DRAFT: Minimum-viable DAOs using thresh-hold signature schemes

Brian Planje
b.o.s.planje@student.tudelft.nl
Delft University of Technology
Delft, The Netherlands

***Abstract*—This document is a model and instructions for LaTeX. This and the IEEEtran.cls file define the components of your paper [title, text, heads, etc.]. *CRITICAL: Do Not Use Symbols, Special Characters, Footnotes, or Math in Paper Title or Abstract.**

***Index Terms*—component, formatting, style, styling, insert**

I. Introduction

The illusion of decentralization.

A traditional organization is defined as a group of people working together with a particular purpose towards a collective goal. They are hierarchical in nature and suffer from power concentration of large share-holders which control decision making. In other words, they are are centralized in nature. They leverage this centralization for efficiency. The introduction of the internet and web 2.0 technologies have only accelerated this process.

The aforementioned aspects resulting from centralized authorities are problematic for many reasons. They can at any time change the rules by which users interact. Users have no control over this decision making. Furthermore, we can say that their interests do not align with the interests of the users, due to their profit-seeking behaviour. In addition to other problems, they use algorithms to maximize user retention rates in order to maximize profit, ignoring all social-economic problems, and abuse their user data.

Decentralized autonomous organizations (DAO) are a new form of organization which are both decentralized and autonomous. These organizations operate without a centralized authority. The rules are transparent and enforced by an underlying decentralized protocol, such as a public blockchain. The rules of such organizations can be changed collectively by its members through the voting in a governance protocol. While such organizations are autonomous to an extent, they will still rely on human individuals to perform certain tasks. A recent definition proposed by Vitalik, one of the founders of Ethereum, for DAOs is "it is an entity that lives on the internet and exists autonomously, but also heavily relies on hiring individuals to perform certain tasks that the automaton itself cannot do [1]".

The main advantages of DAOs are thus summed by the following:

1) Efficiency: avoiding managatorial overhead by replacing it with code
2) Decentralization: avoiding all the disadvantages which centralization brings such as corruption, collusion, profit as interest only

In this research paper we introduce a novel architecture for an academically pure DAO which focuses on upholding complete decentralization throughout all layers of the DAO while providing scalability using the novel thresh-hold signature scheme FROST [2]. We use this architecture to implement a proof-of-concept implementation of a DAO which aims to replace the music industry, following our zero-server-architecture stack [3].

II. Related Work

We discuss what layers there are, various initivaties. The world of fake decentralization. The promises of fake decentralization.

III. Problem Description

IV. Design

! Iets beter introduceren. Niet te snel introduceren. Noem EVM. Noem Bitcoin als simplest coin om te gebruiken.

! Design primitives noemen. Thresh-hold crypto primitives, off-chain. Wallet centric. Uncomompromising non-custodian. Highlighten dat het geen compromis. Compromisloos. Radically decentralized. Ruthlessly decentralized.

We now propose an architecture for the DAO which aims to provide a way to collectively manage funds and make decisions in a decentralized manner, without making use of smart contracts.

All members collectively own a shared public key. This key is created by a secure Distributed Key Generation (DKG) protocol in a collective manner using a pre-agreed upon thresh-hold value. The shares of the corresponding private key are held by the members. In order to sign a message, t-n members need to participate in a thresh-hold signature signing protocol. A collective decision is simply the signing of an arbitrary message, since implicitly t-n members are needed to sign a message which means t members have agreed upon a proposal for a decision.

The implicit governance structure present here is based on the ownership of the private key shares. Using sybil-resistance mechanisms, a one-token-one-vote [4] model can be realized. Otherwise, a single user can create sybils in order to acquire more shares based on the criteria which are needed to join.

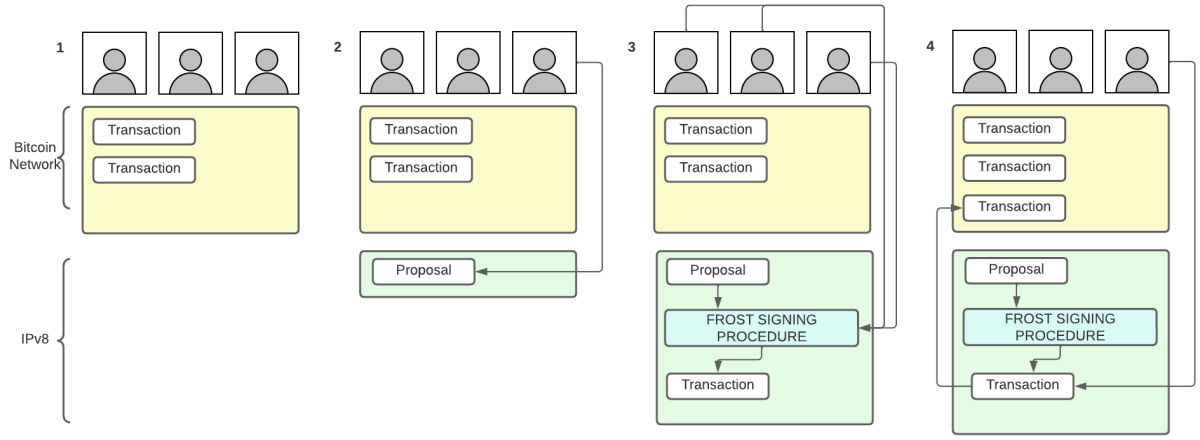


Fig. 1. Spending process

This can be desirable when i.e. the members of the DAO want to create incentives for more participation in the DAO (financial or other activity) which can be rewarded with more private key shares.

A double-spend proof consensus layer is required to have users commit to collectively made decisions, such as the acceptance of a new DAO members or the spending of funds. For this, a DLT can be used which has a sound consensus mechanism with proper incentives. It is important for such a DLT to be decentralized, secure and performant. In practice is appears to be hard, as can be seen by the blockchain trillema [5].

In this solution, we limit the need for on-chain storage and verification to a minimum, compared to traditional multi-sig solutions [CITE] or the solutions us- ing smart-contracts. Only data which is required to have confidence in commitment of decisions is stored and verified on-chain. This allows us to remedy the throughput issues of DLTs such as Bitcoin.

Building upon the aformentioned primitives, we design the DAO such that it is a collection of UTXO (wallet) locked up by a Taproot script (described later) using the shared public key. Decisions in this DAO can be arbitrary, but for the management of funds we identify two decisions which are important. Namely 1) the joining of the DAO 2) the spending of funds.

In order to join the DAO, we propose two seperate join models which are akin to real-life set-ups of organizations.

1) Closed Join Model. A set of n users agree to join or create the DAO at once. This is more efficient since the DKG only needs to run once.
2) Open Join Model. A user joins an existing DAO 1-by-1. This is less efficient as the DAO grows since the DKG needs to run on an increasing larger amount of participants.

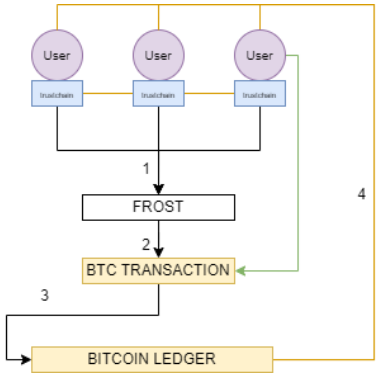


Fig. 2. Architecture

Existing members will have to participate in a key generation protocol with the new member. The existing members can place arbitrary requirements for the new member before they participate in such a protocol. Existing members require new members to first lock-up a minimum amount of funds using the existing shared public key.

The spending of funds is done in a similar manner. A proposal is a yet to be signed Bitcoin transaction spending the amount of funds to a certain address. If t-n members decide to sign the transaction, a valid signature is created and any member can broadcast the transaction on the Bitcoin network to spend the funds.

All coordination between members to construct the shared public key is done using ipv8/trust-chain [6].

1) Digital Democracy Problem: Locked up funds run the risk of being locked up forever if participants do not ever agree on a decision or if participants become in-active. We coin this the digital democracy problem. One solution to remedy this, which we use in our architecture, is the ability

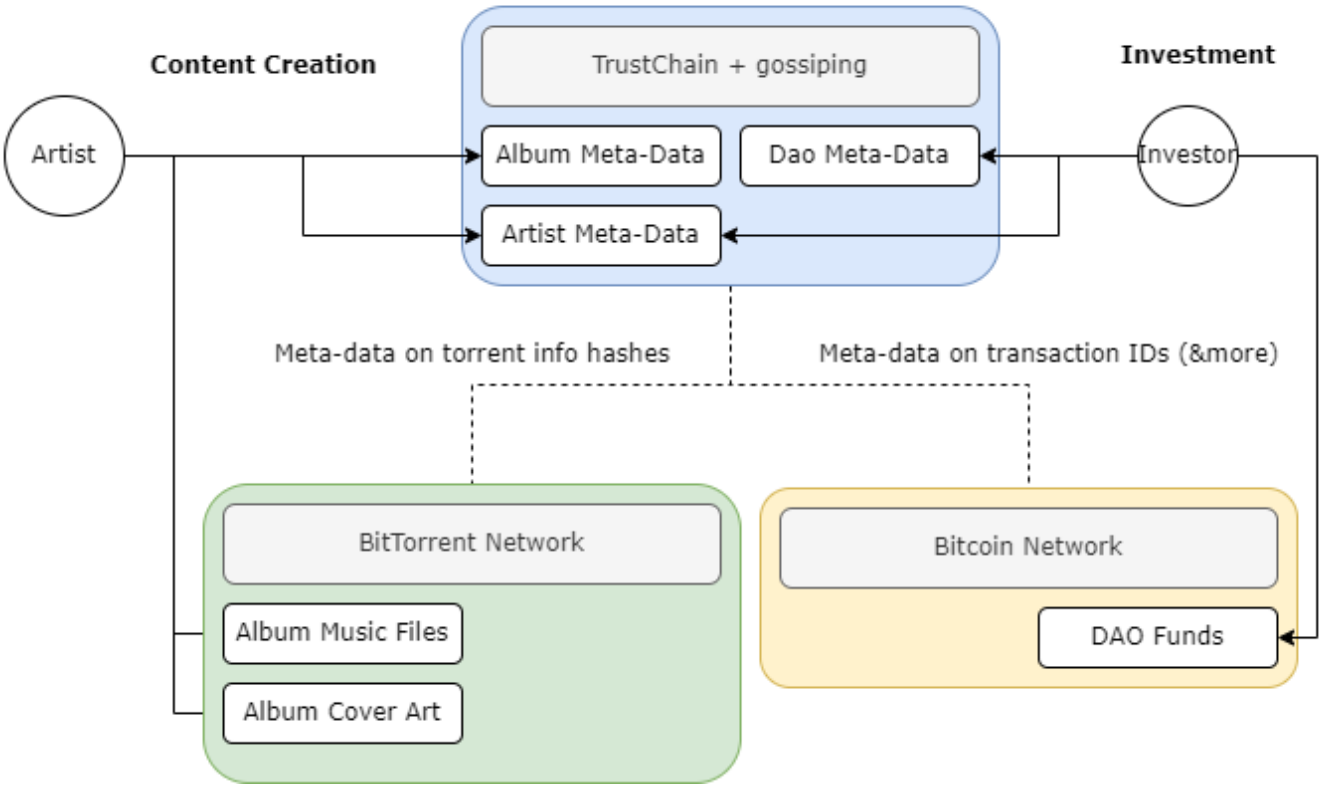
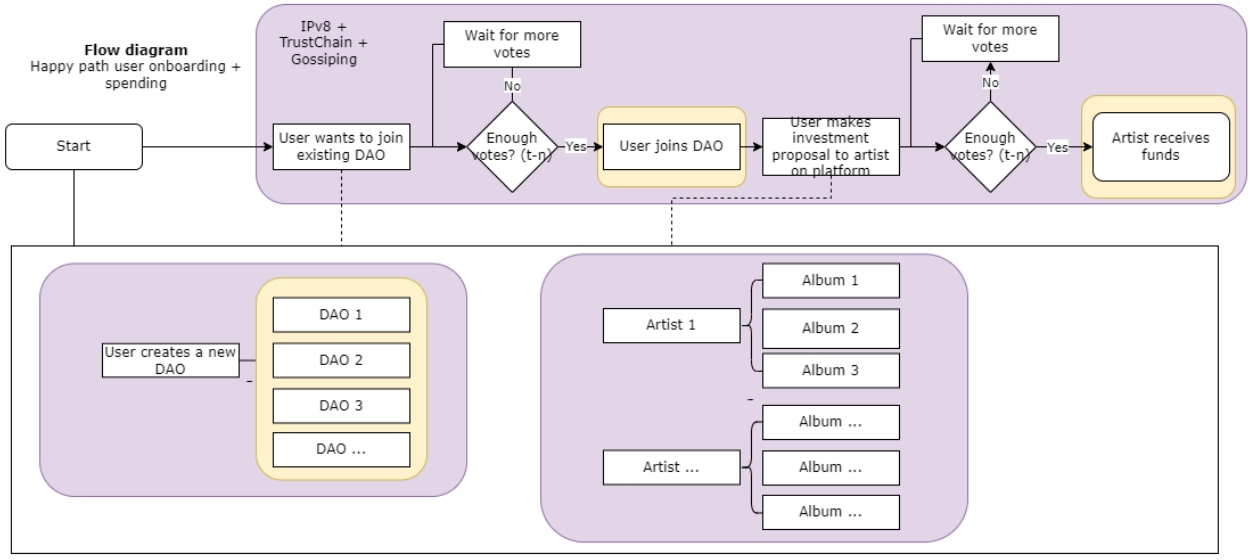


Fig. 3. content



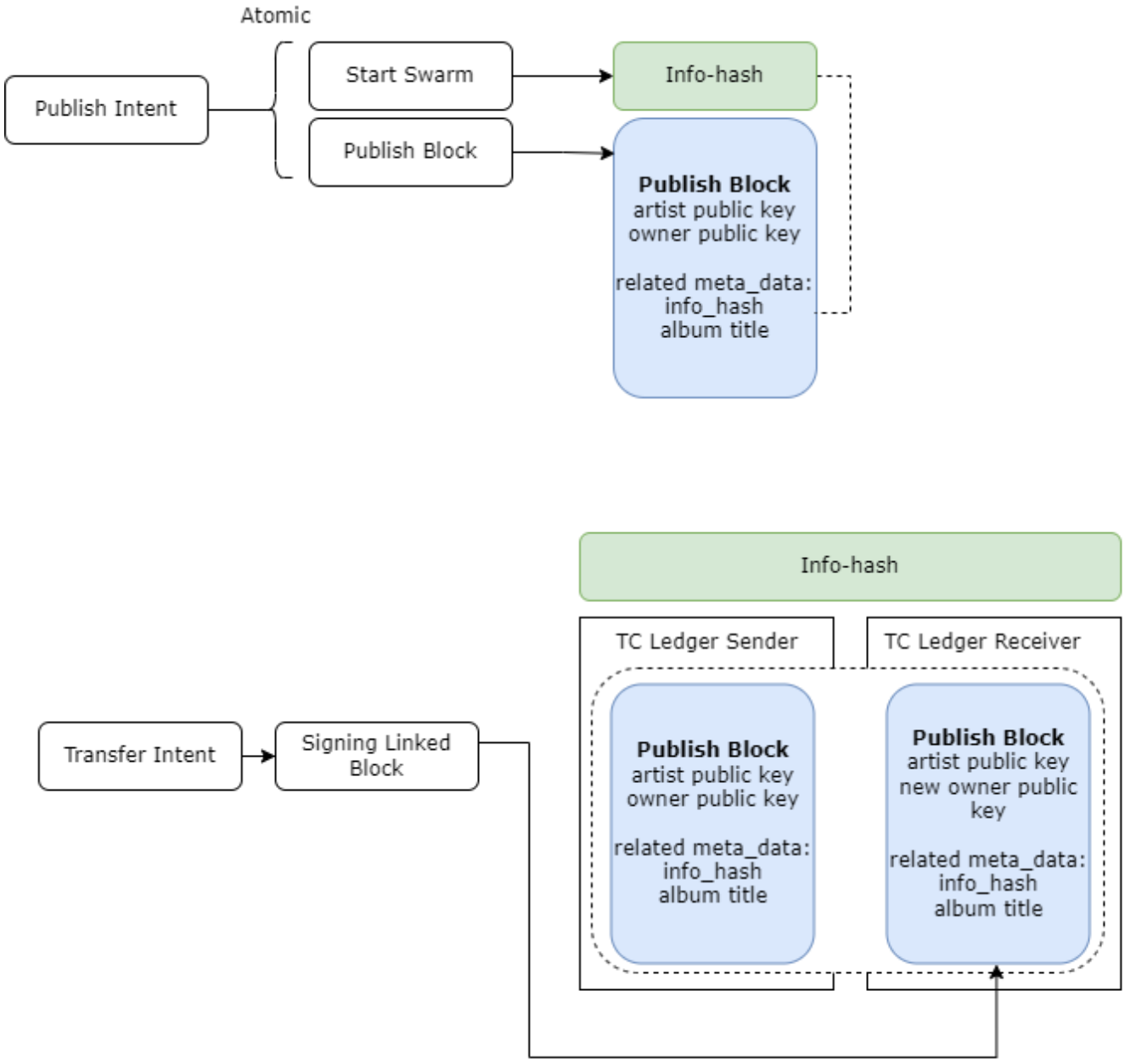


Fig. 5. nft

for an increasingly lower thresh-hold number of members to be required over time to spend the funds.

Funds are locked up using a specially constructed Taproot script. When members decide to construct a shared key, an additional set of shared keys is constructed as well using lower thresh-hold amounts. In the Taproot script hashed time locked contracts are combined with the different public keys over time. The public keys with lower thresh-holds will be locked with the time locks which are the largest. As time passes, smaller amount of participants will be able to unlock the funds in order to spend them.

V. Implementation

We have created a proof-of-concept implementation of our design to create a crowdfund DAO for music artists which additionally aims to show that dis-intermediation of all un-need institutions [7] in the music industry is possible on a technical level. T

Our implementation is based on the zero-server-architecture stack [3]] and is works on Android mobiles. It uses IPv8/TrustChain [6] as the overlay network for communication between peers.

Streaming of songs is handled by the BitTorrent protocol.

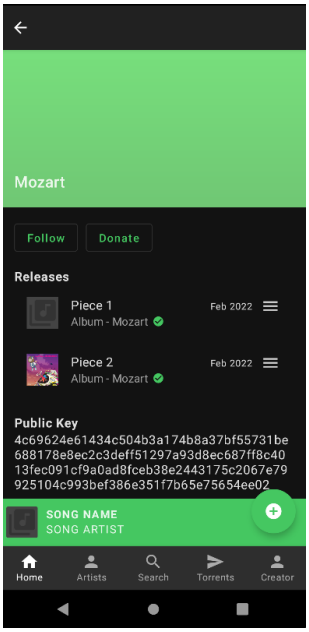


Fig. 6. Home screen of PoC application

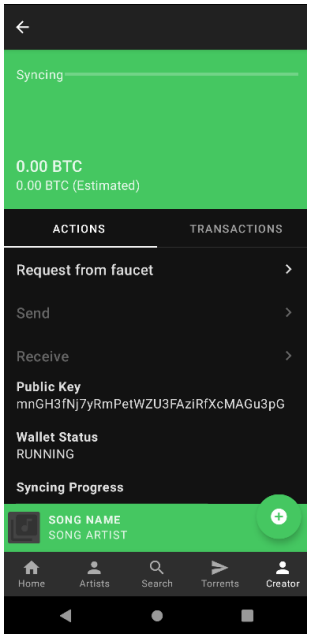


Fig. 7. Artist screen of PoC application

Discoverability of such data will be done through the BitTorrent DHT protocol through querying info-hashes. Meta-data such as info-hashes will be distributed through the platform using the IPv8 and Trust-chain. Users can publish meta-data on their own chain, or, in case transactions with other users data will be published and signed by two users on both their chains.

To access any type of meta-data three strategies wil be used:

1. Passively gossiping data to other peers on the overlay
2. Querying a specific user for all their meta-data 3. Querying random users in the overlay for a specific users meta-dat

Artists can set-up a crowdfund wallet within the DAO to request for funds from their listeners in return for a promise for music.

VI. Evaluation Results

VII. Conclusion

Acknowledgment

The preferred spelling of the word “acknowledgment” in America is without an “e” after the “g”. Avoid the stilted expression “one of us (R. B. G.) thanks ...”. Instead, try “R. B. G. thanks...”. Put sponsor acknowledgments in the unnumbered footnote on the first page.

References

[1] E. Foundation, “Daos, dacs, das and more: An incomplete terminology guide.” [Online]. Available: https://blog.ethereum.org/2014/05/06/daos-dacs-das-and-more-an-incomplete-terminology-guide/

[2] C. Komlo and I. Goldberg, “Frost: flexible round-optimized schnorr threshold signatures,” in *International Conference on Selected Areas in Cryptography*. Springer, 2020, pp. 34–65.

[3] J. Pouwelse, “Towards the Science of Essential Decentralised Infrastructures,” in *Proceedings of the 1st International Workshop on Distributed Infrastructure for Common Good*. Delft Netherlands: ACM, Dec. 2020, pp. 1–6. [Online]. Available: https://dl.acm.org/doi/10.1145/3428662.3429744

[4] E. G. Weyl, P. Ohlhaver, and V. Buterin, “Decentralized society: Finding web3’s soul,” *Available at SSRN 4105763*, 2022.

[5] Q. Zhou, H. Huang, Z. Zheng, and J. Bian, “Solutions to scalability of blockchain: A survey,” *IEEE Access*, vol. 8, pp. 16 440–16 455, 2020.

[6] P. Otte, M. de Vos, and J. Pouwelse, “Trustchain: A sybil-resistant scalable blockchain,” *Future Generation Computer Systems*, vol. 107, pp. 770–780, 2020.

[7] A. Torbensen and R. Ciriello, “Tuning into blockchain: Challenges and opportunities of blockchain-based music platforms,” in *Twenty-Seventh European Conference on Information Systems (ECIS2019), Stockholm-Uppsala, Sweden*, 2019.

[8] S. Wang, W. Ding, J. Li, Y. Yuan, L. Ouyang, and F.-Y. Wang, “Decentralized autonomous organizations: Concept, model, and applications,” *IEEE Transactions on Computational Social Systems*, vol. 6, no. 5, pp. 870–878, 2019.

[9] V. Buterin *et al.*, “A next-generation smart contract and decentralized application platform,” *white paper*, vol. 3, no. 37, pp. 2–1, 2014.

[10] “The state and future of Decentralized Autonomous Organizations (DAOs) including 6 leading examples - Ross Dawson.” [Online]. Available: https://rossdawson.com/futurist/companies-creating-future/top-decentralized-autonomous-organizations-dao/

[11] S. Wang, W. Ding, J. Li, Y. Yuan, L. Ouyang, and F.-Y. Wang, “Decentralized Autonomous Organizations: Concept, Model, and Applications,” *IEEE Transactions on Computational Social Systems*, vol. 6, no. 5, pp. 870–878, Oct. 2019. [Online]. Available: https://ieeexplore.ieee.org/document/8836488/

[12] Q. Zhou, H. Huang, Z. Zheng, and J. Bian, “Solutions to Scalability of Blockchain: A Survey,” *IEEE Access*, vol. 8, pp. 16 440–16 455, 2020. [Online]. Available: https://ieeexplore.ieee.org/document/8962150/

[13] X. Xu, I. Weber, M. Staples, L. Zhu, J. Bosch, L. Bass, C. Pautasso, and P. Rimba, “A Taxonomy of Blockchain-Based Systems for Architecture Design,” in *2017 IEEE International Conference on Software Architecture (ICSA)*. Gothenburg, Sweden: IEEE, Apr. 2017, pp. 243–252. [Online]. Available: http://ieeexplore.ieee.org/document/7930224/

[14] “bips/bip-0340.mediawiki at master · bitcoin/bips — github.com,” https://github.com/bitcoin/bips/blob/master/bip-0340.mediawiki, [Accessed 30-Jun-2022].

[15] W. Stallings, *Handbook of computer-communications standards; Vol. 1: the open systems interconnection (OSI) model and OSI-related standards*. Macmillan Publishing Co., Inc., 1987.
[16] J. Schickler, "Sweden, EU Discussed Bitcoin Proof-of-Work Ban: Report — coindesk.com," https://www.coindesk.com/policy/2022/04/21/sweden-eu-discussed-bitcoin-proof-of-work-ban-report/, [Accessed 30-Jun-2022].
[17] "Helium x2013; Introducing The Peopleapos;s Network — helium.com," https://www.helium.com/, [Accessed 30-Jun-2022].
[18] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," Dec 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf