10 PRINCIPLES FOR BLOCKCHAIN GOVERNANCE

by DONALD MCINTYRE

Founder of ETHERPLAN

Email: donald@etherplan.com

Twitter: @TokenHash

1. Trust Minimization: To reduce the reliance on trusted third parties for entering, processing and finalizing transactions and smart contracts.

1. Trust Minimization: To reduce the reliance on trusted third parties for entering, processing and finalizing transactions and smart contracts.

Trusted third parties are security holes because:

- They hold our money and wealth
- They hold our personal data
- Manage everything on centralized servers
- They can be hacked
- They can behave badly

Traditional trusted third parties are, amongst others:

- Banks
- Credit card companies
- Tech companies and apps
- Certification authorities
- Corporations
- Governments

1. Trust Minimization: To reduce the reliance on trusted third parties for entering, processing and finalizing transactions and smart contracts.

Blockchains have trusted third parties as well:

- Developers
- Miners
- Validators
- Node operators
- And other kinds of participants and stakeholders

However, blockchains are trust minimized because:

- They have no central authority
- Data is distributed amongst many nodes globally
- Cryptographic components protect property and agreements
- The consensus mechanism prevents tampering
- The coordination problem prevents community collusion

1. Trust Minimization: To reduce the reliance on trusted third parties for entering, processing and finalizing transactions and smart contracts.

So, what problems does trust minimization solve?

- Eliminates central control and authority of blockchain networks
- Significantly reduces vulnerability to single points of failure
- Reduces trusted third party costs
- Reduces trusted third party delays
- Expands access to larger populations worldwide

2. Immutability: Accounts, balances and smart contracts cannot be modified except by holders of corresponding private keys by entering transactions according to protocol rules.

2. Immutability: Accounts, balances and smart contracts cannot be modified except by holders of corresponding private keys by entering transactions according to protocol rules.

Immutability is really about the integrity of property and agreements.

Property and freedom of contract are represented by accounts, balances and smart contracts on public blockchains, therefore they need to be immutable to protect property and agreement security.

2. Immutability: Accounts, balances and smart contracts cannot be modified except by holders of corresponding private keys by entering transactions according to protocol rules.

The phrase “corresponding private keys” means that there should not be any alternative way of modifying accounts, balances and smart contracts. That includes, but is not limited to, hard forks, changes of state, ad hoc transactions, backdoors, or third party account freezing mechanisms.

3. Fungibility: Native tokens must all be the same and interchangeable globally.

3. Fungibility: Native tokens must all be the same and interchangeable globally.

Establishing the native token as a generally accepted medium of exchange significantly helps the underlying economics of a blockchain network. It is an important component of the price system due to its common acceptance, ability to communicate price information, ease of use, and reduced mental costs.

4. Finality: Transactions and executed smart contract code cannot be reversed once entered, processed and finalized according to protocol rules.

4. Finality: Transactions and executed smart contract code cannot be reversed once entered, processed and finalized according to protocol rules.

Irreversibility creates certainty and helps the free and continuous circulation of capital globally.

Blockchains, with their shorter finality turnover times, also reduce capital costs in the economy by freeing capital faster and reducing settlement and transaction default rates.

5. Censorship resistance: As long as they are compliant with protocol rules, transactions or smart contracts cannot be prevented from being entered, processed and finalized.

5. Censorship resistance: As long as they are compliant with protocol rules, transactions or smart contracts cannot be prevented from being entered, processed and finalized.

Censorship resistance is about not censoring transactions or smart contracts.

6. Permissionlessness: As long as they are compliant with protocol rules, anyone from any place in the world can create accounts, enter transactions and smart contracts, or participate in the network as a competent developer, miner, validator, node operator, user, or any other prescribed participant or stakeholder.

6. Permissionlessness: As long as they are compliant with protocol rules, anyone from any place in the world can create accounts, enter transactions and smart contracts, or participate in the network as a competent developer, miner, validator, node operator, user, or any other prescribed participant or stakeholder.

Permissionlessness is similar to censorship resistance, but is really about not censoring people.

Censoring users, or any other network participant or stake holder, by geography, nationality, culture, ideology, or any other human condition should not be allowed.

7. Auditability: Transaction and smart contract history must be analyzable and reconcilable by anyone or by holders of corresponding private keys.

7. Auditability: Transaction and smart contract history must be analyzable and reconcilable by anyone or by holders of corresponding private keys.

Auditability is about the availability of information for verification purposes. The phrase “or by holders of corresponding private keys” applies in the case of zero-knowledge blockchains where the information may not be available publicly, but it should be to account and smart contract private key holders.

8. Reconcilability: Transaction and smart contract history must match mathematically to the latest and all future states according to protocol rules.

8. Reconcilability: Transaction and smart contract history must match mathematically to the latest and all future states according to protocol rules.

Reconcilability reinforces immutability because it solves two controversial points in blockchain debates:

A. It invalidates the argument that a change of state or ad hoc transaction does not violate immutability because they don't change the transaction or smart contract history. Example: TheDAO hard fork.

B. It invalidates the argument that when there is out of blockchain proof of private key ownership, then a change of state or arbitrary ad hoc transaction is valid. Example: EIP 867 that proposed a standard for funds recovery on Ethereum.

9. Least authority: Developers, miners, validators, node operators, users, and all other prescribed participants and stakeholders must limit their participation to practicing only the functions of their roles in accordance with protocol rules and these common principles.

9. Least authority: Developers, miners, validators, node operators, users, and all other prescribed participants and stakeholders must limit their participation to practicing only the functions of their roles in accordance with protocol rules and these common principles.

To ensure social scalability, blockchain communities need to focus on network functionality, security, and new features. All legal, ethical or moral considerations need to be set aside and resolved off-blockchain between the private parties.

10. Adherence: Developers, miners, validators, node operators, users, and all other participants and stakeholders must make sure they collectively decide and implement future changes to the protocol in accordance with these common principles.

10. Adherence: Developers, miners, validators, node operators, users, and all other participants and stakeholders must make sure they collectively decide and implement future changes to the protocol in accordance with these common principles.

To guarantee the benefits of trust minimization, immutability, property rights, freedom of contract, wide adoption, and social scalability of their networks globally, blockchain communities need to make sure they comply with these principles when implementing future changes.

10 Principles for Blockchain Governance

1. Trust Minimization: To reduce the reliance on trusted third parties for entering, processing and finalizing transactions and smart contracts.

2. Immutability: Accounts, balances and smart contracts cannot be modified except by holders of corresponding private keys by entering transactions according to protocol rules.

3. Fungibility: Native tokens must all be the same and interchangeable globally.

4. Finality: Transactions and executed smart contract code cannot be reversed once entered, processed and finalized according to protocol rules.

5. Censorship resistance: As long as they are compliant with protocol rules, transactions or smart contracts cannot be prevented from being entered, processed and finalized.

6. Permissionlessness: As long as they are compliant with protocol rules, anyone from any place in the world can create accounts, enter transactions and smart contracts, or participate in the network as a competent developer, miner, validator, node operator, user, or any other prescribed participant or stakeholder.

7. Auditability: Transaction and smart contract history must be analyzable and reconcilable by anyone or by holders of corresponding private keys.

8. Reconcilability: Transaction and smart contract history must match mathematically to the latest and all future states according to protocol rules.

9. Least authority: Developers, miners, validators, node operators, users, and all other prescribed participants and stakeholders must limit their participation to practicing only the functions of their roles in accordance with protocol rules and these common principles.

10. Adherence: Developers, miners, validators, node operators, users, and all other participants and stakeholders must make sure they collectively decide and implement future changes to the protocol in accordance with these common principles.

Credits and Suggested Videos and Reading

- Trusted Third Parties are Security Holes by Nick Szabo: http://nakamotoinstitute.org/trusted-third-parties/

- The Problem of Trust by Vitalik Buterin: https://blog.ethereum.org/2015/04/27/visions-part-2-the-problem-of-trust/

- Interpreting Power: The Principle of Least Authority by Nick Szabo: http://archive.is/mtixJ#selection-195.0-195.52

- Governance by Vlad Zamfir: https://youtu.be/w8DjFbCTjus

- Notes on Blockchain Governance by Vitalik Buterin: https://vitalik.ca/general/2017/12/17/voting.html

- Bitcoin's Anarchy Is a Feature, Not a Bug by Elaine Ou: https://www.bloomberg.com/view/articles/2018-03-14/bitcoin-blockchain-demonstrates-the-value-of-anarchy

- Against on-chain governance by Vlad Zamfir: https://medium.com/@Vlad_Zamfir/against-on-chain-governance-a4ceacd040ca

- Scaling and Blockchain Governance by Donald McIntyre: https://youtu.be/DJCnUrrgKzs

- Note: Fourteen references by Satoshi Nakamoto about trusted third parties and reducing trust on the Bitcoin white paper: https://bitcoin.org/bitcoin.pdf

THANK YOU

by DONALD MCINTYRE

Founder of ETHERPLAN

Email: donald@etherplan.com

Twitter: @TokenHash