Unification - A Vehicle for United Network Distribution (UND)

A hybrid public/private blockchain ecosystem built for enterprises

Version 3.0 Published
February 11th, 2019
www.unification.com

To give context of the problem being solved, one should understand that Unification began as a “2nd layer” protocol - Drawing from the core teams collective experience in enterprise consulting and software development - UND was originally designed to be solely a “data liquidity” protocol which would allow enterprises to standardize/tokenize their data and place it in a liquid format to be bought/sold/transferred over a blockchain. What we were building was not “sexy,” rather it was fulfilling a very lucrative, yet possibly boring need for enterprises and the future of data.

As the team spent better part of a year developing the codebase and engaging in early enterprise outreach - over the course of hundreds of conversations and then subsequent verification of realities, it became quite apparent that it was not possible to create a functional “2nd layer” when in practical reality there was no “1st layer” that worked in any way that would be functional for any sort of serious enterprise trying to do “work”.

By “work” we mean the daily mundane - sometimes automated execution of smart contracts that happen in the thousands/tens of thousands/millions and are not directly related to any sort of immediate monetary gain/loss of money/tokens.Early concept chains such as ETH and EOS gained prominence in 2017-18 and laid out a vision of how things “should be” - but limitations were quickly exposed when it became apparent that current technological constraints would not allow “all the smart contracts in the world” to validated by any single blockchain.

Even with the best of intentions, when placed in a “n+1” scaling situation any “closed” system quickly achieved critical mass and all of the “work” transactions got pushed to the back while “high value” transactions such as coin-speculation, (erc-20) gambling, (EOS) and pseudo-gambling (crypto-kiddies etcetera) would by nature clog the network.

The other side of the solution that has been approaching from the corporate side has been the deployment of fully private “consortium” blockchains as proposed by offerings such as Corda and Hyperledger. Being built on the “linux/redhat” model - the idea was to create open source software that “does useful things” and then bill for consulting to implement and maintain. This would effectively and instantly solve the “scalability” issue as the required amount of validators is (n) - ie. .whatever the deployer determines and only transactions allowed by the validators will be allowed on the network.

Meaning that these fully “private” implementations are useful in theory - but depending on use case can sometimes be regulated to nothing more than a glorified database so that someone can say “we are on the blockchain”.

Solution:

Evolving to the “useful” endgame -Unification has been through numerous iterations all of which have built on each other - and through each phase - we continued to ask ourselves the obvious but often muted question - *“how does this benefit our user?”*

To answer this, we engaged in hundreds of conversations with existing enterprises/governments about how the blockchain can practically benefit their endeavors. Three practical examples and requests that came across our desk were:

- A government bank in a developing country wants to build a stable coin - this stable coin would be issued to all agencies to deploy for contracts awarded. Contractors would be paid in the stable coin and would need to redeem it at the government bank for fiat. The purpose for this is to monitor government payments and cash flow in an ecosystem where corruption and fraud is abundant. For this stablecoin, what is important to the government is fast, consistent and extremely inexpensive transactions. Actual full public consensus from a system such as POW is not as important as they trust entities within their network to run the validation nodes - however users and agencies will need full public transparency in order to trace the history of transactions.

- A gaming company is building an card game where each card will be non-fungible tokenized and an ingame currency will allow to be traded for cards and/or loot boxes. Most users won’t even understand they are on the “blockchain” and can’t be expected to hold/stake a wallet balance in order to execute smart contract transactions. However they want these cards and tokens to be publicly tradable and accessible. Transactions needs to be fast, consistent and free for the end user.

- An umbrella organization of clinics in a developing country with over 2 million yearly patients on record wants to place all of their clients data (EHR) on the blockchain to be accessible via a data wallet. The end consumer will be able to access and deploy their data to different providers but can’t be expected to hold and operate a “speculation coin and private key” in order to access this data. This group of clinics will be the beginning of a consortium organization and handle the validation themselves. Later when other clinics or entities join the consortium - they will bring over their user-bases along with joining the consortium to participate as a validator.

These examples are just three of dozens that we have have laid out business models and implementations - speaking with all of the government and enterprise clients we have learned that far beyond a simple majority they all have the same basic needs/requests for a blockchain for their specific usage:

1. To be fast and consistent - they should not have to compete with entities outside their consortium for network resources.
2. Transactions essentially need to be free or nearly free (pennies of pennies) - if there is a transaction cost, then users of the blockchain should not be expected to have to pay or stake to execute these transactions.
3. None had a particular desire, need or allegiance to use a “global” coin or token for daily transactions (such as ETH, BTC or UND) as those can have fluctuating prices. Most requested to use their own internal coin to be used as a marker for transactions. This internal coin (if they even choose to issue one) could be stable or fluctuate depending on the parameters set by the validators.
4. On the same note - most wanted a mechanism of interoperability where there would be the ability to change fungible/non-fungible assets into other implementations on the global UND ecosystem under the correct circumstances.
5. All had no problem handling their own validation methods and had no desire to subject their projects to outside validation and costs.
6. On the same note - all supported an outside oversight mechanism/auditor which would stamp “trust” on top of their validation so that users could gain trust.

There were also various opinions of network/data accessibility and privacy. Some would want the data transacted to be fully publically traceable and transparent - others would would want it encrypted to protect privacy or locked behind firewalls like a private database. In these requests - all implementations are possible.

Working with our clients on a daily basis and seeing their needs and reality of business, led us to an understanding that there is an answer to the quintessential question of scalability of blockchain that involves a hybrid public/private approach which encompases the UND ecosystem.

Introducing UNIFICATION

There are two aspects Unification - we can call them simply “Mainchain” and “WRKChain” which can be more commonly understood as in the same category as a “sidechain” - let us break down their responsibilities.

At its base - Mainchain is more or less what you imagine a smart contract based blockchain to be. It is EVM (Ethereum Virtual Machine) compatible and has a native currency called UND (United Network Distribution).

Governance of Mainchain is executed via DSG (Distributed Stake Governance) which is explained in detail further in the document, however the summary version is that there are 96 EVs (elected validators) who maintain the network and collect tax for validating blocks. These 96 are rotated in 4 sets of 24 to maintain the network. To become an EV - requires a vote/stake - which occurs every 72 hours. During the vote tally time, the 96 EVs with the largest amount of UND staked will receive a 72 hour medallion which will allow them to validate the network and collect tax . This effectively means to control a lifetime node, one would have to accumulate approx 1.04% of the token supply and actively place that on stake - this is assuming all tokens are circulating and fully staked for voting.

DSG has been designed so that the amount of resources required to effectively hostile takeover and disrupt the network would by nature put the attacker in a position where they would be inherently vested in the success of the network.

Simple enough?

Now if we had a world where there was only Mainchain - we would effectively have *“Ethereum with DSG governance instead of POW”* - which may be considered an incremental improvement with faster TPs due to reduced amount of validators (24 at a time as opposed to 10K++ with POW) - however many projects are attempting something similar and ultimately without a major technological jump - then previous adoption and comfort will still win the day.

Where it starts to get fascinating is where we go back to these conversations where we understood what real-world entities truly need in a blockchain. These are the entities that need blockchain to do “actual work” that is not directly related to direct monetary gain per transaction and need that blockchain to produce this work in a consistent and price controlled manner.

As we discussed earlier, private implementations such as Hyperledger Fabric can theoretically solve this - however they are implemented in closed gardens with no oversight on the transparency and no possibility of interoperability.

The solution is a variation of “sidechains” which we are calling “WRKChains” which takes a public/private approach to execution.

When an entity wishes to open up a WRKChain - they upload to Mainchain along with a payment of UND an “expansion log” following a standard. This is more or less technically equivalent to a smart contract - this expansion log will state the number of validators in the WRKChain, how these validators are selected, details on the token being generated on the WRKChain (if they decide to have one) and how tax is paid to the WRKChain validators - if it is even taxed. (via the native WRKChain coin).

The expansion log also describes how the WRKChain will “check in” with Mainchain. Typical usage will find that WRKChain Validators will work in their own trusted vacuum - validating transactions with the WRKChain coin and broadcasting the headers of each of their blocks to Mainchain which then includes this information in its own trusted block.

The nature of this system assumes that we cannot guarantee that the information produced by WRKChain validators is immutable as they are operating typically on a POA/Federated basis. However Mainchain can verify each header they submit and guarantee that they have not changed information or reorganized previous blocks due to a merkle tree root.

WRKChain *Validators are able to:*
-Process INTRA-WRKChain smart contracts and token transfers of the WRKChain Coins

WRKChain *Validators are NOT able to:*
-Control or submit changes for transfers of UND as UND is controlled only by the fully trustless DSG consensus of Mainchain.

This creates a practical ecosystem where Mainchain is a “Blockchain of Blockchains” - allowing independent entities to deploy useful scaled solutions that share the trust and interoperability of Mainchain, while maintaining the speed and scalability of a private implementation.

This is a good theoretical start to solving a complex and universal problem - however the reality of usage and uptake is in the technical details, which we will now explore.

DISTRIBUTED STAKE GOVERNANCE

At 00.00 UTC time every 72 hours a “stake auction” is held and the 96 accounts who have placed in stake the highest amount of UND are awarded a 72 hour medallion. This medallion allows them to be an elected validator which has a certain set of responsibilities and rewards

1 - EVs are responsible for validating the UND Mainchain and producing blocks according to a consensus model. Blocks are currently set to produce every 15 seconds and EVs are assigned in non-predictable fashion who has the rights to produce the next block from which others in the ecosystem will have to reach consensus for it to be finalized.

2 - The EV upon producing a successful block will receive a set block reward on a certain schedule from the network along with all of the tax submitted. All of this UND is placed into the same wallet the Validator has used to stake.

3 - To be an EV is not a technically intense operation and can be executed by a simple AWS configuration that will be provided. EVs are not expected to execute any other role other than validate the network and collect tax.

The purpose of this system is to create an ecosystem where staking of UND tokens for the top 96 is rewarded with interest from the job of being an EV while immutably securing the network.

It is important to note that during our testnet phase, the foundation has distributed 1,000,000,000 ERC-20 UND tokens. These are fully swappable to the mainnet UND tokens and stakers of these tokens will compete to claim one of the 96 Validator spots in order to accumulate UND as rewards.

Block Rewards Schedule: *This is designed to incentive early network activity* - all dates begin at Mainnet deployment.

All blocks produce every 15 seconds according to current schematics. Please note these block rewards are in addition to claiming of the tax submitted by users of the ecosystem. The reason for the high block rewards at the beginning is to incentive early validators to secure the network as the ecosystem develops and more tax is able to be collected with each block produced.

Year 1:
Day 0-50 - Block Rewards - 100 UND per block - 28,800,000 UND generated
Day 50-100 Block Rewards - 50 UND per block - 14,400,000 UND generated
Day 100-365 - 25 UND per Block - 38,160,000 UND Generated
Year 1 Interest paid = 81,360,000 UND

Year 2:
Day 0-150 - 16 UND per Block -13,824,000 UND Generated
Day 150-365 - 12 UND per Block - 14,860,800 UND Generated
Year 2 Interest Paid = 28,684,800 UND

Year 3-4
8 UND per Block
Year 3,4 Interest Paid = 16,819,200 UND

Year 5-8
4 UND per Block
Year 5,6,7,8 Interest Paid = 8,409,600 UND

Year 9-12
2 UND per Block
Year 9,10,11,12 Interest Paid = 4,204,800 UND

Year 13+
1 UND per Block
Year 13+ Interest Paid = 2,102,400 UND

THE MAINCHAIN

The Mainchain is the backbone of the network, and is serviced by EVs, which are selected according to the DSG process outlined above. The Mainchain's primary roles are to increase the trust of a WRKChain by recording a submission of its headers, and maintaining a chain of those recordings - which is accomplished by acceptance of data deposits from any WRKChain that it currently services - and additionally facilitating the native transfer of UND between Accounts on the Mainchain.

Each WRKChain will be rooted on the Mainchain with its own "expansion log", which will contain the WRKChain's data deposits, in addition to WRKChain metadata, which are discussed in more detail below.

Expansion Logs

Expansion Logs are the method by which Mainchain can store, track and validate the state changes made by a WRKChain. When a WRKChain produces a new block, it generates a transaction with the merkle roots for the current state of the WRKChain, the block number, header hash, and any signatures of the WRKChain block validators (if applicable).

Mainchain can then process this transaction, adding the data to the WRKChain's WRKChain Root smart contract.

Proof of Genesis

When a WRKChain is initially deployed, it will store a hash of its genesis block in its Mainchain root. This further enhances the immutability of the WRKChain, and allows the full history of the WRKChain to be audited via the Mainchain, right back to the point of genesis.

WRKChain ID

Upon registration, each WRKChain will be assigned a unique ID, the master record of which will be stored within the WRKChain's root on the Mainchain. This ID will also be embedded within the signature of every transaction executed within the WRKChain.

WRKChain Metadata

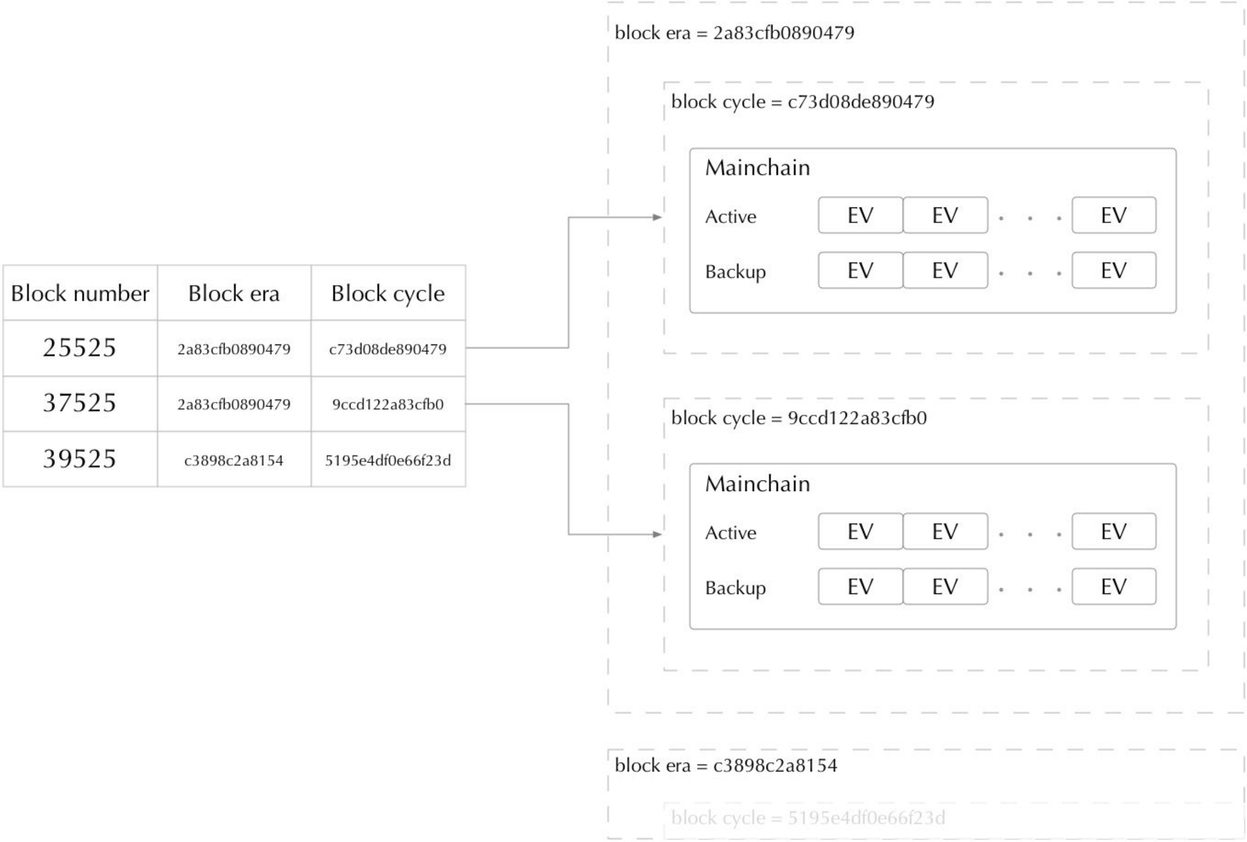
The WRKChain Root will also contain metadata associated with the WRKChain, which may include data such as:

- Consensus method
- INTER WRKChain Transaction fees (or lack thereof)
- WRKChain Token Information (if one exists)
- Bootstrap nodes
- TPS Cap (if applicable)

Mainchain will not have native support for dApps/generic smart contracts, which will require their own WRKChain in order to run. The reason for this is that the UND WRKChain is not designed to be a “global supercomputer” - rather it is a trusted entity that validates information and collects tax from entities in the ecosystem.

Mainchain Block Generation and Consensus

Block generation, validation and finalization occur during block eras and block cycles. Each block era consists of a number of block cycles, and every block cycle begins at a particular block number. A set of active and backup EVs servicing the Mainchain are associated with each block cycle. This entire hash-map is written onto the Mainchain by the UND Voting smart contract.

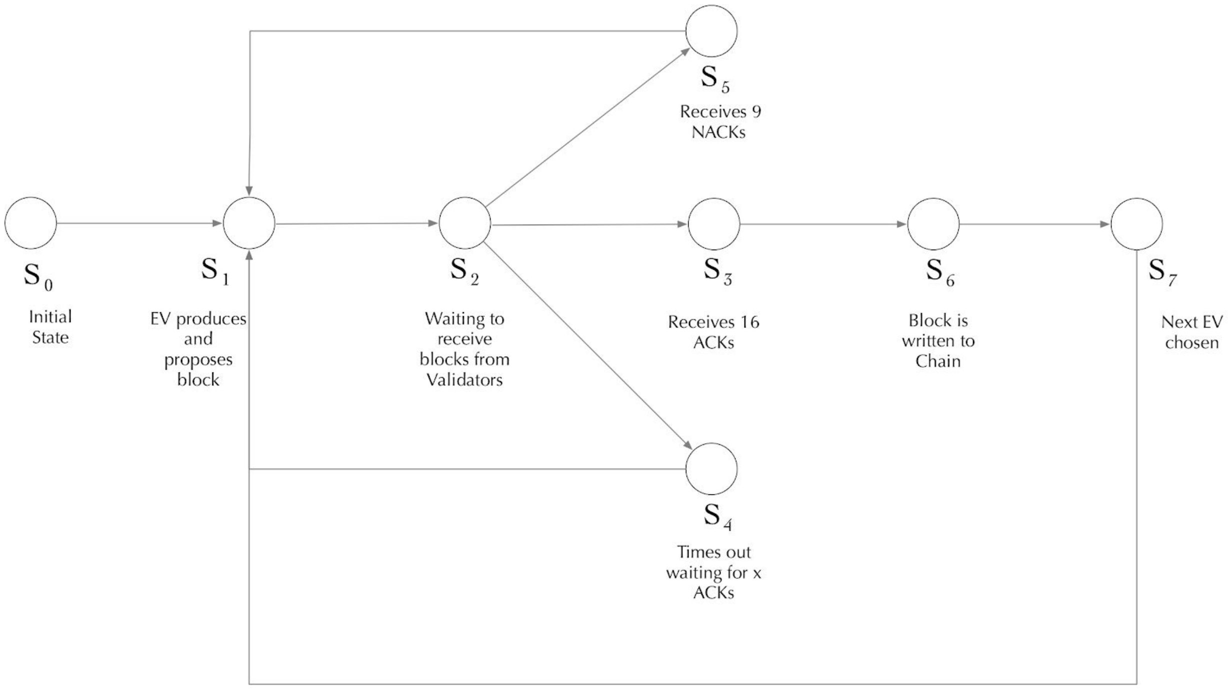


Block number	Block era	Block cycle
25525	2a83cfb0890479	c73d08de890479
37525	2a83cfb0890479	9ccd122a83cfb0
39525	c3898c2a8154	5195e4df0e66f23d

block era = 2a83cfb0890479
block cycle = c73d08de890479
Mainchain
Active
EV
EV
EV
Backup
EV
EV
EV
block cycle = 9ccd122a83cfb0
Mainchain
Active
EV
EV
EV
Backup
EV
EV
EV
block era = c3898c2a8154
block cycle = 5195e4df0e66f23d

For every block period, the UND Voting Smart Contract will write a non-predictable ordering of which EV is assigned as the block generator. This selection is weighted by the EVs current reputation.

For the generation of each block, a number of states are observed.


S_5
Receives 9 NACKs
S_0
Initial State
S_1
EV produces and proposes block
S_2
Waiting to receive blocks from Validators
S_3
Receives 16 ACKs
S_6
Block is written to Chain
S_7
Next EV chosen
S_4
Times out waiting for x ACKs

EVs read their assignments off the Mainchain. When an EV has decided that it should produce the next block, it begins by popping off transactions off the mempool and validating them. Transaction validation includes checking:

- if the account is able to pay for the tax price * tax fee
- if the account has enough UND to transfer out (if the transaction is of a transfer type)
- for invalid signatures
- that nonce is unique, and has been sequentially incremented from the previous nonce

The Block Generator applies the transactions to the current state of the chain, thus producing the resultant chain state. A block is produced with this state, along with the transactions, and the Block Generator signs it with it's private key.

The generated block is then propagated to all the EVs in the Mainchain.

Each other EV receives the produced block, validates both that the block is well formed and that it was created by the appropriate Block Generator. The validating EV, pops the same transactions from the mempool, and also produces a block. However, this block is simply used to confirm the correctness of the received block. Upon agreement, or disagreement, either an ACK block or an NACK is signed and propagated to all the EVs in the Mainchain, and added to the block header.

Upon reception of sixteen ACKs, each EV will finalize the block by adding it to their blockchain. If sixteen ACKs are not received, the current block will be discarded, and will wait for the next Block Generator in line to produce the next block.

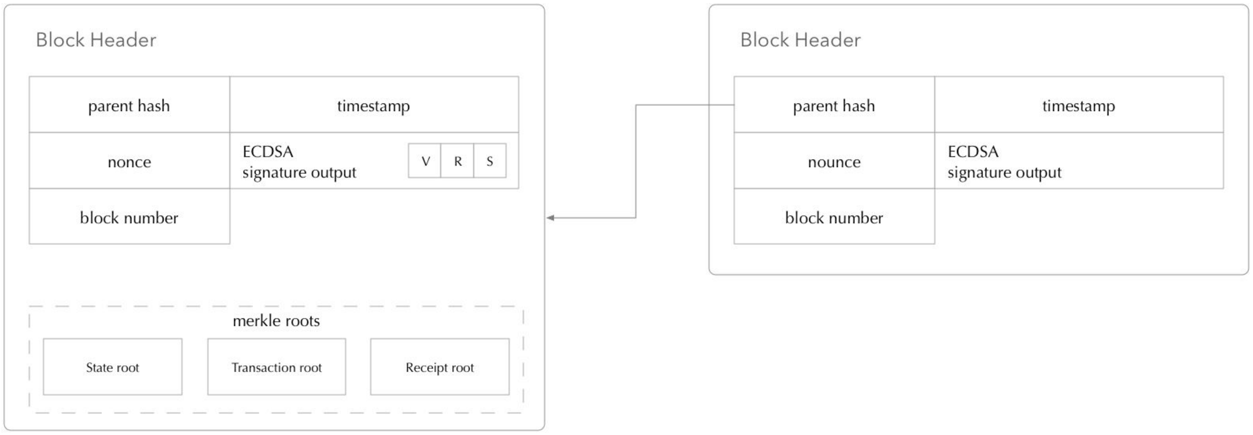
Mainchain EV Reputation

Mainchain will internally track the reputation of EVs producing Mainchain blocks. When an EV produces a “bad” block - for example when consensus is not reached on the block a Block Generator has proposed, or the Block Generator doesn’t produce its block in the expected time, it will receive negative reputation. Negative reputation will reduce the probability that an EV is selected to generate a new block. An EV may regain reputation by consistently generating valid blocks. Positive reputation will not affect how frequently an EV is selected to produce the next block - EVs with non-negative reputation will have an equal chance of being selected to generate a block.

Reputation points will be publicly visible.

Structure of the Block

Blocks propagated under the UND WRKChain have the following structure:



WRKCHAINS

WRKChains can be deployed by anyone. WRKChain deployed using the SDK provided by Unification Foundation are fully EVM compatible chains, and can therefore support any dApp and smart contract, and may have their own native coin (or not). WRKChain operators may define and implement their own consensus methods and transaction fee structure.

Each WRKChain will be rooted to the Mainchain with its own Expansion Log (root smart contract). When a WRKChain adds and finalises a new block to its chain, it will also be responsible for generating the required transaction to call its root, anchored on the Mainchain, to which it will send its Expansion Log data deposit (merkle roots, block header etc.).

Depending on the level of validation WRKChain operators require, they will be able to define whether they require every new block validation, or a less frequent interval (for example, every 10, or 250 blocks require validation by the Mainchain). The higher the level of validation required, the more Mainchain network tax the WRKChain operators will be required to pay.

BEACONS

Beacons are to be considered a value add Timestamp SDK which can be applied to most modern databases. A beacon can work in two different ways depending on the needs of the user

OPTION 1
A - Every change to the database is recorded and that change is encrypted into a hash
B- Every XX minutes these hashes are used to generate a merkle tree, and sent directly to be recorded/time stamped on Mainchain along with a small payment of UND

OPTION 2
A - Every XX minutes a snapshot of the DB is recorded and condensed into a hash, this is then sent to Mainchain along with a small payment of UND.

Note: due to the potential for extreme size of databases being hashed, the user will be able to define which critical data they want to timestamp

The purpose of a beacon is to add a layer of immutable trust to existing or newly built centralized database projects.

By timestamping with a beacon, an entity can be guaranteed that information has not been modified by unseen forces -hence enhancing security and immutability. Unification will make available an API which will allow nearly any sort of entity or configuration to hash and timestamp whatever information they please.

Locked Accounts and Ecosystem Development

The critical flaw with almost every major blockchain is that end users of the technology are constantly at odds with validators and coin holders. Meaning that due to the speculative nature of most decentralized blockchains, a functioning enterprise cannot have a predictable approach to price and network resources.

In order to provide a usable environment, the foundation has earmarked a certain amount of mainnet tokens to be sold at a fixed cost so as to remove speculative pricing for our enterprise users. These tokens are the same as any other UND token, except that they will be distributed to a locked wallet that can only be used to pay network tax for running beacons or WRKChains. This means that these tokens cannot be speculated, resold or transfered.

Once a validator processes a transaction with these locked tokens as tax, the validator will then have ownership of the tokens in their unlocked wallet and will be able to transfer them freely.

This dynamic ensures

1 - A predictable price schedule for the users of the network
2 - Massive incentive to become an elected validator to be able to collect “tax” from working enterprises in addition to scheduled block rewards.
3 - An ongoing revenue stream for The Foundation as history has shown that “one time raises” typically lead to failed projects and that a lasting project should be required to generate ongoing interest and funding for the value it provides to the community.

Project ETHOS as a pure Utility

Unification is designed to be something “useful” Very clearly stated the business mode of Unification is not to “sell tokens” - there has been no ICO and we have developed the project through private generous funding. The United Network Distribution (UND) token is a utility token in the purest sense as distribution has been through an airdrop and by purchasing on the free market. It is designed to be used as a utility for tax on the Mainchain with ongoing funding for the project through selling tokens into locked wallets.

The purpose of Unification is to create an public/private hybrid ecosystem which allows operators of WRKChains to control cost/speed for themselves and their clients while sharing the immutable trust of Mainchain. We believe this is the solution that blockchain has been waiting for and are happy to present it to you today. For more information please visit www.unification.com

The Unification Team
Singapore Q1 2019