Governance on StarkNet

Abstract:
This paper focuses on the highlighting StarkNet and Cairo's roles, Scope of governance and a brief on DAO frameworks and tools in starknet. This research was a part of Starknet Asia Research Fellowship Program 2023

Author: Rashmi V Abbigeri (https://twitter.com/rashmivabbigeri (https://twitter.com/rashmivabbigeri))

1. Introduction

Decentralized Autonomous Organizations (DAOs) are a form of member-owned community governance facilitated by blockchain technology.

They are designed to operate without centralized leadership, providing a collaborative environment where decisions are governed by collective agreement rather than hierarchical structures.

DAOs are essential for several reasons:

Trustless Collaboration: DAOs allow people to work together without needing to place trust in a single leader or small group of managers. This is particularly beneficial for internet-based collaborations, where participants might not have personal relationships or trust established.

Transparency and Security: All decisions and transactions within a DAO are transparent and recorded on the blockchain, making the process secure and verifiable by all members. This ensures that funds and operations are managed democratically and transparently.

Global Participation: DAOs enable global collaboration, as they do not require geographical proximity or centralized control. This opens up opportunities for diverse and widespread participation.

Autonomous Operations: DAOs operate according to rules encoded in smart contracts on the blockchain, ensuring that decisions are executed automatically and in accordance with the agreed-upon rules.

2. StarkNet in Focus

StarkNet, an emerging player in the blockchain space, stands out for its innovative approach to scalability and security, an solution to blockchain trillema.

Key features of StarkNet include:

- **Layer-2 Scaling Solution**: StarkNet operates as a Layer-2 network over Ethereum, offering enhanced scalability by batching multiple transactions into a single proof. This capability significantly reduces the load on the Ethereum mainnet, facilitating faster and more cost-effective transactions.

- **Use of STARK Proofs**: StarkNet employs STARK proofs, a form of zero-knowledge proofs, providing robust security against quantum attacks and ensuring the privacy and integrity of transactions.

- **Cairo Programming Language**: At the heart of StarkNet's innovation is Cairo, a Turing-complete language specifically designed for creating STARK proofs. Cairo's role extends beyond just security; it introduces programmability and flexibility into the StarkNet ecosystem. This allows developers to build more complex and versatile smart contracts compared to traditional blockchain platforms.

- **Decentralized Applications (DApps) Support**: StarkNet supports a wide range of DApps, enabling use cases that were previously constrained by Ethereum's limitations.

Starknet, is future proof because it provides robust security against quantum attacks and also we can leverage provable computation with Cairo.

3. Scope of Governance

With Starknet and verifiable computation we have the potential to build true decentralized trustless governance systems.

Verifiable computation can significantly contribute to the development of decentralized autonomous governance systems in several ways:

- **Enhanced Trust and Transparency:** Verifiable computation ensures the integrity and correctness of computations within a decentralized governance system. Since the results of computations can be independently verified, it fosters trust among

participants, which is crucial in decentralized systems where no single authority is in control.

- **Automated Governance Decisions:** With verifiable computation, certain governance decisions can be automated. For instance, smart contracts could automatically execute actions (like fund allocation or rule changes) based on predefined conditions, with the assurance that these computations are correct and tamper-proof.

- **Efficient Consensus Mechanisms:** Verifiable computation can improve the efficiency of consensus mechanisms in decentralized governance systems. By ensuring that the data and computations that form the basis of consensus are correct, the system can operate more smoothly and with fewer disputes.

- **Data Integrity and Security:** In governance systems, the integrity of data (like voting records or proposal submissions) is paramount. Verifiable computation ensures that data has not been tampered with, maintaining the security of the governance process.

- **Reduced Costs and Increased Accessibility:** By automating and verifying computations, the costs associated with governance processes (like auditing or manual verification) can be reduced. This makes decentralized governance systems more accessible and viable for various applications.

- **Customizable Governance Models:** Different governance models can be implemented and verified using verifiable computation, allowing for the design of systems that best fit the needs and goals of the particular decentralized autonomous organization.

4. Lack of Governance Tools on Starknet

With all the potential of Starknet, Starknet ecosystem severly lacks toolings for governance. DAO governance frameworks and DAO tools could really help caputure this potential.Further more, DAOs on starket could be built with coordination mechanisms and operations in mind.

Comparing StarkNet's DAO ecosystem to Ethereum DAO ecosystem,

Ethereum's DAO Frameworks and Tools:

- **Frameworks like Aragon and DAOstack:** These provide ready-to-use, customizable templates for DAO creation, governance, and management.
- **Governance Protocols:** Ethereum hosts various governance protocols like Compound's Governor Alpha/Beta for creating proposals and voting.

StarkNet's Potential for DAO Ecosystems:

- **Cairo Language for Advanced Smart Contracts:** With Cairo we can build robust DAO Smart Contracts, potentially allowing for intricate governance models. It can support advanced cryptographic techniques like STARKs for enhanced security.
- **Scalability with Layer-2 Solutions:** StarkNet's Layer-2 scaling provides higher transaction throughput and lower gas fees. This is crucial for DAO operations like voting, which can be costly on Ethereum's mainnet.
- **STARK Proofs for Enhanced Security:** STARK proofs offer quantum-resistant security, making StarkNet potentially more secure for DAO operations involving significant asset management.

DAO Frameworks and Tools That Could Be Developed on StarkNet:

- **Advanced DAO Templates:** Leveraging Cairo, developers could create sophisticated DAO templates with complex governance mechanisms.
- **Efficient Voting Mechanisms:** Utilizing StarkNet's scalability, more efficient, frequent, and cost-effective on-chain voting systems can be developed, possibly integrating advanced cryptographic voting methods for privacy and security.
- **Automated Governance Tools:** StarkNet could enable more complex automated governance processes, leveraging Cairo's advanced computational capabilities for executing predefined governance actions.

In conclusion, while Ethereum's DAO ecosystem is more mature, StarkNet, with its unique features, especially the Cairo programming language and scalability solutions, has the potential to innovate and expand the capabilities of DAO frameworks and tools. This could lead to more secure, efficient, and complex DAO structures, enabling broader and more effective decentralized governance.