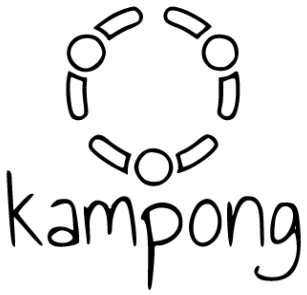


1. Project Vision *

Kampong Protocol is a composable and adaptively secure *communication infrastructure* for decentralized applications such as metaverses, games, marketplaces, DAOs, and any other web3 primitives.

Just like a physical kampong [1], it takes joint effort and consensus of a village to raise a safe and secure web3 community. Kampong Protocol is a key enabler of such villages..

The protocol offers the following major advantages:
- **Real-time decentralized communication** and collaboration orchestrated by a community's native tokens
- **Community-driven** seamless **authentication** and group **consensus**: Peer-to-peer and peer-to-many multi-factor, multi-modal authentication is supported with empathy to user experience.

Current problems faced by the communities:

The project is addressing two key problems of cyber-physical communities:

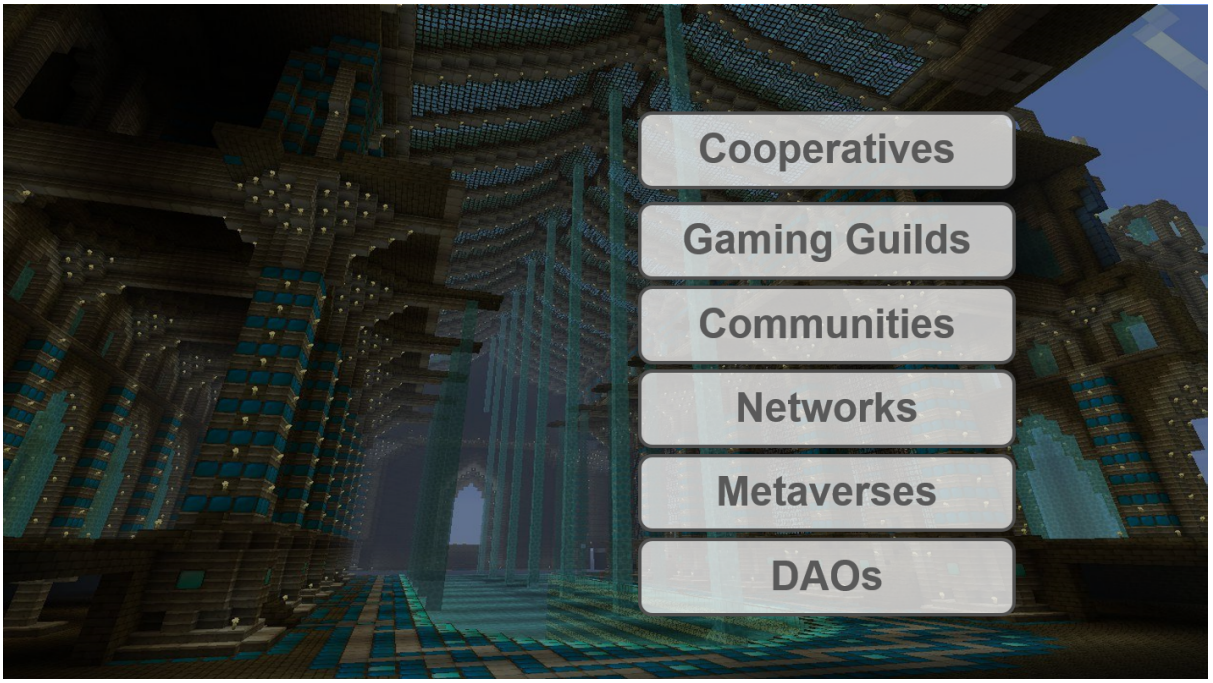
A. **Communication** is centralized, controlled and spread out across multiple Web2 platforms: Current communication infrastructures do not meet the demands of Web3 decentralized communities and self sovereign groups or *Kampongs*.

B. **Authentication** (multi factor authenticator (MFA)) is clunky, insecure and controlled with imbalances between security and usability. Conventional methods are susceptible to OTP interception, SIM swapping attacks, and TOTP copying. Also, a member of a community should be able to control and provide/release information related to authentication and

claims when needed. Also, a bad (time consuming and distracting) user experience is one of the reason that community might not readily accept current forms of MFAs

Target audience

Every DAO and metaverse dApp and their communities irrespective of blockchain.



Solution

Kampong Protocol provides the following:

- A Javascript library for the Kampong protocol-
- utility crypto token
- an app to serve as a multi-factor token device
- various communication+collaboration+authentication use cases.

References

[1] https://en.wikipedia.org/wiki/Kampung_(village)

2. Project Construction *

Project cycle

The core features of the demo for Kampong Protocol were developed in the last two weeks of December soon after we heard about the Moledao hackathon.

Project roadmap

Our roadmap included the following key stages.

A. Inception of the Kampong philosophy

B. Architecture Decision for peer to peer communication

C. Securing communication channels with user centric MFA so that there is no excuse for not adopting it

D. Defining befitting use cases such as group chat, live scratchpad etc

E. Scaling

F. Tokenization

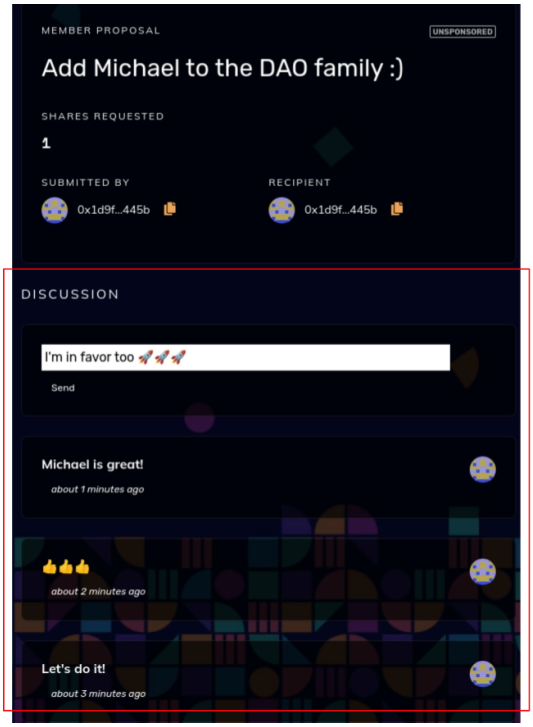
The business model of the project

What if you could collaborate with your community

***on the very platform** where all the action is?*

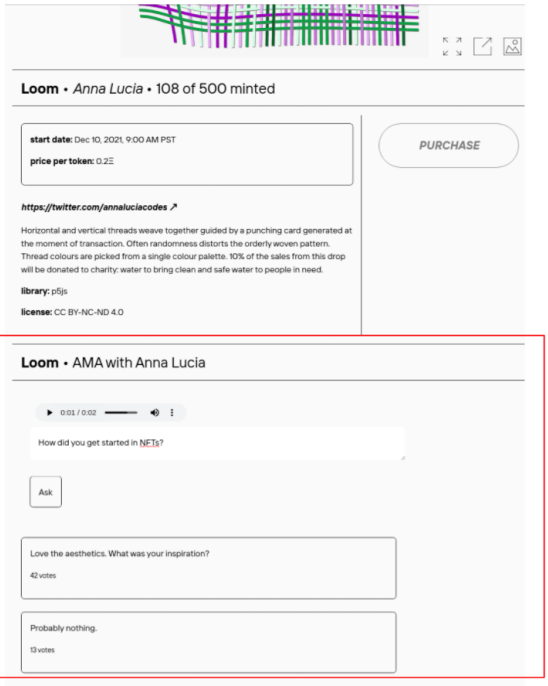
Kampong Protocol brings decentralized communication and authentication on any platform of your choice. Here are a few examples:

DAOhaus

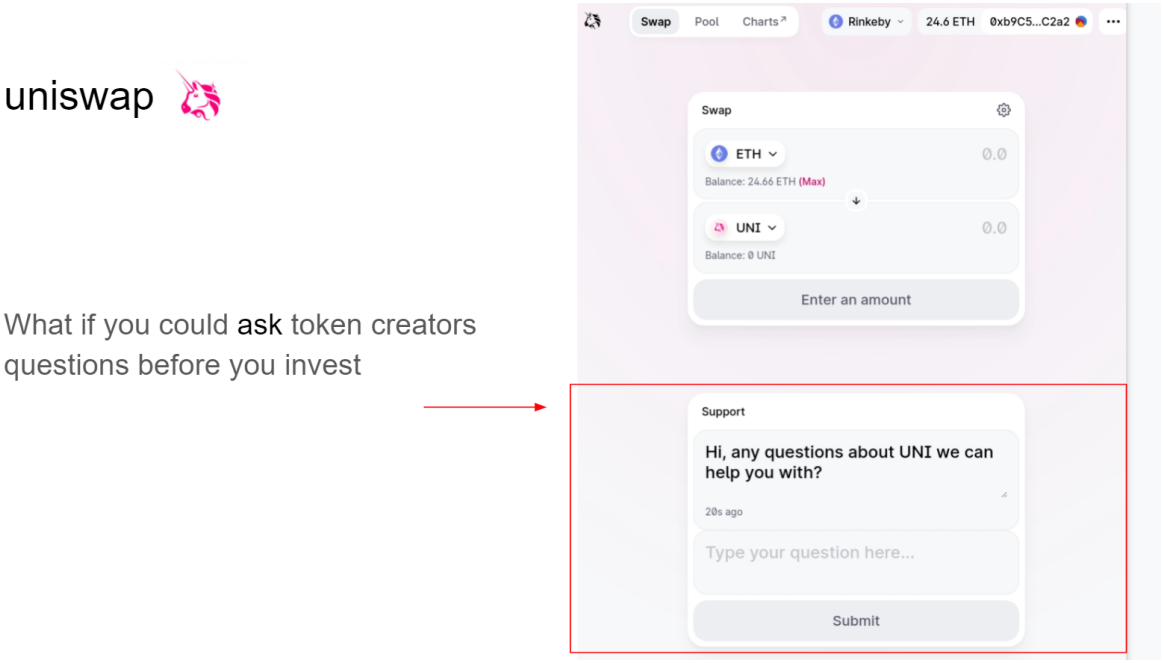


What if DAO members could discuss proposals before committing on chain

art blocks



What if an artist could hold a voice chat with their fans during a NFT drop



Kampong's native utility token **PONG** is used to run a **community-run network** of bootstrap nodes powering the global network. In the future, other nodes including browser nodes can participate in the network to help audit other nodes and detect malicious actors. The nodes are incentivized to secure the network and ensure accountability.

Additionally, **a community's native token** can then be used to provide the same auditing and detection of malicious nodes in their own private networks. This is useful for token-gating primitives which are a norm in communities such as DAOs and participatory games which rely on crypto tokens (such as ERC20/ERC721 tokens like currencies/NFTs).

Team division of labor

Simon: building out the decentralized communication infrastructure and integrating it with Kampong Auth
Jay and **Saket**: building out the secure and usable multi-factor authentication infrastructure (Kampong Auth)
Sanskar: design

Technical architecture

A. Decentralized Peer-to-Peer Communication

Kampong is a **new**, fully **decentralized** peer-to-peer **network** enabling **browsers** to **communicate** and **collaborate** with each other **without** requiring any plugins or **extensions**.

On the **network level**, the innovation is to enable browsers to form a p2p network **without** a **centralized** service. Once a browser is part of the global p2p network, it can be used to find and connect with other peers to form a **private network**.

Kampong is the **first** communication network built from **scratch** that is fully decentralized and **crypto-native**. It **solves** the **bootstrap** problem in a general way and provides the **bridge** for **Web2** to **Web3** with every dApp or DAO website integrated with Kampong serving as the user's entry point.

Because **tokens** are **natively** supported, private communities are **token-gated**, the **wallet** serves as a user's **identity** and the **number** of **tokens** held by the user as a **trust** signal.

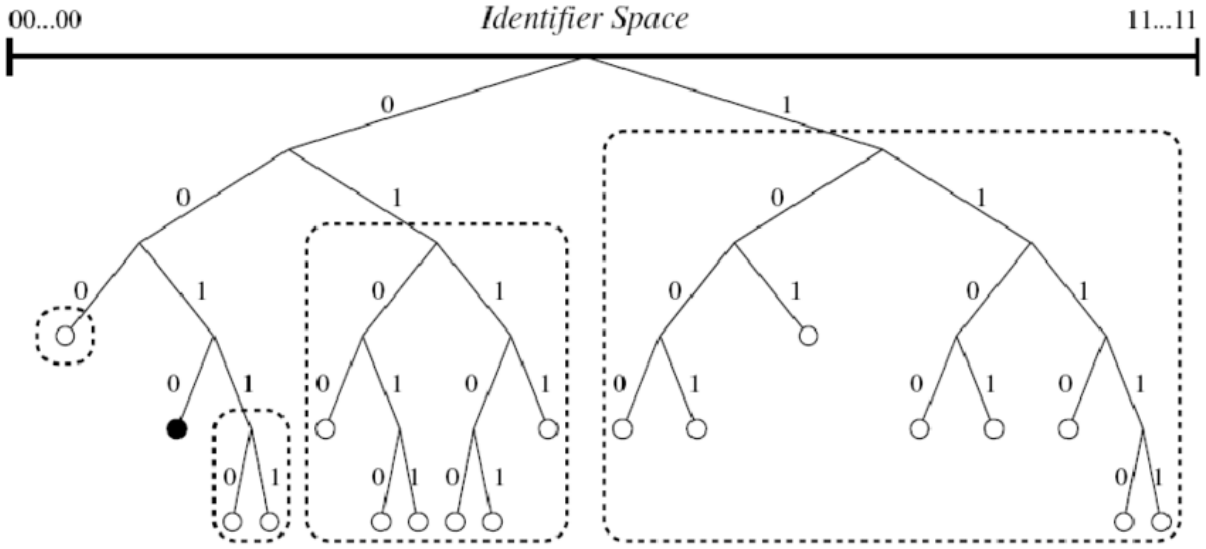
Because communities are decentralized, there is no platform enforcing their rules, but every community defines their **own governance rules** and **collectively enforces** them holding each other **accountable** using **cryptographic proofs**.

Integration can be as simple as using the **JavaScript SDK's** standard widgets and **no coding** required. For a more **custom experience**, Kampong can be integrated with **any UI framework** such as React or Vue.js.

Since the token defines the community and users use their wallet, there is **no registration** or **signup** required - true **permissionless** collaboration and integration.

The core protocol of Kampong allows nodes to form a **decentralized peer-to-peer network**. The participating nodes form a structured overlay network and are able to send messages to any other node in the network efficiently using the Kademlia routing algorithm.

The protocol implements a distributed hash table (DHT) to store key-value pairs across the network. The DHT (**distributed hash table**) is used to also implement a **decentralized publish/subscribe system**. BitTorrent famously uses DHTs to look up files in the network.



Furthermore, the protocol also implements an accountability protocol ensuring Byzantine faults are eventually detected and relies on game theory by using incentives to be resistant to selfish nodes and freeriding.

- Every node has a unique 32bit ID (SHA-256 of its DTLS certificate) and establishes a limited number of bi-directional connections with other nodes roughly following the Kademlia DHT routing protocol and thus reaching any other node **in O(log(n)) hops**.
- Besides providing a key-value store, the network can also be used as a decentralized publish/subscribe system using the SCRIBE algorithm.

Digital spaces exist without scarcity where people can come and collaborate with each other using their own norms, rules and structure. This results in an ownerless collaboration platform designed to incentivize pro-social behavior and cooperation.

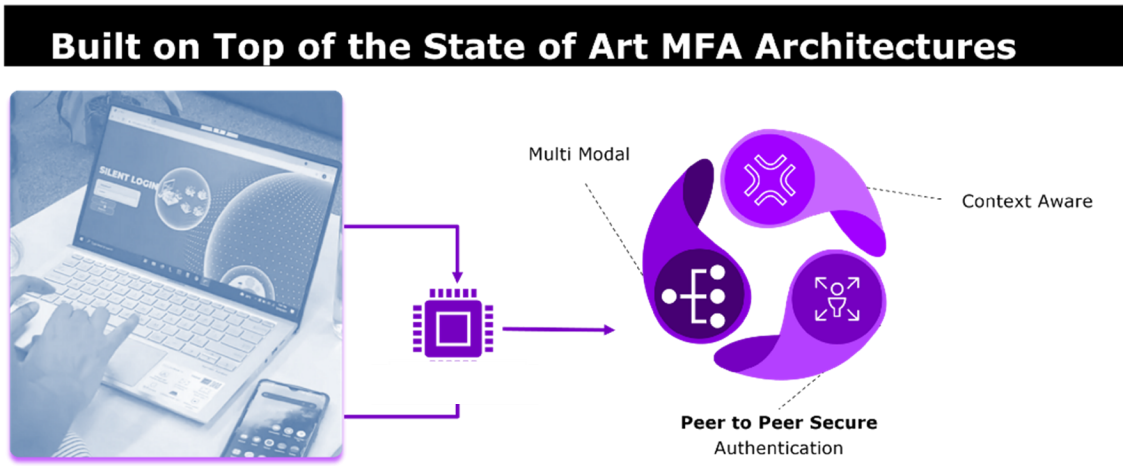
B. Authentication:

Kampong Auth is pushing unique affordances for authentication to make dApp/community experiences more usable and secure.

B.1 **Unique Proofs:** On top of existing multi-factor authentication architecture, unique proofs have been designed for higher confidence among the community participants. These include proof of possession of the authentication device, proof of liveliness and proof of co-location. For higher risk applications, Kampong Auth does check if peer-to-peer

communicating applications and the tokens are in proximity or not (not based on GPS, but rather using peer-to-peer communication channel). It also supports proof of liveliness and continuous authentication as.

B.2 **Adaptiveness and Composability**: Compared to standard adaptiveness which is based on the perception of risk using network layer parameters (location, IPs, device IDs) and the nature of transactions, we have added an extra layer for the perception of risk: physical context and understanding of spatiotemporal parameters governing the dynamics of the users. **Multi-modal risk estimation** brings more confidence in the community.



B3: **Defence**: Proofs of **liveliness** and a unique **context verification algorithm** (based on proximity) will rule out bot farms [where multiple phones are placed in co-located farming units]. We have developed algorithms to identify bots which are co located using spatial and temporal data fusion across **acoustic**, **radio frequency** and **sensory domains.**

Additionally, these proofs will deter attacks which haunt contemporary MFA supports to communication channels such as OTP (one-time password) interception, SIM swapping attacks, TOTP (time-hashed OTP) copying due to accessibility based vulnerabilities in

smartphones, automated or habituated approvals of push notifications in 2FAs (two-factor auth) and proxy authentication due to lack of proofs.

In Kampong Auth, a community's activity helps to authenticate itself with these proofs.

3. Project Demo

https://www.youtube.com/watch?v=e0jf5hXKpcI

Key project results

Repo: https://github.com/simonpure/kampong
Live website: https://simonpure.github.io/kampong/
Recorded demo: https://www.youtube.com/watch?v=e0jf5hXKpcI

Project operation status: **Successfully running** (**anyone can build and try it out**)

The following features are showcased in the project demo video, available on the live website to try out or run locally from the GitHub repo:

- Authentication
- Multiple blockchain support
- Wallet as identity including token holdings
- Accessing token gated private community
- Shared scratchpad for live collaboration
- Group chat messaging

User experience

User experience demo https://www.youtube.com/watch?v=e0jf5hXKpcI
This is an infrastructure project. The UX is best experienced when teams integrate Kampong Protocol into their own products natively. Feel free to reach out to us at simon.l@gmail.com