Unichain

The technical white paper

UniLab

December 15, 2021 - Version 2.0

Abstract

Unichain is a highly scalable blockchain platform that takes advantage of cutting-edge technologies, and has the capacity of handling from several thousands and up to millions of transactions per second while preserving decentralization and security. UniChain is designed for general purpose and aimed at bringing decentralized technologies and convenient tools to the smart society 5.0 so that everyone can totally control their digital assets, identity and privacy ... They can also enjoy the free financial system that cannot be managed by any single administrator.

UniChain is a product of the Uniworld Ecosystem [1] and has been developed by Uni Dao Network with the philosophy "*All values created by people are for people's happiness*".

The mainnet was officially launched on June 4th, 2020. There have been hundreds of accounts (wallet addresses) registered since then [2] and UNW (native token of platform) has been widely accepted by the large community and big exchanges.

I. Introduction

Blockchain is getting more and more popular today. It is not just a crypto-currency but also applying in many traditional applications such as loyalty program, user identity, supply chain, health care, insurance and banking [3] … the first and most famous blockchain is Bitcoin which is described as p2p electronic cash can process around 3 -7 transactions per second (TPS) [4]. Ethereum is described as blockchain 2.0 that supports smart contract and decentralized application. The maximum number of transactions that Ethereum can handle is 15 TPS [4]. Some recent blockchain platforms promise to increase the TPS to hundreds or thoudsands TPS by changing the consensus algorithm (for example: Proof of Stake, Proof of Authority …) or applying the sharding, multi chain technologies.

It is clear that those above-mentioned blockchains cannot be used in real and daily applications. The more people join the network, the more transactions and the more time to wait for transactions to get confirmed.

Scalability is one of the most important factors of blockchain platforms besides decentralization and security.

We also believe that for mass adoption, the blockchain platform must be scalable, cheap and extremely convenient for users.

In the following sections, we propose a new blockchain platform that combines advantages of many current blockchain technologies including side chain architecture, Dpos-HotStuff consensus algorithm, bridge protocol, platform native features and also the incentive model. We call it the Unichain.

II. Side chain architecture

Unichain is a blockchain platform that supports multi-chain, the root and central chain is Unichain which plays an important role to validate all side chain’s states and also link them together.

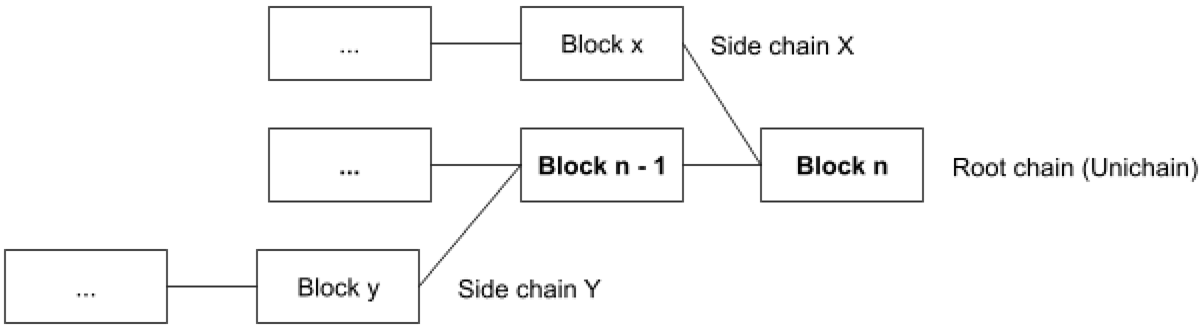


Figure 1. Side chain architecture

Each side chain has its own block and transaction validators. Side chains are independent from each other, they have a separate ledger, operation from chain X cannot take effect to chain Y and vice versa. Because of this independence, we can scale out the platform as much as we want. Imagine that each side chain can handle around ten thousand transactions per second. We will reach millions of transactions per second if the platform has 100 side chains.

Communication between chains

Side chains communicate with root chains and other chains via smart contract. Unichain provides a smart contract system for this communication called *Uni bridge protocol*. Funds on side chains are also held on the root chain. This allows for deposit and withdrawal of side chains with state transitions enforced by fraud proofs.

Side chains do not disclose all information on the root chain. Instead, blockheader hashes and a little bit of state are submitted and if there is proof of fraud submitted on the root chain, then the block is rolled back and the block creator is penalized by a smart contract system governed by the root chain.

Uni bridge protocol also help Unichain communicate with other blockchain platform, ie. information, tokens in Unichain can be exchanged to Ethereum, Bitcoin, EOS ...

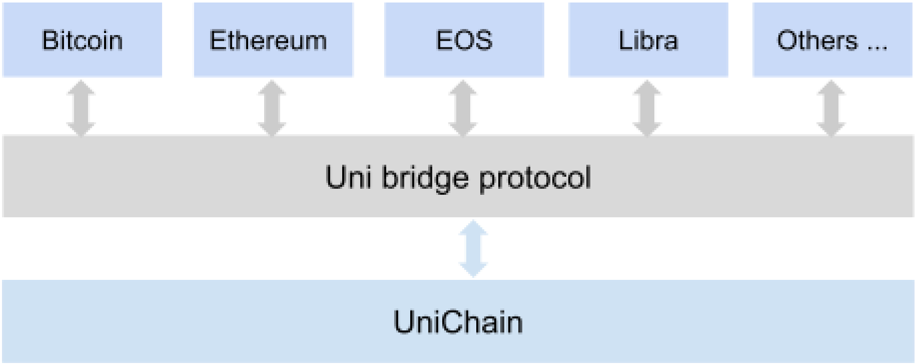


Figure 2. Uni bridge protocol

In the case of exchanging a token for another blockchain platform, Uni Bridge protocol works as a decentralized exchange.

III. DPOS-Hotstuff consensus algorithm

Consensus is the heart of any blockchain platform. The popular consensus algorithm in Bitcoin and Ethereum is proof of work (PoW) which consumes huge amounts of energy to secure the ledger. This type of consensus algorithm makes the blockchain totally public and decentralized but cannot scale to adapt to the big volume of transactions. In this paper, we apply the Delegated Proof of Stake (DPOS) to our platform. DPOS is not a new consensus algorithm, it has been applied in Bitshare, EOS … But we try to combine the DPOS with HotStuff [6] and side chain architecture to make our system scalable and reach the block finality exactly after one second.

DPOS algorithm

DPOS is a consensus algorithm developed to secure a blockchain by ensuring representation of transactions within it. DPOS is designed as an implementation of technology-based democracy, using voting and election processes to protect blockchain from centralization and malicious usage. Before fully understanding how Unichain DPOS works, here are some basic terminologies.

- Account: Is the unique identity on Unichain, each account has its key pairs, address is an account representation on blockchain.
- Uni token: is the native token curriculum in Unichain and other side chains.
- Stakeholder: any account with token balance > 0.
- Node: as referred to a normal node is a software that anyone can download and run. The node maintains the ledger, validates and updates transactions.
- Witness node is a full node that is represented by an account with a minimum of 1,000 Unitoken and receives enough votes from the community. Transactions and blocks are only validated by witness nodes.

In Unichain, there are 33 active witness nodes by default but not limited to increasing that number in the future. To become a witness node, the stakeholders must deposit at least 1,000 Unitoken (UNW) to their accounts then broadcast transactions to register as witness candidates. Other stakeholders will vote for the witness, the power of vote is based on the token that stakeholders have. Top 33 candidates with largest votes will become the witness nodes. The voting process is repeated after every 7,200 blocks, called the epoch. In each epoch, every witness node has the capacity to produce about 218 blocks.

How witness nodes produce block in Unichain

After the election process, 33 elected witness nodes are now ready for producing blocks. The traditional DPOS algorithm round-robin produces block, ie. block n is produced by witness n

$$Witness \in \{1, 2, 3, n-1, n\}$$
$$Block \in \{1, 2, 3, n - 1, n\}$$

The process is predicted and may be broken up by some dishonest witnesses. To protect the block producing prediction turn, we propose a random witness producing block while ensuring that every witness producing equal number of block (218 blocks for each epoch)

Random witness chosen algorithm

$$Witnesses \in \{1, 2, 3, n-1, n\} n = 33$$
$$magicNumber = hexToIn(last10Digit(previousBlockHash))$$
$$index = magicNumber \bmod 33$$
$$Witness = Witnesses[index]$$

Because the previous block hash is only known at the processing calculation time, the magicNumber is the unknown number and therefore the next selected witness remains a secret. By using the fore-said formulations, one witness may be chosen n-time to produce blocks and it may exceed the capacity of 218 times. To solve this problem, when any witness reaches the maximum number of producing blocks, it is removed from the random selection pool, giving other witnesses a chance.

HotStuff

HotStuff is a leader-based Byzantine fault-tolerant (BFT) replication protocol for the partially synchronous model which is used in the Libra project. It reduces the communication complexity to linear in the number of replicas. HotStuff changed the BFT communication from mesh to star network, which relied on the leader.

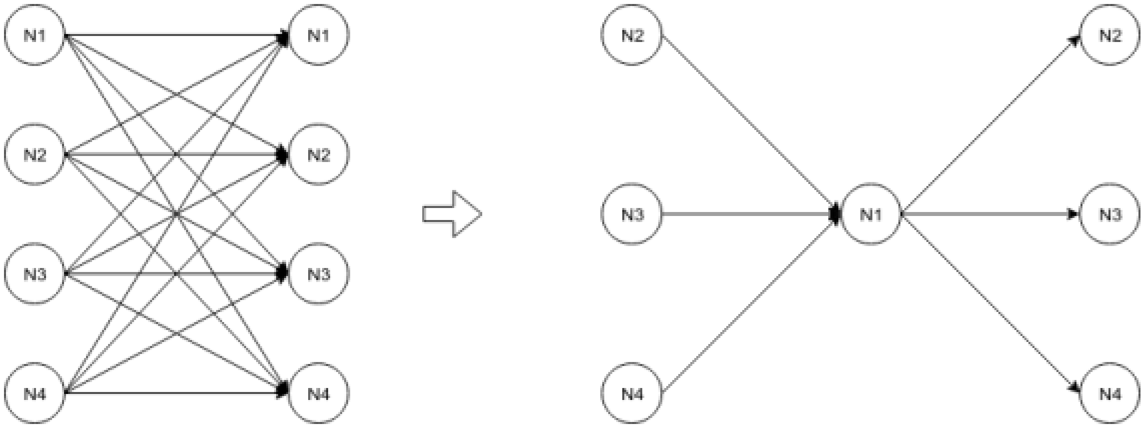


Figure 3. BFT' mesh vs. HotStuff's Star network

The traditional practical BFT uses two rounds of message exchanges. The first phase guarantees proposal uniqueness through the formation of a quorum certificate (QC) consisting of (n – f) votes. The second phase guarantees that the next leader can convince replicas to vote for a safe proposal. The algorithm for a new leader to collect information and propose it to replicas—called a view-change. The view-change based on two-phase in traditional BFT is not simple, bug-prone [5] and complex communication. Any proposal in BFT has a communication footprint of $O(n^3)$ authenticators. The total number of authenticators transmitted if $O(n)$ view-changes occur before a single consensus decision is reached is $O(n^4)$.

HotStuff revolves around a three-phase core, allowing a new leader to simply pick the highest QC it knows of. It introduces a second phase that allows replicas to “change their mind” after voting in the phase, without requiring a leader proof at all. This alleviates the above complexity, and at the same time considerably simplifies the leader replacement protocol

	Authenticator complexity		
Protocol	*Correct leader*	*view-change*	*f leader failures*
DLS	$O(n^4)$	$O(n^4)$	$O(n^4)$
PBFT	$O(n^2)$	$O(n^3)$	$O(fn^4)$
SBFT	$O(n)$	$O(n^2)$	$O(fn^2)$
Tendermint/Casper	$O(n^2)$	$O(n^2)$	$O(fn^2)$
HotStuff	$O(n)$	$O(n)$	$O(fn)$

The phase in HotStuff

- Pre-commit phase: When the leader receives the *prepare-vote* for current proposal, it combines to *prepareQC* and then broadcasts the *pre-commit* to all nodes in the network.
- *Commit phase*: The leader receives *pre-commit* votes from *(n-f)* nodes, then combines it into a precommitQC message and broadcasts to all nodes in the network. When replicas receive the message, they lock the state transition request so that the consensus decision can be reached.
- *Decide phase*: When the leader receives enough commit votes from the network, it combines all commitments to *CommitQC* then broadcasts the *decision* message to the network. Replicas in the network receive the *decided* message, execute the state transition, commit the state and start the next view.

The pipelined HotStuff

HotStuff has the same phase at all times: prepare (not an official phase), pre-commit, commit, decide. The flow structure: other nodes vote on a message, and the leader combines the votes and broadcasts them to other nodes. These phases can be represented uniformly and pipelined

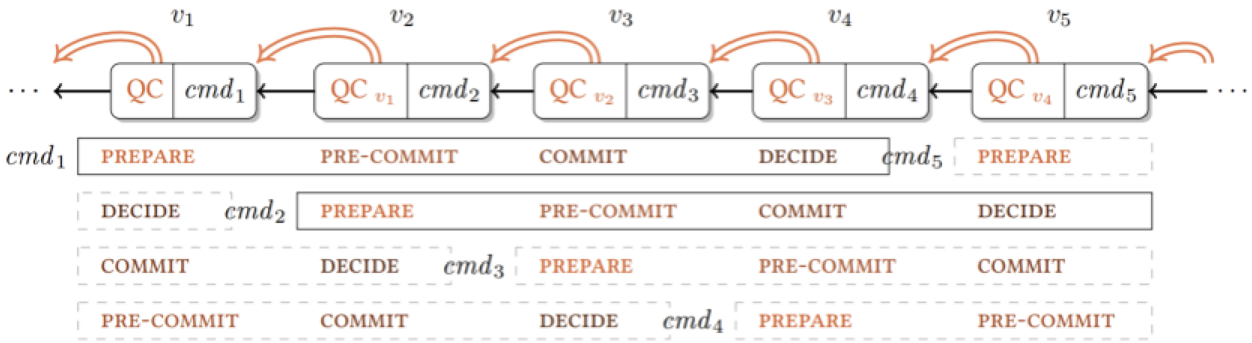


Figure 4. The pipeline HotStuff

IV. UniChain native features

Native features are one of the special features of UniChain. It helps non-crypto users to access blockchain technology easily without using intermediate applications or having in-depth technical knowledge. Imagine if a farmer can create a token or put his digital assets on a decentralized ledger with some simple clicks on the unichain tool web app.

The native token (URC-30)

URC-30 is similar to the ERC-20 standard on the Ethereum network. The difference is that ERC-20 is managed by a smart contract system, i.e it must be developed and deployed by technical users. URC-30, on the other hand, is the native code that executes on top of the VM and everyone can create the token by filling parameters on the web or mobile application interface. Another special feature is that users can transfer URC-30 tokens to each other without the transaction fee in terms of UNW (gas fee) instead the fee is calculated from the tokens themselves.

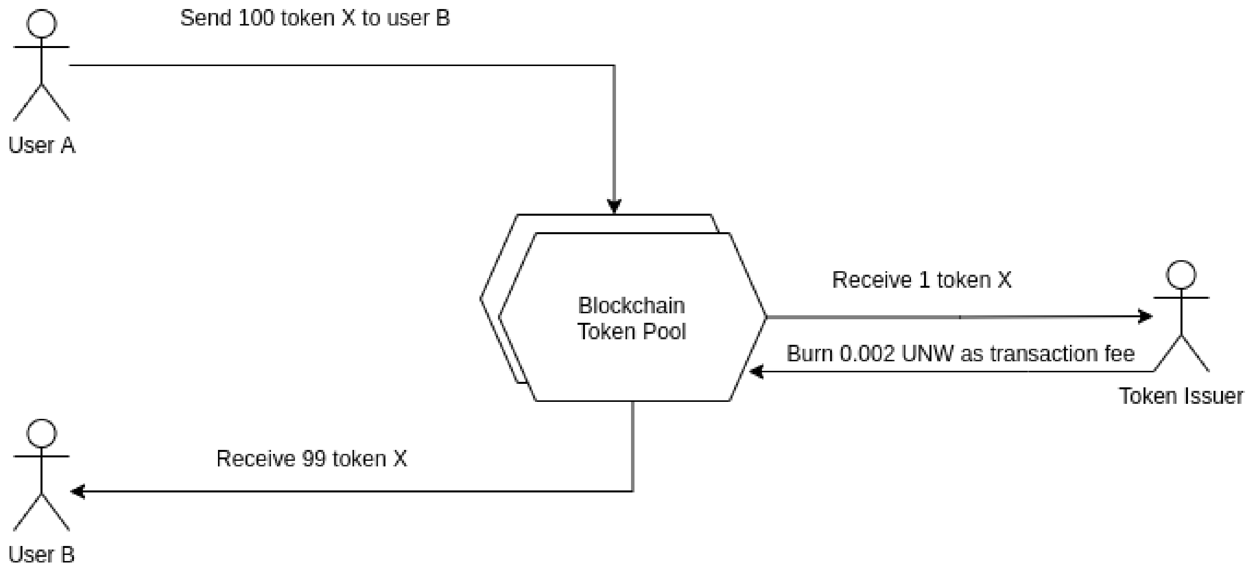


Figure 5. URC-30 token fee mechanism

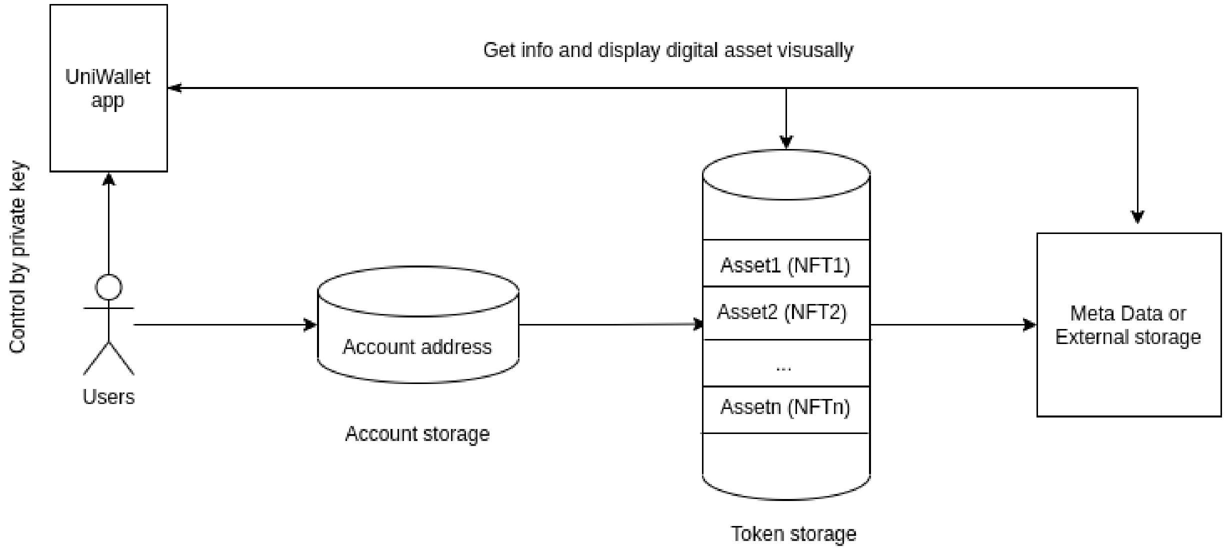
URC-30 Token supports the following functions:

- Create token;
- Transfer token;
- Mint token (only token owner to increase the circulation);
- Burn token (only token owner to decrease the circulation);
- Donate token pool fee;
- Transfer token owner;
- Transfer future token;
- Claim future token; and
- Update token params.

The native NFT (URC-721/URC-1155)

UniChain supports native NFT (Non-fungible token) and follows the ERC-721/ERC-1155 standards. Tokens run on top of UVM (UniChain VM - like EVM on Ethereum) without any smart contracts system.
With this feature, users can create any NFT token representing their digital assets by using a popular web/app interface and with the help from Uniwallet [7], the digital assets can be displayed visually (for example the

image, video, 3D avatar or any other assets following the Uni NFT standards)



Picture 6. Native NFT token in UniChain

Others native features

Many other features will be added to UniChain as long as it conforms to certain standards and brings convenience to users. These native features will remove the middleware and complexity of using blockchain technology

V. Unichain ecosystem & Incentive model

As mentioned above, Unichain is a product of the UniWorld Ecosystem. Many other UniWorld products that use UniChain will create a side chain on the UniChain network. These chains will link together, complement and share to each other.

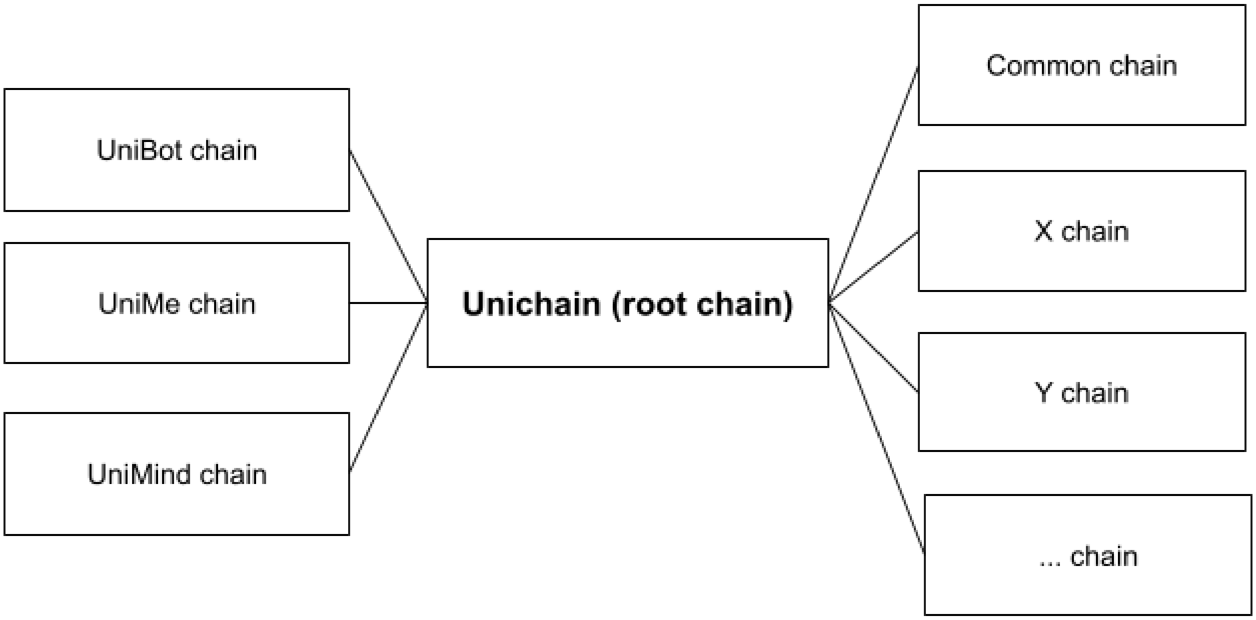


Figure 5. Unichain ecosystem

- UniBot (https://unibot.org) chain is a blockchain for Chat bot application. We deploy smart contracts to verify the chat bot, store online payment history and protect fraud transactions.
- UniMe (https://unime.world) is a secure end-to-end encryption chat (and also audio/video call) mobile application. It also integrates the multi-chain wallet and blockchain hub so that users can interact with many types of blockchain in just a single app.
- UniMind is related to Artificial Intelligence. This is the first blockchain that combines two hottest technology trends.
- Common chain is for any other applications such as finance, gaming …
- X, Y, Z … chain is the chain created for any other purposes.

UniWorld token (UNW) is the main token curriculum on Unichain, although each side chain can create its own token using smart contract curriculum in its chain, it is worth noting that UniWorld token is the valid token to all chains and is the medium to link the chain together. UniWorld token is also used for transaction fee to protect the network from spammers, exchange for other tokens (coins) in Unichain exchange platform (if UniWorld token is using as exchange fee, the fee is reduced by 80%)

Create new side chain

Everyone can create a new side chain if she/he has some token balance in her/his wallet. Currently it is set to a minimum of 250,000 UNW. The following steps describe how K creates a side chain.

- K creates a new wallet and deposit > 250k of Unitoken to her wallet.
- K creates a special transaction (calling a smart contract on the root chain) that requests creating a new side chain. This transaction will cost 250,000 UNW and directly burnt to burnt address.
- K's transaction is validated by root chain validator (witness), and because K meets the condition, transaction is valid, successfully added to ledger and returns the chainID.
- K creates a side chain with the chainID above. At this time, the side chain has only one member (ie. K) and K is the *creator* of this chain.
- K invites more people to join the new side chain, operate, deploy smart contracts and use that chain for K's purpose.

Become a Witness Node

Every stakeholder can be a witness candidate. To become a witness node, a stakeholder must have at least 1,000 UNW in her/his wallet. The following steps describe how stakeholder K become a witness:

- K deposits 1000 Uni tokens to K's wallet.
- K creates a proposal transaction to become a witness node, the transaction fee for witness creation will be 1,000 UNW and it is burnt directly to the burnt wallet address.
- If K's transaction is valid, K will be listed as a witness candidate and wait for the voting process.

- Other stakeholders see the list of witness nodes in the pool, and start voting for nodes that they feel trusted. The voting power depends on the total number of token stakeholders.
- 33 witness candidates received the highest votes will become the official witness, others still in the pool, waiting for the next voting process or become the alternative witness (in case of witness nodes fail or cannot produce block within a specific time).

Incentive Model

To encourage users for their voting and witness nodes for their works (verify and produce transactions, blocks), UniChain has the reward mechanism for both of them. The rewards are accumulated every 6 hours (election time). The following accounts will receive rewards:

- The active witness nodes (33 nodes).
- The candidate nodes (55 candidates).
- Voters who vote for active witness nodes or candidate nodes.

Please note that the active witness nodes are also the candidate nodes

Reward calculation

Because rewards are accumulated every 6 hours, let's calculate the rewards in that duration:

- For active witness nodes: Reward per each block is 1 UNW. Assuming that block time is 3 seconds, the total reward for active witness nodes is *1x6x60x60/3 = 7,200* UNW. However, active witness nodes share reward with their voters by a specific ratio, so the actual reward that an individual active witness may receive is *0.2x7200/33 = 43.6* UNW (assume that the ratio is 20%:80%).

- For candidate nodes: 55 candidate nodes share 7,363 UNW for every 6 hours. The actual reward that an individual candidate node may receive will depend on the votes that the candidate node receives and the distribution ratio sharing with his voters. The amount is calculated as following formula:

  $$candidateReward = ratio_{candidate} * 7363 * \frac{vote_{candidate}}{vote_{totalNetwork}}$$

  assume that the distribution ratio is 0.2 (20%), and the votes/total_network_votes is 1/55 (equal voting) so the reward is 0.2x7363x1/55 = 26.7 UNW.

  The active witness node is also the candidate node so the actual reward in example above would be 43.6 + 26.7 = 70.3 UNW (~281.2 UNW/day)

- For voters:
  - If the votes are on the active witness nodes, reward will be calculated as follows:

    $$reward = (1 - ratio) * 7200 * \frac{vote}{totalActiveVote*33}$$

  - If the votes are on the candidate nodes, reward will be calculated as follows:

    $$reward = (1 - ratio) * 7363 * \frac{vote}{totalNetworkVote}$$

  Please note that the active witness node is also the candidate node and therefore, if users vote on the active witness node, they get both rewards. The actual reward will change by time because the witness ratio and the vote count on the witness nodes and on the total network.

Burning tokens

Unlike other blockchain platforms, transaction fee in Unichain does not go directly to block producers (witness nodes). It goes to a special address (*U0000000000000000000*) and because no one knows the private key of this address, It means that the token is burning. Burning tokens make the UniWorld token more valuable in the future. The table below shows some of transaction fees to burn

Transaction type	Fee to burn (Uni token)
Transfer token to account	0.000267
Register as witness node	1000
Create new side chain (feature feature)	5000
Create token	500
Call smart contract function	Based on smart contract complexity

VI. UniChain Specifications

- Block time: 1 - 3 seconds.
- Transactions per second (TPS): 5,000 for a single chain.
- Block confirmation (finality): 1 - 3 seconds.
- Native token: UniWorld Token (UNW).
- Total token: 1,000,000,000 (one billion tokens).
- Transaction fee: based on computational complexity, the normal transfer token cost 0.000267 UNW.
- Consensus algorithm: DPOS-HotStuff
- Number of witness nodes: 55 nodes, 33 active and 22 alternatives.
- Smart contract language: currently supports solidity. (Nodejs and Java in the future).
- Digital signature algorithm: ECDSA.
- Multi chain: Yes.
- Cross chain communication: Yes.

The following compares some popular blockchains with UniChain

Technical Spec	Bitcoin	Ethereum	IOTA	EOS	UniChain
Consensus algorithm	PoW	PoW	Tangle	DPOS-BFT	DPOS and Hotstuff
Transactions per second (TPS)	3	15	300	thousands	Millions
Block time (second)	600	15	NA	~1	~1-3
Confirmation time (in seconds)	1800	150	NA	~1	~1-3
Smart contract	x	✔	x	✔	✔
Multi chain	x	x	X	x	✔
Cross chain communication	x	x	x	x	✔

VII. Conclusion

In this paper, we propose the combination and modification of many cutting-edge technologies to UniChain. We believe Unichain is one of the most powerful blockchain platforms that meets the requirement from real applications (ie. scalability, decentralization, security and user-friendliness).

Our target is to make Unichain not only be used for the crypto world but also for every decentralized application around the world.

VIII. Reference

(1) *Uniword ecosystem (https://uniworld.io) including UniBot (https://unibot.org), UniMind, UniLab, UniChain (https://UniChain.world), UniCom (https://mia.world) ...*

(2) *https://uniscan.world UniChain scan (or explorer https://explorer.unichain.world) to explore blockchain details such as the account, block, transaction …,*

(3) *Shiroq Al-Megren, Shada Alsalamah, Lina Altoaimy, Hessah Alsalamah, Leili Soltanisehat,Emad Almutairi.* Blockchain Use Cases in Digital Sectors: A Review of the Literature

(4) *Dejan Vujičić, Dijana Jagodić, Siniša Ranđić.* Blockchain Technology, Bitcoin, and Ethereum: A Brief Overview

(5) *Maofan Yin, Dahlia Malkhi, Michael K. Reiter, Guy Golan Gueta, Ittai Abraham.* HotStuff: BFT Consensus with Linearity and Responsiveness

(6) *Ittai Abraham, Guy Gueta, Dahlia Malkhi, Lorenzo Alvisi, Ramakrishna Kotla, and Jean-Philippe Martin. 2017. Revisiting Fast Practical Byzantine Fault Tolerance. CoRR abs/1712.01367 (2017). arXiv:1712.01367*

(7) *UniWallet (https://uniwallet.world)*