Devote: A blockchain voting system

Finlay Campbell

finlay.business@protonmail.com

Introduction:

Devote is a blockchain based voting system which aims to provide a trust-less, open source [1] and secure means of voting in any given scenario. Devote can be developed and deployed in many ways, which can improve the security and trust from the end users and improve efficiency of the voting system in these given scenarios.

[1] trust-less and open source – a system which does not rely on a single source, node, or entity, in this case with an open source, blockchain based solution.

In this modern-day society, trust is diminished by corruption, greed and hunger of rulers and other governing entities. While this does not apply to every person in power, to achieve the highest level of functioning as a growing and changing society, there should be a system that the masses can trust, not just a solution we are told is trustworthy. With verifiable code instead, which is accessible to both rich and poor, influential, or powerless. This does not just apply to voting either, as many parts of our society face the same issue. We have seen the start of a switch to cryptocurrencies, the finance sector being revolutionized by decentralization and blockchain based solutions, with the masses gaining interest in the benefits cryptocurrencies can provide. We hope Devote can carry some of these aspects across to voting. This is not all without stigma, of course, but that is only natural with change. With publicly accessible source code, Devote and other blockchain based applications can be trusted and verified based on the source code. This makes our goal of creating a blockchain based voting platform achievable for the masses to adopt, accept and appreciate.

How does Devote work?

Devote is a blockchain based voting application, but is not a cryptocurrency, therefore, there are some major differences. These differences make Devote a unique product with new functionality, taking aspects from other blockchain based applications which will be useful in terms of security for Devotes intended purpose.

The base:

The base of Devote is a flask server application which accepts HTTP POST and GET requests in the form of “voting” or “check vote”. The /vote url will only accept POST requests with the arguments “recipient”, “sender” and “proofofwork” and not GET requests. The server then creates a block with the variables sent over and the block index, the timestamp, the current hash, previous hash and unique voter ID. The /checkvote url will only accept GET requests with the arguments “id_to_get” and “hash_to_get” and not POST requests. The server then checks the blockchain for a block which contains the hash and unique voter ID.

The Variables:

The variables are as such:

block_id: The id or index of the block, incremental

timestamp: The current time of block being added

sender: The person voting

block_content: The person being voted for

proof_of_work: The proof of work which was calculated

current_hash: A sha256 hash constructed of the sender, recipient, the current time and proof of work

previous_hash: The hash from the previous block

unique_id_num: A unique number given out, such as social security number, to be able to identify voters aside from name

The genesis:

Similarly, to Bitcoin, the genesis block is hard coded, with no real purpose other than to have at least one entry in the chain, to make sure the block creation works and to serve as a reference to the start of the chain.

The start of the server script checks if there is a genesis block in main-chain.csv. If there is, it skips the genesis creation and allocates the previous hash and chain counter. If the genesis block does not exist, the addGenesis function will be called which will add the genesis block to the chain.

The client:

The first choice of the client accepts three variables, who is voting, who is being voted for and the unique voter ID. It will then calculate the proof of work and send the POST request with the sender, recipient, unique voter ID and proof of work and shows the block that was made, assuming there were no errors.

The second choice in the client accepts two variables, the current hash of the vote and the voter id that the client wants to check is included in the ledger. It then sends a GET request with the hash where the server returns the block that the hash is in, if it exists in the ledger.

Proof of Work:

The proof of work serves as an anti bot and an extra layer of security by making every user required to compute a hash of a certain difficulty. Wikipedia describes proof of work as:

"a form of cryptographic proof in which one party proves to others that a certain amount of a specific computational effort has been expended."

Link: https://en.wikipedia.org/wiki/Proof_of_work

The Security:

There are multiple security measures integrated within Devote to protect the end user, the chain and the server.

Blockchain: Blockchain is used to prove that all votes are counted within a digital ledger, and to guarantee all votes are counted.

API: The API will only allow POST/GET methods with certain parameters.

Checksum: A checksum of both the client and server will be generated at the start of the scripts, this will guarantee the files have not been altered before use. (NOT IMPLEMENTED YET)

Unique Voter ID: A unique voter ID is input, which adds a controlled but random variable to the block which stops people being able to check blocks that are not theirs.

<u>What problems will devote solve?</u>

Devote will solve a couple of issues with the current voting system, and open up the door for more to be solved with further development and adaptions.

One of these issues is verifying that your vote was counted. Since a blockchain can be a part of a ledger, each entry can be searched for and displayed. As a hash is given, a given user

can search for that hash with their unique voter ID and guarantee that the block was counted. This also eliminates human error in forms of counting votes.

Another issue is regarding people's voting ability and how difficult it is for some people to get out and vote, juggling a busy lifestyle. Devote can be deployed in many different situations and as many different program types, meaning anyone can access Devote and vote.