Blockchain as a Tool to Shore Election Confidence and Integrity

Samir Farhat Dominguez

September 20, 2021

1 Problem Statement

In November of 2020, the US presidential elections took place. This election was unique in several distinct ways, many of them due to it being the first federal election taking place during the pandemic. An enumeration of these can be found below.

1. An unprecedented proportion of votes, several magnitudes more than in previous years, were mail-in ballots.
2. Due to social distancing and capacity regulations. Poll watcher numbers were at their lowest, and at times unable to witness all counting activities.
3. Capacity and hygiene regulations meant that several states were unable to count and verify votes at previous rates. Leading to several counting 'pauses' in the process.
4. The country was arguably more politically polarized then ever before, likely due to the economic and societal strain caused by coronavirus and mandates pertaining to these.
5. The first in-the-field use of the Dominion voting system occurred in a several districts, a number of which were contentious and significant in the ultimate results in so-called 'swing states'.
6. Ubiquity of social media and real time updates allowed for dissemination of misinformation and out-of-context videos.

The amalgamation of these factors, led to a never before seen skepticism of the legitimacy of the results of the election. There are several metrics by which this skepticism can be quantified, but the most illustrative of these was that, in the first days after the election, it was reported that about 40% of voters believed that their was "A significant amount of deliberate fraud which may have altered the final results of the election".[6]

1.1 Rationale/Importance

Regardless of what one believes about the legitimacy of the election, it does not take a sociologist, politician or economist to determine that a plurality of voters distrusting election results presents several threats to the stability of a nation, particularly one that finds its identity in expression and democracy. This has been exemplified multiple times since the election. Most notably with the series of protests that culminated in the events at the capitol on January 6th, the stark rise in information distribution control on the part of social media companies, and to a lesser extent the skepticism in the recent California recall election. From a game theory perspective, the current state of affairs is simply unsustainable in terms of maintaining a coherent, healthy, and directed nation.

1.2 Project Focus

While no single project, even with the loftiest ambitions, could ever seek to resolve every single point of contention and risk created in the election, this work will seek to tackle a somewhat compartmentalized point of contention. The Dominion voting system, including its hardware, native software, and its network infrastructure.

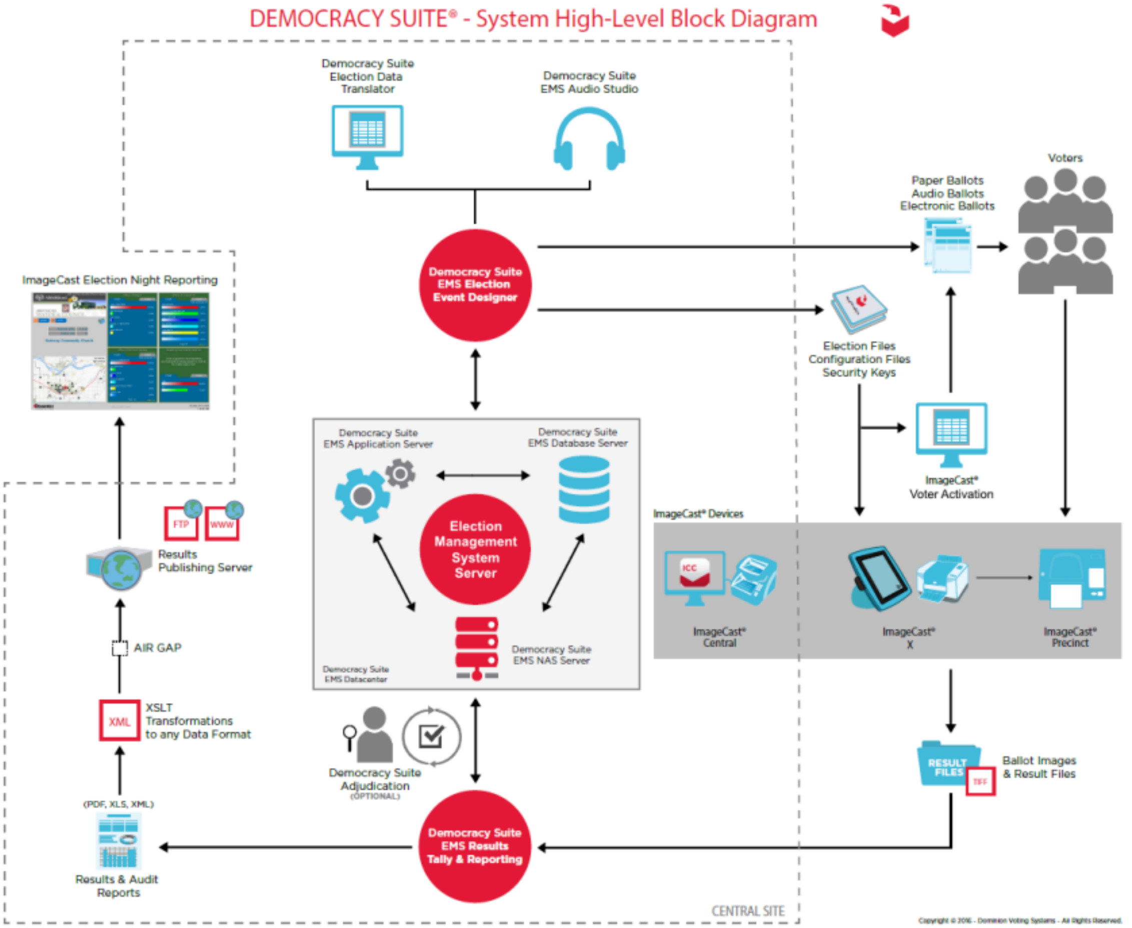

DEMOCRACY SUITE® - System High-Level Block Diagram
Democracy Suite Election Data Translator
Democracy Suite EMS Audio Studio
Democracy Suite EMS Election Event Designer
ImageCast Election Night Reporting
Democracy Suite EMS Application Server
Democracy Suite EMS Database Server
Election Management System Server
Democracy Suite EMS NAS Server
Democracy Suite EMS Datacenter
FTP
WWW
Results Publishing Server
AIR GAP
XML
XSLT Transformations to any Data Format
(PDF, XLS, XML)
Results & Audit Reports
Democracy Suite Adjudication (OPTIONAL)
Democracy Suite EMS Results Tally & Reporting
Voters
Paper Ballots Audio Ballots Electronic Ballots
Election Files Configuration Files Security Keys
ImageCast® Voter Activation
ImageCast® Devices
ICC
ImageCast® Central
ImageCast® X
ImageCast® Precinct
RESULT FILES
TIFF
Ballot Images & Result Files
CENTRAL SITE
Copyright © 2016 - Dominion Voting Systems - All Rights Reserved.

Figure 1: Block diagram of the native and virtualised Dominion voting scheme[7]

Specifically, allegations about data manipulation, miscounts, illegitimate votes and other oddities in the Dominion machines and systems to cast and count votes in numerous voting districts during the November election. While this work does not seek to engage with the veracity of these allegations, it seeks to produce a system with the security mechanisms and transparency that would either definitively prove these allegations, or definitively establish the integrity of this aspect of the election. This work will also develop a solution that is significantly more cost-effective, as the decentralization of blockchain allows for fair pricing, when compared to the federal 'carte blache' given to Dominion.[9]

1.3 Project Proposal

The proposal of the project is to utilize the growing technology known as blockchain, and its numerous strengths in terms of security and transparency, to supplant the current E-voting system which Dominion is a part of. The specifics of achieving this, will be delineated in the following sections of the report, after a brief discussion of what a blockchain is and offers.

2 Literature Review

2.1 Blockchain

Blockchains are cryptographically secure, distributed ledgers which can hold records on any smart contract that is called on the blockchain. As the name entails, it is a sequence of blocks linked cryptographically, usually by hashing the timestamp associated with each new data creating event.[1] These blocks each contain information on any supported smart contracts called on the chain, most commonly individual transactions and movements of the cryptocurrency they maintain. This is depicted in the figure below

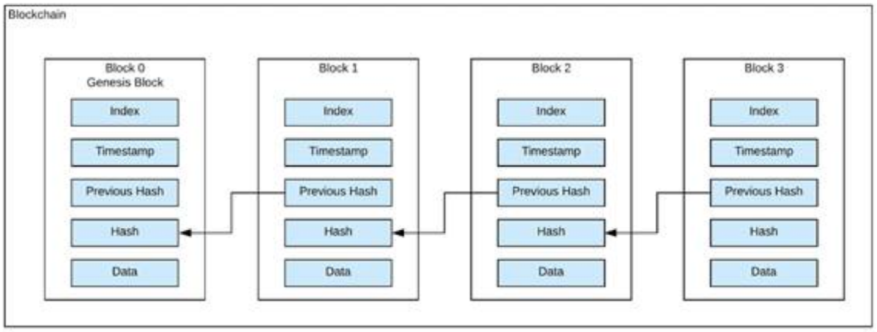


Figure 2: Applications supported on the NEO blockchain

A blockchain often uses multiple separate servers which function as nodes. These nodes record, share, and synchronize the transactions in their respective electronic ledgers. This is what allows them to maintain their two strongest selling points, decentralization and security. A natural consequence which emerges from multiple devices across different networks verifying and checking against each other to ensure the blockchain has not been modified or tampered with by an outside entity.[1] This characteristic, alongside strong cryptographic protocols, make blockchains almost completely resistant to modification, which is inimical to ensuring the security and reliability of the ledger.

As a result, the only known adverse event that could feasibly lead to the manipulation of a blockchain is a '51 percent attack' or '67 percent attack' depending on the validation algorithm run by the blockchain. This attack, as the name indicates is one where either half or two-thirds of all nodes/miners running on a blockchain were to be compromised and hash blocks with incorrect or manipulated data. Taking Bitcoin as an example, it has been shown that no single individual, entity, institution, or government possesses enough computing power to perform this sort of attack and overwrite the ledger. While Bitcoin is the blockchain with the most computing power at its disposal, most mature and adopted blockchains possess enough computing power that from a risk assessment perspective, the probability of a successful attack is infinitesimally small. In addition to this, almost all blockchains have oracles and built in smart contracts to freeze or protect the blockchain should an attack be detected.

Users and programs can interact with a blockchain through a construct known as a smart contract.[5] In the context of blockchains, smart contracts represent programs that delineate transaction protocols. Essentially, they are highly secure algorithms that control the distribution and ownership of a cryptocurrency. The network of nodes that maintain the blockchain verify that the smart contracts have not been tampered with.[1] A simple example of a smart contract process would be when a fee payment is made to the Ethereum blockchain. When a user completes a payment, a program sends the record of this transaction to a smart contract, which updates the blockchain to include this movement of funds and issues the corresponding Ethereum to the cryptocurrency wallet associated with the user. This transaction record is then synchronized with all the nodes in the blockchain.[5]

For the purposes of this project, we will explore those blockchains that support the following services:

- In chain, third party tokens
- Token distribution
- Token ownership
- Public block explorer and private address system.
- Non-fungible token attribution.

This will allow for a system to be created where voting tokens are given on a one-to-one basis for voters, and voters can cast their vote through the execution of a smart contract. Said smart contract will track data that will allow to verify the validity of a vote, while maintaining the anonymity of the voter. Alternatively, votes could be cast as a non-fungible token, once again ensuring that the owner of the token is a legitimate voter through calling a smart contract on the chain.

From the perspective of cost, all that would be needed is for the federal government enough gas currency(cryptocurrency required to run smart contracts on a blockchain) to perform the 10s of millions of votes on the chain. Considering that each dominion voting machine cost upwards of 100,000 dollars, the gas fees would almost certainly be cheaper. This will not be fully explored till later on in the development of the project.

3 Open Source Research

Fortunately, most blockchains, cryptocurrencies, and tokens are open source. So we truly do have our pick of the bunch when selecting a blockchain to build on.

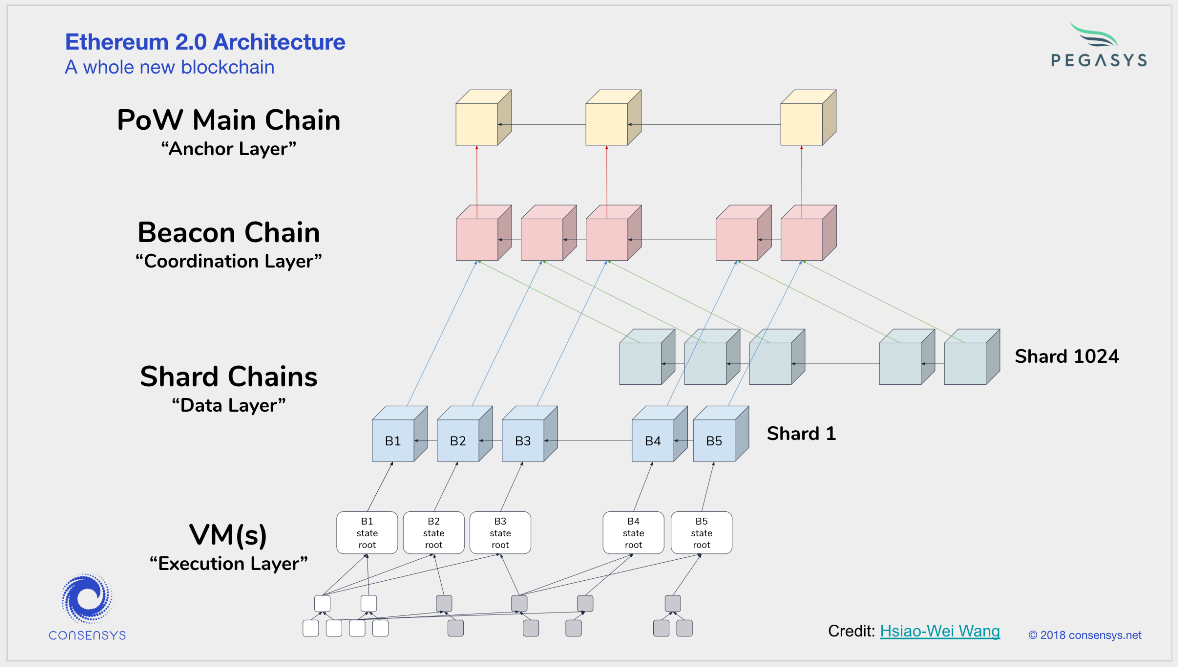
3.1 Bitcoin

While the discussion on Bitcoin, will be brief,and ultimately dismiss the blockchain, its status as the most widely adopted and famous blockchain means its always worth mentioning. Bitcoin,in its current state only supports token ownership and distribution, nowhere near our established requirements for the blockchain voting system proposed. Additional, the cost of transaction and node confirmation/consolidation times are prohibitively long. That being said, Bitcoin and its creator are of tremendous importance in the creation of digital currencies and blockchains.[2]

3.2 Ethereum

Without a doubt, the Ethereum network and ERC-20 protocol is the most developed, robust, matured, and proven blockchain system out there. Also called the 'World Computer', Ethereum allows for on-chain third party tokens, token distribution, token ownership, public block explorer, non-fungible token attribution and private address system. Additionally, Ethereum allows for the outsourcing of computation, governance systems, complex oracles, test net experimentation and many other use cases. On the downsides, Ethereum's gas token, ETH, is notoriously expensive and block times are rather slow.[3]

However, the Ethereum blockchain is expecting a massive upgrade dubbed ETH2.0, estimated to take place in 2024. This would theoretically resolve the issues with gas fees and block time.



Credit: Hsiao-Wei Wang

© 2018 consensys.net

Figure 3: Proposed architecture of ETH 2.0

3.3 NEO

NEO is not as developed as ethereum, but still contains the necessary services to develop the voting system. Additionally,its gas fees and block times are exceptional, and its block explorer API would be tremendously useful to create a voting transparency application.[4]

Figure 4: Applications supported on the NEO blockchain

3.4 Algorand

Algorand only recently implemented a fork capable of NFT creation. Its block times and gas fees also makeit exceptional among the competition. [8]

4 Duplicate the Results

You can find, on the github repository, an example of NFT creation and deployment on a public Ethereum testnet.

References

[1] E. Shi Z. Wen A. Kosba, A. Miller and C. Papamanthou. Hawk: The blockchain model of cryptography and privacy-preserving smart contracts. *2016 IEEE Symposium on Security and Privacy (SP)*, pages 839–858, 2016.

[2] Eric Budish. The economic limits of bitcoin and the blockchain. Technical report, National Bureau of Economic Research, 2018.

[3] Monika Di Angelo and Gernot Salzer. Tokens, types, and standards: identification and utilization in ethereum. In *2020 IEEE International Conference on Decentralized Applications and Infrastructures (DAPPS)*, pages 1–10. IEEE, 2020.

[4] Elad Elrom. Neo blockchain and smart contracts. In *The Blockchain Developer*, pages 257–298. Springer, 2019.

[5] Antonio Fatas. *The Economics of Fintech and Digital Currencies*. CEPR Press, 2019.

[6] Emilio Ferrara, Herbert Chang, Emily Chen, Goran Muric, and Jaimin Patel. Characterizing social media manipulation in the 2020 us presidential election. *First Monday*, 2020.

[7] Joshua Franklin and Jessica Myers. Interpreting babel: classifying electronic voting systems. In *5th International Conference on Electronic Voting 2012 (EVOTE2012)*. Gesellschaft für Informatik eV, 2012.

[8] Yossi Gilad, Rotem Hemo, Silvio Micali, Georgios Vlachos, and Nickolai Zeldovich. Algorand: Scaling byzantine agreements for cryptocurrencies. In *Proceedings of the 26th symposium on operating systems principles*, pages 51–68, 2017.

[9] Isabel Murdock, Kathleen M Carley, and Osman Yagan. Multi-platform analysis of 2020 us election fraud and protest related posts.