Blockchain-Based Election Infrastructures

Rafer Cooley
Computer Science Department
University of Wyoming
Laramie, Wyoming
rcooley2@uwyo.edu

Shaya Wolf
Computer Science Department
University of Wyoming
Laramie, Wyoming
swolf4@uwyo.edu

Mike Borowczak
Computer Science Department
University of Wyoming
Laramie, Wyoming
mike.borowczak@uwyo.edu

***Abstract*—Students at the University of Wyoming designed two blockchain-based voting systems during a class offered only once at the University. The first system (re-use) branched Ethereum to leverage its security and privacy benefits. The second system (re-invent) created a new blockchain voting system which used two separate chains, one for validating voters and another for securing votes. This research looked at the benefits and flaws of current election systems as well as benefits a nd fl aws of blockchain technology to improve upon the current election infrastructure. These systems aim to provide integrity, privacy and security to its users. Further, they strive to be fault-tolerant. Finally, these systems could be extended to mobile voting platforms and smart contracts. Based on current decentralized services, this research demonstrates a proof-of-concept that elections could benefit from blockchain-based systems. These types of systems would be ideal in smart cities to ensure the reliability of the voting procedure.**

INTRODUCTION

Smart cities empower citizens by bringing distributed computing capabilities to various services through Internet of Things (IoT) devices. City administrations benefit t heir constituents with smart services through cyber-physical systems that allow for smarter ecosystems, faster emergency response times, and more reliable and comprehensive sensor networks. To leverage these advances, cyber-physical systems require computational power. Researchers further these strides by improving cloud/edge computing to allow for a more seamless interaction between devices and servers. As a result, smart city designs and implementations can evolve to fit emerging necessities [2]. This means new systems and improvements that better serve smart city citizens. Current voting systems and methods contain many avenues for potential improvements. Lacking security and transparency, current voting systems are not fault-tolerant and voter information is vulnerable to security leaks.

To improve upon current methods and systems, a proof-of-concept was designed for a blockchain voting system. Blockchains are distributed ledgers where participants keep and agree on a history of transactions. Cryptocurrencies leverage blockchain technology to create currencies that are secure, fault-tolerant, and transparent. In the same way, blockchain technology can be leveraged to create voting systems that ensure integrity, security, and voter privacy. This work takes two approaches to creating a blockchain-based voting system. The first a pproach u tilizes (re-uses) e xisting t echnology t o create a voting system branched from Ethereum. This leverages the same benefits from existing blockchain models and seamlessly brings those benefits to a voting system. Second, a blockchain voting system was created (re-invented) from scratch. By re-inventing a new blockchain, the system is tailored to exact preferences. Finally, local voting officials contributed insight into what current voting systems provide for their constituents and these benefits were maintained in each of the voting systems.

978-1-5386-5959-5/18/$31.00 © 2018 IEEE

BLOCKCHAIN VOTING SERVICES

In its most basic form. voting enables civilians to induce change in their government. This staple of democracy allows for efficient checks and balances to be afforded to citizens in order to maintain a government for the people. Voting extends beyond civics and into corporate board rooms and investor meetings. Future smart devices may even vote to decide in ethical dilemmas involving human-autonomous machine interactions. In smart cities, this system ought to be as seamless and efficient as possible to eliminate barriers preventing citizens from voting. Many elections taking place around the world today are systematically flawed, where the distributed populous must trust a single central authority in order to collect, count, and validate votes. In many cases these central agencies struggle to provide the integrity and security necessary to ensure a reliable election infrastructure and succumb to fraud and errors. Blockchain-based voting systems allow for reliable systems that do not require trust between any of the parties. The distribution of a common shared ledger, or record of votes, between hundreds or thousands of parties allows for the people to truly be in charge of their elections. The integrity, security and privacy offered by a blockchain creates many opportunities to change the way we think about voting standards [7]. With these goals in mind, two voting mechanisms were created that improve on our current centralized voting system. This work focuses on two different methods of developing a voting systems, the first system was created by the ”Re-use” team and the second system created by the ”Re-invent” team.

DECENTRALIZED SERVICES

Many cities currently utilize systems of blind trust where citizens trade the responsibility of maintaining and securing their data for very little peace of mind. In centralized services, one security breach impacts everyone who is using that service. Centralized data storage allows for an easier and

more profitable attack vector on consumer data. In contrast, decentralizing data spreads an attackers focus and makes a successful data breach less lucrative [3]. Take for example a situation where Alice and Bob want to exchange goods, but they do not trust each other. Normally, this problem is solved by introducing a third party that both Alice and Bob have to trust. However, the selection of the central third party should not be taken lightly. This third party now has access to the goods coming from both sides and stands to profit double what either Alice or Bob stand to gain. Likewise in any centralized system, the central agency creates a hub that allows for parties to do business, but also gathers all of the commodities into one convenient place for attackers.

Likewise, current voting systems rely on central election agencies to facilitate the voting process and tally the votes. This requires a lot of trust from the constituents and the central agencies experience security vulnerabilities. In our voting systems, we improve on these centralized systems with a decentralized service. By decentralizing voting services, voters are not required to trust a central election agency. Because each voting machine holds a copy of the voting ledger, and everyone agrees on the contents of the ledger, votes are not swayed by third party interests. Ethereum, one of the largest and most successful cryptocurrencies, brings the same benefits to participants through a distributed ledger. By branching Ethereum, the re-use voting mechanism leverages decentralized services by maintaining the same distributed ledger. The re-invent voting mechanism mirrors this type of decentralized service, but instead implements a custom solution to achieve this goal. Each voting machine was set up with access to the chain and stored a copy of the ledger. Each machine maintained consensus between itself and all of the other voting machines. This allowed for votes to be recorded and counted while ensuring agreement on the count. Each of these systems leverages the benefits from decentralized services without requiring trust from voters.

Smart cities enable citizens with high levels of connectivity and strive for smart ways to carry out business. Elections in a smart city would ideally be distributed, such that no single agency can effect the vote. By distributing the vote, there is less chance for corruption and constituents can have more faith in a reliable system. An additional benefit of digital voting procedures is the new capability to increase the number of voting cycles, where municipal codes and policies can be voted on as they arise instead of batching the issues into one or two elections per year.

INTEGRITY

Valid election infrastructures require a reliable and trustworthy system in order to provide the level of trustworthiness that is demanded by voters. To implement such a system, it is necessary to have a system with integrity where only authorized actions are allowed. Blockchain technology provides a decentralized system built on credible authentication. Since everyone on the chain has a copy of the ledger, everyone can detect a fraudulent action. This provides an ideal basis for a secure election protocol [5]. Elections necessitate this level of integrity and smart cities can leverage blockchain technology to provide their citizens with a voting system they can rely on. In our re-use system, we ensure the same level of integrity as Ethereum ensures its users. By using a trusted and proven blockchain, the re-use mechanism provides a great deal of integrity which ensures credible authentication through the same modified proof-of-stake measures that Ethereum uses. Further, it provides a reliable service by ensuring only verified voters can cast a legitimate vote. API calls facilitate passing information from the user to the chain. The chain requires a voter identification number to validate a voter with an approved voter database and only provides a legitimate voter with their appropriate voting information.

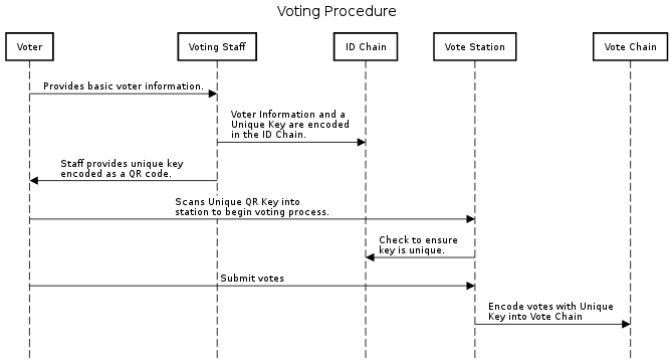

Fig. 1. The voting procedure followed by the Re-invent system.

The re-invent system utilizes two separate blockchains, one for voter identification and one to hold the actual votes. The votes are held on a separate chain than the voter information to treat vote authentication separately from voter authentication and make appropriate design decisions for each part. Since the validation mechanisms are separate, the blockchains can be tailored to handle authorizations appropriately in each situation. Voters would be given an ID from an election official at the time of voting. Then, using this ID, they complete their ballot on a dedicated voting machine. To validate that a voter is legitimate, they must use their voter ID to access the ballot and to cast a vote. This prevents votes from being cast that are not associated with a specific voter and prevents any voter from placing more than one vote. Additionally, votes are required to hold the associated voter ID and for the vote to be validated and added to the ledger, that voter ID cannot be associated with any other votes already on the chain. The voting procedure can be seen in Figure 1. This maintains the integrity of the system and improves upon the reliability of the current system.

Smart cities benefit from being in touch with new technology. Blockchain technology offers smart cities a way to ensure integrity and reliability in their election infrastructure. It is difficult to trust a person or organization, however, these systems only require trust in the math and code. This is not a blind trust either. With blockchain technology, smart cities could implement an open-source voting system, where anyone could look up and see how the math and code works. By being

transparent on how the procedure operates, and because this procedure does not require the trust of a third party, civilians can rely on the voting system and be confident in the accuracy of the outcome.

SECURITY

Growing in popularity, blockchain voting systems ensure a secure e-voting platform that utilizes an immutable ledger [4]. By ensuring privacy and protecting against voter fraud, blockchain technology offers a lot for online voting systems that require transparency. Additionally, blockchains are difficult to hack as well as easy to audit. This allows for a more open voting system that civilians can feel confident using. More importantly, blockchain voting systems surpass current voting systems that lack transparency and security. The re-use voting system guarantees a secure platform by implementing protections against voter fraud like validating voters and auditing the vote chain. Further, it allows for transparency throughout the vote, allowing constituents to watch an election unfold in real time.

The re-invent system utilizes separate chains for voter identification and ballot information to anonymously store the vote and secure the identity of the voter. Further, no voter can vote more than once since the voter identifications are also kept on a auditable chain. The id is validated as well as the vote. This system uses ring signatures which allow for blocks to be signed by an individual in a group and for the identity of the signer to be anonymous, adding security to the system while still giving a valid paper trail. Additionally, both of these systems are a drastic improvement over current voting systems that are provably hackable and vulnerable to voter fraud. Because all of the polling stations hold a copy of the vote history, it is difficult to dispute the results of an election. A hacker would not need to hack into one system, but would have to successfully hack 51% of the voting systems to effect the chain, at which point a hacker has very little hope of being undetected.

Smart cities already handle large security concerns. When everyone is connected, vulnerabilities are easily shared. This can span not only users, but platforms as well. These issues are addressed in these voting systems by leveraging distributed systems and transparent blockchain implementations. Election security is currently lacking in voting systems that we implement today, but a blockchain-based system would secure smart city constituents identities as well as their votes.

PRIVACY

Blockchain technology thrives on the promise of privacy. Due to their strength against hackers, blockchain systems ensure the safety of the users data from tampering. Additionally, added security measures allow a system to provide privacy and anonymity for a user [8]. Voting systems demand a high level of anonymity to prevent bribes and extortion. Auditability frequently trades off with anonymity. How can a system keep users anonymous while still verifying each persons vote? The perfect voting system allows a user to see who they voted for, but does not allow them to see anyone else's vote. Blockchain technology provides for both within reason. In the re-use voting system, we were able to guarantee privacy by using hashes of voter ids to validate a voter and secure their vote anonymously. By doing this, we both validate their vote as well as ensure their privacy. Because this system uses hashes of the voter id, it is easy to see that a person voted, but not as trivial to see who they voted for. Instead, the system shows who each hash voted for.

In the re-invent mechanism, privacy was not as straight forward since it trades off with auditability. Because this system ensures security and reliability, the opportunity to show a receipt of a person's vote becomes feasible. After voting, a constituent could potentially see who they voted for. This increases the reliability and security of the chain since it is then auditable by any voter. However, showing a voter who they voted for after the fact poses a risk for privacy and opens the door to bribes and extortion. If anyone can look back on the chain and see who they voted for, the chain becomes simple to audit but also compromises the integrity of the vote, since a voter could then prove they voted for a specific person. Therefore, the re-invent system allows for a user to see that they voted and that their block was successfully added to the chain, but it does not allow anyone to see the contents of a vote. We do this by encrypting the vote as well as hashing the users voter ID. This prioritizes privacy over auditability, but maintains the integrity of the election procedure.

Privacy is not always maintained in many cities. However, in smart cities, privacy can be maintained during an election. This is vital in preserving the democratic ideals of a vote and ensuring the means by which we elect officials. By maintaining privacy, smart cities allow for large connectivity without fear of adversarial turmoil.

FAULT TOLERANCE

Blockchain technology offers recovery mechanisms in the case there are issues. For this reason, many blockchain applications are being implemented in other domains, most notably in the medical field. Systems used in this field must be able to reach a consensus. In other words, everyone must agree on what is accurate. By reaching consensus, all participants understand and agree on the collected data. The main concern in many systems is Byzantine fault-tolerance. A Byzantine fault is a discrepancy in the data that presents itself differently to different users. Discrepancies that appear diversely make it nearly impossible to reach a consensus. Therefore, many blockchain application seek to avoid these faults. Blockchain lends itself quite well to practical fault tolerance and many systems in medicine have seen good results with fault-tolerance applications [9]. In our systems, we strive for fault tolerance. This brings forward an opportunity to fix an incorrect vote. This however, brings us back to the trade-off between auditability and privacy.

It would be possible in either mechanism to correct a vote, however, to do so in either system means compromising the identity of a voter. Although we are not improving on the

current system in this way, we are maintaining privacy and integrity. Further, both systems still allow for a high level of fault tolerance. If there is an issue with some of the polling machines, the system continues to run without compromising the election process. This allows for technical issues and unforeseen difficulties to occur without damaging the voting procedure and thereby heightens the integrity of the vote. Further, since all of the nodes have a copy of the voting history, votes cannot be lost or tampered. Due to the higher levels of security and integrity, the auditability of the chain becomes less important. Due to the soundness of the system, the chance that one would need to audit the chain resolves to being very slim. Also, we allow users to double and triple check their vote before it is submitted to the chain, lowering the likelihood that a vote would be cast incorrectly.

Since smart cities leverage many new technological advances, issues with implementing these fresh system are likely as people start to learn new ways of completing tasks. However, much of the new technology being implemented in smart cities tolerates issues. In a voting system, this means that an election cannot be compromised easily and that issues that arise during the election do not effect the outcome.

Mobile Voting

Technology advances allow us to be more connected then ever. In smart cities, individuals maximize their technology. Not only do we strive to connect with each other, but we want connectivity amongst our IoT devices. This creates cyber-physical systems that connect us with the world. Blockchain technology allows us to create order in cyber-physical systems. Built on fault tolerance, consensus, and information sharing, distributed ledgers enable users to reliably and transparently connect all of their devices [6]. Cyber-physical systems boost the functionality of smart cities, allowing for user to not only connect their own devices, but also connect with other people.

In a voting system, this raises the question of mobile voting. Is it feasible to think someone could securely vote from their phone? We found that we could very feasibly allow this. Using our re-invent system, we created multiple front ends that could serve as voting platforms. This allows for flexibility in how users can cast their vote and would even allow for troops oversees to vote anonymously. By allowing for mobile voting, voter turnout can be improved as well as alleviating common problems constituents have with voting such long lines and having to take time off of work. Mobile voting does however have its drawbacks. Using dedicated voting machines and limiting approved maintenance personnel ensures more control over the system. A mobile voting app would require a system for secure downloading as well as secure networking. In the re-invent system, networking was done through peer discovery. This could be extended to mobile devices, but would require higher levels of security.

Smart Contracts

The systems implemented place a lot of trust in the individuals who set up the voting booths. Node creation is crucial to maintain a viable system. This reintroduces trust into the system that was designed to be trustless. In future iterations of this work, smart contracts may be able to solve this problem. Smart contracts are autonomous functions that carry out transactions on the blockchain [1]. A variation of these functions, a smart contract that adds a new node with the permission from the majority of the chain, could remove the security threat in the current systems. This could enable mobile voting as well as ensure that the there is minimal control over the vote from a central voting agency.

Conclusion

Smart cities connect people by leveraging cloud/edge computing capabilities in IoT devices to provide smarter services to its civilians. Through research of current voting systems, we find that these primitive systems can be improved to better fit into the smart city scheme. Election infrastructures should be reliable, secure, private, and fault tolerant. Without these corner stones, we cannot provide the system integrity that constituents expect. With a distributed system however, we can continue to leverage emerging technologies to improve aged election systems. Through blockchain-based voting systems, we can better serve voters with more legitimate elections.

We created two different voting systems. The first branched Ethereum and leveraged that technology to create a reliable election system. This system provides security and privacy and sticks with the same blockchain standards that are currently flourishing in cryptocurrencies. Our second system was built from the ground up. This system strives to balance auditability and privacy. This system also opens the door to mobile voting platforms powered by smart contracts. With the main goal of improving the current system, we were able to research the current system and create new decentralized systems that are more secure and provide a more viable election infrastructure.

References

[1] K. Christidis and M. Devetsikiotis. Blockchains and smart contracts for the internet of things. *IEEE Access*, 4:2292–2303, 2016.

[2] Franco Cicirelli, Antonio Guerrieri, Giandomenico Spezzano, and Andrea Vinci. An edge-based platform for dynamic smart city applications. *Future Generation Computer Systems*, 76:106 – 118, 2017.

[3] Jan Thomas Frec and Thomas Selzam. Tokenized ecosystem of personal data exemplified on the context of the smart city. *JeDEM - eJournal of eDemocracy and Open Government*, 9(2):110–133, 2017.

[4] Darin Stanchfield. Blockchain technology can make voting systems more secure, Nov 07 2016. Copyright - Copyright Networld Media Group DBA Networld Alliance, LLC Nov 7, 2016; Last updated - 2016-11-08.

[5] Jianjun Sun, Jiaqi Yan, and Kem Z. K. Zhang. Blockchain-based sharing services: What blockchain technology can contribute to smart cities. *Financial Innovation*, 2(1):26, Dec 2016.

[6] van Lier Ben. Can cyber-physical systems reliably collaborate within a blockchain? *Metaphilosophy*, 48(5):698–711.

[7] Baocheng Wang, Jiawei Sun, Yunhua He, Dandan Pang, and Ningxiao Lu. Large-scale election based on blockchain. *Procedia Computer Science*, 129:234 – 237, 2018. 2017 International Conference on Identification, Information, and Knowledge in the Internet of Things.

[8] J. Wang, M. Li, Y. He, H. Li, K. Xiao, and C. Wang. A blockchain based privacy-preserving incentive mechanism in crowdsensing applications. *IEEE Access*, 6:17545–17556, 2018.

[9] Lijing Zhou, Licheng Wang, and Yiru Sun. Mistore: a blockchain-based medical insurance storage system. *Journal of Medical Systems*, 42(8):149, Jul 2018.