WASMIUM

Pseudonymous. Community Banking.

LITEPAPER

https://wasmium.network

CC0-1.0

No Rights Reserved

The ideas in this document are licensed under the creative commons zero license which is a public domain license.

However, the branding, like logos and the name “Wasmium” cannot be used by other projects and are not part of the public domain therefore are not covered by the CC0-1.0 license.

PUBLIC DOMAIN

Introduction

Community banking is the most widely used form of savings in developing nations. In East Africa, these micro-savings groups are called `Chamas`. These micro-savings groups have a few members saving a few hundred dollars a month. These micro-savings groups are responsible for managing more than $3 Billion.

These micro-savings groups are exclusive. To join, an existing member must provide assurances about your capacity to make contributions and abide by the group's constitution.

The most common structures of these micro-savings groups are Rotating Savings and Credit Associations (ROSCA) and Pooled Investment with Shares.
Micro-savings groups are not regulated. Most of them are composed of leaders without the financial know-how to manage members' funds.

ROSCA structure is the most common structure. This structure involves members contributing a certain amount of funds every week, fortnight or month as outlined by the constitution of that particular micro-savings group. The funds collected from all the members are given to the member in the current rotation. The risk with this structure is that the unfaithful members early in the rotation can refuse to make contributions to a member. The outcome is that at the next rotation, certain members will receive a lower amount of funds. Jealous members will refuse to contribute their fair share to a member.

The Pooled Investment with Shares structure is where members contribute a certain amount of funds every month to buy a certain percentage of shares representing an investment made by the group. The investments can be in transportation, real estate, agriculture, stocks and bonds. Members are also offered loans at a high interest rate, as much as 20%.

Problem Statement

These micro-savings groups have a bad reputation due to lack of regulation, poor governance and mismanagement. The Wasmium Peer-to-Peer Wealth Management protocol uses smart contracts and encryption to solve most of these issues like:

1. Mismanagement of funds
2. Lack of transparency
3. Lack of oversight from all members
4. Control of the pooled funds by a few members
5. Lack of access to equal opportunities in invested funds
6. Lack of access to a stable currency
7. Security of funds
8. Lack of anonymity on voting
9. Improper implementation of penalties for defaulters
10. Lack of access to global financial infrastructure

The Wasmium Network will solve all these issues and improve financial inclusion in third world countries.

Wasmium Wallets

A Wasmium Network wallet implements asymmetric key cryptography which is the building block of most blockchain protocols. An Ed25519 version of the Edwards-Curve Digital Signature algorithm is used as the digital signature scheme due to strong security guarantees with shorter keys (256bit public keys and 256 bit private keys) with support for batch verification of 512bit signatures. This makes the algorithm the ideal choice for a great user experience due to it's speed and reasonable security guarantees while conserving some battery life on mobile devices.

The blockchain of choice for the Wasmium Network must have fast transaction speeds and support Ed25519 keys out of the box. This allows a Wasmium account to integrate directly to the blockchain simplifying the network structure and reducing the surface area of attack at the protocol level.

A Wasmium Account is, therefore, able to sign hashes for messages, MACs, ECDH message keys like X25519 keys, attachments, contracts and other files while at the same time being able to perform authorization transactions from multi-signature accounts and Web3 authentication requests; making it the perfect workspace tool for DAOs, individuals and enterprise users.

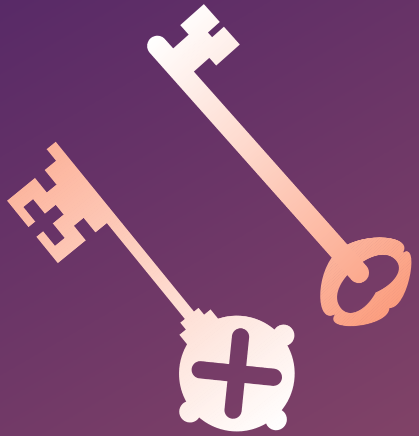
Community Strength

A Wasmium Wallet implements multi-signatures using **`custodians`**. A custodian is a singular application capable of signing a message using Ed25519 asymmetric keys.

A Wasmium Wallet can be configured to reside on the blockchain as a smart contract. To authorize the execution of tasks that involve transactions, the wallets registered as custodians on the smart contract must sign the transaction or message.

Using a smart contract wallet allows an individual to secure their funds using multiple “Ed25519 Capable” applications.

A smart contract wallet can be configured as the account of a micro-savings group solving the problem of a few members only having access to those funds and ensures that a majority approves a transaction to debit funds from the pool.



Key Exchange

Members of a micro-savings group need to chat and propose spending funds in the pool. To do this, the Wasmium Network will provide chatting capabilities using Extended Triple Elliptic-Curve Diffie-Hellman (X3DH) key exchange and Double-Ratchet protocol to secure messages between members.

The blockchain provides auditable and transparent storage of the X3DH long-term static keys and ephemeral public keys. A Wasmium Account Client is responsible for the generation of the X3DH keys, publishing them to the program associated with the Wasmium Account and updating new ephemeral keys in case existing keys are used up.

The structure of the storage on the blockchain is a simple stack storing `N` number of tuples with each tuple consisting of a X3DH public key and the TAI64N timestamp when that public key was generated.

```
struct X3DHStore {
     (timestamp, static_key),
     (timestamp, signed_prekey),
     [(timestamp, unsigned_prekeys); N],
}
```

Custodians

A custodian program is an app with a Signer and Verifier E25519 algorithm to sign messages. A group member can use another E25519 capable wallet to sign transactions and messages.

Hardware keys configured to sign a message and produce Ed25519 signatures are also supported.

A timestamp is used to co-ordinate between the signing applications. An increasing monotonic timestamp is used to ensure time-drift can be detected especially on blockchains that rely on chronological occurrence of events for consensus. In this case, Tai64N (12 byte timestamp) is used for timekeeping.

```
struct Custodians<const N: usize> {
        public_key: [u8; 32],
        custodians: [[u8; N], [u8; 12]]
}
```

Voting on Proposals

Wasmium Network safeguards the confidentiality of votes of each member by ensuring only the network knows who voted. Only the outcome of the results is revealed to the group members.

This voting mechanism is simple. A user sends a vote and a signed hash of the proposal they are voting for. The network verifies that a user is part of the group, verifies that the signature of the proposal is valid and then increments a counter for “Approve” or “Reject” a proposal. If signatures don’t match, the vote is rejected. If the hash of the proposal doesn’t match, the vote is rejected.

Stable Coins

Several third world countries have a weak currency against other currencies like USD, GBP, Euro or CHF. In some countries, hyper-inflation is a serious problem affecting the purchasing power of citizens.

Through the Wasmium Network, micro-savings groups have access to various stable coins. Stable coins will ensure savings are secure and the value of their hard earned money will stay relatively stable for a long time.

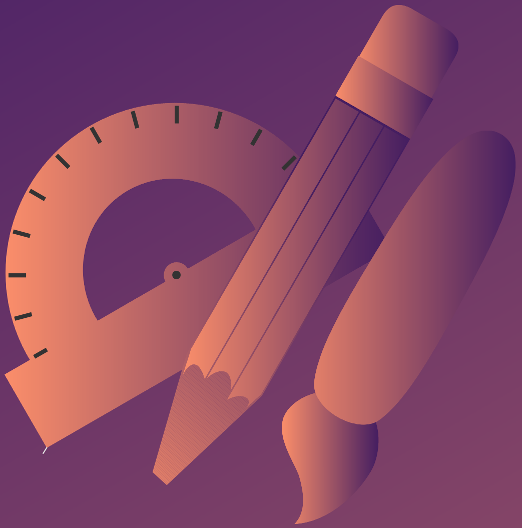
Members will be able to exchange stable coins for cash through peer-to-peer transactions ensuring that the network offers a one stop solution for savings, investment and a decentralized exchange .

Micro-savings groups can even trade with other groups and ensure transparency in peer-to-peer transactions.

De-Fi Vaults

Growing the investment of the micro-savings group could mean investment in real estate, transport, government bonds or any other traditional investment opportunity.

The Wasmium Network will provide access to DeFi fixed savings protocols, liquidity pools, yield farming and other investment opportunities in the DeFi metaverse. To achieve this, the Wasmium Network will collaborate with an autonomous DeFi interest generating protocol on a fast blockchain.



Extra Tools

The Wasmium Network will provide access to financial analysis tools that track the growth of a member's funds. To ensure transparency on how the yield on investment is generated, analytics are provided on each individual's wallet in real-time.

This will counter the problem of reliance on leaders to provide an accurate assessment of the investments.

A Wasmium wallet will offer tools to create or upload a constitution, proposal generation and voting tools.

Two factor authentication is also provided by the Wasmium Network in case a user wants to further safeguard their wallet.

WASMIUM

Pseudonymous. Community Banking.

Decentralized Financial Independence for the developing world.