Duke CS+ Summer 2021: Decentralized Finance: Cryptocurrency and Blockchain on the Internet Computer: https://ic.pubpub.org/pub/7ms2ilwh/

On-Chain Governance: Liquid Democracy on Blockchain

By Malika Rawal

Project Leads: Profs. Luyao Zhang, Yulin Liu, Kartik Nayak, Fan Zhang
Graduate mentor: Derrick Adam

Project Summary

As a product of the interaction between Chain and Key technology and the NNS (Network Nervous System), the Internet Computer has the potential to break big tech's trillion-dollar industry. Dfinity has pushed liquid democracy to a new extent, whereas Ethereum still has some centralized components to it. Ethereum uses off-chain governance protocols that require developer communication with stakeholders, users, and other developers. As there is an increase in the scale of users, both blockchain technologies must be more cautious with approving unknown protocols. Additionally, it will become harder to follow public sentiment. By analyzing the differences between the governance protocols on the IC and Ethereum, we can discover potential future implications and possibilities for additional change. Most importantly, we can discover how to ensure the safety of both networks. Project ICy will be utilized in creating a comparative analysis between the two, by creating calls to the NNS or EIP (Ethereum Improvement Protocols).

Intellectual Merit

Information on governance for both Ethereum and the Internet Computer, besides the basic functionality, is very informal and not yet fully discovered. Often, you can find bits and pieces on reddit or the Dfinity forum, but that is all. This project will not only establish a formal procedure of governance on both, but will also determine the merits to prevent security breaches. We have established security guidelines to look at, and we can further investigate which avenues have been covered and which ones still need to be protected. Furthermore, we will be able to understand the different features and off-chain governance versus on-chain governance. Project ICy will also be utilized to create calls to the NNS and EIP for the price oracle canister, so that we can see if it will be compatible on both the Internet Computer and Ethereum and the differences between the two.

Table of Content

Abstract 2

Defining Security 3

Concept Review 5

Current Governance Protocols on the Internet Computer 6

Project Proposal 8

Project Specifics 9

Abstract

DFNITY’s Internet Computer is the third great innovation in blockchain, following Bitcoin in 2009 and Ethereum in 2015. As a product of the interaction between Chain and Key technology and the NNS (Network Nervous System), the Internet Computer has the potential to break “big tech’s” trillion-dollar industry. The NNS uses governance canisters, registry canisters, and ledger canisters to allow users the ability to propose and vote on their modifications to the Internet Computer. Dfinity has pushed liquid democracy to a new extent, whereas Ethereum still

has some centralized components to it. Ethereum uses off-chain governance protocols that require developer communication with stakeholders, users, and other developers.

A blockchain technology's form of governance is incredibly important because as there is an increased scale of users, the system needs to be more cautious with approving unknown protocols since there is more at stake financially wise. Moreover, with increased scale, it is harder to follow public sentiment; that is a challenge that must be addressed by both communities. By analyzing the differences between the governance protocols on the IC and Ethereum, we can discover potential future implications and possibilities for additional change.

Defining Security

For comparative purposes, the criteria for security must maintain consistency. Therefore, in this paper, Business Process Model Notation (BPMN) is utilized for structural consistency. The goal is to maximize security on both platforms by using enhanced governance protocols. There are several components to an enhanced security platform, defined as followed:

- **Identity and access management**: Managing electronic and digital identities, some examples include two-factor authentication, privileged access management, and more.
- **Key Management**: Keys are used for data encryption as well as decryption for user authentication. If an attacker has access to a compromised key, they can decrypt private information, give themselves private access, and a whole host of other actions. Key Management includes the "creation, exchange, storage, deletion, and refreshing of keys." (Puneet 2021)

- **Data Privacy**: Data Privacy concerns handling "personal data, confidential data, financial data, intellectual property data, and protecting the immutability of the data." (SNIA 2021)
- **Secure Communication**: Ensuring that when two entities are sending information back and forth, there is no third party involvement or interception.
- **Smart Contract Security**: Enhanced security for transaction protocols that execute actions from an agreement, "signed into contract."
- **Prevention of Attacks**: The most common attacks on blockchain technologies are phishing, routing, Sybil, and 51% attacks.
    - **Phishing**: A hacker can send wallet key owners fake emails seemingly legitimate. If fallen for, users may accidentally insert their credential into the fake links presented in the email. The hacker can then have full control over the user's account.
    - **Routing**: A hacker can intercept a transfer of data to an internet service provider. Blockchain users typically do not notice these threats, and in the background the hacker has extracted secure information.
    - **Sybil**: A sybil attack includes a hacker creating many false network identities to crash a system. Once crashed, the hacker will have access to private information. (IBM Security)
    - **51%**: If a miner gains enough computing power, they could have more than 50% of a blockchain network's mining power. Therefore, they would have ultimate power over the ledger. (IBM Security)

Concept Review

The Internet Computer's foundation is in nodes. Nodes are physically located in various data centers, and can communicate to each other to initiate proposals. A collection of nodes located in the same center is known as a subnet. Moreover, a canister is a program that can communicate with other canisters (just like nodes), and includes a state + behavior. Increasing the number of nodes increases the robustness of an application, and increasing the amount of subnets increases the capacity. This project will be also exploring the Network Nervous System which is a "tokenized open governance system that manages the Internet Computer, stores which nodes belong to which subnets, and lastly, how to update nodes and the recovery plan for when they crash." (Dfinity "Understanding the Internet Computers' Network Nervous System" 2021).

Current Governance Protocols in Ethereum

Ethereum governance involves the core protocol as well as projects built on Ethereum. EIP (Ethereum Improvement Protocols) can create, for example, ERC-20's and all users can replicate this method. The EIP process requires a draft, peer review, final specs, and then lastly, anyone can use the method. Changing the Ethereum core protocol is much more difficult and will be the central focus of this project. Every node on the network has to accept the proposal to amend the ECP at a single point in time. Afterwards, developers ensure the security of the proposal and for bugs then the "new rules go into effect." (EthHub 2021)

Additionally, Ethereum uses off-chain governance systems as well as on-chain governance systems. On-chain governance systems are very similar to the IC's governance system; code updates are proposed and nodes vote to accept or decline. It is also a stake-based model, so those with a larger holding of coins have more power. An on-chain governance system works well because of its quick turnaround times so if there is no need to hold off on an important proposal. (EthHub 2021) Moreover, hard forks are reduced because there is less time for conflict amongst user ideas. (Cryptotesters 2021) The issue with the informal governance system is that there is typically less voter turnout, especially with Ethereum since there is no rewards system in place currently. (Cryptotesters 2021)

Off-chain governance is when interest groups advocate for their project proposals on Ethereum. Developers and group members send in proposals, and they must achieve consensus with stakeholders (so for Ethereum, minors), developers, and users. If a majority agree, the change is made, but if there is disagreement they must hard fork their proposal. This causes major rifts in terms of "brand, users, developer mindshare, and hash power." (EthHub 2021)

Current Governance Protocols on the Internet Computer

On the IC, users can propose and vote on modifications through the governance canister in the NNS. The governance canister stores user proposals and neurons (those who are allowed to participate in governance). The other two canisters in the NNS are the registry canister and ledger canister; the registry canister stores a configuration of the IC so the users can vote on proposals meanwhile the ledger canister stores accounts and transactions. (Dfinity 2021)

Walking through a proposal to an accepted change starts first with the Governance canister. A user can make a proposal by a simple command with the type of proposal, parameters, and vote registry. For example, a proposal could be create_subnet(), Node_id1/ Node_id2, and 100 yes 200 no votes. Those that can create proposals are part of the governance system, to do so they must create an account with the IC and then will need to lock tokens in their user-specific neuron. The system also uses a stake-based model, therefore the users with the most locked tokens will have a proportionally larger amount of voting power. (Dfinity 2021) Users are incentivized to participate in governance due to Dfinity's reward system. Rewards entail many different forms, but are usually in the form of tokens. Reward tokens are minted and directly sent to the accounts of the users that are consistently involved with governance. (Dfinity 2021)

The ledger canister stores data about user accounts and their amount of tokens, as well as transactions between lenders/borrowers. For example, a data entry in the transaction sub canister would be " 2021 07 04 03:15 Transfer 20 Tokens User A → User B."

Project ICy is currently using the NNS to update it's exchange rate used within the project. The exchange rate is updated every 10 minutes. The DFINITY beacon neuron uses automated oracles that each control 5 neurons. Typically, a user controls the neuron or is at least connected to it, but in this case to make it automated it's done through the oracle. The oracles receive price data from several exchanges and use this data to infer a correct estimate for an exchange rate. One oracle makes a proposal and if the others approve it's because it's within the margin for the correct price. You need ⅗ to vote yes, and change the currency rate.

All of the canisters used on the Internet Computer have to utilize cycles to run as well as cycles to store. Frequently, the token prices will change, but the cycles should keep the price of computation consistent so users don't have any fluctuations in cost.

Governance on the Internet Computer versus Ethereum

	Internet Computer	Ethereum
Proposal Process	- Simple command with the type of proposal, parameters, and vote registry. - Done through the governance canister on the NNS.	- Requires Draft, Peer Review, and Final Specs - Proposals generally require very technical terms and skills, so usually only developers send in proposals.
Voting Regulations	- Stake-Based Model, those with more tokens stored have more voting power. - Majority votes win	- Every node on the network has to accept the proposal to amend the ECP at a single point in time.
Enactment Process	- Sent for review to Dfinity engineers, if no issue then the proposal will be enacted on the IC	- Ethereum developers ensure the security of the proposal and check for bugs, if all good, the proposal will be implemented.

Project Proposal

There are two routes this project could go, one can be looking at the framework of Ethereum and IC governance that is not controlled by users, and the other, the governance that is controlled by users.

The first route would involve an oracle for a specific DeFi price to report from a chain, such as the price oracle canister used in project ICy. An experiment can involve creating a price oracle canister on both Ethereum and the Internet Computer. The developer then would query into the NNS or a similar structure for Ethereum to check for the conversion rate. Statistical analysis can determine the percentage error on both to determine the accuracy of both architectural structures on determining the exchange rate from actual indices. This study is novel because it will determine the validity of both blockchain technologies' governance protocols that provide hard coded facts to users to implement. If there is substantial error, that means either technology has gone about determining the index the wrong way, and our team will develop an appropriate method to propose to them.

The second route would involve creating wallets and locking tokens/coins for 50 sample users in both Ethereum and the Internet Computer. A large upcoming issue is representing public sentiment in the decision making process as scaling increases. Therefore, we will test the representative sentiment passed along by 50 users in both communities. Although this is more of a qualitative test, to make it more quantitative we will take the proportions of their decision numbers compared to all the user's decisions on an issue. After conducting tests on 10 proposals, we can again use statistical analysis to estimate the likelihood of an issue of scale occurring in the future. From this user experience, we can furthermore develop solutions to scaling and other formats for user-governance to test out in future projects.

Project Specifics

The dates of this project will run from August 6- December 1st or longer depending on the team's progress. The location is dependent on the team member's, but the project can be done virtually. The cost for the first project should be minimal and dependent on the stipend required for the participants within the project. However, the cost for the second project idea may be higher due to the costs allocated to hold tokens and cycles within the framework. Currently the price for a token is $38.51, so multiplying that with 50 would require $1925.50, but upon more research there can be a workaround to this financial barrier. There is still more research to be done on the second project idea, so that the goals are more clearly outlined.

Citations

"Aave vs. Compound: Which DeFi Lending Platform Is Better?" 2021. CoinCentral. June 3. https://coincentral.com/aave-vs-compound-defi/.

"Blockchain Solutions for Syndicated Loans." 2021. ConsenSys. Accessed June 15. https://consensys.net/solutions/capital-markets/syndicated-loans/#:~:text=Syndicated%20loans%20solutions%20built%20on,settlement%20times%20in%20today%27s%20industry.

Carlson, Jill. 2018. "Decentralized Credit Scoring." Medium. Medium. May 25. https://medium.com/@jillcarlson/decentralized-credit-scoring-fe2c6c0611c6.

Dfinity. 2021. "Understanding the Internet Computer's Network Nervous SYSTEM, Neurons, and ICP Utility Tokens." *Medium*. The Internet Computer Review. July 8. https://medium.com/dfinity/understanding-the-internet-computers-network-nervous-system-neurons-and-icp-utility-tokens-730dab65cae8.

Dfinity. 2021. "The Network Nervous System: Governing the Internet Computer." *Medium*. The Internet Computer Review. June 21. https://medium.com/dfinity/the-network-nervous-system-governing-the-internet-computer-1d176605d66a.

"Governance on Ethereum." 2021. *EthHub*. EthHub. Accessed July 28. https://docs.ethhub.io/ethereum-basics/governance/.

"How Does Ethereum Governance Really Work? - Everything You Need to Know BY CRYPTOTESTERS." 2021. *Cryptotesters.com*. Accessed July 28. https://cryptotesters.com/blog/ethereum-governance.

"Open Source DeFi Protocol." 2021. Aave. Accessed June 15. https://aave.com/aTokens/.

Puneet. 2021. "What Is KEY Management?: How Does Key Management Work?: Encryption Consulting." *Encryption Consulting | Encryption Consulting*. July 14. https://www.encryptionconsulting.com/education-center/what-is-key-management/.

Sandner, Philipp. 2020. "Decentralized Finance (DeFi): What Do You Need To Know?" Medium. Medium. May 22. https://philippsandner.medium.com/decentralized-finance-defi-what-do-you-need-to-know-9cd5e8c2a48.

Schär, Fabian. 2021. "Decentralized Finance: On Blockchain- and Smart Contract-Based Financial Markets." Economic Research - Federal Reserve Bank of St. Louis. Accessed June 15. https://research.stlouisfed.org/publications/review/2021/02/05/decentralized-finance- on-blockchain-and-smart-contract-based-financial-markets.

Werner, Sam, Daniel Perez, and Lewis Gudgeon. 2021. "SoK: Decentralized Finance (DeFi)," April, 1–17. "Will Blockchain Technology Disrupt the ICS World? -ISA."

2021. Isa.org. Accessed June 15. https://www.isa.org/intech-home/2017/november-december/features/will-blockchain-technology-disrupt-the-ics-world.

“What Is Blockchain Security.” 2021. *IBM*. Accessed July 28. https://www.ibm.com/topics/blockchain-security.

“What Is Data Privacy?” 2021. *SNIA*. Accessed July 28. https://www.snia.org/education/what-is-data-privacy.

Yec. 2020. “Council Post: The Rise Of Decentralized Cryptocurrency Exchanges.” Forbes. Forbes Magazine. November 30.https://www.forbes.com/sites/theyec/2020/12/01/the-rise-of-decentralized-cryptocurrency-exchanges/?sh=487c226f16e7.