Daniel Larimer
Jun 21 · 8 min read

Decentralized Blockchain Governance

We, the EOS community, have embarked on a grand experiment to see if a global community can govern itself without the well documented pitfalls of existing world governments. Bitcoin was created as a “trustless” money system because the governance structures in control of the world monetary system abused their power to exercise undue influence over world governments and their populations.

If we are to understand the value of decentralized blockchain governance, then we must first understand what problems with central bank governance that blockchains were created to solve.

1. Unpredictable Monetary Policy
2. Uncontrollable Government Spending
3. Instability of Debt-based Money
4. Fraudulent use of Bank Deposits
5. Capital Controls
6. Identity Theft

7. Moral Hazard of Bailouts

The global population is powerless to prevent world governments from consuming our capital base so long as we rely upon their currencies. Through limitless money printing, governments and the banks that fund them can confiscate the majority of the world's resources without a tax revolt. It isn't until years later when the economy slumps under the burden of prior capital consumption that people notice what happened.

With Bitcoin and early smart contract platforms came the concepts that "code is law" and "hash power makes right". This combined with the belief in censorship resistance gave people a new level of "trust" in the monetary governance. The big idea is that we should remove all of the potentially corrupt people from the equation. With no one in charge the rules can never change and we can be free of corruption, confiscation, inflation, and capital controls.

Has Bitcoin & Ethereum Improved Things?

For the past 10 years we have had the opportunity to observe a live experiment in the effectiveness (or ineffectiveness) of blockchains in protecting people from loss of funds. I have created a list of all the ways people lose money under existing governments and under code-is-law.

Losing Money & Freedom on Blockchain

1. Forget Password / Lost Keys
2. Keys Compromised
3. Phishing Scams
4. Exchange Hacks
5. Bugs in Code
6. Double Spend Attacks (multiple chain reorgs)
7. Mugging / Kidnapping / Extortion
8. Social Engineering
9. Capital Gains Taxes
10. Government Seizing Tokens
11. Supply Growth

12. Fees
13. False Sense of Privacy from All
14. Denial of Service by Spam
15. Send to wrong Address

Losing Money & Freedom in Banks

1. Seizing Bank Accounts by Court Order
2. Bank Defaults not covered by Deposit Insurance
3. Identity Theft
4. Supply Growth
5. Fees
6. Capital Controls / Denial of Service by AML / KYC Compliance
7. Loss of Privacy to Government, Private from neighbors.
8. Credit Card Fraud passed on to Merchants

For the average man, their money is far more vulnerable in cryptocurrency than it is an bank account. This is especially true for the vast majority of people who manage to stay on the right side of the law. Like it or not, the AML / KYC rules combined with insurance on credit cards and bank deposits protect people from many crimes because it is harder to hide your identity and move money. If your bank password is compromised the bank eats the loss, not you. If your bank loses all of its money, insurance backed by inflation covers the losses. If you lose your password the bank can validate your identity and give you your money back. If the bank makes a mistake in authenticating a withdraw, the bank is liable for the losses.

What we can conclude from this is that despite corruption in the monetary policy, individual users are far more secure in the existing banking system than in the existing blockchain systems. This is because the existing banking system socializes most of the losses. The negative externalities of the corruption in monetary governance are imperceivable for the individuals, but the failures of blockchain security to individual accounts is well documented.

I don’t have exact numbers to prove it, but I suspect that the loss of funds due to smart contract bugs and hacks is greater than the loss of

individual funds due to bank failures/hacks/corruption as a percentage of the respective dollar/token economies.

Making Blockchains Safe for Users

The primary cause of loss of funds is losing passwords and/or transferring funds by mistake. The next most common problem is the use of software keys which get compromised. Hardware wallets can mitigate the loss of funds due to compromised software keys, but they are powerless against losing the physical keys or forgetting the pin that protects the device. Hardware keys also do little to protect users from attacks that attempt to trick people into signing the wrong thing. Furthermore hardware devices can fail or be stolen. All of this together means that relying on hardware alone is like losing a physical key to an impenetrable home safe.

One thing that the existing banking system does is make people safer from physical mugging and/or home invasions. Thieves know that people don't carry cash on them and that they cannot easily get away with forcing someone to log into their bank and transfer funds. With cryptocurrency, the only way to protect yourself from similar situations is to rely on a trusted party to co-sign your transactions. This might prevent the mugger from getting your tokens, but it doesn't stop you from being mugged in the first place. In order to minimize risk of mugging, the vast majority of people must adopt multi-sig accounts with trusted 3rd parties (e.g. banks). This is similar to the concept of herd immunity.

The Code is Law Myth

There is widespread belief that there is no "governance" of Bitcoin or Ethereum and that these protocols are decentralized. There is further a belief that the code should be law. In reality all blockchains have human governance processes that reveal themselves in emergencies and when the protocol upgrades. All code has bugs; and bugs in the law create injustice and violation of expected property rights.

Ethereum's shadow-government hard-forked to fix the DAO hack. Bitcoin mining pools voted on which fork to support when a software upgrade introduced a long unintended fork. The Ethereum foundation has used Trademark law to define the official version of the chain that exchanges are allowed to list. Segwit was accepted due to a summit of community leaders who voted on a compromise that included

increasing the block size only to be betrayed due to the phased-rollout plan that later abandoned big blocks.

Large miners have cornered the market on ASIC with the benefit of economies of scale. Mining pools have cornered the market on block production (2–3 pools control Bitcoin and Ethereum). Fees (aka producer bribes) have risen to be higher than bank transfers. Lightning networks create new bank-like-intermediaries and are vulnerable to censorship attacks by mining pools and ASIC cartels.

Every blockchain that has a "process for upgrading" has a governance structure that is capable of changing the rules, rolling back stolen funds, etc. It is the good-old-boy network of Github admins, exchange connections, and mining pool operators. The problem is that these processes are informal and less predictable and even less accountable than the governmental structures we hope the blockchains would replace. Insiders take stealth control of these informal processes while the masses perceive coordinated governance chaos.

EOS Solution to Decentralized Governance

EOS is taking a new approach to solving the problems with centralized governments that doesn't throw the baby out with the bathwater. In this case, the baby is civilized dispute resolution among consenting adults along with the broader concept of peer to peer community enforced contracting.

The EOS community constitution aims to establish a set of principles which differentiate it from existing centralized governments and from all prior blockchains. For starters, it makes a commitment to non-violent governance. All parties agree that disputes may only be resolved by appending to the blockchain. If world governments had this clause they couldn't throw you in jail or start wars. If you didn't like their taxes, their policies, their regulations, you could just leave. This is a ***FUNDAMENTAL*** difference in how a global community can govern itself without repeating the mistakes of existing governments.

The EOS constitution also establishes a formal process and basis of authority by consent. Those who do not consent can take the open source code and start their own community with their own rules. Unlike traditional governments which have monopolized the livable land area, there's always a new frontier for freedom loving people to experiment with new governance structures. All it takes is a large

enough group of like-minded individuals to bootstrap a new community and compete against any corrupted community.

This free market competition in community governance introduces market forces to the governance equation. A blockchain that is operated by a corrupt dispute resolution system will see its currency sold in the market as people leave in droves seeking safe haven in new communities that better protect their rights. Only the most universally competent dispute resolution systems and blockchains will survive. Communities that enact unpredictable monetary policies contrary to their constitution will see their tokens fall in value rapidly in favor of more responsible communities.

Blockchains create a far more efficient market because there is no captive population forced to use the currency at gunpoint. Furthermore, there is no geographical constraints that force a person to use the same currency as their neighbors.

Enforcement of Contracts

Blockchains are designed to execute objective and deterministic contracts. Arbitrators are designed to be oracles for subjective evaluation of non-deterministic contracts. EOS combines these two concepts with the goal of minimizing the opportunity for dispute, maximizing the quality and transparency of evidence of agreement, and creating the technical tools to allow human intervention to correct bugs in execution or violations of subjective agreements.

In this sense, EOS is the first contracting platform focusing on formalizing, automating, and clarifying agreements among consenting well-intentioned adults. This is far broader and more powerful than blindingly enforcing bug-ridden contracts without any respect to the intention of the parties.

Baby Steps

EOS is a new community building the tools necessary to achieve this vision of a global community governing itself without the use of violence. Over time the community will formalize arbitration processes, constitutional amendments, division of power, and limitations of liability. In the meantime the community is using the tools it has today to enforce its contracts and combat the blatant fraud & theft so prevalent in the cryptocurrency industry.

If everything develops as I hope, the EOS community will be the safest place to hold tokens without fear of unjust rulings, identity theft, token hacks, lost passwords, etc. It will have stable monetary policy with civilized dispute resolution.

There will be bad actors and communities will live or die based upon how quickly they identify and removes them. All other blockchains are incapable of removing bad actors because they are not based upon the premise of contractual cooperation for a common good, but instead upon the premise of the law of the jungle where technical might makes right. Brains are the new brawn and nerdy cavemen are arguing that they have the divine right to whatever property they can hack. When hacks do occur, people resort to violence at the hands of governments they ask to track-down and punish the hackers and scammers. EOS is fundamentally different from other governments and blockchain communities in that its community wishes to operate at the highest possible ethical standard of voluntary consent and non-violence.

Where as other blockchain communities rely on existing governments to get retribution, EOS is the first blockchain to take responsibility for its own community and not depend upon the corrupt, violent, legacy dispute resolution systems. EOS is designed to focus on restorative restitution rather than punitive retribution.

It is my hope that the EOS community can level the playing field and secure life, liberty, property, and justice for all.