The Presidency Protocol

Blockchain Based Centralized Government

Hassib Ashouri, Jenil Thakker

April 11, 2019

1 Abstract

In this proposal for a cryptocurrency, we try to target the problem of government not able to track cash flow in the system, large amount of cash is black market, and fraudulent businesses. Also, the notion of sales tax will be implemented to allow money to be owned by the govenment at the time of the transaction. Our protocol (protocol name) will digitize the economy of a country. To ensure Sybil resistance, we implement a consensus algorithm called Delegated-Proof-of-Democracy (DPoD) that trusts a subset of the nodes to be delegates that verify transactions. While this approach has some centralized aspect to it, it is in the interest of a government to hold some power over the system.

2 Sybil Resistance

2.1 Consensus Protocol

The Presidency Protocol utilizes a modified delegated proof-of-state consensus algorithm, that allows participating voters to elect multiple delegates. DPoS is similar to PoS, but instead of stakeholders creating and validating the blocks, they nominate N number of witnesses to do it on their behalf. The elected delegates can collectively validate a transaction and obtain an even share of the miner rewards [2].

In order to prevent the formation of sybil identities and biased voting strategies, every node willing to participate in the election establishes a unique identity. This unique identity is a social security number (SSN) that can be purchased from the government entity for a small fee. This allows the government to monitor and check whether a node is eligible to vote.

2.1.1 Delegated-Proof-of-Democracy

The consensus algorithm follows the following procedure:

1. Registering to vote: In order for a node to vote in the elections, the government checks for a valid digital SSN (Boolean value). If the node does not possess a valid digital SSN, it can choose to purchase one for a small fee of 5 JH-Coin. Note the nodes who do not wish to take part in the elections still have the ability to do transactions with different peers.

2. Electing delegates: Eligible nodes (voters) can then vote for trusted delegates who can validate transactions. DPoD selects the top four voted nodes and appoints them as delegates. After the addition of each block to the blockchain, a re-election takes place, giving chance to the remaining nodes to become a delegate [3].

3. Validating Transaction: The four elected delegates can then vote (validate-counter) for a valid transaction. If the predefined threshold of three votes or 75 percent is achieved, the transaction is flagged as valid. A set of validators with at least 2/3 of total voting power is also called a 2/3 majority of validators. Similarly, a set of validators with at least 1/3 of total voting power is called a 1/3 majority of validators [1].

2.1.2 Mining

The process of mining is performed by the elected group of delegates, who aim for gain mining rewards. These mining rewards are aggregated from the transaction fees and stored in a reward pool, which is not accessible to the government entity, to prevent any corrupt motives.

3 Novelty

The novelty of this system is in it's ability to eliminate cash money that could flow through the black market, give the government direct acess to sales tax money at time of transaction, therefore preventing businesses to misreport their sales tax.

4 Cryptocurrency

To describe the operations of the cryptocurrency, we need to specify the functionality of the abstract components of the system.

4.1 Government

The government component of the system is the heart of the sibyl resistance in the system. The government will validate clients wanting to participate in the voting process by give the client a Boolean value the represents its ability to be part of the voting process for a fee paid by the client (citizen). The government also is the entity where the tax money collected from transactions will go to allowing the government direct access to sales tax money versus acquiring it by the end of the every year.

4.2 Blockchain

The blockchain will be used to maintain the public ledger of the transactions. Since the we don't use PoW for consensus, the block do not need to have a solution type of information.

4.3 Client

The client here is synonymous to a citizen who makes the transactions as purchases that happen on the blockchain. Clients can register to vote and be approved by the government to do so. With that ability clients can participate in the process of electing the delegates that will do the mining. These clients will pay fees with their transactions that consists of tax and mining fees.

4.4 Wallet

The wallet component in this cryptocurrency is one store keys generated for each transaction. This means that everyone wallet will hold the keys to the key that it can unlock.

4.5 Conclusion

We present a novel blockchain-based consensus protocol, Delegated Proof-of-Democracy that allows the government to retain their authority while securely collecting taxes from the citizens. However, only one of the proposed notions of voting and transactions (taxes) may be implemented, given the short time constraint. The authors of this protocol are also aware of potential vulnerabilities that might allow citizens to cheat, however, those will be mitigated to the best of our efforts.

References

[1] Jae Kwon. Tendermint: Consensus without mining. *Draft v. 0.6, fall*, 2014.

[2] A Shahaab, B Lidgey, C Hewage, and I Khan. Applicability and appropriateness of distributed ledgers consensus protocols in public and private sectors: A systematic review. *IEEE Access*, 2019.

[3] Brent Xu, Dhruv Luthra, Zak Cole, and Nate Blakely. Eos: An architectural, performance, and economic analysis.