UNOCHAIN

Double-Layered Public Blockchain Ecosystem

Version 0.9.1

unochain.io

INTRODUCTION

At its most basic core, the concept of a blockchain is understood to be a data structure that has the ability to maintain records of transactions, and all the time it is doing so, maintains a high level of security, decentralization, and transparency. The decentralized nature of the blockchain ensures that no part of it is controlled by any specific and singular authority, but rather a ledger that is open for viewing by anyone that uses it, i.e. a distributed ledger. One main benefit of the decentralized, distributed ledger is that it cannot be changed by any one person that would like to alter it, and thus it is safer from abuse than a centralized register is.

Digital signatures are used to secure each transaction that is performed on a blockchain in order to prove that the transaction is authentic. Information on a blockchain like a digital signature is encrypted and as such, it is safe from being tampered with and is unable to be changed. Agreements are reached across the blockchain by network participants in relation to reaching a consensus. Information which is stored on a blockchain is digitally recorded and the history of the blockchain transactions are common, available to all network participants. In this regard, there is no chance of having fraudulent activity or transaction duplication.

To understand the idea of blockchain a little better, one can consider what happens when you think about sending money to someone that lives far away from you. Contemporary options for this include PayPal, or by creating an electronic funds transfer through a bank account. Both of these options involves at least one third party to be involved in the process, which will by default mean that an additional fee is charged for the transaction by that third party. When you transfer money in these ways, you cannot guarantee the safety of the money because it becomes more possible for a hacker to intercept it than if you sent the money directly to the other person without any third party involvement. Using a blockchain is safer than using a bank.

Blockchain also does not charge any additional fees to transfer money, as you are the one who is processing the funds – making the transaction both easy and more secure. Blockchain databases are decentralized so they are not limited to any specific location, and all records and related information are publicly kept on the blockchain. This stops the information from being corrupted by someone as it could not be corrupted everywhere across the chain, and such an event is only possible in traditional centralized banking.

The main problem with blockchain at present it its handling ability; that is to say, the ability to scale as needed. Most of the platforms that exist, and certainly the main blockchains like Bitcoin and Ethereum, cannot handle the volume of transactions per second that they would need to handle for the chain to operate efficienctly with any number of new transactions. Those platforms that are able to do so have sacrificed their higher level of security in order to accomplish it, which is obviously not ideal. The only way to deal with scalabilty and decentralization while retaining the level of security that would be expected from a blockchain is to adapt to a new strategy. Sharding for us is that new strategy; with sharding, we have been able to address these issues and can offer on Unochain the ideal solution that cryptocurrency users require in modern times – fast transactions, safe and secure.

The Unochain Vision

The Unochain network introduces a completely workable solution in terms of operating a scalable and secure, decentralized cryptocurrency platform that is capable of handling loads of 100,000 transactions per second by leveraging sharding in the core creation of the platform. Our team has extensive cryptocurrency experience and have created the Unochain vision with the most up to date technology. By making a change at the core in terms of how transactions are handled, with sharding integrated as the solution, Unochain will be a fast, inexpensive, secure choice for any cryptocurrency user to prefer. This will allow blockchain's usability to expand in a way that does not limit the size of the blockchain in the future and will not cause lagging times. A brilliant solution which is necessary to deal with the problem of time and lagging, without foregoing the proper level of security all cryptocurrency users have come to expect in their preferred blockchain. Unochain will bring blockchain to the next generation and will stand as the solid go-to choice for the foreseeable future.

The volume which we will be able to handle, and the speed we will be able to handle it at, can be applicable across many different industries that require high volume capabilities. Our consensus algorithm allows for normal people to access the blockchain and use it for their everyday needs in real time without worrying about more users creating larger lags.

Proof of work

Proof of Work is what Bitcoin uses, and the whole idea of proof of work was developed when the Bitcoin was incepted. PoW is a piece of data that is extremely difficult to produce (which means, it either takes a lot of money or a lot of time to do so), but which can be verified by other uses quite easily and meets certain other requirements. In Bitcoin, creating proof of work is done in a competition by miners who work to add to the blockchain, the work being to find the nonce value for the block through completing a mathematical puzzle. Once a nonce value is found by a miner, they can tell other miners in the network. If other miners are able to validate the claim, the miner will be rewarded with bitcoins. Once a nonce value is found, a block is then added to the blockchain.

For a miner, one objective is to choose the most appropriate nonce value. The value must be less than the value of the target, since if the value is greater then all the effort the miner has undertaken will be rejected. If the miner is able to generate a hash value successfully using a nonce which is less than the value of the target, their effort will be accepted. This means that the computational power that the miner has is used when they create a hash value. A lot of resources, including time and money, are needed to find a nonce value. The miner that is the first one to find the nonce value gains the bitcoins for doing so, while the block for that nonce creates another block to the overall blockchain. The amount of the reward decreases over time, but the only way to get the value of the block is to mine it still, which is the same as it was when it was created. The aspect of mining the coin means that the chain ultimately controls the number of coins created, since they can only be created in one fashion, and the blockchain can also limit the amount of coins that will ever exist in the marketplace.

A blockchain that is based on the proof of work concept requires that 51% of the blockchain’s hash power be used to create a double spend attack which could effectively reverse any transaction. The more decentralized the blockchain is, the harder it becomes to effect such a double spend attack, as it becomes impossible to gain the necessary hash power to deliver the malicious attack. This means that any miner or group of miners who might have thought about creating such an attack will find that it becomes too expensive to be considered viable for them. There are many miner pools that are formed by such proof of work concepts which allows even a weaker miner to gain a proportional share of the block reward. This tends to lean towards centralization, with the top six mining pools in bitcoin taking 75% of the chain’s overall hash power.

Multiple Blockchains and Lightning Networks

One way that traditional cryptocurrency users have found to process their transactions in light of lag times is across multiple blockchains, such as processing one transaction across Bitcoin, Litecoin, and Ethereum blockchains. The problem with this is, even though it creates a lower transactional demand, it also means that each blockchain is operating on a lower hash power. On a smaller chain a malicious attack is more possible as it takes less hash power to execute. So even though it makes scalability possible, it sacrifices security. It also means that users have to maintain an address on each of the platforms which would create even more security concerns as well as issues in relation to private key management.

A further way in which this issue has been dealt with by users who do not rely on platforms that have high enough transactions per second to not cause a lag, is through the use of a lightning network. This effectively means that transactions which are considered to be frequent might be deferred between a fixed group of users until all users have finalized the transaction. Then only one of those users would need to post the final result, eliminating the need for multiple historical transactions to be made. This requires two channels; one to create and one to destroy any payment channel, which accepts an infinite number of off chain transactions. The downside to this option is that it is only good for that fixed group of users, while it would remain quite irrelevant for any user that only had a sporadic transaction. Transparency becomes another issue with the lightning network approach because it is not showing up in the main blockchain, so only the user group doing it can actually see it.

Proof of stake

Proof of stake was created to be an alternative to the proof of work process in order to fix the issues that the proof of work based system created. In proof of stake, at the point the transaction is created, the data for that transaction is fit into a block that can hold up to one megabyte, and then it is duplicated across several computers in the blockchain network. Nodes are considered to be the administrative part of the blockchain and have a job to verify the accuracy or legitimacy of each transaction in each block. Carrying out the verification process entails that the computational puzzle is solved by the miners, or nodes, which is effectively known as the ‘proof of work’ problem. The computational power that is required for mining takes a lot of power for the calculations to be ran by the computer as they are beyond the capability of any person doing without the help of the computer. This creates a very high electrical cost to mine bitcoin, with one bitcoin costing at least the same amount of energy as over one and a half homes in the US each day. In order to pay for that extremely high electric bill, miners often end up selling their bitcoin for a fiat currency, which creates a downward movement in price.

Problems of blockchains

There are a few problems which can be found in blockchain, including:

Scalability

Blockchain technology is becoming better known these days, and it will not be a surprise that every blockchain developed to date has their own unique selling points. One aspect of similarity for most, however, is the unfortunate nature of their lack of being able to scale efficiently, or at all sometimes. Each block has a gas limit and the miners creating a block can only add transactions to that block whose gas requirements add up to a number that is either less than, or equal to, the gas limit of the entire block. This means that a number of transactions that are being sent through are limited.

The time it takes to reach a consensus is based on the peer-to-peer network, with each participant node having equal privileges to one another, creating a network that is suitably egalitarian, with no central authority or hierarchy to follow, i.e. a topology that is flat. So far, all decentralized cryptocurrencies have been structured like this for one reason, to stick to the core philosophy. To maintain a system where everyone is treated equally without any type of governing body and where a currency value can be based on nothing. Ethereum and Bitcoin both operate this way. Without a central entity, how else would everyone throughout the system get to know whether a transaction has happened or not? This is done through the gossip protocol, and works just like gossip in the real world, except the nodes pass the information to one another across the chain and keeps spreading the information until every node can be seen to have it.

Nodes follow a trustless system, so it is the same as each person calling the last person a liar until they prove the same information to be true themselves. For nodes, this is accomplished by running the same calculations that they were just told created something, to prove that it is true. In order for each node to be able to do this, they must all have the same ledger with their own copy of the blockchain. As a result, the entire process is quite slow. This also means that as more nodes appear in the blockchain, the time it takes to process information becomes slower.

Consensus is also accomplished on blockchain in a linear manner. To understand what this means, consider that there are three nodes, A, B, and C. For the consensus to start and complete, it would start with node A, which would run calculations and verify, then node B would do the same, then node C would do the same. When another node enters the system, the next node D, the process gets slower, and slower again as nodes E, F, G, etc are added. In Ethereum this problem is more obvious, because so many people want to have some Ethereum. This makes the number of nodes exponentially increase in the network. Ethereum has had multiple times more nodes than Bitcoin has had due to this, and the rate of increase has been seen to double within a month at times.

Decentralization

While blockchain technology offers users a promise of being able to be their own bank, most of the exchanges will only allow individuals to buy cryptocurrencies through a centralized exchange. This is a problem that is fundamentally plaguing the industry, with centralized exchanges occurring more frequently. Remembering that centralization can lead to hacking, this problem could be seen when Mt. Gox was hacked, when BitFinex was hacked, and when Bithumb was hacked, which was the 5th largest cryptocurrency exchange at the time. The problem with a centralized blockchain is the same as the problem that is created when you hold all your money in one bank, i.e. all your eggs in one basket.

Given that these were some of the most valuable heists of all time and the price of Bitcoin continues to increase, it is natural to conclude that such hacking attempts are not a thing of the past. Even traditional firms that have extensive measures in place to provide assurances against attacks are still vulnerable. Cryptocurrency sites differ from banks in this way, there is no requirement for the crypto exchange to replace the money that you lost through a breach in their accounts. The majority of cryptocurrency platforms provide no such guarantee.

Security

A main security issue in blockchain is a costly one. Since cryptocurrency is so valuable, the idea of hacking it becomes quite lucrative to any black hat hacker. Some cryptocurrency platforms do not have as robust security features as other platforms do, which makes them even more rife for hacking. Early cryptocurrency users will remember the 2014 Mt. Gox hack, which at the time happened to the largest exchange processor of the time. Almost 850,000 Bitcoin were stolen in that hack, with users losing all of their investment. Every year, losses from hacking for cryptocurrency platforms total in the hundreds of millions of dollars. Storing crypto is very important, and a good point to remember is that you should have either a hardware or a paper wallet. Both methods have less online touchpoints, so that will keep your coins out of the reach of any malicious hacking. If you trade with cryptocurrency regularly, it is advisable to use a decentralized exchange which allows trading directly from the cryptocurrency wallet you have.

Our proposed solution

Our aim is to get up to 100,000 TPS on a decentralized, scalable and secure platform. We will do this through sharding, and through algorithm consensus. In this section we will describe what is meant by sharding, and by a consensus algorithm.

Consensus Algorithm

A consensus algorithm is a mechanism that a blockchain network can use to reach a consensus. Without a central authority, the decentralized blockchains are instead built through distributed systems. Distributed nodes have to agree between themselves abou the validity of any transaction. This is where a consensus algorithm takes part, assuring each of the nodes that the same protocol is being used and all the same rules are being followed by all nodes. This ensures that each and every transaction is completed in the same trustless way, so that the coins can only be spent one time. These consensus algorithms are imperative to making sure that the security and the integrity of any cryptocurrency network remains intact. They act to provide the means by which each distributed node can reach a consensus on determining the proper version of the blockchain. The agreement of the current state of the blockchain is a primary requirement of the cryptocurrency platform and is key to making sure that the system works as intended.

Sharding

Sharding is a type of partitioning on a database and is also called horizontal partitioning. Sharding involves the breaking up of a large database into much smaller and thus more manageable segments for the purpose of improving the overall performance and for reducing each query's response time. Even centralized database management uses sharding, and has done since the 1990s. Businesses also commonly shard their information across different segmented lines, such as by geographic location. Unique, geographically specific servers are used by very large businesses to break down their overall pile of information into a more manageable section that is easier to review.

Nodes represent individual data servers across the blockchain, so when sharding is applied, it is the same as breaking up the blockchain network. Each shard has a unique piece of the smart contract and the account balances that exist across the blockchain. Nodes can be categorized to each specific shard for the purpose of verifying operations and transactions and in this sense every node is not responsible for verifying the exact same information as every other node in the blockchain. By breaking the blockchain down into smaller pieces that are more easy to manage, there is an increase of activity that is able to go through without becoming jammed. This is key to overcoming any scalability issue that is constant across traditional blockchains.

Sharding itself is best explained through the Ethereum blockchain example. The Ethereum blockchain is created by thousands of different computers, each acting as a node, over 10,000 of them. Each node will lend a certain level of hash power to the network and its this hash power that facilitates the functioning of the Ethereum Virtual Machine. In order for the EVM to execute any smart contracts or to run DApps, i.e. decentralized applications.

Ethereum operates on a sequential execution basis that means each of the nodes must calculate the same exact operation every single time for every transaction. For this reasons, transactions can take a long time to pass through the system, with an average processing speed of ten transactions per second. Even a basic financial instrument like Visa can handle 24,000 transactions per second, or tps. The act of adding more computers to the network does not increase the speed, since the entire ledger is kept on every computer node in the network, it will just make it take longer.

This is what sharding fixes; the concept of moving away from a linear execution model wherein all nodes complete all transactions to one where nodes are assigned a specific part of the transaction to process only, in a parallel execution model, is a much better idea and allows for multiple transactions to run in parallel in processing all at the same time. Sharding blockchains are separated into different subdomains called 'buckets', and nodes then only have to run their own part of the ledger which is assigned to their bucket for the execution of validating and processing transactions.

There are some challenges that sharding introduces, such as cross sharding or single shard takeovers. Sometimes sharding also creates partitions in user's accounts, so that they have multiple transactions across multiple accounts rather than having all transactions in one place. Despite this concerns, Unochain has been created to ensure that the highest level of safety is maintained throughout, while retaining the ability to be scalable. We have been able to do this through enabling seamless cross shard transactions with an account that is easy for clients to manage, in our incentive driven ecosystem that operates in an open standard to support DApps.

How do we intend to harness this power?

Our proposal is based on sharding protocol and the Proof of Stake consensus scheme; assuming the foundational number of nodes across the network is cn, the cn nodes will form c groups, meaning each group contains an n node. A c node group will then work as a validation node group and the rest of the c-1 nodes will be regular groups. Regular node groups will create middle blocks from transaction shards that have been assigned to them. Middle blocks are then used to process within the validation node group for the purpose of producing final blocks in the process. The final block is generally represeneted in capital letters whereas the middle block is expressed in lower case letters. Each of the epochs will contain four distinct steps.

Step 1: The first step will always be to formulate a group of nodes, with each node being part of, and participating in, a specific group. After the formation of the node group, a leader node is the next step and must be chosen at random. All of the different node identities in that group will then be sent to the leader node through a broadcast to all nodes. This process will act to decrease the level of complexity that is normally seen in communicating between nodes from O(n2) to O(cn).

Step 2: Running internal group consensus is the second stemp; a transactional shard will be assigned to a node group at random with an internal proof of stake consensus to be run within each node group. The node with the largest coin amount holding times will have the highest probability of being chose to generate the newest middle block.

Step 3: The generation of the final BLOCK; within the final validation group, blocks will be collected and combined. A proof of stake consensus is operated to create a final BLOCK that is then broadcast to the entire network.

Step 4: The nodes are then reshuffled; after t epochs, every one of the nodes will be reshuffled in order to form different, new node groups.

This example can extend to the execution of a single payment within this example. In its most basic term for a single payment, user A and user B are on the same shard and the validations that have to happen within that shard are able to be processed within the transaction without any type of issue. What happens if user A and user B have accounts on different shards? If this were to happen, and user A is on shard 1 with user B on shard 2, the validators on the individual shards would not be able to debit or credit the users' accounts due to the fact they have no authority on each other's respective shards. However, by using a synchronous, or same time, cross shard transaction, a solution readily appears.

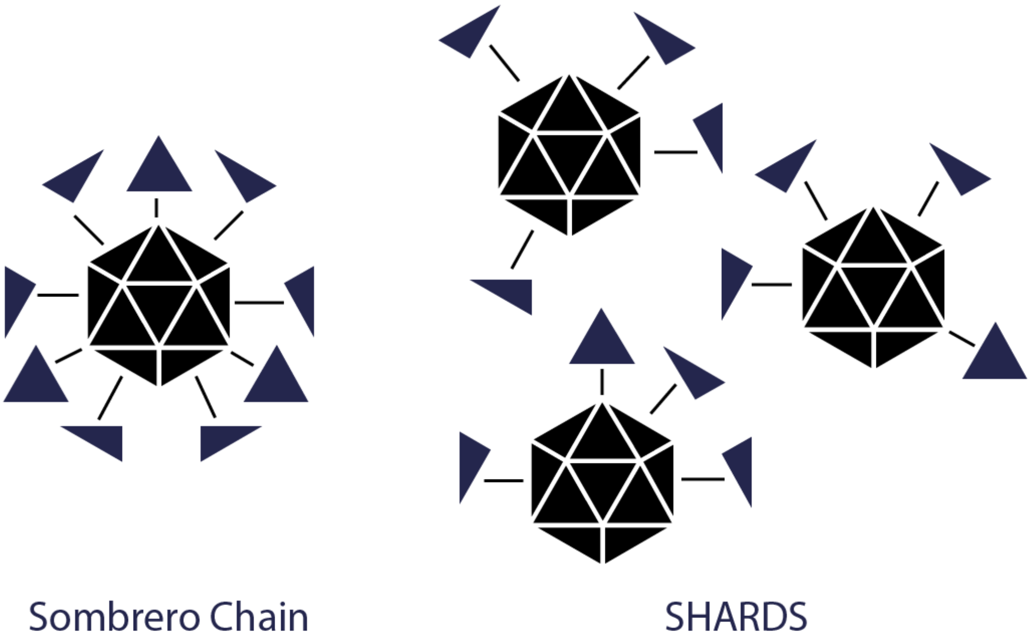
Unochain has been created to contain a sharding blockchain layer that is elastic and which contains a list of all minor blockchain shards. A subset of the transactions are independently processed by individual shards. This means that each shard can process multiple transactions concurrently, which means the ability increases as the system capacity increases. The Unochain blockchain will also root blockchain which has the requirement of confirming all of the blocks contained in all the shards across the chain. The root blockchain will not be used to process any transaction on the chain but will instead act to make it economically unviable to attempt any reverse spend transaction. Users will not even feel the additional shards come on board as the scalability is so seamless it will not lead to lag in the system. This concept is the most efficient use of blockchain that has came to the market.

Synchronous (same-time) Cross-Shard Transactions

In the case of a same time synchronous cross shard transaction, if user A is on shard 1 and needs to send funds over to user B on shard 2, the blocks within each of those shards will contain a state transition that has been created simultaneously on each shard. The validators on each of the shards will work together to confirm the transaction. This solution was proposed in 2018 by Vitalik Buterin.

Asynchronous Cross-Shard Transactions

An asynchronous cross shard transaction is a bit easier than the former example to complete, and much easier to coordinate. Using the same user A user B different shard example, in this instance the shard that would be in charge of crediting user B's account would only have to validate its own part of the transaction at one time when it has enough proof that the shard which is in control of debiting user A's account has finished doing what it needs to do. Even though this approach isn't perfect, there is a non-zero chance that one of the blocks in either of the shards would be orphaned. A non-zero chance is always considered a vulnerability, however, and as such it must be remembered.



In this example, there are three shards to the blockchain, and only by coincidence do they all fork at the exact same point where the transaction becomes incorporated. If forks happen like this, the shard must orphan one of the chains in order to accept the other. IF chain A, B, C or beyond has to accept the chain in shard 1, and chains W, X, Y etc become the newly accepted chain in the second shard, the transaction is finalized and everyone wins. The entire transaction would fail if the A, B, chain in shard 1 is accepted and the W, X, etc chain in shard 2 is accepted. This is still an acceptable conclusion because the transaction can be redone and no one is out of pocket.

If the A’, B’ etc. chan in shard #1 is accepted and chain W, X etc. in shard #2 is accepted, then the entire transaction fails, which is also an acceptable outcome, because the transaction can be resent.

Conclusion:

In response to the fast adoption of blockchain, not all eventualities were though of at the outset and it is now time to create a solution that takes the shortcomings of the past into considerations. By using our own sharding technique with the consensus algorithm we will create a scalable, decentralized and secure platform that is able to operate at an acceptable 100,000 transactions per second rate. This will take care of the backlogs that happen on Ethereum and similar networks, and ensure that transactions will be prioritized in real time ongoing. We have been able to develop Unochain with the future in mind.

Unochain has considered all of the negative aspects that are being seen and felt by cryptocurrency users in traditional blockchains as these methods of sending money between users becomes more popular. By creating an enlightened vision of what the cryptocurrency chain is meant to operate like, we have ensure that the system Unochain uses is free of error, cannot be hacked easily or cheaply, is able to scale efficiently and safely, and will be able to continue to scale as needed into the future.

Safe, secure, inexpensive, easy, exponential growth, and fast. That is what Unochain stands for. Come on board and see for yourselves the benefit that Unochain gives users. If you are sick of waiting long periods of time or worry about safety of your transaction as it is spread across multiple platforms, you will see the benefit of what Unochain has to offer. With the most experienced cryptocurrency team on board, we have considered every angle and are assured that all aspects have been considered and improved upon in a solid, seamless way.

UNOCHAIN TOKEN

Contract address: 0x1fff4dd33105054e853955c6d0dba82859c01cff

Decimals:18

Total supply: 5 000 000 000 UNOC

Token name: Unochain Token