

Voteproject: Smart Democracy
A Blockchain Voting System Proof of Concept

By

Jennifer Gale Carson

A Project
Presented to the Faculty of
The Department of Computer Science

In partial fulfillment
Of the requirements for the degree
Master of Science

Huntsville, Texas

December 1, 2017



Terms of use: Voteproject including this work and related code is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License, by Jennifer Gale Carson, Eduardo de Luna, Dr. Umit Karabiyik, Dr. Li Jen Lester, Dr. Hyuk Cho, Sam Houston State University, and the original version and code repository is found [here](#).

Table of Contents

1. Dedication	4
2. Abstract	5
3. Introduction	6
3.1 Status Quo	6
4. Related Work	8
4.1 Bitcoin	8
4.2 “Electronic Voting Service using BlockChain”	10
4.3 Follow-My-Vote	10
5. Background	11
5.1 Voting Process: United States	11
5.2 Blockchain	13
5.2.1 Transactions	13
5.2.2 Timestamp Server	14
5.2.3 Merkle Tree	15
5.2.4 Security	16
6. Proposed Model	17
6.1 VoteProject: Smart Democracy	17
6.2 Pseudo-centralized	17
6.3 Design	18
6.3.1 Blockchain Network: Multichain	20
6.3.2 Client Program: Voteproject.py	22
6.3.3 Authentication Server	24
7. Proof of Concept	28
7.1 Connections	28
7.2 Main Program Execution	30
7.3 Results and Confirmation	31
8. Future Work	32
9. Conclusion	33
9.1 Legal and Political Limitations	33
9.2 Security Concerns	33

9.2.1 Double Spending	33
9.2.2 The 51% Attack	34
9.3 Practical Applications	35
9.3.1 Vote Reconsideration & Real Time Data	35
9.3.2 Providing Financial and Technical Mining Incentives	36
9.3.3 Democracy in a box	36
9.4 Closure	36
10. Table Of Figures	37
11. Bibliography	39

1. Dedication

To my graduate project committee and Dr. Karabiyik for your unending patience, understanding, and belief in me. You reminded me becoming a master is more than producing a final result but the experiences gathered along the journey.

To my family for supporting me through the trials of young adult life.

To my good friend Eduardo de Luna, you are a genius.

2. Abstract

In recent years, blockchains have gained popularity for transaction management beyond financial transactions. The rise of blockchain technology is pushing contemporary boundaries and has the capability to revolutionize many of our social and business processes. While verifying transactions across publically a decentralized network, blockchains can maintain user anonymity. These attributes make blockchain technology a perfect platform for transacting democratic elections. This paper focuses on the technical feasibility and potential advantages of blockchain voting systems. As well as, presenting an implemented proof of concept, named Voteproject. On the surface, our research proves the technological viability of adapting blockchain voting systems but also conceptually, Voteproject's design represents a realistic solution to realigning the balance of electoral power back to the citizens: restoring confidence in the American democratic process.

[Keywords: Voteproject, Blockchain, Decentralized Network, Pseudo-Centralized Network, Electronic Voting System]

3. Introduction

The American democratic landscape is primed for reform. In the aftermath of the recent US presidential election, we the people saw the uncertainty and doubt caused by a traditional digital voting systems. In 2016 alone, Crowdstrike, an information security company, identified two separate Russian intelligence-affiliated advanced persistent threats (APT) present within the DNC network¹. As well as the U.S. Department of Homeland Security confirmed Russian affiliated APTs attempted to hack election related systems in 21 States². It is only a matter of time until malicious actors successfully infiltrate the US electoral process and voting systems. This problem will not solve itself without a change in digital platform.

3.1 Status Quo

The United States of America is known for its democratic elected Government. However, its electoral process has been historically plagued with accusations of illegitimacy stemming from a flawed registration processes, inconsistent voter identification practices, voter fraud, voter restrictions, and a general lack of transparency. In terms of information security, the most troubling of these issues is the current vulnerable state of voting machine technology. Most electronic voting systems are black box, proprietary, and average 10-15 years old³. Due to neglect and legacy software, they are riddled with vulnerabilities. Once physical access was obtained, security experts at Defcon 25 exploited the system within 30 minutes⁴. The current method for electronic voting fails in all aspects of the information security 'CIA' triad: Confidentiality, Integrity, Availability.

¹ (2016, June 15). Bears in the Midst: Intrusion into the Democratic National Committee ». Retrieved October 14, 2017, from <https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/>

² (2016, August 29). Hackers hit Arizona, Illinois voter databases - USA Today. Retrieved October 14, 2017, from <https://www.usatoday.com/story/tech/news/2016/08/29/hackers-hit-arizona-illinois-voter-databases/89547326/>

³ (2016, May 2). How old, faulty voting machines undermine American democracy Retrieved November 6, 2017, from <http://thehill.com/blogs/ballot-box/278422-how-old-faulty-voting-machines-undermine-american-democracy>

⁴ (2017, July 30). Hackers at DefCon conference exploit vulnerabilities in voting machines. Retrieved October 14, 2017, from <https://www.usatoday.com/story/tech/2017/07/30/hackers-defcon-conference-exploit-vulnerabilities-voting-machine-s/523639001/>

Confidentiality & Integrity

In an analysis of a Diebold AccuVote-TS voting machine, showed that it is vulnerable to extremely serious attacks. An attacker who obtained physical access to a machine or its removable memory card could install malicious code to steal votes undetectably, modifying all records, logs, and counters to be consistent with the fraudulent vote count it created⁵.

Availability

Have you ever experienced long lines during election days? Due to limited supply and system costs, voting machine kiosks create a ‘bottleneck’ during elections. Therefore, system failures have a high probability of negatively impacting the electoral process and community engagement. Below are actual examples computer errors reported in recent elections using U.S. voting systems: ⁶

Carteret County, North Carolina, November 2004

Software problems caused 4,438 electronic ballots to be lost and never recovered. The vendor acknowledged responsibility for the loss.

Fairfax County, Virginia, November 2003:

Testing ordered by a judge revealed the several voting machines subtracted one in every hundred votes for the candidate who lost her seat on the school board.

Broward County, Florida, January 2004:

134 electronic ballots were blank in a one-race election held on direct recording electronic (DRE) voting machines in which the margin of victory was 12 votes. Florida law required a manual recount of the ballots, but that recount was impossible because there were no physical ballots to recount.

⁵ (2006, September 13). Security Analysis of the Diebold AccuVote-TS Voting Machine. Retrieved October 14, 2017, from <https://s3.amazonaws.com/citpsite/publications/ts06full.pdf>

⁶ (2004, October). Summary of the Problem with Electronic Voting - Verified Voting. Retrieved October 15, 2017, from https://www.verifiedvoting.org/downloads/revised_summary31.pdf

Current voting practices are vulnerable to technical malfunction, system exploitation, and special interest corruption. These reported cases were detected, but it is reasonable to assume this will continue to occur and that the current system is compromised. It is only a matter of time until a major election is impacted because of these issues. Democracy needs an upgrade: Voteproject.

4. Related Work

4.1 Bitcoin

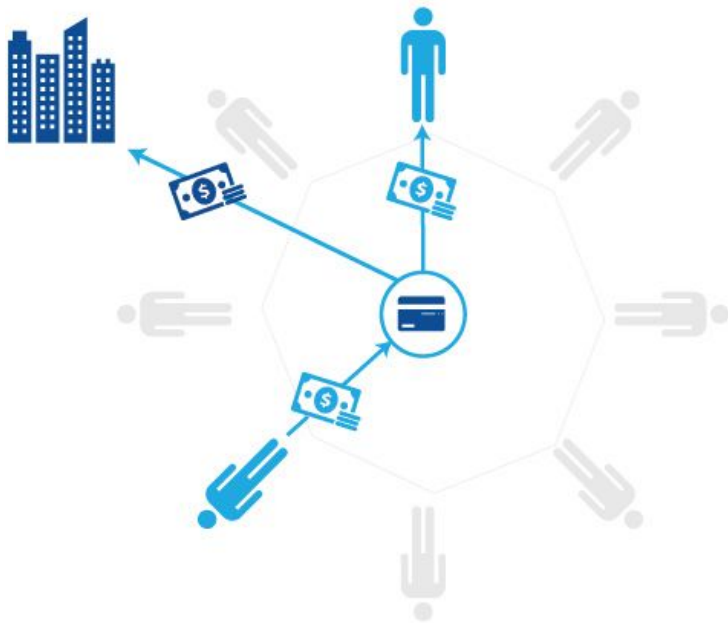
In 2008, an alleged hacker with the alias Satoshi Nakamoto released a white paper titled Bitcoin: A Peer-to-Peer Electronic Cash System.⁷ Conceptually establishing a new resilient, smart, and secure decentralised ledger. Bitcoin and blockchain was not officially created until 2009 when Nakamoto mined the first coins. This revolutionary idea cascaded into the current cryptocurrency environment of Bitcoin, Litecoin, Ethereum to name a few; created an entire new form of democratized investment crowd funding via Initial Coin Offerings (ICO)⁸; and inspired many derivative works, such as IBM Blockchain services⁹ and Voteproject. At its core, Bitcoin is just a digital file that lists accounts and money like a ledger. A copy of this file is maintained on every computer in the Bitcoin network. To send money a user will broadcast to the entire Bitcoin network that the amount in a sender's account will go down and the amount in receiver's account will go up. Nodes in the Bitcoin network apply that transaction to their ledgers, and pass on the transaction to other nodes within the network. This is an all-to-all communication structure. Figure 1 compares the contemporary design for issuing centralized payments and bitcoin's decentralized transaction design¹⁰.

⁷ (2008, October). Bitcoin: A Peer-to-Peer Electronic Cash System - Bitcoin.org. Retrieved October 15, 2017, from <https://bitcoin.org/bitcoin.pdf>

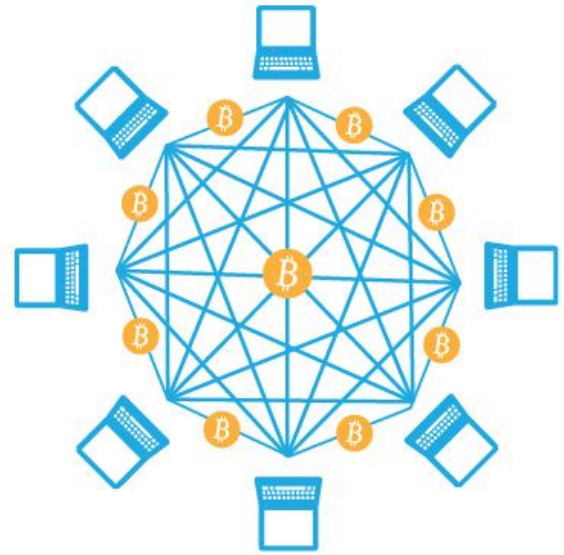
⁸ (2017, September 24). How Blockchain and ICOs Are Changing the Funding Game for Retrieved October 15, 2017, from <https://www.wsj.com/articles/how-blockchain-and-icos-are-changing-the-funding-game-for-startups-1506304861>

⁹ (n.d.). IBM Blockchain. Retrieved October 15, 2017, from <https://www.ibm.com/blockchain/>

¹⁰ (2014, June 26). Bitcoin: Fact. Fiction. Future. | Deloitte Insights. Retrieved October 15, 2017, from <https://dupress.deloitte.com/dup-us-en/topics/emerging-technologies/bitcoin-fact-fiction-future.html>



Current payment systems require third-party intermediaries that often charge high processing fees ...



... but machine-to-machine payment using the Bitcoin protocol could allow for direct payment between individuals, as well as support micropayments.

Figure 1 - Payment process: Current Versus Bitcoin

The decentralized database configuration allows for collaborative processing units, also known as nodes, to maintain multiple copies of a transaction ledger instead of a single instance. Thus, producing a more resilient and available system compared to our current centralized transaction processing system. Essentially, every node within the network knows about each other transaction and updates their ledger in near-real time. Adapting this approach, Voteproject maximizes availability in the form of resilience and data integrity in the form of non-reputable copies into its design. Decentralized networks render large scale denial-of-service attacks virtually useless.

4.2 “Electronic Voting Service using BlockChain”

Published 2016 in the journal of Digital Forensics, Security and Law, researchers Kibin Lee (Korea University), Joshua I. James (Hallym University), Tekachew G. Ejeta (Korea University) and Hyoung J, Kim(Korea University) proposed a potential voting model to conduct blockchain based elections ¹¹.

¹¹ (2016). Electronic Voting Service Using Block-Chain | Lee | Journal of Digital Retrieved November 18, 2017, from <http://ojs.jdfsl.org/index.php/jdfsl/article/view/414>

Their design consisted of four (4) parts: An authentication organization, a trusted third party, a blockchain network, and voters. They propose utilizing the current Bitcoin blockchain to process the transactions.

1. *A company or government does not need to operate an independent blockchain*
2. *There is less risk for transactions to be forged*
3. *Blockchain mining can incur a cost, but voters could receive a tax benefit for voting, thus alleviating the costs of transaction fees while stimulating participation.*

Voteproject was inspired by their research; however, ensuing citizen oversight over the transaction process was a major concern. Therefore, our design does not require the use of the Bitcoin blockchain and the trusted third party and authentication organization is the United States government.

4.3 Follow-My-Vote

Voteproject is not the only initiative to incorporate blockchain voting into democratic process. We introduce to you the great minds behind the Follow-My-Vote project. Follow-My-Vote was born on the 4th of July in 2012, founded on the principles of freedom, as a tribute to the Founding Fathers of the United States. A nonpartisan organization on a mission to change the world, it is in the works to develop applications intended to improve elections around the world. They are developing a voting platform utilizing Decentralized Autonomous Company (DAC) technology.¹² Follow-My-Vote provides end-to-end transparency into the results of any and all elections hosted within it by utilizing the blockchain and modern cryptography technology. With this voting DAC, their goal is to begin unlocking the black boxes that elections are being hosted within today, allowing voters to audit election results while respecting each voter's right to privacy, in order to ensure that each vote in every election truly counts.

¹² (2014, July 4). The Key To Unlocking The Black Box - Follow My Vote. Retrieved October 15, 2017, from <https://followmyvote.com/wp-content/uploads/2014/08/The-Key-To-Unlocking-The-Black-Box-Follow-My-Vote.pdf>

5. Background

In order to understand the impact of adopting a decentralized voting platform, it is important to explain how the United States voting process currently operates.

5.1 Voting Process: United States

Current United States democratic elections are centrally managed by each individual State. County precincts begin the voting process by authenticating the voters and processing their votes. Further complicating the process, all States and the District of Columbia have established alternatives for voters to cast a ballot other than at their precinct polling station on Election Day, including absentee voting and early voting. Voters generally cast their ballots at the polling places for the precincts to which they are assigned by election authorities. For the purposes of in-person voting on Election Day, election authorities subdivide local election jurisdictions into precincts. Absentee Voting has its own share of complications, with variations on who may vote absentee, whether the voter needs to provide an excuse for requesting an absentee ballot, the time frames for applying for and submitting absentee ballots, who may accept the absentee ballot, and when those votes are announced. In addition to absentee voting, some States allow early voting. In general, early voting allows voters from any precinct in the jurisdiction to cast their vote in person without providing an excuse before Election Day either at one specific location or at one of several locations. Within the polling place, there are three stages in the voting process. The process is displayed in figure 2:¹³

Arrival

Poll workers manage the arrival of voters, which may include tasks such as greeting and directing voters and assisting with questions

Check-in

Before voters can gain access to a voting booth, poll workers determine their eligibility to vote by verifying their registration using voter lists or poll books: paper or electronic lists of individuals eligible to vote within the voting precinct.○ In some states further proof of identification is required. This additional proof usually is some form of picture identification as is found on current driver's licenses. This requirement may cause the voter to be turned away if the election judges deems the proof of identification is insufficient.

Marking and submitting ballots

¹³ (2014, September 30). U.S. GAO - Elections: Observations on Wait Times for Voters on Retrieved October 15, 2017, from <https://www.gao.gov/products/GAO-14-850>

Voters are directed to a voting booth to mark their ballots and then submit the ballots for counting. The manner in which votes are cast and counted can vary depending on the voting method and technology employed by the jurisdiction

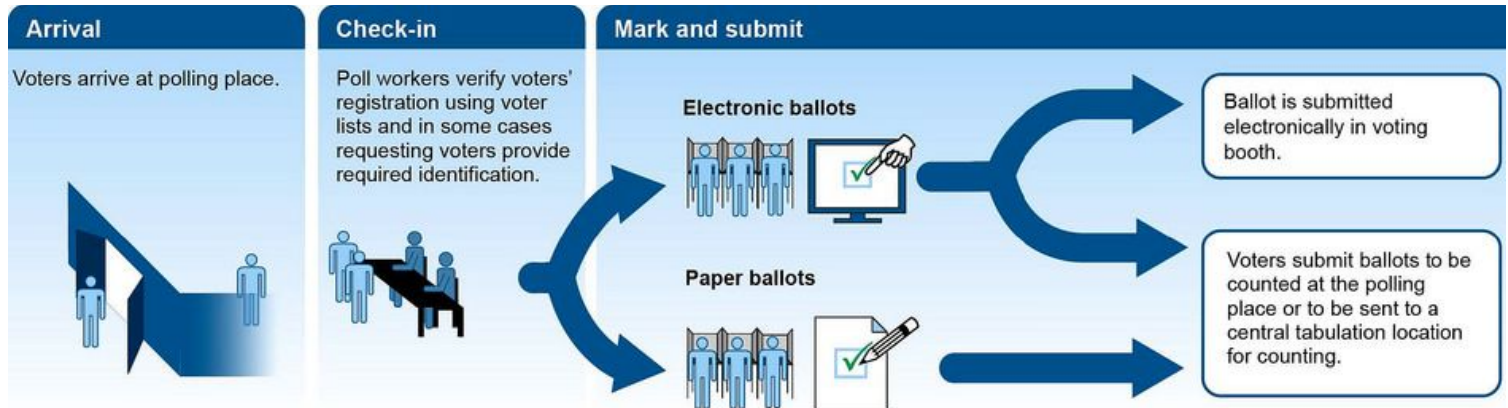


Figure 2 - Voting Process in Polling Places on Election Day

Voting in the United States is a touchy issue at best. The United States has a long history of restricting the vote to produce desired electoral results. Each State writes their own own voting laws and implementation processes. Unfortunately, state voting laws are not standardized across the nation. This presents unique challenges for those seeking technical solutions to streamline the voting process. In addition to legal standardization challenges, most state procured voting systems are proprietary black box systems that are created by for-profit companies, and often utilize non-secure privatized proprietary software. Currently, most votes are cast and counted by one of two types of electronic voting systems: direct recording electronic (DRE) systems and optical or digital scan systems.

DRE machines.

These systems include the hardware and software used to define ballots, cast and count votes, report or display election results, and maintain and produce a printed record of voters' selections.

Optical or digital scanner.

An optical scan system consists of computer-readable paper ballots, appropriate marking devices, privacy booths, and a computerized tabulation device. Optical scan ballots are marked using an appropriate writing instrument to fill in boxes or ovals next to a candidate's name or an issue. If ballots are counted at a central location using a central count optical scan, voters deposit their ballots in a sealed box. If ballots are counted at the polling place using a precinct count optical scan, voters or election officials feed ballots into the scanner for tabulation.

This is an obvious conflict of interest. For profit private companies can not be expected to preserve the democratic process. It is the role of the public to securing our votes from fraud, hackers, and special interest groups must be provided by the public and with maximum transparency and oversight.. When you think about the voting process in the United States, voting essentially takes place in a black box, providing the voter with no assurance that their vote will actually be counted once their ballot has been cast. VoteProject effectively replaces pre-existing electronic voting machines with a community auditable, secure, and special interest free platform. Voteproject utilizes the blockchain for processing and storing transaction records. Obtaining basic knowledge of blockchain technology is imperative to understanding how Voteproject operates.

5.2 Blockchain

A blockchain is a shared decentralized ledger used to process, monitor, and verify electronic coin transactions¹⁴. Essentially, Blockchains maintain the record of coin activity. Bitcoin and Voteproject are alike in this respect because both platforms utilize an electronic coin. Similar to Bitcoins, Votecoins are chains of digital signatures recorded by a blockchain.

5.2.1 Transactions

Transactions are the base layer of the blockchain. Each owner transfers a coin to the next owner by digitally signing a hash of the previous transaction and the public key of the next owner and adding these to the end of the coin. The important element about the transaction chain is the digital signature found within each transaction. Each transaction inherits information from the previous transaction. The signature hashes must match in order to ensure a valid and non-corrupt transaction chain. Figure 3 shows the interconnection between each transaction and the necessary asymmetric encryption.

¹⁴ (2008, October). Bitcoin: A Peer-to-Peer Electronic Cash System - Bitcoin.org. Retrieved October 15, 2017, from <https://bitcoin.org/bitcoin.pdf>

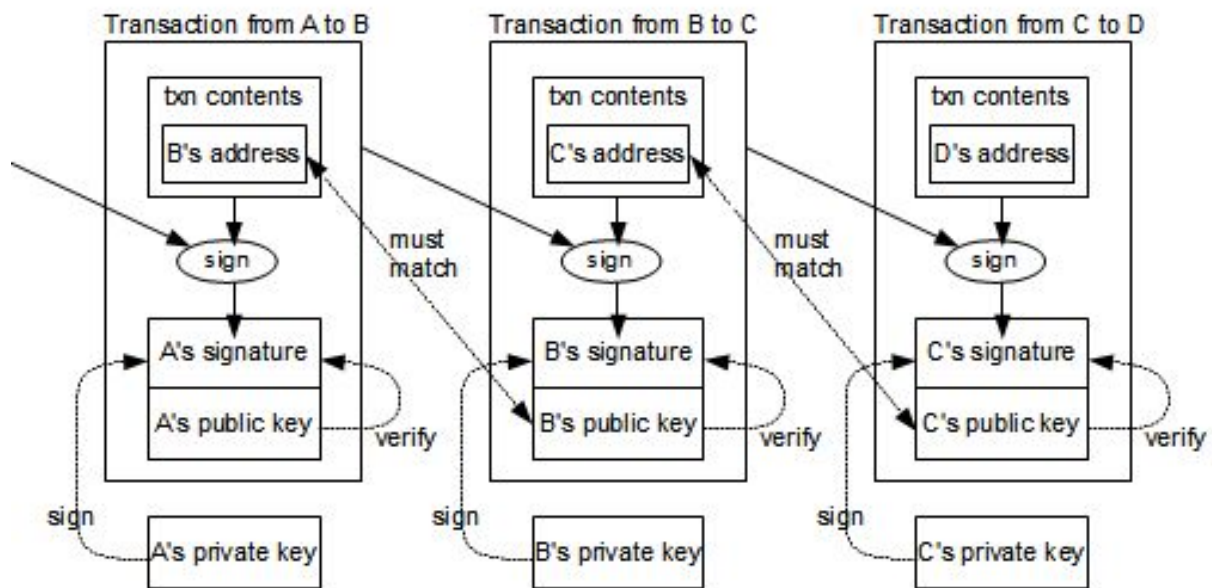


Figure 3 - Blockchain Transaction Process

Each transaction references the previous transaction. This reference is integrated into each transaction by digitally signing the previous transaction. This means, the current transaction directly possesses specific information of its previous transaction thus creating a transaction chain. Chaining the transactions in this configuration reinforces the security of all transactions produced. This is known as the transaction chain and is different from the blockchain.

5.2.2 Timestamp Server

Transactions are placed into groups called blocks, and linking those blocks together called the blockchain. Transactions in the same block are considered to have happened at the same time, and transactions not yet in a block are called “unconfirmed”. Unconfirmed transactions have not yet been ordered and wait to be processed by the network. To begin the ordering process, a timestamp server hashes a group of transaction information known as blocks, with the previous hashed block. During this process, an official time stamp is also included. The timestamp acts as a unique identifier for verifying block integrity and is widely published across the network. Figure 3 displays the contents of a block. Along with a timestamp, within each block consists a block information, a nonce, a hash of the previous block, and a merkle root header (detailed in figure 4).

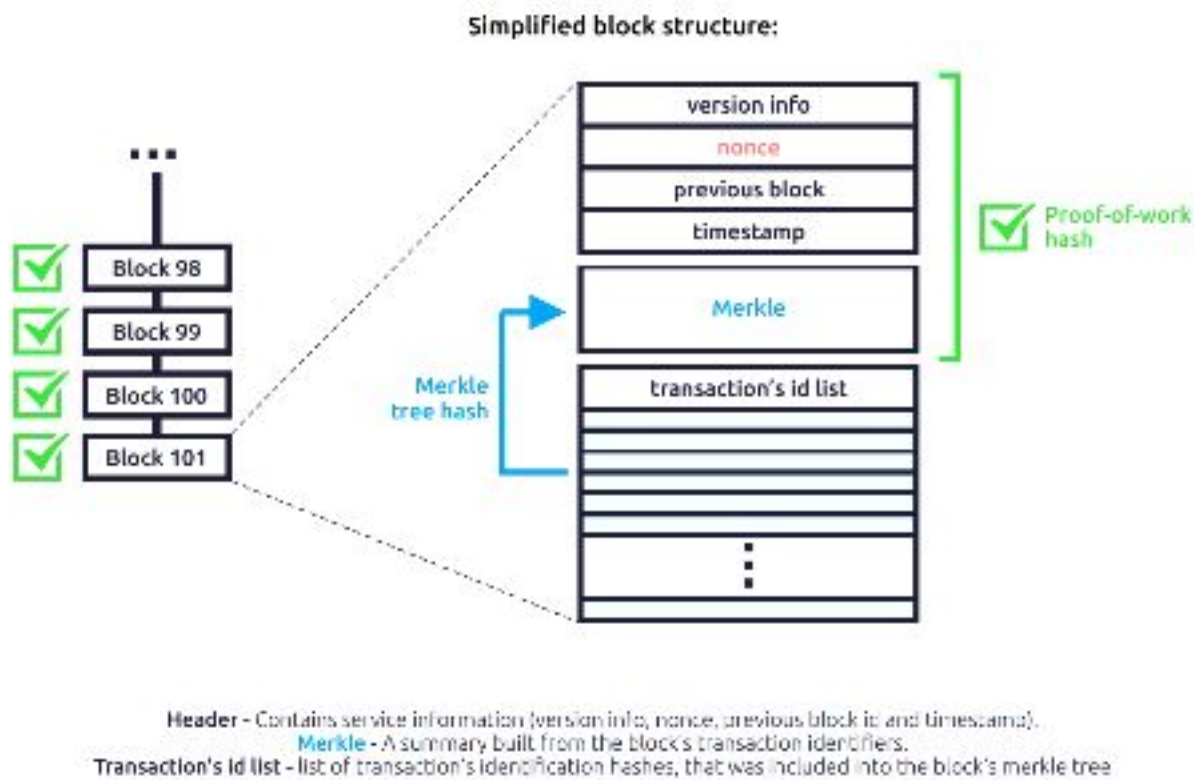


Figure 4 - Simplified Block Structure

The time stamping process links the hash values of each block. Time stamped blocks then can be verified based on its specific time. If any data in a block is modified, the hash value of the block will be changed. Resulting in the hash of all blocks will be changed and all blocks from that point in time and to the most recent block will be changed. The altered chain will not be accepted as a consistent block chain and will eventually be rejected. Although similar, the blockchain is different from the transaction chain as previously discussed. The block chain is used to order transactions. When compared to the transaction chain, the blockchain's purpose is to keep a log of how coin ownership changes. Within the block chain, each block has a reference to the previous block and this mechanic allows for the traversal of transactions to the genesis of the bitcoin.

5.2.3 Merkle Tree

A Merkle tree, also known as a binary hash tree, is a data structure used for efficiently summarizing and verifying the integrity of large sets of data. Merkle trees are binary trees containing cryptographic hashes.

The term "tree" is used in computer science to describe a branching data structure, but these trees are usually displayed upside down with the "root" at the top and the "leaves" at the bottom¹⁵. Each block contains the following:

1. Hashes of the current transactions within the block
2. A hash of the previous block
3. A timestamp
4. A nonce (an arbitrary number that can only be used once)

All transaction hashes within a block include information of other transactions. In other words, each block is a Merkle root consisting of the hash of all the hashes of all the transactions in the block. Displayed in figure 4, each transaction within a block is individually hashed. Then each individual transaction hash is coupled with another transaction hash within the block creating a new hash. This process is repeated until a merkle root header is obtained and included within a block.

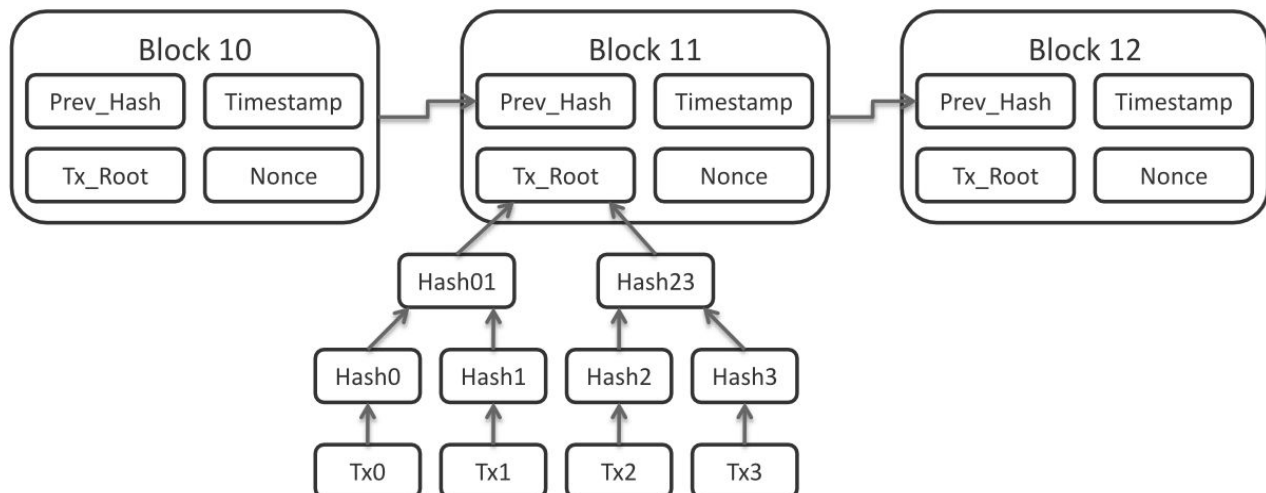


Figure 5 - Merkle Tree expanded and Block contents

Note: the Merkle root is included in the block header.

Utilizing this scheme, it is possible to securely verify that a transaction has been accepted by the network without downloading the entire block chain and all accompanying transaction information. Consider the merkle tree block headers as tiny transaction 'bread crumbs'. Verifying transactions using merkle tree headers save storage space and enhancing processing efficiency.

¹⁵ (2013). Mastering Bitcoin - O'Reilly Chimera - O'Reilly Media. Retrieved October 15, 2017, from <http://chimera.labs.oreilly.com/books/1234000001802/ch07.html>

5.2.4 Security

The change of a single letter of context will cause a change of the entire fingerprint of the block; thereby, affecting the whole context of all blocks ‘stacked’ upon this block. In order to validate forged or pass the forged blocks as valid blocks, an attacker must find the hashes to each block faster than the current hashing speed of the entire network. Continuing with the bitcoin example, it is virtually impossible for individual attackers to corrupt the bitcoin blockchain without massive processing and resource support. Even then, the corruption would be financially infeasible to maintain. The blockchain and its security mechanisms are complex; however, only basic understanding of blockchain functionality is needed to grasp our proposed model: Voteproject. Voteproject’s design can provide the best scalable infrastructure to preserve U.S. election integrity and availability.

6. Proposed Model

6.1 VoteProject: Smart Democracy

This paper details an operational blockchain voting system design, and offers proof of concept using the designed system. Voteproject makes the following contributions:

Introduction of Pseudo-centralized configuration

Pseudo-centralized provides the best realistic solution considering U.S. legal and political challenges. Intended to provide minimal control to centralized organizations, the term Pseudo-centralized accurately describes the conceptual functionality of Voteproject and a practical approach to shifting state electoral control to the public.

Voteproject Blockchain system design

Any Government or organization can have safe and secure elections with minimal infrastructure. They only manage user authentication.

6.2 Pseudo-centralized

Voteproject is a Pseudo-centralized auditable, anonymous, and scalable blockchain voting platform. In this design, the Government (Local/State/Federal) only registers and authenticates voters and candidates. All transaction calculation, processing, and storage are decentralized using a public blockchain.

Our design introduces separation of duties, increases voter security, and reduces the direct influence of the Government in the transparency of the democratic election process. Thus, the prefix ‘pseudo-’ was determined appropriate because the Government possesses only the ‘veil’

of full control while conducting elections. As long as each voter identification and registration laws are non-standardized, state governments still possess ample influence in the outcome of U.S. elections and it is important to acknowledge their power choosing or in this case, authenticating the electorate. The Voteproject pseudo-centralized design retains State user authentication controls but decentralizes the transaction process; therefore, increasing technological security, auditability, and availability. It has the potential to shift the balance of power back to the citizens by providing election transparency, voter accountability, and real time public opinion data.

6.3 Design

Voteproject begins with a user operating a kiosk. The kiosk is any node within the Voteproject decentralized network. It can be a home computer, library, or official voting booth. This feature allows for nationwide scalability, while substantially saving taxpayer dollars by circumventing the demand for purchasing and maintaining dedicated black box systems. Not only does this configuration save taxpayer dollars, it would expand the voting convenience into the home of every citizen with a computer or access to a public facility computer. Hopefully, this would increase voter participation and inject confidence into the American democratic electoral process. When the user is ready to vote, Voteproject.py, the main program, prompts them with a login page.

Note: this project's purpose was to present operational success of a Pseudo-centralized blockchain voting platform.

Authentication of users is not the purpose of this report and minimal resources were allocated to the authentication security of this project's proof of concept. However, industry standard authentication processes could be designed into the project including multi factor authentication and biometrics with the creation of a mobile application. In this proof of concept, a student user is prompted to input basic personal information. Once the information is gathered, it is sanitized and hashed together. This is sent to the authentication server for a simple hash compare against a pre populated voter registration database reflecting the exact user information. Upon successfully completing authentication, Voteproject generates a new public address for the voter and requests the network to issue them a new coin. If valid, the coin is created by the network and sent to the user's new address. Once the address is generated and coin is received, the user is prompted to vote by selecting a candidate's name via radio buttons. For this proof of concept, the following election was conducted:

Choose your favorite ice cream flavor:

1. *Vanilla*
2. *Chocolate*
3. *Strawberry*

It is important for the audience to visualize the program reflecting actual candidate information or referendum items. Next, the user clicks submit and the generated coin is automatically sent to the public address of their chosen candidate. One coin equals one vote and anyone can see, in real time, the results as they are submitted via a blockchain explorer. Once this final step is completed, the program loops back to the login page and begins the process over again. Figure 6 is a complete UML and network diagram of Voteproject:

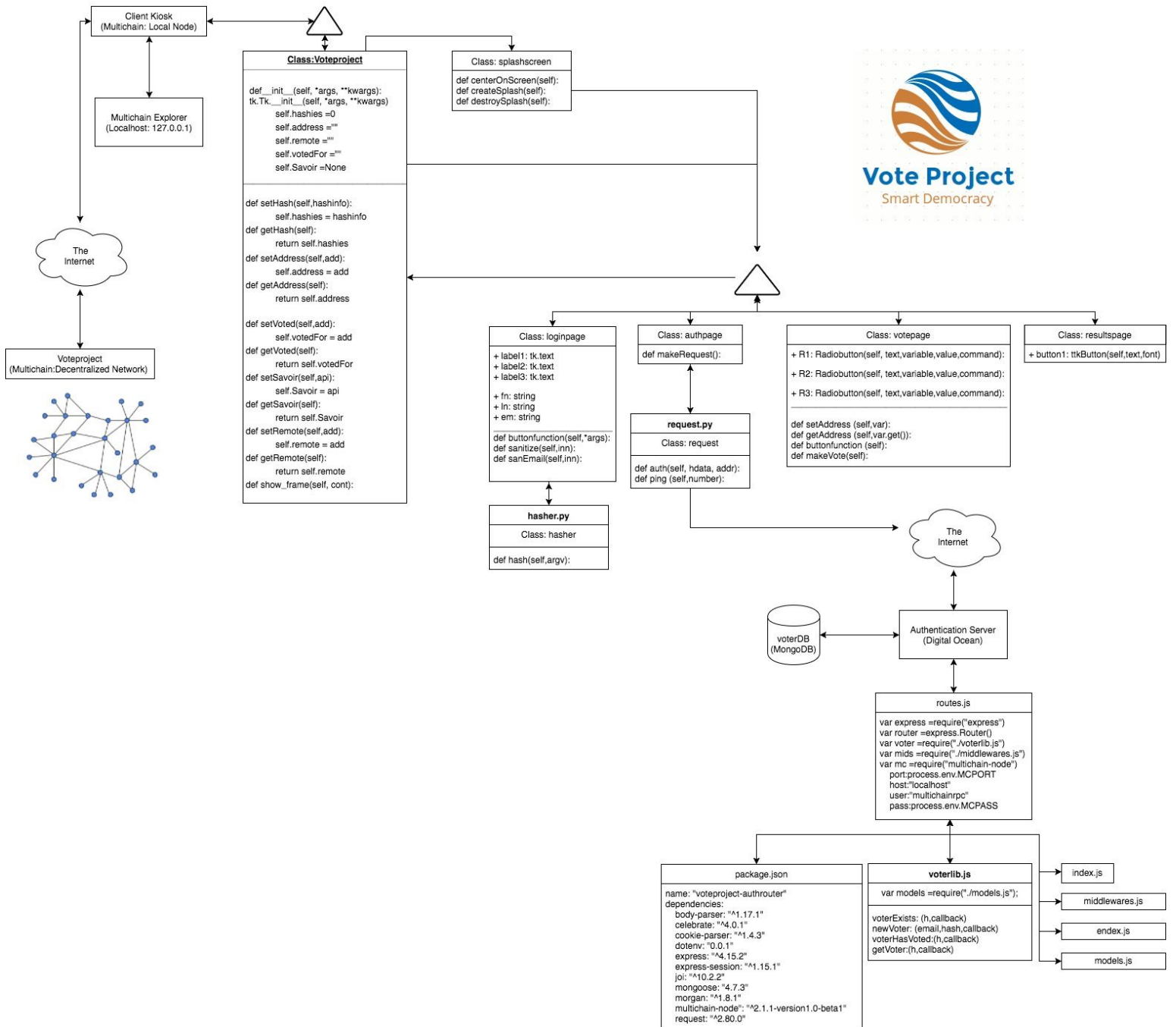


Figure 6 - Complete Voteproject UML & Network Diagram

Note: Readers may need to enhance figure sizes to comfortably reveiw diagrams.

In order to best understand the flow of information it is important we break down each element of the network diagram and explain their functionalities. Voteproject can be broken down into the three following segmentations:

1. *The Blockchain network: Multichain*
2. *The Client Application: Voteproject.py*
3. *Authentication server*

6.3.1 Blockchain Network: Multichain

The blockchain is built using the Multichain open source software. Multichain is an “off the shelf” platform used for the creation and deployment of private blockchains, either within or between organizations. Its purpose is to overcome a key obstacle to the deployment of blockchain technology in the institutional financial sector, by providing the privacy and control required in an easy to use package¹⁶. Multichain provides a cost effective solution to deploying trusted and operational blockchain. Voteproject utilizes simple JSON commands to control and manipulate the private blockchain created through Multichain. Figure 7 is a closer look at the decentralized blockchain elements of Voteproject:

¹⁶ (June 2015.). MultiChain Private Blockchain — White Paper. Retrieved October 26, 2017, from <http://www.the-blockchain.com/docs/Multichain%20Whitepaper.pdf>

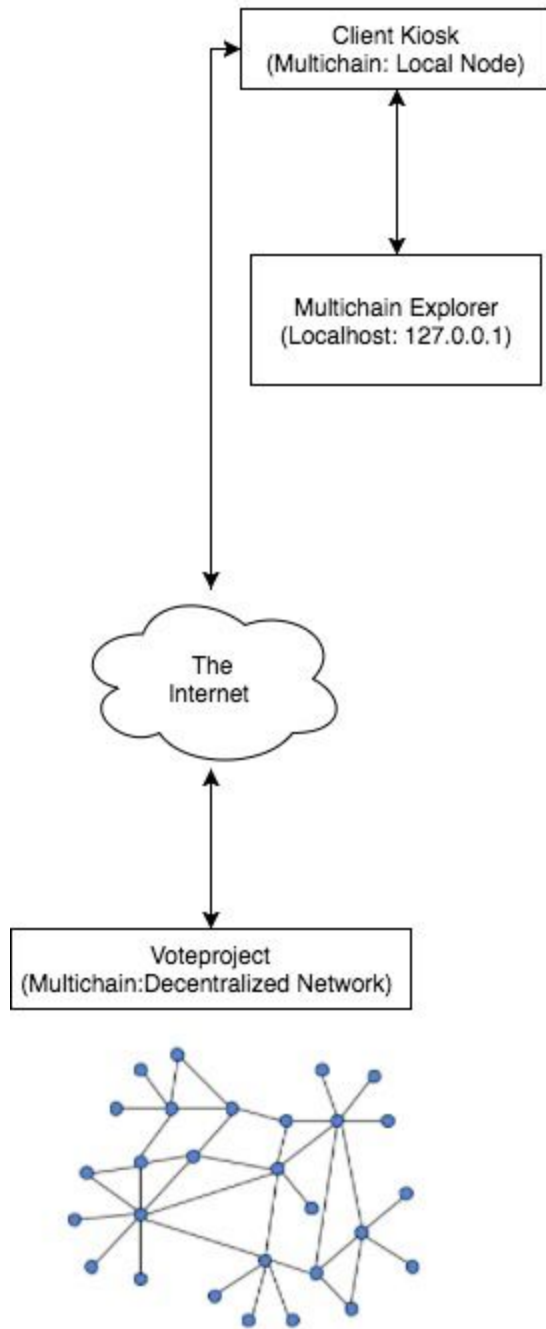


Figure 7 - Voteproject Decentralized Network Diagram

Note: the client kiosk is simply any other node connected to the decentralized network.

As previously mentioned, Voteproject leverages a blockchain explorer to display real time and transparent electoral results. The blockchain explorer used for this project is called Multichain Explorer¹⁷. Blockchain explorers, also known as blockchain browsers, are tools usually web based, that provides detailed information about a blockchain on a timed sequence. For this proof of concept, Multichain Explorer monitors each transaction on the local client node. It uses JSON commands to request information from the node and displays the information via localhost: 127.0.0.1. Multichain Explorer was specifically chosen because of its direct compatibility with Multichain private blockchains.

6.3.2 Client Program: Voteproject.py

Voteproject.py is the main program. All other modules either is apart of its functionality or supports its operations. Voteproject.py is coded in Python and leverages TkInter to create the graphical user interface. The majority of program functionality is broken down into a four frame sequence and loop. Figure 8 represents the tkinter frames and alludes to the logic embedded within each class.

1. *Loginpage*
2. *Authpage*
3. *Votepage*
4. *Resultspage*

¹⁷ (2017.). GitHub - MultiChain/multichain-explorer: Web-based explorer for Retrieved October 28, 2017, from <https://github.com/MultiChain/multichain-explorer>

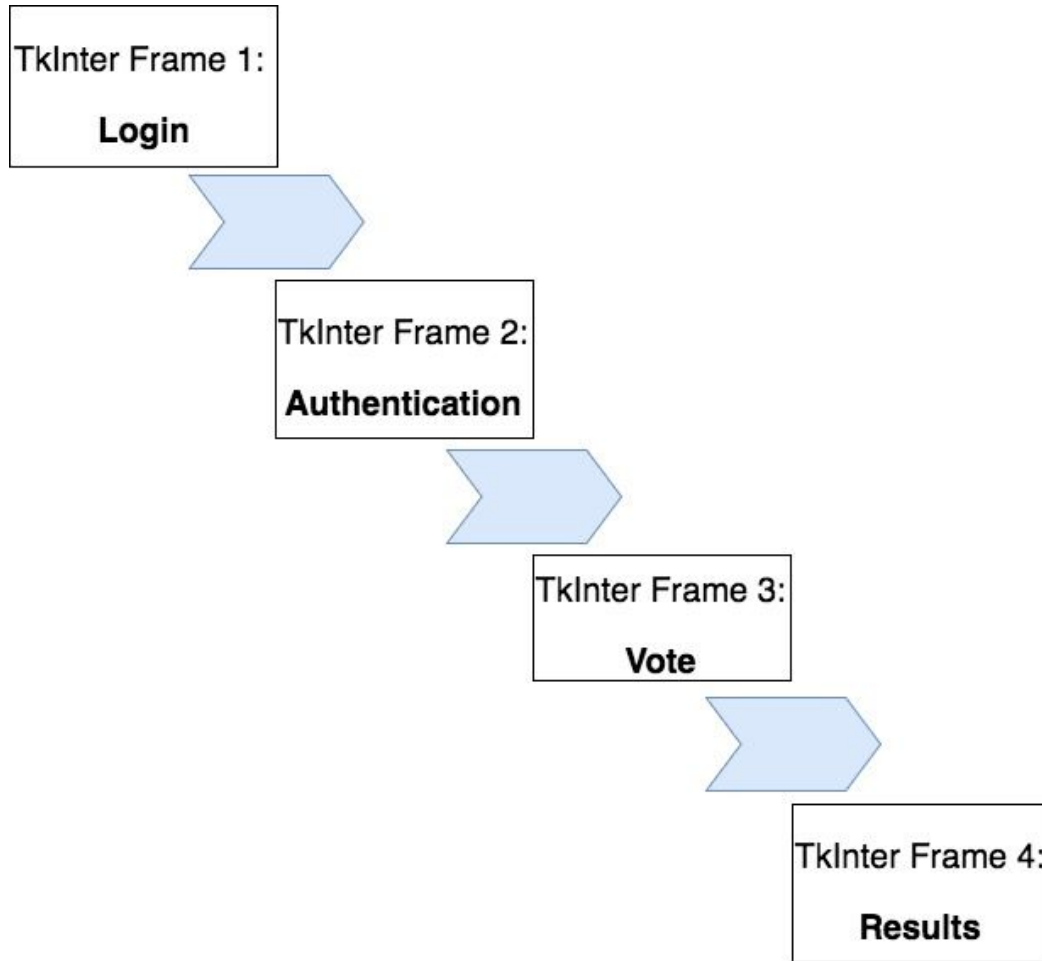


Figure 8 - Voteproject TkInter Frame Structure

Note: each TkInter frame represents the logical operations of Voteproject.py: login, authentication, voting, and results.

Figure 9 presents a closer look into the structure and logical functionality of Voteproject.py:

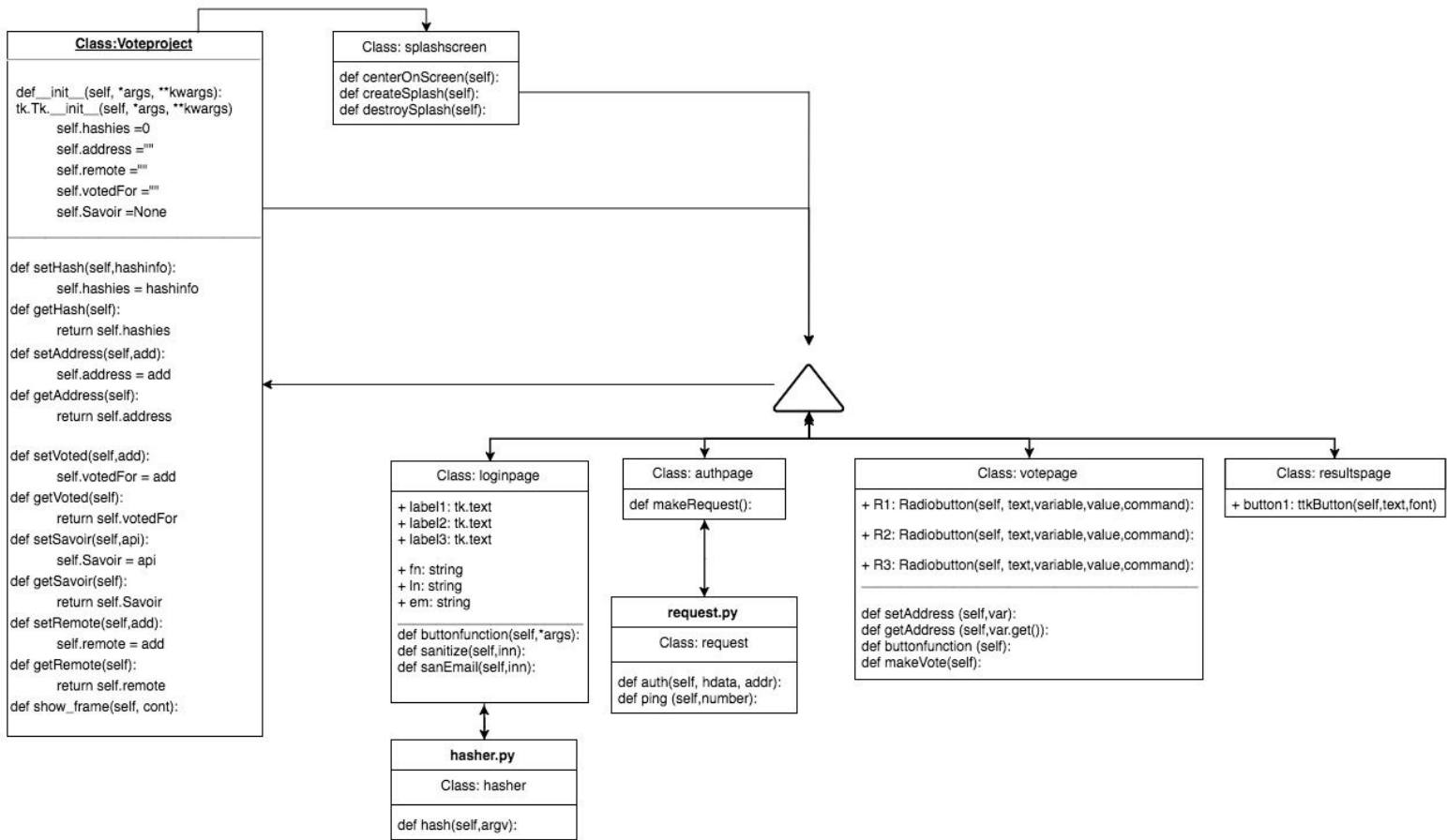


Figure 9 - `VoteProject.py` UML

6.3.3 Authentication Server

VoteProject is a proof of concept for a blockchain voting platform. It does not solve for secure authentication. For this proof of concept a simple unsalted hash compare table was used. The design uses a hash compare function to authenticate voting users.

Note: authentication security was not within scope of this proof of concept. Minimal resources were utilized to create the authentication process.

However, readers should not be worried because user authentication best practices will be included in later project iterations. VoteProject has the capability to include secure practices such as salted hash tables, multifactor authentication, and biometric technology. Figure 10 presents a closer look at the authentication server architecture and the routing modules created to handle JSON commands:

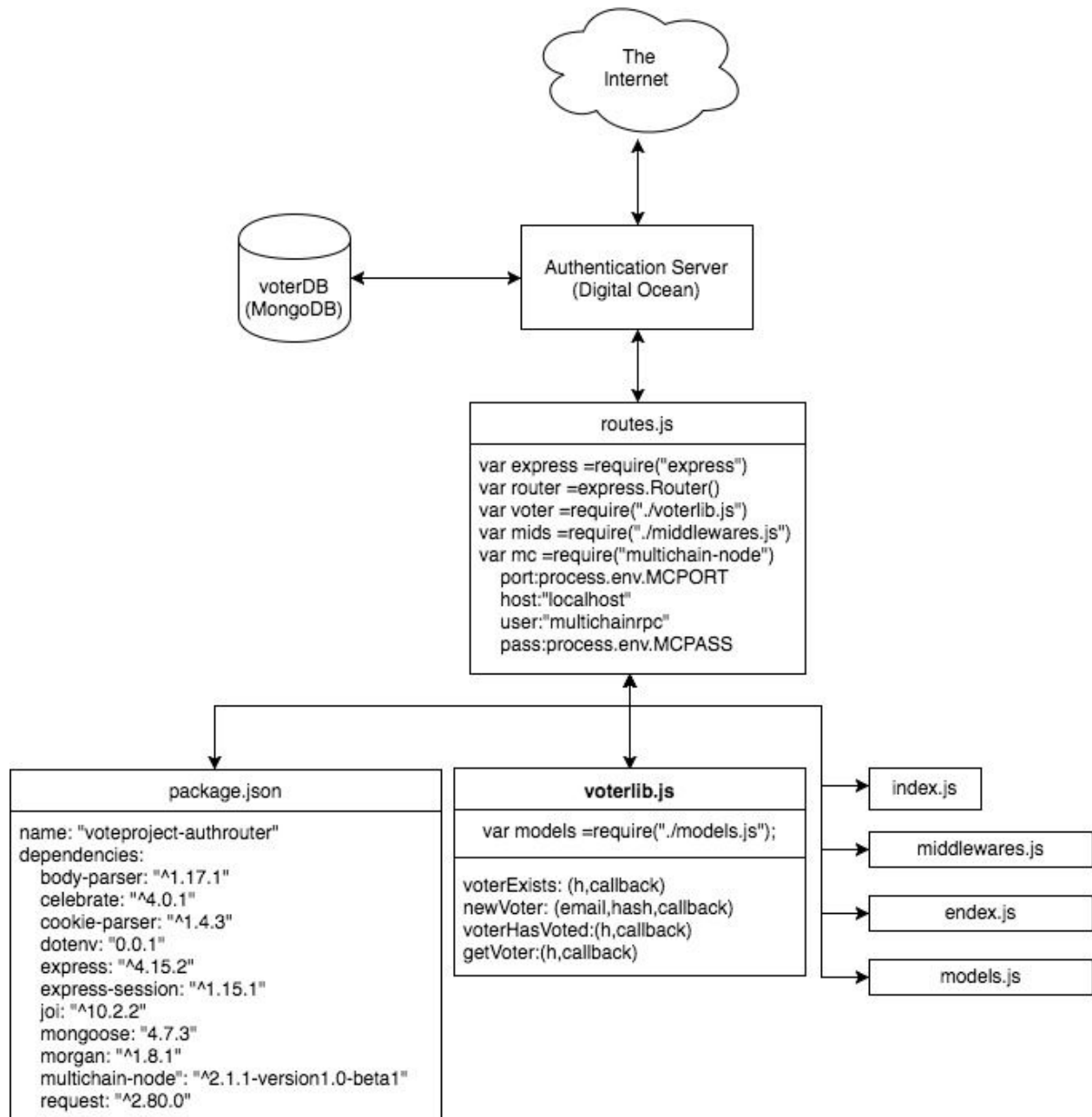


Figure 10 - Proof of Concept Authentication Server Architecture

Prior to executing the proof of concept, a student database was created with the following information:

1. *First name*
2. *Last name*
3. *Sam Houston State University email address*

Together this information is sanitized and hashed together for authentication comparison. The voter information is stored using MongoDB. MongoDB is an open source database that uses a document-oriented data model and is built on an architecture of collections and documents rather than rows and columns¹⁸. Compatibility was the main reason MongoDB was chosen for this project. MongoDB stores data in a binary representation called BSON (Binary JSON)¹⁹. The BSON encoding extends the popular JSON (JavaScript Object Notation) representation to include additional types such as int, long, date, floating point, and decimal128. BSON documents contain one or more fields, and each field contains a value of a specific data type, including arrays, binary data and subdocuments. Multichain operates using JSON commands and standardizing markup data is a strong advantage to utilizing MongoDB. Another powerful advantage of utilizing MongoDB was the swift indexing structure. MongoDB uses a system of collections and documents. This allowed Voteproject to create a tree structure for indexing voter information. The database tree is extremely fast and scales directly with storing United States voter information. Figure 11 presents a closer look at the database structure of Voteproject:

¹⁸ (2017.). Architecture Guide | MongoDB. Retrieved October 28, 2017, from <https://www.mongodb.com/lp/white-paper/architecture-guide>

¹⁹ (2017.). BSON (Binary JSON) Serialization. Retrieved October 28, 2017, from <http://bsonspec.org/>

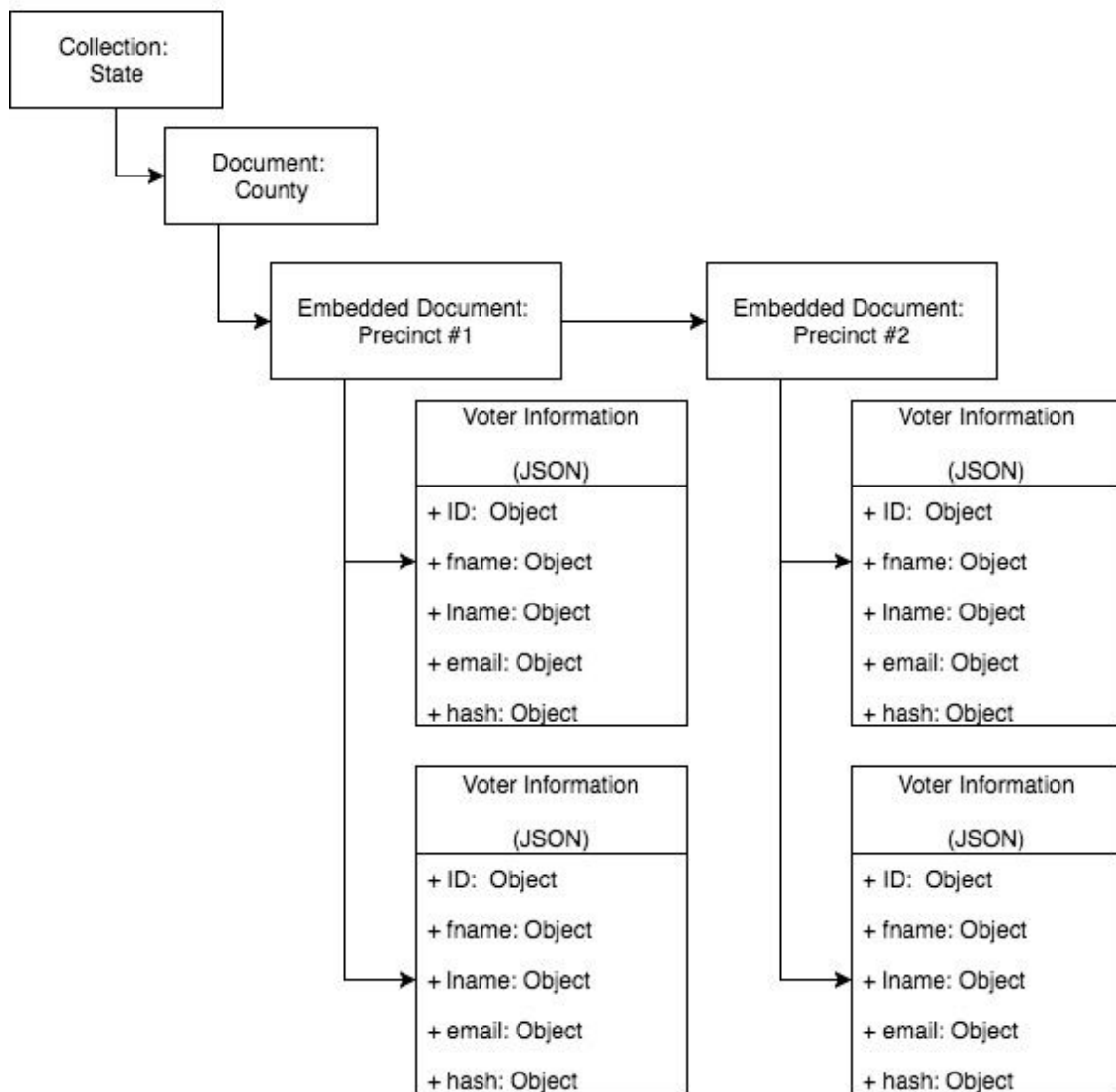


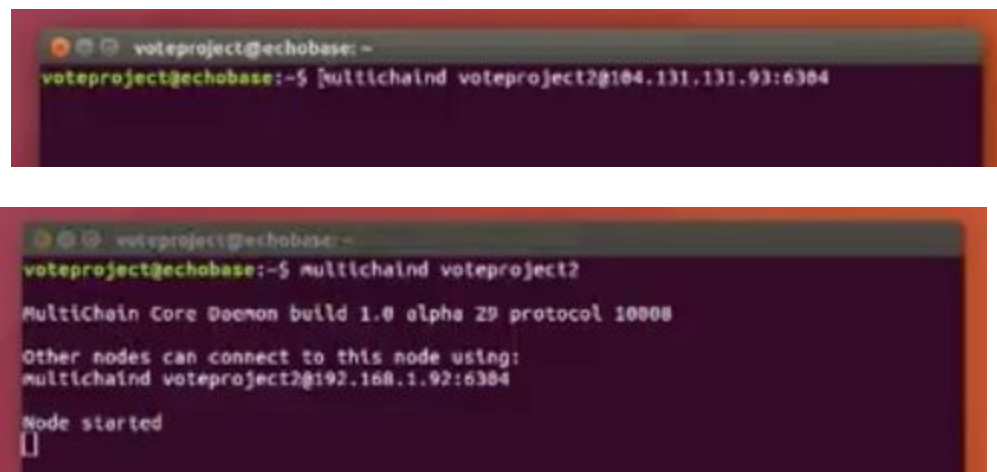
Figure 11 - Voteproject Database Structure

7. Proof of Concept

The following proof of concept is a mock election for a user to select their favorite ice cream flavor, but utilizing a Pseudo-centralized voting platform. The following figures detail the voting process from blockchain node connection, executing the main program, and viewing real time election results.

7.1 Connections

Figure 12 displays the command [`multichaind voteproject@104.131.131.93:6305`] used to connect to a local multichain node. If connection is successful, multichain issues a command for other nodes to connect.



The image consists of two screenshots of a terminal window. The top screenshot shows the command `multichaind voteproject2@104.131.131.93:6304` being entered at the prompt `voteproject@echobase:~$`. The bottom screenshot shows the output of the command: `voteproject@echobase:~$ multichaind voteproject2`, followed by `MultiChain Core Daemon build 1.0 alpha 29 protocol 10008`, `Other nodes can connect to this node using:`, `multichaind voteproject2@192.168.1.92:6304`, and `Node started` with a cursor on a new line.

Figure 12 - Voteproject: Connecting to Blockchain

Multichain explore must be launched next. This application runs every 60.0 seconds, querying the local blockchain for data. In order to connect multichain explorer, a multichain blockchain must be actively running on the local node and all previously mined blocks must be committed to multichain explorers sql database. Figure 13 displays the connection/committing command [`python -m Mce.abe --config voteproject2.conf --commit-bytes 100000 --no-serve`] and figure 14 displays the execution command [`python -m Mce.abe --config voteproject2.conf`] for multichain explorer. When successfully connected, the local host address [`127.0.0.1`] of the local node is transformed into a real time blockchain monitor as shown in figure 15.

```

voteproject@echobase: ~/Downloads/multichain-explorer-master
voteproject@echobase:~/Downloads/multichain-explorer-master$ python -m Mce.abe -
-config voteproject2.conf --commit-bytes 100000 --no-serve

block_tx 300 312
block_tx 301 312
block_tx 302 313
block_tx 303 314
commit
voteproject@echobase:~/Downloads/multichain-explorer-master$

```

Figure 13 - Voteproject: Committing Blocks To Explorer


```

voteproject@echobase:~/Downloads/multichain-explorer-master$ python -m Mce.abe -
-config voteproject2.conf

voteproject@echobase:~/Downloads/multichain-explorer-master$ python -m Mce.abe -
-config voteproject2.conf
block_tx 304 315
commit
Abe initialized.
Listening on http://localhost:2750
Launched background thread to catch up tx every 60.0 seconds

```

Figure 14 - Voteproject: Launching Explorer



MultiChain Explorer

Search by address, block number or hash, transaction or chain name:

Address or hash search requires at least the first 6 characters.

Status	Chain	Blocks	Transactions	Assets	Addresses	Streams	Peers	Started	Age (days)
Connected	MultiChain voteproject2	277	315	2	8	1	1	2017-09-13	0.0

Latest Transactions

Txid	Type	Confirmation	Time
19a710b0474478308d67208042409304729d5ce1c473f812d78099483b0396ea	Asset	187 confirmations	< 26 minutes
d4705b3d6562e6cb7cc55d64616b48498154e465576b31462776fb34fe8c01b	Asset	187 confirmations	< 26 minutes
9fc2b8e9e70a8113f178b6cafc08e20e2e420330563ca4e575e26ec3e1799	Asset	129 confirmations	< 32 minutes
9efc5cd9cc3472273ad1455e11341d859b0c441f6cc8544be791daeb7f298b	Asset	129 confirmations	< 32 minutes
c30ca74e450bd030292447035aedc11e02439aa27d30953a27b6dab075b06c	Permissions	132 confirmations	< 33 minutes
9e06e0824d7d340997fc728926b753a5e34206ad610c24d89172dc4ede2c8a72	Permissions	132 confirmations	< 33 minutes
ab79d12a256961dcb5d2a609e463a75c732d31439d79f20edced41139bc377f	Asset	178 confirmations	< 42 minutes
ab6d1fb2b1898d9ce87dc2901a5aa8fcc87c7c8e909a924c61f458748574e282	Asset	178 confirmations	< 42 minutes
b652ec9d2fb9662b537e02a270e93956e534e93442984a30d4761c025420b	Permissions	182 confirmations	< 48 minutes
9607d92667548aa389c18e1f453e45b70a78e404098a7e7ade06762244546af	Asset	185 confirmations	< 49 minutes

Figure 15 - Voteproject: Multichain Explorer Connected

7.2 Main Program Execution

Voteproject is a python script that controls other software and libraries. Figure 16 is the command [`python voteproject.py`] to execute the script.

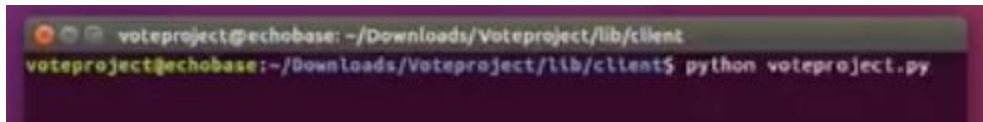


Figure 16 - Voteproject: Launching Voteproject

After the program is launched, an window appears and prompts the user for their voter information, see figure 17.



Figure 17 - Voteproject: Login

For this demonstration the program was not run in “--Daemon” because the authentication information can be shown in the terminal. Figure 18 shows each argument (arg01-firstname,arg02-lastname,arg03-email) being processed, hashed and authenticated. Once authenticated, Voteproject rewards the user with a new coin. Confidentiality best practice recommend creating a new address for each transaction. This new address shown in figure 18 is an indicator a new coin was generated and sent to the user.

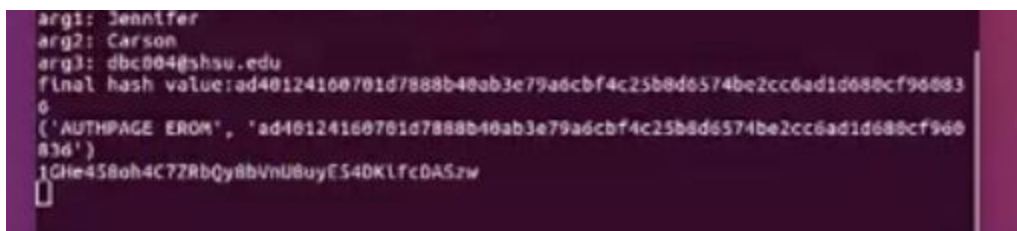


Figure 18 - Voteproject: Hash Compare and Address Creation

After authentication is successful and a new coin is generated, the user is prompted with a new window: VotePage. Figure 19 displays an example of the voteproject votePage window.



Figure 19 - VoteProject: VotePage

Once the candidate is selected and vote is submitted, the generated voteCoin is sent to the appropriate candidate address. VoteProject creates a new address for the user as shown in figure 20 and send the voteCoin.

```
arg1: Jennifer
arg2: Carson
arg3: dbc004@shsu.edu
final hash value: ad40124160701d7888b40ab3e79a6cbf4c25b8d6574be2cc6ad1d688cf96883
6
('AUTHPAGE ERON', 'ad40124160701d7888b40ab3e79a6cbf4c25b8d6574be2cc6ad1d688cf968
836')
1GHe458oh4C72RbQy8bVnUBuyE54DKLfcdASzw
JC6CohXYacws jLqpEcAKnerHexxZ9qTfbYxEpQ
|
```

Figure 20 - VoteProject: VoteCoin Creation

Shifting to multichain explorer displaying information on [127.0.0.1], figure 21 and figure 22 displays the news addresses and transaction details that took place during this particular voting proof of concept.

7.3 Results and Confirmation

Txid	Type	Confirmation	Time
3fdad90ba7e04f206f5362860a84c8e2f82902e9440f0dbb77b80880d2835ea	Asset	Minimised	< 1 minute
8f5e3c4632b20ed483aa00e035063f4be73cb2c7fe4a4954ae238e9e7dbd3f	Asset	Minimised	< 1 minute
19a716947447830896720847409304729df0w1c473812d780964638d386ee	Asset	115 confirmations	< 20 minutes
d4705f038542efcb7cc55864818b48498154e485578b314627788b534ef8cd1b	Asset	115 confirmations	< 20 minutes

Figure 21 - VoteProject: Multichain Explorer Transaction Logs

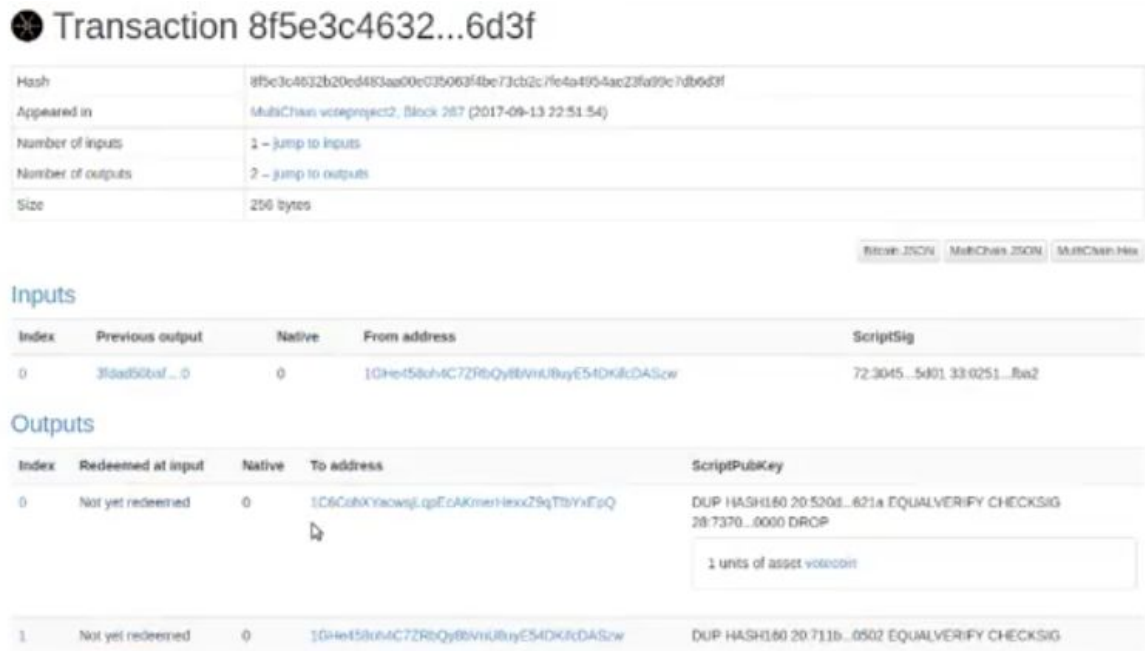


Figure 22 - Voteproject:Multichain Explorer Transaction Confirmation

8. Future Work

Our future work will orbit towards strengthening the security and increasing the convenience of using the software.

8.1 Authentication Security

Authentication security is a chief security concern for future project iterations. As previously mentioned, Voteproject does not address the authentication security issues. Due to lack of resources being an academic project, authentication security was not within scope of this proof of concept and it is knowingly flawed. Standard authentication practices already exist and are secure enough for the confidential information of our daily and business lives. Future authentication redesigns will include multi-factor authentication, secure transmission, salted hash tables and biometric technology.

8.2 Setup script

In its current form, Voteproject installation requires an experienced technical user to install and operate. There are many “moving parts” to the installation process including library dependencies, platform version controlling, and custom command line operations. Part of the beauty of blockchain voting systems is the increased availability of applicable voting “kiosks”. Voting systems of the future must be simple, consistent, and available. These attributes are necessary to ensure the platform is adapted as a national standard and decrease voter apathy during official elections. To begin this process, Voteproject’s future work includes an “all-in-one” install script for linux systems. This change will encourage early adoption of the platform, community interest, and decrease barriers of entry for less technical audiences.

8.3 Blockchain platform

Multichain was still relatively new when Voteproject adopted it as its private blockchain engine. When Voteproject was implementing its software design Multichain was in its Alpha_16 version. It is currently in Beta_1 testing. As Multichain refined its platform, Voteproject systematically experienced many of the same “growing” pains. Redesigns and scope creep was experienced directly in part to development changes in the Multichain platform. Also there is a lack of procedural and set up video tutorials; however, a great repository of Multichain api and FAQ documentation is now available. Overall, Multichain is a wonderful project and we recommend it as the best cost effective personal blockchain platform available.

Future work may include exploring additional enterprise Blockchain platforms such as IBM Blockchain Cloud or in-house development of a Voteproject specific blockchain platform.

9. Conclusion

Voteproject's ultimate purpose is to inspire, influence, and empower the next generation of democratic election technology. Our conclusions can be separated into three (3) categories: Legal and Political Limitations, Security Concerns, and Practical Applications.

9.1 Legal and Political Limitations

The 52 U.S. States have different election and voting laws. Standardizing State law is a big barrier to electoral reform. Considering the US history of voter repression, politics of change may be the largest barrier to achieving this goal. Politics being politics, the issue of bipartisanship fairness is a given. The difficulty of providing efficient, available, and convenient

access to voting systems to everyone will require the willingness on political parties to relinquish their gerrymandering and voter repression powers. The removal of the advantage certain political parties over other political parties that benefit from limiting voter access will be challenged should this system be adopted. This change in the balance of power will invite special interest groups and political establishments to resist electoral modernization efforts. Therefore, VoteProject and any other innovative voting technology may experience deliberate barriers by established political and economic powers.

9.2 Security Concerns

9.2.1 Double Spending

As with all ledger based transaction systems, double spending is a major concern. Double-spending is the result of successfully spending some “money” more than once, or in this case, voting multiple times. Double spending can corrupt the integrity and public confidence of any transactional system. However, Bitcoin has methods built in to successfully prevent this attack via timestamps, proof of work, and forking.²⁰ In order to universally maintain its blockchain, Bitcoin often produces a fork (branching). A fork is a byproduct of distributed consensus and happens anytime a block is mined at similar times by more than one miner. Figure 23 presents an example of a fork created when a buyer attempts to double spend their bitcoin. Overtime the longer, “most trusted”, fork wins out and the other side is culled from the ledger and reprocessed. Resulting in an invalid transaction and a record of incomplete funds.

Note: Distributed consensus is an algorithmic process to allow a set or network of computers to all agree on a single value that one of the nodes in the system proposes.

²⁰ (2017, August 7). What is Double Spending & How Does Bitcoin Handle It? - CoinSutra. Retrieved October 29, 2017, from <https://coinsutra.com/bitcoin-double-spending/>

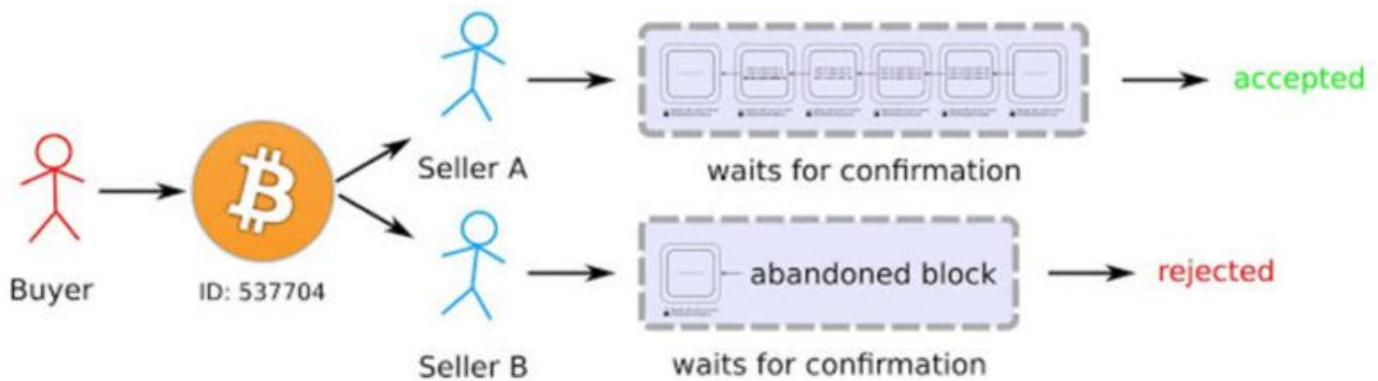


Figure 23 - Bitcoin Branching Process

This discrepancy in the Blockchain is resolved when subsequent blocks are added, making it the longest chain.²¹ Simply put, the longest chain wins and the blocks of the other side of the fork get "orphaned" (or abandoned) by the network and reprocessed after the fork is resolved. VoteProject takes this attack very seriously and ensure to mirror Bitcoin's double spending safeguards in future iterations.

9.2.2 The 51% Attack

This attack is currently hypothetical and pretty straight forward. A 51% attack refers to a coordinated effort by a malicious entity to manipulate a Blockchain network by controlling more than half of the decentralized processing nodes. Hence the "51%" percent nomenclature is assumed. In the case of Bitcoin, once a block is finalized (mined) it generally can no longer be altered. Due to the checks and balances in Bitcoin such as timestamps, proof of work, and forking. However, if an entity is controlling the majority of the computing power on the network, an attacker or group of attackers could interfere with the process of recording new blocks. Or even go so far as preventing miners from completing blocks. This attack is troubling to VoteProject because votes could be manipulated to produce a desired electoral outcome. As of August 2017, cost calculations to launch and maintain a 51% attack against the Bitcoin network are the following:²² The malicious entity would need more than **478,400** hardware units with an estimated value of **\$1,004,669,000**. The electricity required to power the hardware units with electricity is estimated at **\$1,578,000** per day.

²¹ (2017, March 27). A Short Guide to Bitcoin Forks - CoinDesk. Retrieved October 29, 2017, from <https://www.coindesk.com/short-guide-bitcoin-forks-explained/>

²² (2017, August 1). Cost of a 51% Attack and Security of Bitcoin, Monero, Litecoin and Retrieved October 29, 2017, from <https://freedomnode.com/blog/86/cost-of-51-attack-and-security-of-bitcoin-monero-litecoin-and-other-cryptocurrencies>

Producing a final total of **\$1,006,247,000** for the first day not including maintenance and upkeep costs external to daily electrical consumption. Nation States and large corporations have the financial resources to conduct a 51% attack but corrupting the network unnoticed would be considerably difficult considering the United States' computational and financial resources; intelligence and technical monitoring capabilities; and public demand to maintain election integrity. Generally, the more independent nodes within a Blockchain network, the stronger the network. Blockchains can scale to remediate this attack vector.

Note: this attack vector remains theoretical for established blockchains such as Bitcoin. It is considered technologically and financially infeasible for most attackers.

9.3 Practical Applications

Even with limitations and security concerns of adapting a blockchain voting systems, it is my professional analysis that the positive results outweigh any negatives. Practical applications and conceptual use cases for VoteProject provides enough purpose for adaption. The following large scale applications are what we determined as the most impactful advantages to utilizing a Blockchain voting system over the current voting system.

9.3.1 Vote Reconsideration & Real Time Data

VoteProject produces real time results and inherently consists of a transparent audit trail. Blockchain based voting systems allow for voter reconsideration. A voter could cast, remove, or reconsider their vote during a voting cycle without compromising the integrity of the election. When using this technology a voting cycle could begin at the moment any candidate officially registers their candidacy with the appropriate authorities. Because once officially registered, a public address is generated and publicized across the blockchain network.

Instantly, voters can begin casting their votes for that candidate until the election ends on an agreed upon date (e.g. November 7th). Candidates and public opinion often change throughout each election cycle. Accompanied with real time and true voting results rather than the straw polls as currently used, voters would have the opportunity to reconsider their vote based on changing circumstances. This may produce momentum for non-establishment candidates; provide the most accurate data for analysis by all candidates, and help reduce or eliminate voter apathy while increasing voter participation. The real time results act as an election forecast and can be used by the candidates as a marketing tool to support their election. We believe this technical advantage to using a Blockchain based voting system presents an invaluable asset to the democratic process.

9.3.2 Providing Financial and Technical Mining Incentives

As previously mentioned Blockchain security guards against 51% attacks by relying on the quantity and integrity of independent mining nodes and financial barrier of entry for obtaining and maintaining large scale information technology infrastructure. In order to ensure as critical mass of mining node quantities, I propose creating financial incentive and technological convenience for citizen mining operations. A simple tax deduction on energy cost or subsidies for technological purchases could be provided to individual citizens and business for assisting the democratic process. Providing individual citizen mining incentives is the best method of ensuring the health and security of blockchain voting systems in a mixed free market economy.

9.3.3 Democracy In A Box

Since the 20th century, the quantity of functional democratic countries has substantially increased compared to previous centuries throughout history. Especially for newly formed democratic nations, the infrastructure required for conducting an election with transparency, integrity, and nationwide availability continue to prove to be a challenge. Blockchain voting systems present a unique solution to this issue. Consistent energy and availability of computer systems (desktops, laptops, smart devices) represent the first and most basic step. Then the developing democratic nation could utilize the pre existing blockchain network to conduct their elections. This means the United States and its allies could provide a global democratic election service to the world at minimal additional costs or infrastructure. Developing democratic countries would have this infrastructure instantly and the global democratic leaders can ensure not only their elections, but the entire world's elections are transparent, secure and available. Think of Voteproject as democracy in a box. And the majority of the world already has the “box”, they would only need to open it.

9.4 Closure

Blockchain technologies are the future. Bitcoin may not be the ultimate application of the blockchain but, merely, its first successful user. Many industries are beginning to utilize blockchain technology beyond its cryptocurrency applications. Public and private organizations, including technology firms, financial institutions, supply chain industries and the State of Delaware, are using this technology. As of August 1, 2017, a new law permits companies in Delaware, where more than two-thirds of Fortune 500 companies are incorporated, to keep their

list of shareholders on a Blockchain²³. The biggest question is not if but when, the world will adopt Blockchains as the defacto transaction and record keeping standard. The biggest question is not if but when, the world will adopt Blockchains as the defacto transaction and record keeping standard, but when this adoption will occur.

²³ (2017, August 22). Blockchain: Why Delaware Is Backing Blockchains - Fortune. Retrieved October 29, 2017, from <http://fortune.com/2017/08/22/fortune-500-blockchain-ledger-delaware/>

10. Table Of Figures

Figure 1 - Payment process: Current Versus Bitcoin:

<https://dupress.deloitte.com/dup-us-en/topics/emerging-technologies/bitcoin-fact-fiction-future.html>

Figure 2 - Voting Process in Polling Places on Election Day

<http://www.gao.gov/assets/670/666252.pdf>

Figure 3 - Blockchain Transaction Process

<https://bitcoin.org/bitcoin.pdf>

Figure 4 - Simplified Block Structure

<https://www.slideshare.net/boolberry/boolberry-reduces-blockchain-bloat/1>

Figure 5 - Merkle Tree expanded and Block contents

<https://bitcoin.org/bitcoin.pdf>

Figure 6 - Complete Voteproject UML & Network Diagram

Figure 7 - Voteproject Decentralized Network Diagram

Figure 8 - Voteproject TkInter Frame Structure

Figure 9 - Voteproject.py UML

Figure 10 - Proof of Concept Authentication Server Architecture

Figure 11 - Voteproject Database Structure

Figure 12 - Voteproject: Connecting to Blockchain

Figure 13 - Voteproject: Committing Blocks To Explorer

Figure 14 - Voteproject: Launching Explorer

Figure 15 - Voteproject: Multichain Explorer Connected

Figure 16 - Voteproject: Launching Voteproject

Figure 17 - Voteproject: Login

Figure 18 - Voteproject: Hash Compare and Address Creation

Figure 19 - Voteproject: Votepage

Figure 20 - Voteproject: Votecoin Creation

Figure 21 - Voteproject: Multichain Explorer Transaction Logs

Figure 22 - Voteproject: Multichain Explorer Transaction Confirmation

Figure 23 - Bitcoin Branching Process

<https://coinsutra.com/bitcoin-double-spending/>

11. Bibliography

[1] FBI director says bureau probing election interference from abroad

<http://www.newsjs.com/url.php?p=http://www.usatoday.com/story/news/politics/elections/2016/09/08/james-comey-fbi-russia/90067608/>

[2] Hackers hit Arizona, Illinois voter databases

<http://www.usatoday.com/story/tech/news/2016/08/29/hackers-hit-arizona-illinois-voter-databases/89547326/>

[3] How old, faulty voting machines undermine American democracy

<http://thehill.com/blogs/ballot-box/278422-how-old-faulty-voting-machines-undermine-american-democracy>

[4] Hackers at DefCon conference exploit vulnerabilities in voting machines

<https://www.usatoday.com/story/tech/2017/07/30/hackers-defcon-conference-exploit-vulnerabilities-voting-machines/523639001/>.

[5] Security Analysis of the Diebold AccuVote-TS Voting Machine

<https://s3.amazonaws.com/citpsite/publications/ts06full.pdf>.

[6] Summary of the Problem with Electronic Voting

https://www.verifiedvoting.org/downloads/revised_summary31.pdf

[7] Bitcoin: A Peer-to-Peer Electronic Cash System

<https://bitcoin.org/bitcoin.pdf>

[8] How Blockchain and ICOs Are Changing the Funding Game for Startups

<https://www.wsj.com/articles/how-blockchain-and-icos-are-changing-the-funding-game-for-startups-1506304861>

[9] IBM Blockchain website

<https://www.ibm.com/blockchain/>

[10] Bitcoin: Fact. Fiction. Future.

<https://dupress.deloitte.com/dup-us-en/topics/emerging-technologies/bitcoin-fact-fiction-future.html>

[11] Electronic Voting Service Using Block-Chain

<http://ojs.jdfsl.org/index.php/jdfsl/article/view/414>

[12] The Key To Unlocking The Black Box

<https://followmyvote.com/wp-content/uploads/2014/08/The-Key-To-Unlocking-The-Black-Box-Follow-My-Vote.pdf>

[13] Observations on Wait Times for Voters on Election Day 2012

<http://www.gao.gov/products/GAO-14-850>

[14] Bitcoin: A Peer-to-Peer Electronic Cash System (2. Transactions | 3. Timestamp)

<https://bitcoin.org/bitcoin.pdf>

[15] Mastering Bitcoin

http://chimera.labs.oreilly.com/books/1234000001802/ch07.html#_the_genesis_block

[16] Multichain Explorer - GitHub

<https://github.com/MultiChain/multichain-explorer>

[17] Multichain White Paper

<http://www.the-blockchain.com/docs/Multichain%20Whitepaper.pdf>

[18] MongoDB Architecture Guide

<https://www.mongodb.com/lp/white-paper/architecture-guide>

[19] Binary JSON Project

<http://bsonspec.org/>

[20] What is Double Spending & How Does Bitcoin Handle It?

<https://coinsutra.com/bitcoin-double-spending/>

[21] A short guide to Bitcoin forks

<https://www.coindesk.com/short-guide-bitcoin-forks-explained/>

[22] Cost of a 51% Attack and Security of Bitcoin, Monero, Litecoin, and other cryptocurrencies

<https://freedomnode.com/blog/86/cost-of-51-attack-and-security-of-bitcoin-monero-litecoin-and-other-cryptocurrencies>

[23] Why Delaware Made It Easier for Businesses to Use Blockchains

<http://fortune.com/2017/08/22/fortune-500-blockchain-ledger-delaware/>