Foundations for Grassroots Democratic Metaverse

Ehud Shapiro
Weizmann Institute of Science and Columbia University
Rehovot and New York, Israel and US
ehud.shapiro@weizmann.ac.il

Nimrod Talmon
Ben-Gurion University
Be’er Sheva, Israel
talmonn@bgu.ac.il

ABSTRACT
While the physical lives of many of us are in democracies (one person, one vote — e.g., the EU and the US), our digital lives are mostly in autocracies (one person, all votes — e.g., Facebook). Cryptocurrencies promise liberation but stop short, at plutocracy (one coin, one vote). What would it take for us to live in a digital democracy? This paper offers a vision, a theoretical framework, and an architecture for a grassroots network of autonomous, people-owned, people-operated, and people-governed digital communities, namely a grassroots democratic metaverse. It also charts a roadmap towards realizing it, and identifies unexplored territory for MAS research.

KEYWORDS
Digital Democracy; Digital Social Contracts; Sybil Resilience; Democratic DAO; On-Chain Governance; Social Choice; Grassroots Cryptoeconomy; Personal & Community Cryptocurrency; Grassroots Protocol Stack; Blockchain

ACM Reference Format:
Ehud Shapiro and Nimrod Talmon. 2022. Foundations for Grassroots Democratic Metaverse: Blue Sky Ideas Track. In Proc. of the 21st International Conference on Autonomous Agents and Multiagent Systems (AAMAS 2022), Online, May 9–13, 2022, IFAAMAS, 5 pages.

1 INTRODUCTION
A key obstacle to digital equality and digital democracy is fake and duplicate digital identities, aka sybils [17]. Facebook eliminates billions of sybils every quarter [51] and even if it would decide to go democratic [21], it is technically unable to [38]. Cryptocurrencies employ plutocratic proof-of-work [36] or proof-of-stake [31], partly for lack of a better way to defend against sybils [15].

Here we describe a vision, a theoretical framework, and an architecture for the grassroots formation of a network of autonomous, people-owned, people-operated, and people-governed digital communities, referred to as democratic DAOs (Decentralized Autonomous Organizations), which jointly form a grassroots democratic metaverse. A central theme of our approach is sybil resilience: means to minimize sybil penetration into the democratic digital communities that form the metaverse, and means for a digital democracy to function despite a limited sybil penetration. More concretely, our proposed architecture for a grassroots democratic metaverse calls for the design and implementation of several inter-related components, which have equality as a fundamental tenet, and to achieve that must be sybil-resilient.

2 DIGITAL SOCIAL CONTRACTS
Philosophically, a digital social contract is Proudhon’s [40] notion of the social contract—a voluntary agreement among free individuals—ported to the digital realm [12].

(1) Digital social contracts (Section 2) are Proudhon’s [40] notion of the social contract—a voluntary agreement among free individuals—ported to the digital realm [12].

(2) Democratic Governance of DAOs (Section 3) considers the broad range of issues that need to be addressed by digital social contracts that instruct democratic governance, namely democratic DAOs [1, 4, 9, 11, 18, 35, 44].

(3) Grassroots cryptoeconomy (Section 4) aims to facilitate the capital-free bootstrap of grassroots cryptoeconomic communities, starting from self-sovereign personal cryptocurrencies [48].

(4) Grassroots protocol stack (Section 5) supports the entire spectrum of communication and coordination needs of a grassroots democratic metaverse [47].

We expect this theoretical foundation and architecture to be realized as a common good, open and available to all. With it, autonomous democratic alternatives to existing digital autocracies and plutocracies may flourish.
members. In a digital social contract people agree to abide by the rules of the contract in their digital interactions with other parties to the contract. These rules are specified by a working code—as in standard communication protocols and in cryptocurrency-based smart contracts—so that the execution of a correct code by the people participating in the contract ensures that they abide by the contract. Unlike standard smart contracts, the intended parties to a digital social contract are people, digitally identified, not anonymous accounts or wallets. Digital social contracts are truly autonomous and egalitarian in their execution: They are executed by the parties to the contract themselves, using their own computing devices (smartphones, at present), rather than by anonymous third parties, namely miners that charge a fee (gas) for their service. The digital social contract may aim to exclude sybils with various sybil-resilient mechanisms discussed in Section 3.

Computationally, we distinguish two types of digital social contracts, depending on the depth of the protocol stack they employ (Section 5): Consensus-based and consensus-free.

A consensus-based digital social contract is a smart contract autonomously executed by its vetted participants [10, 12, 16]. It execution requires the full protocol stack presented in Section 5, including the ordering layer, as a correct execution of a smart contract requires consensus on the ordering of the acts of the parties to the contract. A key application of smart contracts are DAOs [19, 27], which typically specify a form of plutocratic governance. Similarly, a key application of consensus-based digital social contracts are democratic DAOs (Section 3).

A consensus-free digital social contract is a voluntary agreement among free individuals that employs a consensus-free protocol, namely a protocol lower down the protocol stack. In general, constitutional democratic vetting requires a consensus-based protocol. But in case of a digital social contract for leader-based group, vetting of participants can be done by the group leader, similarly to standard server-based social networks, based on a simpler dissemination protocol. Other consensus-free digital social contracts, e.g. the personal cryptocurrency network [48] discussed in Section 4, are open, or permissionless, in that any person may participate.

We envision digital social contracts that could cut the umbilical cord that today connects the multitudes to surveillance capitalism-based services [57] (e.g. Facebook), autocratic ‘sharing-economy’ apps (e.g. Uber, Airbnb), and plutocratic cryptoeconomy platforms (e.g. DeFi on mainstream cryptocurrencies), and supplant them with grassroots, peer-to-peer and community-based digital conduct – social, economic, and political. This could be achieved via digital social contracts for a host of cryptoeconomic applications discussed in Section 4.

Research challenges:

- Developing a programming language for digital social contracts.
- Programming use-cases of digital social contracts.

3 DEMOCRATIC GOVERNANCE OF DAOS

We consider issues that need to be addressed for the coding of digital social contracts for democratic governance, namely democratic DAOs. Democratic DAOs are related to today’s DAOs [19, 27], but with important differences: Today’s DAOs are usually among anonymous accounts, or wallets; their governance is typically plutocratic (one coin – one vote; or one coin – square-root vote, as in quadratic voting [32]); it is executed by anonymous third parties – miners that require remuneration (gas); and it is executed on a pre-determined platform and protocol. In contrast, a democratic DAO is among digitally identified individuals; its intended governance is democratic; it is executed by its participants; it is amenable to encompassing constitutional governance, as every aspect of the digital social contract, including the underlying protocol of execution as well as the democratic decision process itself, may be subject to democratic amendment.

The challenges of encoding a practical democratic DAO are immense, as it requires formalizing and integrating all aspects of digital democratic governance. These include: sybil-resilient social choice theory that allows a digital community to govern itself democratically despite a bounded penetration of sybils [35, 44]; digital constitutional governance, which provides for the constitutional democratic governance of a digital community, including the democratic amendment of the constitution itself [4]; sybil-resilient community formation, which provides for constitutionally-instated sybil-resilient community admission and expulsion protocols; effective egalitarian decision making, in which members are equal as proposers, discussants, coalition-builders and voters, addressing elections, legislation, and budgeting within a uniform framework [9, 18]; democratic coalition formation, merging, and forking, which includes democratic procedures for deliberation and coalition formation within a community [18], and for deciding on the merging of communities and the forking of a community [1, 11].

‘On-Chain’ Constitutional Governance: Leading cryptocurrencies employ an informal governance process that often causes so-called hard forks [54], in which an off-chain social decision process results in the previous protocol being abandoned by some or all of the participants; and a new protocol is initialized, ideally in a state (e.g. account balances) that reflects the state of all participants in the abandoned protocol.

On-chain governance [41] aims to avoid hard forks by providing a decision process in which the cryptocurrency’s protocol can be amended ‘from within’ according to the rules of the protocol itself. On-chain governance of cryptocurrencies is an open challenge [24], in particular as the governance shall not be limited only to the contract (e.g., as in Ethereum), but shall include governing the platform itself. A recent work [4] provides an initial axiomatization of relevant constitutional amendments and corresponding algorithmic methods, by considering a multiagent system of agents with preferences over the constitution.

Research challenges:

- Developing the theory of democratic amendments of governance procedures, including the constitution itself.
- Suggesting social choice mechanisms for on-chain forking, following recent work [2].

Sybil-Resilient Social Choice Theory: A cornerstone of the democratic metaverse is the ability to make joint community decisions. Viewing elections and voting as a standard tool for making joint community decisions, it is natural to look at computational social choice (COMSOC) [8] for answers; but keeping in mind that
the problem of sybils poses a serious threat to any online community wishing to use some of these mechanisms: As a simple example, consider a community of 100 agents, out of which 51 are sybils (i.e., fake accounts); then, if a single binary decision is to be made – for which the majority rule is a natural choice [34] – then the sybils effectively "control" the election. More generally, in any classical (non-sybil-resilient) voting scheme, a single sybil may tilt the decision or the elections result.

More concretely, a sybil-resilient election consists of a community of \( n \) agents, out of which at most a \( \sigma \)-fraction of the agents are sybils; and a sybil-resilient voting rule gets a corresponding set of \( n \) votes—without knowing which of the votes are from the sybils—and shall output an election winner, while satisfying some form of sybil safety. COMSOC has yet to consider the problem of sybils in earnest for its methods and results to be applicable for a digital democracy; but there is some initial progress in that direction: To define sybil-resiliency, Shahaf et al. [43] and Meir et al. [35] follow reality-aware social choice [49] in treating reality (i.e., the status quo) as a distinguished alternative that must always be present.

Based on this, sybil safety requires that the status quo should change only if a majority among the non-sybils support the change; and sybil liveness requires that the status quo can be changed even if all the sybils oppose the change. They show that supermajority voting rules—for various degrees of supermajority used—can satisfy both sybil safety and liveness, provided the fraction of sybils is below \( \frac{1}{3} \). Slightly farther away, the works of Tran et al. [52] and Waggoner et al. [53] (as well as others), can be viewed as showing some theoretical impossibility results regarding the possibility of voting rules that are resistant to sybils.

**Research Challenges:**

- Evaluating the theoretical lower bounds on the supermajority degree that guarantees certain safety-liveness tradeoffs practically.
- Studying sybil-resiliency for further COMSOC settings, such as multiwinner elections [20], participatory budgeting [7], and constitutional amendments [3, 4].

**Practical Egalitarian Decision Making:** Practical decision making mechanisms are critical for the success of democratic DAOs.

**Research Challenges:**

- Developing egalitarian decision making procedures, in which members are equal as proposers, discussants, coalition-builders, and voters [18], addressing elections, legislation, and budgeting within a uniform framework [9], to facilitate egalitarian and effective democratic governance.
- Investigating democratic coalition formation, merging, and forking, that are democratic procedures for deliberation and coalition formation within a community [18], and for deciding on the merging of communities and the forking of a community [1, 11].
- Developing unified, generic decision making processes that can encompass different COMSOC settings, similarly to metric-based aggregation methods, that, together with metric embeddings for these different social choice settings, may be useful [9], particularly if it can also be integrated with a uniform process for deliberation, voting, and ad-hoc coalition formation [18, 23].

**Grassroots Community Formation:** Given adequate sybil-resilient voting rules, a digital community can tolerate some sybils, but not so if the fraction of sybils is too large (specifically above \( \frac{1}{3} \) [44]). Considering the dynamic nature of community formation, the question arises how can a digital community grow while retaining a bounded-fraction of sybils? This relates to sybil identification [5] and prevention [33, 50].

First, one has to distinguish between genuine personal identifiers and sybils [45]: Essentially, genuine personal identifiers are unique and singular, while while sybils are either duplicate or fake. Put differently, an honest person would only declare a single identifier as their genuine personal identifier (or declare a new identifier as a replacement, e.g. if their private key was lost or compromised), while a dishonest ("Byzantine") person would peddle sybils – they would create multiple identifiers and claim each of them to be their own genuine personal identifier (duplicates); create identifiers and claim them to be genuine identifiers of people that do not exist (fake); or knowingly perpetuate sybils created by others.

The dynamics of community formation can be modeled via a transition-based system: Initializing with some community seed, the system transitions by adding or removing community members; while some upper bound on the fraction of sybils shall be maintained. In particular, if an initial digital community consists of identifiers of honest people; if honest people tend to trust honest people more than they trust non-honest ones; and if the trust graph of a digital community—the graph depicting the trust relations in the community— is rich enough, then new people can be safely added to the community while maintaining a bound on the sybil penetration of the community. Intuitively, this can be done by ensuring sufficient connectivity in the trust graph. E.g., ensuring that the conductance of the community’s trust graph (which relates to the vertex and edge expansion of the graph) does not decrease following the addition of new (identifiers of) community members guarantees that the fraction of sybils that penetrate the community can be bounded [39].

**Research challenges:**

- Proposing local connectivity measures—in contrast to graph conductance that is a global measure—that make it easier to understand what does a person need to do in order to be admitted to the community.
- Performing extensive simulations to assess the quality of solutions for sybil-resilient community growth.
- Developing mechanisms to encourage honest people to be judicious in granting their trust, encourage sybil hunting, and reward sybil detection; investigating the integration of a due process for sybil determination, and the cross-community interaction for strengthened sybil-resilience.

## 4 Grassroots Cryptoeconomy

Mainstream cryptocurrencies—based on proof of work [36, 55] or stake [31]—grant participants power and wealth in accordance with their capital investment, thus benefiting the few and exacerbating economic inequality. In contrast, the goal of grassroots cryptoeconomy [48] is to bootstrap a thriving trust-based and community-based cryptoeconomy without external capital or credit and without reliance on third-party computing services. The proposed grassroots cryptoeconomic components include:

**Self-sovereign personal cryptocurrencies** [48] can form the basis of grassroots economies, with community cryptocurrencies [46]
as an emergent phenomena. A personal coin is best thought of as a transferable unit of credit issued by one person to another, and two people can establish a mutual line of credit between them [28] simply by exchanging their personal coins. Liquidity in a grassroots economy can be achieved via such mutual credit lines, forsaking initial capital or external credit. Fault-resilience and transaction-finality are provided by each agent regarding its own personal currency. Self-sovereignty means that the responsibility for the economic and computational integrity of a personal currency resides with the person; as the value of a personal currency depends on such integrity, every person is incentivized to maintain them.

**Community banks/credit unions** [48] may be realized as democratic DAOs, owned, operated and democratically-governed by their members. Such a bank may streamline liquidity and simplify payments within a grassroots cryptoeconomic community that employs personal cryptocurrencies. The bank issues its own currency and provides credit to its members at its discretion. It allows each member to deposit their personal coins and draw bank coins, up to the person’s credit limit, in return for the members accepting its coins, which becomes a *community currency* [13, 46, 48]. The deposited personal coins are the bank’s collateral, and any agent may redeem bank coins, first to its own personal coins held by the bank and any remaining balance to other personal coins held by the bank. A community currency can achieve sybil-proofness via a stake-based web of trust [26, 45], being an essential ingredient of the community formation process discussed in Section 3. The process relies on trust among agents, and requires an incentive mechanism that backs up trust edges by mutual sureties [26], denominated in the community currency redeemed by the community if the trusted personal identifier is determined to be a sybil (via a due process specified by the community’s social contract). This may require community members who wish to invite others to the community to lend them coins or provide them credit in this currency, to finance the mutual surety.

**Universal Basic Income (UBI).** External support to a community bank—governmental or philanthropic—can boost the liquidity of the community and allow the bank to provide community members with a growing credit line in community currency, akin to UBI [6, 13, 28, 29, 46, 48].

**Democratic social networks.** Commercial social networks follow the Feudal model of governance, where the corporate chief executive embodies all three branches of government—legislative, executive, and judicial. Members have no civil rights and are meagerly-remunerated, if at all, for the exploitation of their digital capital (personal information) or labor (consuming ads and commercial content, creating engaging content). A democratic social network, realized as a democratic DAO, can be members-owned and operated, have proper democratic governance, and share revenues among members based on their contribution.

**Sharing-economy digital cooperatives.** The ethos of earthly cooperatives includes autonomy and democratic conduct. As such, democratic DAOs offer a natural embodiment for their digital counterparts: members’ owned, operated and governed digital cooperatives. In addition to digital cooperatives for social networks that offer a democratic and income-sharing alternative to Facebook, we envision a true sharing-economy drivers-and-passengers-owned cooperative that may offer a beneficial alternative to Uber, and a true sharing-economy owners-and-renters-owned cooperative that would be preferable to Airbnb.

**Research challenges:**
- Developing the concept of a network of community-issued currencies, concentrating on issues of liquidity and interoperability, both theoretically and practically, using multiagent simulations.
- Validating the notion of personal currencies and its viability as an infrastructure for sureties, theoretically and practically.

5 GRASSROOTS PROTOCOL STACK

Executing the different applications enabled by digital social contracts (Section 2) on networked personal devices requires a novel, alternative communication protocol stack. Such a protocol stack would provide the entire spectrum of communication capabilities needed for the grassroots-formation of a democratic metaverse, starting from peer-to-peer messaging and culminating in democratic DAOs. In contrast to a monolithic protocol (e.g. blockchain consensus [36]), a protocol stack can provide each application class the needed functionality in the most efficient, integrated, scalable way, as depicted in Figure 1. Such a protocol stack should provide in an open and egalitarian way the entire spectrum of communication capabilities needed for the grassroots formation of a democratic metaverse [47], including:

1. *Messaging.* Serverless peer-to-peer communication, enabling serverless alternatives for personal messaging apps such as WhatsApp/Messenger/Telegram/Signal, without control or surveillance by third parties.
2. *Dissemination.* Serverless group formation and communication; enabling serverless alternatives for groups messaging apps such as WhatsApp/Telegram/ Facebook.
3. *Equivocation exclusion.* Serverless and consensus-free prevention of double-spending in NFT trade networks and personal cryptocurrencies [14, 25, 37, 48].
4. *Ordering.* An efficient, autonomous, and egalitarian distributed consensus protocol (e.g. [22, 30, 56]) for the execution of consensus-based digital social contracts.

An example of such a protocol stack is presented in reference [47].

**Research challenges:**
- Considering various architectures for such a protocol stack and efficiently implementing the above-mentioned layers.
- Proposing practical, permissionless trust-based peer-to-peer messaging, dissemination and equivocation exclusion protocols.

6 OUTLOOK

We have described a vision, an architecture, and a roadmap for the grassroots formation of interconnected and interoperable autonomous digital communities, such as democratic social networks, sharing-economy digital cooperatives, democratic social movements, and political parties. We have highlighted different subfields of MAS that are relevant to advance the vision and its different components. Viewed as a whole, we discussed how the presented architecture and its components could enable the grassroots formation of a democratic metaverse.
