UnitedCoin White Paper

Introducing Proof-of-Membership (POM): Hybrid micro Proof-of-Resource (POR)/Proof-of-Stake (POS) blockchain with the UnitedCoin Investment Management Platform

Abstract

Cryptocurrencies have become increasingly popular since the emergence of Bitcoin in 2009. The cryptocurrency market cap as of October 30, 2016 is over $150 billion dollars and is projected to be over $2 trillion by 2027. However, most cryptocurrency services such as encryption, transactions, mining, staking, and trading are only accessible and usable by expert developers and traders. This amounts for less than 1% of the current population. UnitedCoin aims to “bridge the gap” and make these same services accessible to the other 99%, and the majority of the public through the use of a hybrid microPOR/POS blockchain connected to a user friendly desktop/mobile app. Streamlining cryptocurrency services by bridging them with the legacy financial system and services individuals are currently using.

UnitedCoin Network

The UnitedCoin Network is a distributed and decentralized members only Investment Management platform (UIM) backed by members with donated resources and a stake in the network. The UIM platform is accessed via a browser or a mobile/desktop app/GUI. Member Identity and Private data is self-encrypted and stored in the secure element on the members’ device.

UnitedCoin Investment Management Platform (UIM)

The UIM Platform is distributed and stored in chunks on member devices to maintain decentralization. The UIM is a platform where members can conduct P2P transactions and exchange cryptocurrencies from multiple blockchains at a high rate with absolute security and trust.

The UIM platform interconnects multiple blockchains allowing simple and fast transfer of funds. Within this trusted network transactions can occur at speeds of up to 1m tx/s. The UIM holds 98% of all member funds offline in cold storage to maintain the highest levels of security. The platform is secured with a Wildcard SSL certification to maintain security in all environments.

The UNIT

The token connected with the UnitedCoin Network is the UNIT. UNITs are used to pay fees, and for staking in order to receive a portion of the UnitedCoin Monthly Member Benefit (MMB). The MMB is a 2% monthly return on the UNITs held in each member's wallet. This is the method by which new UNITs are created.

UnitedCoin Member Security

Each member's identity is known and verified to the UnitedCoin network, however member identities and private data are not shared with other members. This allows the network to comply with all AML/KYC/BSA/CFT regulations

while still maintaining member privacy. Member Identity may only be disclosed when a member invites another potential member into the network by transferring them cryptocurrency or via referral link. This is done to create familiarity. “I’m in. I’m inviting you to join. Let’s coin together.”

Member UIM platform access is available by user name and password along with a pin and/or 2 factor authentication (2FA) through Google Authenticator. The Member Identity is then self-encrypted and stored in the secure element of the member’s device. A self-authentication feature allows the member to access the UIM platform with privacy and ease.

UnitedCoin Member Vault (UMV)

Each member holds an encrypted chunk of data stored in the secure element section of their device. This area is known as the UnitedCoin Member Vault (UMV). The first chunk of data held in each vault is the encrypted member identity, the UnitedCoin Distributed Hashing Table, a copy of the UIM platform and the last 2 blocks of the UnitedCoin blockchain. The network uses distributed hashing tables with Kadmila to establish a secure peer to peer network.

All data held in a UMV is self encrypted and can only be decrypted by the UnitedCoin Network which holds the UnitedCoin Member Data Table. This method of storing chunks of Member Data in the UMV ensures any individual member device breach will be localized and have no effect on the UnitedCoin Network.

To participate in the microPOR, a member need only activate their UMV with a simple selection in the app settings and select the amount of resources they are willing to donate to the network. Once activated Members are included on the UnitedCoin Member List.

UnitedCoin Pool (UCP)

Through agreed upon permissions a member donates a portion of their device's memory and processing power/ resources to the UnitedCoin Network for data storage and to the blockchain for transaction processing. The collective UMVs create the UnitedCoin Pool (UCP). MicroPOR can be performed on a device as small as a mobile phone or as large as a mining rig.

The amount of resources/power per member allowed in the pool has a ceiling. The network pools all transaction fees, and redistributes them to members based on their participation in the network monthly via the Monthly Member Allowance (MMA). Member portion of the MMA is determined by the amount of resources they donate and the amount of UNITs staking in their app UNIT wallet. The member resources/ power ceiling and fee distribution method discourages large mining farm centralization of processing power/resources and encourages a distributed decentralized network.

Maximum Proof of Resource Donation per Member per Month

- CPU power: 4GHz
- Memory: 128GB
- Hard drive Space: 1TB
- Data: 50GB

All microPOR participating member devices are UnitedCoin Blockchain nodes as well as a UMV. As long as the device is connected to the internet, the member device/node is able to participate in both hosting the UIM platform and in verifying transactions on the blockchain. Additional Member Resources in the UnitedPool can be used for additional tasks. The first of which is cryptocurrency mining and High Frequency Trading (HFT) to increase member MMA.

UnitedCoin Wallet

The UnitedCoin wallet is used in the member app. The member app is accessed by member user name and password. The member app uses a hierarchal deterministic wallet to allow access to wallet funds with a 12 word password phrase. All wallets supporting the UnitedCoin blockchain can be used to access member funds.

Members can access their private keys from the network at anytime but are not required to hold their keys or use them to conduct transactions. Therefore allowing novice users to participate in the network without advanced knowledge and experience of public/private key use and storage. The private and public keys are encrypted and held in the secure element on the member device maintaining the highest levels of security and privacy.

UnitedCoin Blockchain

The UnitedCoin Blockchain uses a hybrid microPOR/POS protocol. The UnitedCoin Blockchain is backed by each UMV and by UNIT token member stake in the network to allow

transactions to take place almost instantly. UIM transactions are check-pointed on the UnitedCoin blockchain every 10 seconds to verify and log each transaction in a decentralized distributed ledger while keeping the transaction value and the identity of the sender and receiver private using ring signatures and zero knowledge proofs.

Using resources from the UCP, the blockchain eliminates double spending attacks and any issues with two nodes solving the same block twice because all network power/ resources are pooled to form one united supercomputer validator. Thus creating only one “longest” chain of verified transactions. If a member device is compromised, the chunk of the network stored in their UMV can easily be found duplicated in another UMV in the pool. UMV data duplication also makes un-desired chain splits impractical therefore securing the longevity of the UnitedCoin blockchain.

Checkpointing allows both double transaction verification through consensus of UIM transactions while also performing remote attestation of all nodes on the network. Creating a trusted verifiable proof-of-membership (POM) on all transactions. Through checkpointing millions of previously verified UIM transactions can be included in a single block and signed with one member signature through the use of snore signatures. Through the use of double transaction verification, member nodes/UMVs need only hold and broadcast a few blocks to maintain consensus throughout the network.

Zero knowledge proofs are able to take place on-chain because transactions are double verified by first the UIM and

second by the blockchain. Member devices are used to store the UIM and the first level of verified transactions. Member UNIT stakes held in account are used to verify and sign transactions on the blockchain to perform the second level of verifying transactions. There is no individual block reward for participating in the microPOR/POS. Large mining farms are again discouraged, securing distribution and decentralization throughout the network.

Blockchain governance and upgrade decisions are conducted via a simple yet mandatory voting system through the member app. Only 1 proposal can be made every 30 days and are held in queue on a first come first served basis. When a new proposal is presented to the network, there is a 30 day voting period to determine if it is a change desired by a majority of members.

A simple in app voting form is displayed prior to access to the member account. The proposal is described in 180 characters or less with a choice of yes, no, or no contest. If the member chooses to ignore/close the voting form without a selection, a vote of no contest is entered. In order to be implemented, a proposal must have 51% member participation with a 51% member approval as well.

References

Maidsafe white papers:
https://github.com/maidsafe/Whitepapers/blob/gh-pages/pdf/AutonomousNetwork.pdf

https://github.com/maidsafe/Whitepapers/blob/gh-pages/pdf/MaidSafeDistributedFileSystem.pdf
https://github.com/maidsafe/Whitepapers/blob/gh-pages/pdf/MaidSafeDistributedHashTable.pdf

https://github.com/maidsafe/Whitepapers/blob/gh-pages/pdf/PeerToPeerPublicKeyInfrastructure.pdf

https://github.com/maidsafe/Whitepapers/blob/gh-pages/pdf/SelfAuthentication.pdf

https://github.com/maidsafe/Whitepapers/blob/gh-pages/pdf/SelfEncryptingData.pdf

https://github.com/maidsafe/Whitepapers/blob/gh-pages/pdf/MaidSafeDistributedHashTable.pdf

https://github.com/maidsafe/Whitepapers/blob/gh-pages/pdf/MaidSafeDistributedFileSystem.pdf

Monero white paper:
https://cryptonote.org/whitepaper.pdf

Zcash white paper:
http://zerocash-project.org/media/pdf/zerocash-extended-20140518.pdf

NXT White Paper:
https://bravenewcoin.com/assets/Whitepapers/NxtWhitepaper-v122-rev4.pdf

https://www.coindesk.com/standpoint-founder-bitcoin-asset-class-will-grow-2-trillion-market/