MULTI-KEY HOMOMORPHIC ENCRYPTION BASED BLOCKCHAIN VOTING SYSTEM

Racco Wang
School of Information Science and Technology
Beijing University
of Chemical Technology
, Beijing Chaoyang
Raccotech@gmail.com

April 10, 2020

ABSTRACT

During the pandemic covid-19. More than 70 national elections scheduled for the rest of the year worldwide, the coronavirus (COVID-19) pandemic is putting into question whether some of these elections will happen on time or at all. We proposed a novel solution based on multi-key homomorphic encryption and blockchain technology, which is unhackable,privacy-preserving and decentralized. We first introduce the importance of a feasible voting system in this special era, then we demonstrated how we construct the system. finally, we made a thorough comparison of the possible solutions.

***K*eywords** Homomorphic Encryption · Blockchain · Voting System · covid-19

1 Introduction

With more than 70 national elections scheduled for the rest of year worldwide, the coronavirus (COVID-19) pandemic is putting into question whether some of these elections will happen on time or at all. The rapidly evolving situation has generated severe disruptions on multiple layers of society, with important impact on the political life, placing world leaders in the position of making rapid critical decisions based on information that emerges by the hour. Depending on the degree of disruptions generated by the COVID-19, organizing elections can be very difficult or even impossible. For example, the production and distribution of ballot papers, voting booths, seals and other supplies needed during the process can be seriously affected by the measures imposed for limiting the spread of the virus. Furthermore, there isahighlikelihood thatpoll workers mayfear infection or get infectedand thereforenot assume their critical roles.[1]
Therefore, it is important to propose a feasible solution for the elections. We proposed a decentralized Multi-Key Fully Homomorphic Encryption based Blockchain Voting System solution that is able to keep away hacker attacks, but also preserve self voting information.

2 Back Groud

2.1 MKHE

Homomorphic encryption is a form of encryption with an additional evaluation capability for computing over encrypted data without access to the secret key. The result of such a computation remains encrypted. Homomorphic encryption can be viewed as an extension of either symmetric-key or public-key cryptography. Homomorphic refers to homomorphism in algebra: the encryption and decryption functions can be thought of as homomorphisms between plaintext and ciphertext spaces.

Homomorphic encryption includes multiple types of encryption schemes that can perform different classes of computations over encrypted data.[1] Some common types of homomorphic encryption are partially homomorphic, somewhat

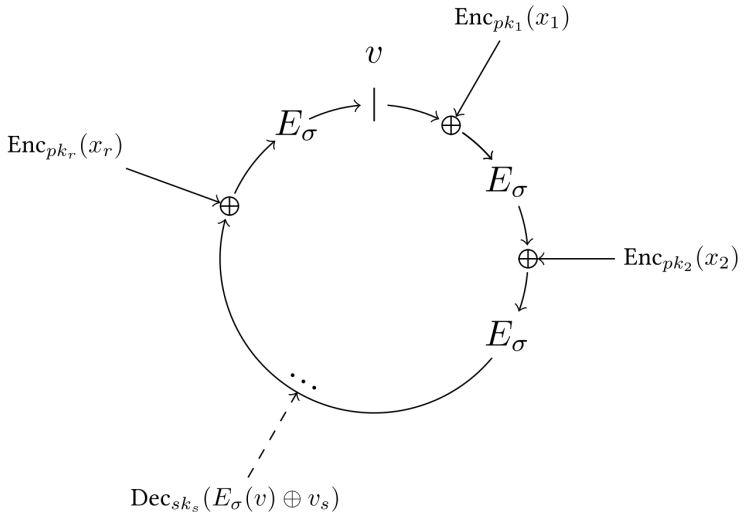

Figure 1: Homomorphic Encryption

homomorphic, leveled fully homomorphic, and fully homomorphic encryption. The computations are represented as either Boolean or arithmetic circuits. Partially homomorphic encryption encompasses schemes that support the evaluation of circuits consisting of only one type of gate, e.g., addition or multiplication. Somewhat homomorphic encryption schemes can evaluate two types of gates, but only for a subset of circuits. Leveled fully homomorphic encryption supports the evaluation of arbitrary circuits of bounded (pre-determined) depth. Fully homomorphic encryption (FHE) allows the evaluation of arbitrary circuits of unbounded depth, and is the strongest notion of homomorphic encryption. For the majority of homomorphic encryption schemes, the multiplicative depth of circuits is the main practical limitation in performing computations over encrypted data.

Homomorphic encryption schemes are inherently malleable. In terms of malleability, homomorphic encryption schemes have weaker security properties than non-homomorphic schemes.[2]

And Multi-Key Homomorphic Encryption (MKHE), which is capable of performing arithmetic operations on ciphertexts encrypted under different keys. When the ciphertexts involved have been changed into ciphertext encrypting the same message under all keys, it is possible to perform homomorphic operations on them. In the multi-key FHE setting we have N participants with their own keypair (sk_i, pk_i), and message m_i , who want to perform computations on all data without revealing any private information to each other. After the computation decryption should only be possible when all the secret keys that were used to encrypt the messages are involved.[3]

2.2 Blockchain

A blockchain, originally block chain, is a growing list of records, called blocks, that are linked using cryptography. Each block contains a cryptographic hash of the previous block, a timestamp, and transaction data (generally represented as a Merkle tree).

By design, a blockchain is resistant to modification of the data. It is "an open, distributed ledger that can record transactions between two parties efficiently and in a verifiable and permanent way". For use as a distributed ledger, a blockchain is typically managed by a peer-to-peer network collectively adhering to a protocol for inter-node communication and validating new blocks. Once recorded, the data in any given block cannot be altered retroactively without alteration of all subsequent blocks, which requires consensus of the network majority. Although blockchain records are not unalterable, blockchains may be considered secure by design and exemplify a distributed computing system with high Byzantine fault tolerance. Decentralized consensus has therefore been claimed with a blockchain.

Blockchain was invented by a person (or group of people) using the name Satoshi Nakamoto in 2008 to serve as the public transaction ledger of the cryptocurrency bitcoin. The identity of Satoshi Nakamoto is unknown. The invention of the blockchain for bitcoin made it the first digital currency to solve the double-spending problem without the need of a trusted authority or central server. The bitcoin design has inspired other applications, and blockchains that are readable by the public are widely used by cryptocurrencies. Blockchain is considered a type of payment rail. Private blockchains

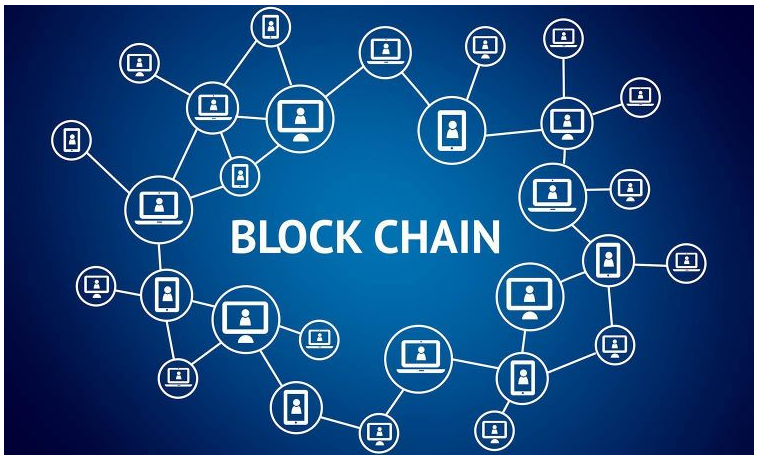

Figure 2: Blockchain

have been proposed for business use. Sources such as Computerworld called the marketing of such blockchains without a proper security model "snake oil".

Blockchain is a shared, immutable ledger that facilitates the process of recording transactions and tracking assets in a business network. An asset can be tangible (a house, a car, cash, land) or intangible (intellectual property, patents, copyrights, branding). Virtually anything of value can be tracked and traded on a blockchain network, reducing risk and cutting costs for all involved.

No participant can change or tamper with a transaction after it's been recorded to the shared ledger. If a transaction record includes an error, a new transaction must be added to reverse the error, and both transactions are then visible.[4]

3 System Description

The Multi-Key Homomorphic Encryption based Blockchain Voting System works as follows: each voter generates a pair of private-key(secrete-key) and cloud-key(public-key) locally. Then use blockchain technology to send his information to the internet to create a block. This information includes unencrypted identification information and encrypted voting information. everybody can check whether their information on the blockchain(C-chain) is the same with their local data. So, they could reconfirm their votings to make hacking nonsense. During the construction of this blockchain(C-chain), all the private key was used to construct another blockchain(P-chian) without order. Because there exists $n!$ possible orders, it is impossible to find out the right order to decipher the encrypted voting information on the other blockchain(C-chain).

Once both the two chains completed. We could do evaluations on the encrypted voting information from the C-chain with the private-keys on the P-chain. As all this are decentralized, everybody could do the counting.

4 Key Properties

4.1 Credibility(Unhackable)

Blockchain technology accounts for the issues of security and trust in several ways. First, new blocks are always stored linearly and chronologically. That is, they are always added to the "end" of the blockchain. If you take a look at Bitcoin's blockchain, you'll see that each block has a position on the chain, called a "height." As of January 2020, the block's height had topped 615,400.

After a block has been added to the end of the blockchain, it is very difficult to go back and alter the contents of the block. That's because each block contains its own hash, along with the hash of the block before it. Hash codes are created by a math function that turns digital information into a string of numbers and letters. If that information is edited in any way, the hash code changes as well.

Here's why that's important to security. Let's say a hacker attempts to edit your transaction from Amazon so that you actually have to pay for your purchase twice. As soon as they edit the dollar amount of your transaction, the block's hash will change. The next block in the chain will still contain the old hash, and the hacker would need to update that block in order to cover their tracks. However, doing so would change that block's hash. And the next, and so on.

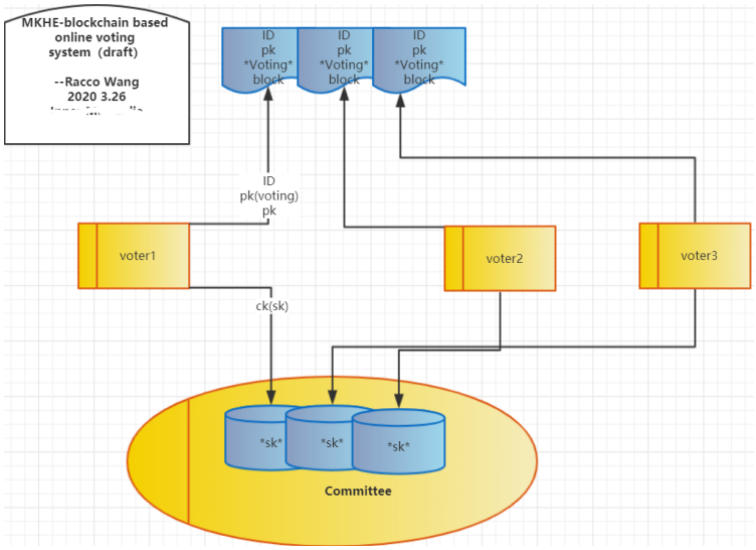

Figure 3: Multi-Key Homomorphic Encryption based Blockchain Voting System

In order to change a single block, then, a hacker would need to change every single block after it on the blockchain. Recalculating all those hashes would take an enormous and improbable amount of computing power. In other words, once a block is added to the blockchain it becomes very difficult to edit and impossible to delete.
To address the issue of trust, blockchain networks have implemented tests for computers that want to join and add blocks to the chain. The tests, called "consensus models," require users to "prove" themselves before they can participate in a blockchain network. One of the most common examples employed by Bitcoin is called "proof of work."
In the proof of work system, computers must "prove" that they have done "work" by solving a complex computational math problem. If a computer solves one of these problems, they become eligible to add a block to the blockchain. But the process of adding blocks to the blockchain, what the cryptocurrency world calls "mining," is not easy. In fact, the odds of solving one of these problems on the Bitcoin network were about one in 15.5 trillion in January 2020.1 To solve complex math problems at those odds, computers must run programs that cost them significant amounts of power and energy (read: money).
Proof of work does not make attacks by hackers impossible, but it does make them somewhat useless. If a hacker wanted to coordinate an attack on the blockchain, they would need to control more than 50% of all computing power on the blockchain so as to be able to overwhelm all other participants in the network. Given the tremendous size of the Bitcoin blockchain, a so-called 51% attack is almost certainly not worth the effort and more than likely impossible.[6]

4.2 Privacy Preserving

While traditional encryption schemes can be used to privately outsource data storage to the cloud, the data cannot be used for computations without first decrypting it. This results in a huge loss of utility. For example, a secure cloud service may require a user to download their encrypted data, decrypt it locally, and perform necessary computations, instead of simply returning an encrypted result to the user.

Homomorphic encryption solves this problem, as it allows the cloud service to perform the computations while protecting the customer's data with a state-of-the-art cryptographic security guarantee. The cloud only ever sees encrypted data, and only the customer can reveal the result of the computation.

4.3 decentralized ballot counting

Everybody could counting the ballots. So the result would be acceptable to every voter.

5 comparison

5.1 In-person Voting

At their best, democraticelections are characterised by high turnout and equal levels of participation across different segments in a societyto avoidthattheoutcome of an electionisunevenly shaped by some groups over others. There is a risk that the decision of continuing to hold an election as originally scheduled, despite pandemic outbreak, could undermine their overall legitimacy by reducing voter turnout. Yet with the need for limited exposure to large groups and social distancing, ccitizens might be less likely to leave their homes to vote because of their health concerns and that of their family members.
There is also a major risk that those deterred from voting would be disproportionately from the older age groupsorthose with underlying health conditions. The legitimacy of the contest may therefore be undermined by unfair restrictions placed on certain segments of the society and thus by their uneven participation.

5.2 Vote-by-Mail

5.2.1 Possible Advantages

Voter convenience and satisfaction—Citizens can vote at home and take all the time they need to study the issues. Voters often express enthusiasm for all-mail elections. Financial savings—Jurisdictions may save money because they no longer need to staff traditional polling places with poll workers and equip each polling place with voting machines. A 2016 study of Colorado from the Pew Charitable Trusts found that costs decreased an average of 40 percent in five election administration categories across 46 of Colorado's 64 counties (those with available cost data). However, the study examines a number of reforms that Colorado enacted in 2013, with all-mail elections being the most significant. Others included instituting same day registration and shortening the time length for residency in the state for voting purposes. Turnout—Some reports indicate that because of convenience, voter turnout increases. These reports assert that turnout increases by single digits for presidential elections and more in smaller elections. See this 2013 report on all-mail ballot elections in Washington and this 2018 report on all-mail ballot elections in Utah. Effects on turnout can be more pronounced for low propensity voters, those that are registered but do not vote as frequently.

5.2.2 Possible Disadvantages

Tradition—The civic experience of voting with neighbors at a local school, church, or other polling place no longer exists. Disparate effect on some populations—Mail delivery is not uniform across the nation. Native Americans on reservations may in particular have difficulty with all-mail elections. Many do not have street addresses, and their P.O. boxes may be shared. Literacy can be an issue for some voters, as well. Election materials are often written at a college level. (Literacy can be a problem for voters at traditional polling place locations too.) One way to mitigate this is to examine how voter centers are distributed throughout counties to best serve the population. Security—During all-mail elections (and absentee voting), coercion by family members or others might occur. Financial considerations—All-mail elections greatly increase printing costs for an election. Additionally, jurisdictions must have appropriate equipment to read paper ballots at a central location, and changing from electronic equipment to equipment that can scan paper ballots can be expensive. Slow vote counting—All-mail elections may slow down the vote counting process, especially if a state's policy is to allow ballots postmarked by Election Day to be received and counted in the days and weeks after the election.[5]

5.3 Multi-Key Homomorphic Encryption based Blockchain Voting System

6 Implementation Details

For fast development we used MKTFHE[7]for the Multi-Key Homomorphic Encryption part and Ethereum[8] for the blockchain part.

7 Conclusion

We proposed a novel and robust solution for election votings during Covid-19, which is unhackable ,privacy-preserving and decentralized.
Hope to help the people in the world to have a safe election.

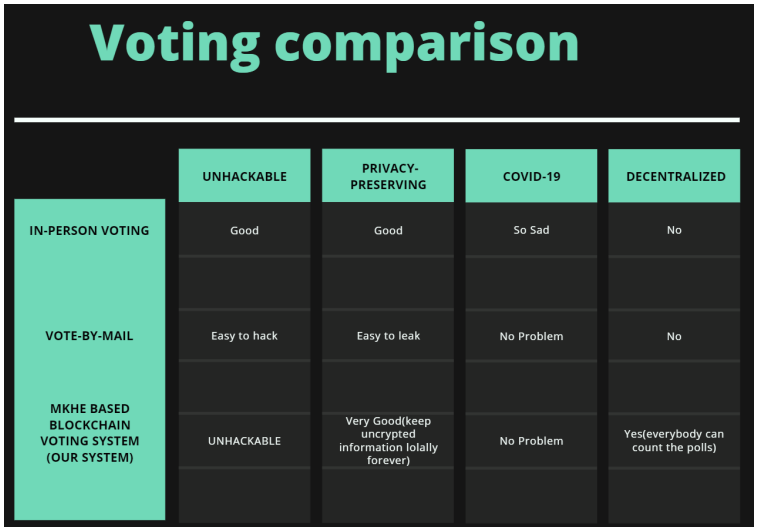

Figure 4: Comparison

References

[1] Elections during COVID-19: Considerations on how to proceed with caution https://www.idea.int/news-media/news/elections-during-covid-19-considerations-how-proceed-caution

[2] J. H. Cheon, K. Han, A. Kim, M. Kim, and Y. Song. Bootstrapping for approximate homomorphic encryption. In Annual International Conference on the Theory and Applications of Cryptographic Techniques, pages 360–384. Springer, 2018.

[3] Multi-key fully homomorphic encryption report Elena Fuentes Bongenaar

[4] Iansiti, Marco; Lakhani, Karim R. (January 2017). "The Truth About Blockchain". Harvard Business Review. Harvard University. Archived from the original on 18 January 2017. Retrieved 17 January 2017. The technology at the heart of bitcoin and other virtual currencies, blockchain is an open, distributed ledger that can record transactions between two parties efficiently and in a verifiable and permanent way."

[5] https://www.ncsl.org/research/elections-and-campaigns/all-mail-elections.aspx

[6] https://www.idea.int/news-media/news/elections-during-covid-19-considerations-how-proceed-caution

[7] Multi-Key Homomophic Encryption from TFHE
Hao Chen , Ilaria Chillotti , and Yongsoo Song

[8] https://ethereum.org/zh/

[9] Z. Brakerski and R. Perlman. Lattice-based fully dynamic multi-key fhe with short ciphertexts. In Annual Cryptology Conference, pages 190–213. Springer, 2016.