Welcome to your Jupyter Book

Contents

This is a small sample book to give you a feel for how book content is structured. It shows off a few of the major file types, as well as some sample content. It does not go in-depth into any particular topic - check out the Jupyter Book documentation for more information.

Check out the content pages bundled with this sample book to see more.

Governance In DeFi

Key Insights!

- The voting power in DeFi protocols becomes increasingly concentrated among a percentage of token holders over time in decentralised exchanges, lending protocols and yield aggregators.
- The paramount wallet addresses ranking within the top 5, 100, and 1000, exercise predominant influence over the voting power in the Balancer, Compound, Uniswap, and Yearn Finance protocols, with Compound displaying the least evidence of decentrality
- The most significant governance challenges identified by DeFi users are voter collusion, low participation rates, and voter apathy.
- To address vulnerabilities in DeFi governance, a novel voting mechanism resistant to sybil attacks called bond voting has been proposed.
- To enhance the manual parameter section, an AI-enabled adjustment solution has been demonstrated to automate governance mechanisms.

Introduction

Decentralized finance (DeFi) has emerged as a potential substitute for traditional financial institutions, offering peer-to-peer transactions and a diverse range of services that democratize finance by enabling users to participate in protocol governance. However, several studies have suggested that the current governance mechanisms require improvements. This article provides an overview of findings associated with DeFi governance.

Centralised Governance in DeFi Protocols

Several studies have identified a significant level of centrality in the governance mechanisms of DeFi protocol. Barbereau et al., [BSP+22a] found that the decentrality of voting in DeFi is significantly low with a majority of the voting power concentrated among a percentage of governance token holders. As evidenced by their findings, there was a significant degree of centrality, in

What are

Lending pr

Skip to main content

lending protocols, decentralisd exchanges and yield aggregators. This study used case studies to comprehend the governance mechanisms of these protocols.

Similarly, Jensen et al. [JvWR21] results demonstrate centrality in voting power with the protcols top 5, top 100, and top 1000 wallet addresses controlling majority of the voting power in Balancer, Compound, Uniswap and Yearn Finance protocols. In this study, the token holdings and users' wallets of protocols were analysed; Compound displayed the most evidence of centrality and Uniswap the least with the top 5 wallet addresses accounting for 42.1% and 12.05%, respectively.

Barbereau et al. [BSP+22b] ascertained that DeFi protocols become more centralized over time. In this longitudinal study, voting patterns demonstrated changes in the voting power dynamics over time. Furthermore, in analysing the governance structures of DeFi protocols, Stroponiati et al. [S+] ascribed reward-based economic incentives as the significant cause behind the development of centralized structures.

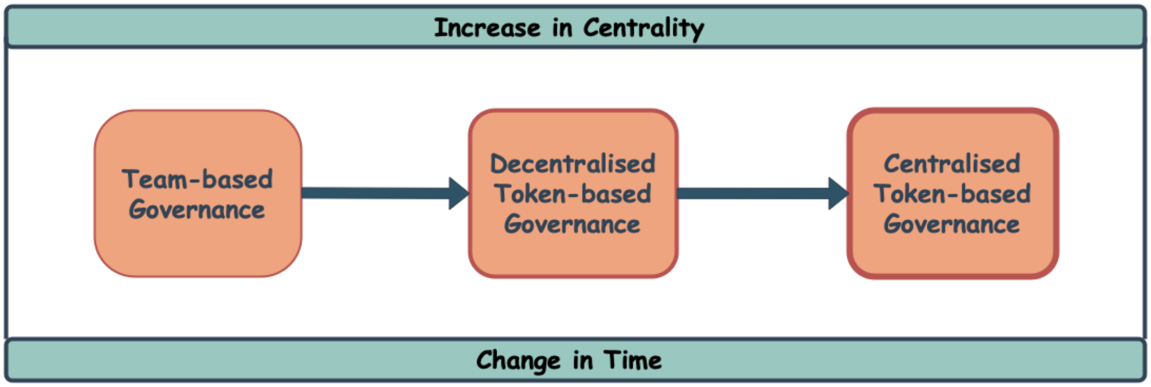
Increase in Centrality
Team-based Governance
Decentralised Token-based Governance
Centralised Token-based Governance
Change in Time

Fig. 1 The Evolution of DeFi Governance.

Challenges & Vulnerability In DeFi Governance

In investigating governance challenges, Ekal et al., [EAw22] identified voter collusion, low participation rates, and voter apathy as the most significant challenges. This empirical investigation utilised an interview survey approach to collect data from protocol users. Furthermore, to address vulnerabilities, Mohan et al. [MKB22] proposed a novel voting mechanism resistant to sybil attacks called bond voting. This solution factors in time commitment to be resistant to plutocracy.

AI-enabled On-chain Governance

To enhance and automate governance mechanisms, Xu et al., [XPFL23] demonstrated an AI-enabled parameter adjustment solution which is more efficent than current current implementations. Specifically, the study employed Deep Q-network (DQN) reinforcement learning to investigate for automated parameter selection in a DeFi environment. Although a lending protocol was employed in the study, the model's application can extend to other categories of DeFi protocols as well. In investigating DAOs, Nabben [Nab23] observes that GitcoinDAO also employs algorithmic governance in various organizational components such as monitoring the compliance with organizsational rules.

observation is that GitcoinDAO employs algorithmic governance in various organizational components and at the same time necessitates the regulation of the algorithmic processes initiated by the community in an open and decentralized manner

Conclusion

Skip to main content

borrow cry
need for ir
traditional

What are

Decentrali
peer tradir
blockchair
cryptocurr
central au

What are

Yield aggr
(DeFi) app
of seeking
cryptocurr
a way to o

What is V

Voter collu
group of v
manipulate
their favor
votes to cr

What is V

Voter apat
holders or
not activel
due to a la

The vision of DeFi is to forster a democratic process of governance and sustain high levels of decentrality finance in the process. However, recent studies have highlighted significant centrality in DeFi governance mechanisms, indicating the need for improvements in the existing governance models. The studies analysed in this article have revealed that the majority of the voting power in several protocols is concentrated among the top token holders, with evidence of increasing centralization over time. Moreover, DeFi governance has been found to face challenges the voting and governance process. In view of these challenges, researchers have proposed novel solutions such as a bond voting and a AI-enabled parameter selection solution to improve the current mechanisms. In conclusion, continued research and development in DeFi governance are crucial for ensuring its long-term sustainability and success.

Self-Sovereign Identity: Technical Foundations and Applications

Key Insights!

- SSI systems use DIDs as unique, resolvable identifiers for each entity, allowing the secure management of digital identities without relying on a centralized authority.
- VCs provide cryptographically verifiable proof of an individual’s attributes or personal information, enabling secure and trustworthy data sharing between issuers, holders, and verifiers.
- SSI incorporates privacy-preserving mechanisms such as zero-knowledge proofs and selective disclosure, allowing users to prove their credentials without revealing their actual identity or unnecessary information.
- While not mandatory, using blockchain as a decentralized data registry in SSI systems enables secure, tamper-evident, and verifiable storage of credentials, enhancing the trustworthiness and reliability of the identity management process.

Introduction

According to World Bank estimates, nearly 850 million people lack an official identity [JC23], and the proliferation of digital devices has made it increasingly essential to possess a verifiable digital identity. This has led to a rise in the number of digital transactions and the need for a secure and reliable identity management system. SSI is emerging as a decentralized alternative to traditional centralized identity management systems, in which identities are cryptographically verifiable. It allows individuals to control their digital identities and share them with trusted parties. Each entity in the SSI system is identified by a unique DID (Decentralized Identifier) as shown below, which can be resolved to reveal information such as the entity’s public key and other metadata.

$$\underbrace{\texttt{DID}}_{\texttt{Scheme}} : \overbrace{\texttt{example}}^{\texttt{DID Method}} : \underbrace{\texttt{BzCbsNYhMrjHiqZDTUASHg}}_{\texttt{Method Specific Identifier}}$$

DID breakdown

See also

Find out more about some of the most commonly used DID methods:

- DID:INDY
- DID:UPORT
- DID:SOV

Skip to main content

While centralized identities and federated identities offer convenience, control remains with the identity provider [LB15]. User-centric identities such as OpenID [RR06] and OAuth [FKustersS16] improve portability but do not give full control to the users. SSI is designed to provide users with full control over their digital identities, and involves guiding principles around security, controllability, and portability. In addition to providing full control, Bernabe et al. [BCHR+19] presented a classification of techniques for maintaining privacy in SSI, which included Secure Multiparty Computation and Zero-Knowledge Proofs, among others.

The three main parties involved in SSI systems are issuer, holder and verifier as shown in [Fig. 2]. The issuer issues a cryptographically signed credential to the holder, and the verifier is the entity that that confirm the authenticity of the credential using a decentralized data registry such as Blockchain. Holders store their credentials in secure digital wallets and can share them with other parties as needed. The holder can also create a presentation request and share it with the verifier.

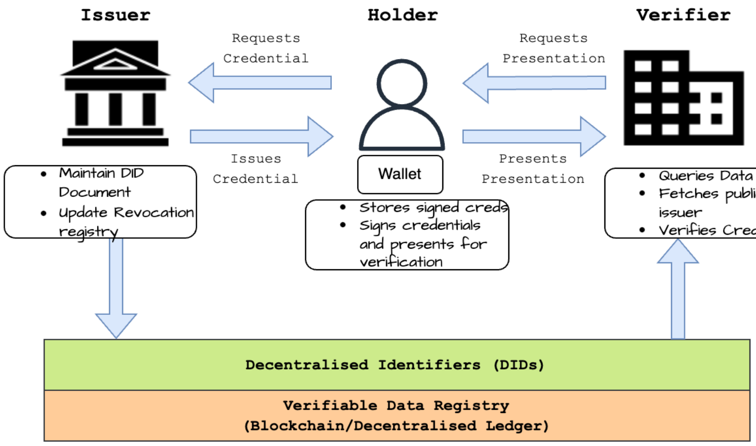
Issuer
Holder
Verifier
Requests Credential
Issues Credential
Requests Presentation
Presents Presentation
Wallet
Maintain DID Document
Update Revocation registry
Stores signed creds
Signs credentials and presents for verification
Queries Data registry
Fetches public key of issuer
Verifies Credential
Decentralised Identifiers (DIDs)
Verifiable Data Registry (Blockchain/Decentralised Ledger)

Fig. 2 SSI entities and their relations

Click here to see how a verifiable credential actually looks like

Nitty Gritties of SSI

- SSI solutions are designed to be blockchain-agnostic and adhere to W3C’s specifications.
- The identity wallets (e.g., uPort, Trinsic, Connect.Me) are different from the digital wallets (e.g., Coinbase, Ledger, Trezor) that store cryptocurrencies in the sense that they store and manage DIDs and VCs instead of cryptocurrencies.
- To protect privacy, SSI solutions (e.g. - Hyperledger Indy and Aries) are increasingly using Zero-Knowledge Proofs (ZKPs) to prove the authenticity of credential```s without revealing the actual data.
- To facilitate secure communication between different SSI components (issuer-holder-verifier), DIDComm and CHAPI protocols have been developed and heavily used.

Applications for SSI

Recent studies have demonstrated the feasibility of using zero-knowledge proofs to disclose information selectively, such as proof of vaccination status, without revealing users’ identities. These studies have employed interoperable open-source tools to implement these systems globally at a minimal cost. Schlatt et al. [SSFU22] illustrates how a customer can leverage a Zero-knowledge Proof concept called ‘blinded link secret’ to disclose information selectively. Similarly, Barros et al.

SSI

Self-Sover
decentrali
system wh
technolog
individuals
identities s

Verifiabl

A verifiabl
provides a
verifiable
informatio

Skip to main content

identities. Furthermore, it uses interoperable open-source tools across countries to implement this system globally at a minimal cost for each country’s government. The NHS Digital Staff Passport solution [LC22] employs the Sovrin Network as a public key infrastructure (PKI) to manage verifiable credentials for staff onboarding. Hospitals register on the network and use their private keys to sign credentials, while staff members utilize Evernym’s Connect.Me SSI digital wallet app to store and share credentials.

Shuaib et al. [SHU+22] suggest that a blockchain-based land registry system can be combined with a self-sovereign identity (SSI) solution to provide a secure and efficient identity management system for landowners. Three existing SSI solutions: Everest, Evernym, and uPort [Ame22], were evaluated based on SSI principles [All16] to determine their compliance and effectiveness in addressing identity problems in land registry systems. The Everest platform was found out to be the most compliant with the SSI principles, whereas Evernym and uPort had some limitations in terms of interoperability and user control.

Estonia is one of the few countries in the world that have managed to make e-voting a reality [SS22]. Sertkaya et al. [SRR22] proposed an EIV-AC scheme that integrates the Estonian Internet voting (EIV) scheme with anonymous credentials (AC) based on self-sovereign identity (SSI). The use of SSI-based anonymous credentials enables voters to prove their eligibility to vote without revealing their identity. The zero-knowledge proof of knowledge is used to prove that the voter has the right to vote without revealing any additional information. The EIV-AC scheme enhances the security and privacy of the EIV scheme, making it more compliant with privacy-enhancing and data minimization regulations.

Can SSI work without Blockchain?

Blockchain is one of many options when implementing the Self-sovereign Identity system. Alternatives like IPFS, Public-key cryptography and even traditional Certificate Authorities can be used to implement SSI []. However, the main advantage of using Blockchain is that it provides a decentralized and immutable ledger that can be used to store and verify credentials.

Conclusion

Self-sovereign identity can potentially revolutionize various industries, including healthcare, voting systems and many more. However, as research and development in SSI progress, it will be crucial to address interoperability, scalability, and usability challenges to realize SSI’s potential in a global context fully.

[All16] Christopher Allen. The path to self-sovereign identity. *Life With Alacrity*, 2016. URL: http://www.lifewithalacrity.com/2016/04/the-path-to-self-soverereign-identity.html.

[Ame22] New America. Three self-sovereign identity platforms to watch. *New America*, 2022. URL: https://www.newamerica.org/future-land-housing/reports/nail-finds-hammer/three-self-sovereign-identity-platforms-to-watch/.

[BSP+22a] **missing journal in barbereau2022defi**

[BSP+22b] Tom Barbereau, Reilly Smethurst, Orestis Papageorgiou, Johannes Sedlmeir, and Gilbert Fridgen. Decentralised finance's unregulated governance: minority rule in the digital wild west. *Available at SSRN*, 2022.

[BCHR+19] Jorge Bernal Bernabe, Jose Luis Canovas, Jose L Hernandez-Ramos, Rafael Torres Moreno, and Antonio Skarmeta. Privacy-preserving solutions for blockchain: review and challenges. *IEEE Access*, 7:164908–164940, 2019.

[dVBSFCustodio22] Mauricio de Vasconcelos Barros, Frederico Schardong, and Ricardo Felipe Custódio. Leveraging self-sovereign identity, blockchain, and zero-knowledge proof to build a privacy-preserving vaccination pass. *Blockchain, and Zero-Knowledge Proof to Build a Privacy-Preserving Vaccination Pass*, 2022.

[EAw22] Hassan Hamid Ekal and Shams N Abdul-wahab. Defi governance and decision-making on blockchain. *Mesopotamian Journal of Computer Science*, 2022:9–16, 2022.

[FKustersS16] Daniel Fett, Ralf Küsters, and Guido Schmitz. A comprehensive formal security analysis of oauth 2.0. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, 1204–1215, 2016.

Skip to main content

[HdHPK14] Christopher Ramsay Holdgraf, Wendy de Heer, Brian N. Pasley, and Robert T. Knight. Evidence for Predictive Coding in Human Auditory Cortex. In *International Conference on Cognitive Neuroscience*. Brisbane, Australia, Australia, 2014. Frontiers in Neuroscience.

[JvWR21] Johannes Rude Jensen, Victor von Wachter, and Omri Ross. How decentralized is the governance of blockchain-based finance: empirical evidence from four governance token distributions. *arXiv preprint arXiv:2102.10096*, 2021.

[JC23] CLAIRE CASHER JULIA CLARK, ANNA DIOFASI. 850 million people globally don't have id—why this matters and what we can do about it. *World Bank*, 2023. URL: https://blogs.worldbank.org/digital-development/850-million-people-globally-dont-have-id-why-matters-and-what-we-can-do-about.

[LC22] Mary Lacity and Erran Carmel. Implementing self-sovereign identity (ssi) for a digital staff passport at uk nhs. *University of Arkansas*, 2022.

[LB15] Maryline Laurent and Samia Bouzefrane. *Digital identity management*. Elsevier, 2015.

[MKB22] Vijay Mohan, Peyman Khezr, and Chris Berg. Voting with time commitment for decentralized governance: bond voting as a sybil-resistant mechanism. *Available at SSRN*, 2022.

[Nab23] Kelsie Nabben. Governance by algorithms, governance of algorithms: human-machine politics in decentralised autonomous organisations (daos). *puntOorg International Journal*, 8(1):36–54, 2023.

[RR06] David Recordon and Drummond Reed. Openid 2.0: a platform for user-centric identity management. In *Proceedings of the second ACM workshop on Digital identity management*, 11–16. 2006.

[SSFU22] Vincent Schlatt, Johannes Sedlmeir, Simon Feulner, and Nils Urbach. Designing a framework for digital kyc processes built on blockchain-based self-sovereign identity. *Information & Management*, 59(7):103553, 2022.

[SS22] Cyber Security and Society. Estonia leads world in making digital voting a reality. *Cyber Security and Society*, 2022. URL: https://www.ft.com/content/b4425338-6207-49a0-bbfb-6ae5460fc1c1.

[SRR22] Isa Sertkaya, Peter Roenne, and Peter YA Ryan. Estonian internet voting with anonymous credentials. *Turkish Journal of Electrical Engineering and Computer Sciences*, 30(2):420–435, 2022.

[SHU+22] Mohammed Shuaib, Noor Hafizah Hassan, Sahnius Usman, Shadab Alam, Surbhi Bhatia, Arwa Mashat, Adarsh Kumar, and Manoj Kumar. Self-sovereign identity solution for blockchain-based land registry system: a comparison. *Mobile Information Systems*, 2022:1–17, 2022.

[S+] K Stroponiati and others. Decentralized governance in defi: examples and pitfalls. squarespace. retrieved december 30, 2022.

[XPFL23] Jiahua Xu, Daniel Perez, Yebo Feng, and Benjamin Livshits. Auto. gov: learning-based on-chain governance for decentralized finance (defi). *arXiv preprint arXiv:2302.09551*, 2023.