THE CHINESE UNIVERSITY OF HONG KONG
Department of Information Engineering
1st Semester, 2017-18

IERG4998 Final Year Project I
Proposal

Supervisor: Prof. LAU, Wing Cheong
Name: WAN Kam Leung
SID: 1155068082

E-commerce Application/Platform Development using Cloud-based Blockchain-as-a-Service

Background

Voting from paper-based system to digital or electronic voting in today's world, technology has change the world in different forms. Digital voting could use different electronic devices, namely the smartphone and tablets to access the system and commit the vote. Another type of digital voting is using a special voting machine in a polling station to vote.

Blockchain is a distributed system with a continuously growing list of records, which is known as the blocks. All the blocks are linked together and hashed using cryptographic technique. It could be decentralised, doing transaction and keeping records or exchanging currency without any centralised authority. After the first distributed blockchain and digital currency bitcoin appeared in 2008 by an anonymous person or group known as Satoshi Nakamoto, people realised that blockchain could be a good tool to serve as a distributed ledger. It provides integrity, security and privacy by the design.

With the characteristic of Blockchain, it will be suitable in providing a better performance in digital voting, comparing with the existing technique.

Description of Problem

When doing the digital voting, it has a serious problem in recognising the voter's' identity, as it is hard to identify the voters without collecting their personal information. In a normal voting we all need to provide our personal information such as ID number, name, date of birth. In this way, the information will be kept by another party and the system.

However, if the system keeps the information of the voters, the voting is traceable. The centralised authority could use the data to trace back the whole voting, the impartiality could not be ensured. Furthermore, if the authority has conflict of interest, we will usually find a 3rd party authority to hold the vote. For example in elections, the government will hire a 3rd party company to do the election work.

Although hiring an external party can fix the problem, when things moved into the digital world, it is hard to prove that the external authority is trustworthy and the vote is untraceable. Thus, to achieve an untraceable digital voting, we need to use other method.

Methodology

In the system design, the application will try to fulfil 4 goals (Lynn, n.d.):
1. Correctness
2. Verifiability
3. User Anonymity
4. Receipt-freeness

To achieve the goals, the design of application must contain a cryptographic technique, for example the blind signature. Blind signature is a type of digital signature which will blind the content of the message when it is being signed (Goldwasser and Bellare, 2008). We will study different cryptographic technique namely blind signatures (i.e. RSA), cryptographic counters and mix nets, we will also use a suitable cryptography to design a secure and anonymity voting system.

In the core part, a Blockchain system will be built to provide the place for voting and keep all the record inside the blockchain. This project will also study different type of blockchain (i.e. public blockchain) and use the suitable one for the application. All the voting records will be stored in the blockchain.

The application will be running on iOS and Android platforms, for different smart devices.

Testing

The application will be running on an existing blockchain platform (i.e. Ethereum), and it will be using the test network (Ethereum.org, 2017) as the testing environment.

The test will be using the application to vote in different situations: the normal voting and the voting with error. The error will include double vote, invalid voter and other abnormal situations. It will go through the whole process, namely the registration, login, logout, voting and confirmation.

In addition, we will also test the application in different platforms and devices for getting a better result in universality.

References

Ethereum.org. (2017). Ethereum Project. [online] Available at: https://ethereum.org [Accessed 6 Oct. 2017].

Goldwasser, S. and Bellare, M. (2008). Lecture Notes on Cryptography. [online] Available at: http://cseweb.ucsd.edu/~mihir/papers/gb.pdf [Accessed 14 Oct. 2017].

Lynn, B. (n.d.). Electronic Voting. [online] Cryptography. Available at: https://crypto.stanford.edu/pbc/notes/crypto/voting.html [Accessed 6 Oct. 2017].

B. Schneier, Applied Cryptography: Protocols, Algorithms and Source Code in C, 2nd ed. [s.l.]: John Wiley & Sons Inc, 2015.