirmed pool for further verification and confirmation. The function getVoteCount( ) retrieves the data. Whenever the voter are successful in their votes, getVotesCount( ) will send eth. call with the Hashed selected candidate for receiving the current total votes depending on the types of time limit and the display of the result or time which can be verified by the voters. The score of the new vote for all selected candidates will be sent as an array in transaction to voting contract. The implementation has been done on Private Network to collect the data of gas use and vote-time duration as shown in Table I.

TABLE I. GAS USE AND TIME IN VOTING (GAS PRICE= 10 GWEI)

Number of Voters	Gas Use (Units)	Time
1	128774	5s
2	113838	4s
3	83774	2s
4	83774	2s
5	113838	4s
•	•	•
•	•	•
•	•	•
50	98838	3s

The record of address data and vote data can be retrieved for verification of their accuracy and transparency in the voting process as shown in Figure 7.

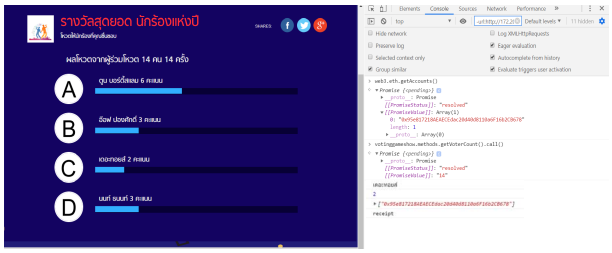

Fig. 7 Voting results and Verifiable voting results to show transparency

Proof of Work (PoW) was compared to Ganache to assess their performance by performing the total test of both systems for 50 times (from 1 time per a person). The Average test results are shown in Table II.

TABLE II. COMPARING THE PERFORMANCE: PROOF OF WORK (POW) AND GANACHE

Type of comparison	Topics		
	Average Transaction Speed (Time interval from voting to score shown instant)	*Ease of use*	*Efficiency*
Proof of Work (PoW)	4s	High	High
Ganache	3s	High	High

V. Conclusion

This research is aimed to develop the voting system for game show program using blockchain technology in order to assess the efficiency and transparency of the system by voting through the application web developed by the researchers. The research found that the vote-time duration did not exceed 5 seconds. The voters could see the real-time scores of the votes. The recorded data were consistent with the real-time data. The selected candidates were consistent with whom the voters voted for. Ganache was slightly faster in transaction sending speed than proof of work (PoW) in the order of seconds. In conclusion, the developed voting system was efficient and transparent.

References

[1] T. Anawushsiriwongse, Social imagination in media languages, Bangkok: Peace medium project, Faculty of communication atrs, chulalongkorn University, 1999.

[2] S. Khattiya and P. Nitikasetsoontorn, Creative for Television Program unit 14 chapter Television Program Development, Nonthaburi: Sukhothai Thammathirat Press, 2009.

[3] Workpoint Entertainment Public Company Limited, "Annual registration statement," 2013.

[4] "Sector Quotation," 1 May 2020. [Online]. Available: https://marketdata.set.or.th/mkt/sectorquotation.do?market=SET&sector=MEDIA&language=th&country=TH. [Accessed 1 May 2020].

[5] " TV Rating," 14 April 2019. [Online] . Available: https://www.tvdigitalwatch.com. [Accessed 1 May 2020].

[6] R. Yuttarin, " Automatic SMS Vote Counting and Summarizing System," 2013.

[7] Digital Government Development Agency (Public Organization) (DGA), Blockchain for Goverment Service (1st ed.), Bangkok Thai Tower Building 108 Rangnam Rd. Phayathai Ratchatewi Bangkok, 2019.

[8] M. Patel, "Consensus Algorithms in Blockchain," [Online]. Available: https://www.geeksforgeeks.org/consensus-algorithms-in-blockchain. [Accessed 9 September 2019].

[9] L. Ismail and H. Materwala, "A Review of Blockchain Architecture and Consensus Protocols: Use Cases, Challenges, and Solutions," Symmetry 2019, vol. 11, p. 1198, 2019.

[10] J.-H. Huh and S.-K. Kim, "The Blockchain Consensus Algorithm for Viable Management of New and Renewable Energies," Sustainability 2019, vol. 11, no. 11, p. 3184, 2019.

[11] Blockchain Technology in Online Voting, [Online] . Available: https: / / followmyvote. com/ online- voting- technology/ blockchain-technology/. [Accessed 9 September 2019].

[12] S. D. Angelis, "Assessing security and performances of consensus algorithms for permissioned blockchains," arXiv preprint arXiv:1805.03490, 2018.

[13] N. Szabo, " Formalizing and Securing Relationships on Public Networks," First Monday, vol. 2, no. 9, 1997.

[14] P. Hegedus, " Towards Analyzing the Complexity Landscape of Solidity Based Ethereum Smart Contracts," in 2018 IEEE/ ACM 1st International Workshop on Emerging Trends in Software Engineering for Blockchain (WETSEB), Gothenburg, Sweden, 2018

[15] J. Frankenfield, "Gas (Ethereum)," 22 October 2019. [Online] . Available: https://www.investopedia.com/terms/g/gas-ethereum.asp. [Accessed 25 April 2020].

[16] I. Karamitsos, M. Papadaki and N. A. Barghuthi, "Design of the Blockchain Smart Contract: A Use Case for Real Estate," Journal of Information Security, pp. 177-190, January 2018

[17] A. Leelasantitham, "A Business Model Guideline of Electricity Utility Systems Based on Blockchain Technology in Thailand: A Case Study of Consumers, Prosumers and SMEs," Wireless Personal Communications, 2020/02/13 2020, doi: 10.1007/s11277-020-07202-8.

[18] Y. Kazeem, "The world's first blockchain-supported elections just happened in Sierra Leone," 13 March 2018 . [Online]. Available: https://qz.com/africa/1227050/sierra-leone-elections-powered-by-blockchain/. [Accessed 27 October 2019].