Unblocked Ledger Coin

A Linearly Scalable, Self-Governing Payment Network

Abstract

The future of blockchain and distributed ledger technology holds enormous promise for radically transforming many of the current trust-based systems and services, as well as impacting just about every industry in the world. However, the delivery of this promise hinges upon the creation of infrastructure software that implements fast, efficient, trustless, secure and highly scalable peer-to-peer networks. The state-of-the-art is currently experimenting with different models of achieving greater scalability and efficient consensus in such networks. The Unblocked Ledger Coin project will showcase novel distributed ledger technology that creates a self-governing, sustainable, peer-to-peer payment network which incorporates sharding and auto-scaling to provide high throughput, low latency, and immediate finality while maintaining the highest level of decentralization and security possible. The availability of such technology will be useful not only to private enterprises, but also to public ledgers, thus enabling global-scale, decentralized applications able to accommodate billions of daily active users.

v 2018.04.15

Introduction

The bitcoin peer-to-peer network software is an engineering marvel. It does not invent anything new, but rather combines existing cryptographic primitives in a novel way to solve the problem of trustless value transfer over the Internet. The key technological elements used in bitcoin such as hashing, digital signatures and communication protocols existed decades before bitcoin was released. Even with some of the best minds working for years to find a way to transfer value over the Internet, without requiring a trusted third party, it was only within the last decade that a solution to this problem was demonstrated with the release of bitcoin.

Solving this problem was such a big achievement, that the finer details of just how efficient or scalable the actual solution was did not matter very much. A small community of users adopted it for the astonishing fact that it provided, for the first time, a trustless payment network along with a very transparent and rule-based money supply. It soon became apparent that bitcoin left considerable room for experimentation, and many academics and engineers began releasing variations to try and improve it. Litecoin tried to make it a bit faster and more decentralized. Ethereum added a Turing complete smart contract layer. Peercoin and Nxt tried to make it more energy efficient. Dash and Monero tried to make it more anonymous.

This first generation of improvements did not focus too much on the scalability of bitcoin as the approximately 3 transactions per second was sufficient to handle the load at the time. But as the bitcoin community grew and the number of transactions on the bitcoin network began to increase, the scalability issue became a major concern and led to a second generation of improvements. Bitshares, Ripple and Stellar are some of the first to achieve 1000+ transactions per second. In the case of Ripple and Stellar the whole network was run by a single organization or its partners, thus sacrificing the decentralized standard of bitcoin. Bitshares used a more novel approach where the holders of the coin select which nodes can generate blocks, thus making it less centralized, but not nearly as open as bitcoin. More recent innovations such as Directed Acyclic Graphs (DAG) used by Nano and IOTA have shown that a blockless architecture can significantly improve transaction throughput compared to a blockchain architecture. HashGraph has also used a blockless architecture to achieve 1000+ transactions per second. Although sharding has been proposed for Ethereum and Zilliqa plans to include it from the beginning, there are currently no production networks currently using it. Sharding is ultimately the best way to tackle the scalability issue, but applying it to blockchain-based networks is not nearly as easy as applying it to databases.

The early bitcoin adopters considered variations to bitcoin unnecessary and a distraction that was diluting the community. To their credit, there were and still are many bitcoin clones which made absolutely no technical enhancements. However, in the midst of this chaos, real progress is being made. It would be very shortsighted to conclude that the architecture of bitcoin is optimal and other ideas should not be tried. We are going through a Cambrian explosion phase

where many different ideas need to be tried and tested to discover new consensus algorithms and architectures to power the future of global-scale decentralized applications.

Project Goals

The Unblocked Ledger Coin project aims to build a peer-to-peer payment network with a native coin that is earned by nodes which contribute resources to the network. The software for this network will not be forked from any other coin and will be a new code base. The network will serve not just to provide a coin and payment network, but to also showcase novel sharding technology applied to distributed ledgers. The project will utilize the newly created "Unblocked Consensus Algorithm" and the "Unblocked Sharded Ledger" to create a payment network with better scaling, decentralization and other features.

Motivation

Many of the current distributed ledger protocols have self imposed scaling limits due to the grouping of transactions into blocks. The maximum size of the block and the rate at which blocks are produced sets an upper limit on the rate at which the network can process transactions. Networks such as Bitcoin and Ethereum have not yet begun to encounter physical scaling bottlenecks from compute, storage, and bandwidth limits.

In addition the current distributed ledger protocols are not horizontally scalable. Adding more nodes to the network does not help increase the throughput or capacity of the network. In fact it increases the total bandwidth requirement of the network since every node must see every transaction. Some networks such as Ethereum have begun to investigate sharding, but only to break the compute bottleneck. Sharding of storage is very difficult since every node needs to know the complete state of the ledger to determine the validity of a transaction. The current approach for sharding of storage is to use additional networks called sidechains that are interoperable with the main network.

We propose a distributed ledger described in the paper "Unblock Sharded Ledger" that processes each transaction separately and does not group them into blocks. In addition the ledger is sharded to evenly distribute compute, storage and bandwidth across all the nodes in the network. Adding more nodes increases the compute and storage capacity of the network while keeping the bandwidth requirements constant. Sharding storage introduces many engineering challenges, but appears to be solvable. Additional technologies such as sidechains and lightning networks which are being proposed for networks such as Bitcoin can also be applied to the Unblocked Sharded Ledger to provide additional layers of scaling.

The motivation for designing a new distributed ledger protocol was to support global scale decentralized applications which aim to reach billions of users and require millions of transactions per second. The transaction throughput and storage requirement would be beyond what any single node could handle. Thus, both processing of transactions and storage of current

ledger state needs to be sharded so that resource requirements for a node are not too great. It is important to keep the resource requirements for a node low so that many unrelated parties can participate in the network, thus increasing the level of decentralization. A new consensus protocol was also designed which supports immediate processing of transactions without grouping them into blocks by a leader or even a temporary leader node. The new consensus protocol is described in the paper "Unblocked Consensus Algorithm".

Premise

We set forth some of the requirements and assumptions in designing this network:

- Anyone should be able to run a node and join the network. It should not require approval from a specific individual or organization.
- The resource requirement for running a node should not be too high, so that many different unrelated parties can run nodes; thus providing a high degree of decentralization.
- The state information of the ledger is assumed to be much larger than what any single node can store.
- The transaction throughput is assumed to be much higher than the network bandwidth of any single node.
- The transaction processing is assumed to be much higher than the compute power of any single node.

Features

The features that will be incorporated into this network include:

- High throughput
- High capacity
- Low bandwidth
- Auto-scaling
- Low latency
- Fast finality
- High fairness
- Steady incentives
- No fees
- Decentralization
- Security
- Sustainability
- Self-governance

High throughput means that the network should be able to process a very large number of transactions per second. In networks like bitcoin where every node must process every transaction (i.e. validate and apply), the bottleneck is the processing power of the slowest full nodes. If the bitcoin network were to increase the self-imposed block size limit, it would run into a more natural bottleneck of processing power. The only way to speed up the network then

would be to raise the processing power of all the nodes (vertical scaling). So all networks where every full node must process every transaction have the same theoretical throughput limit. But in actuality we see very large differences when we compare networks like bitcoin, Litecoin, and Dash. These differences are due mainly to different self-imposed limits of block size and block rate. If these self-imposed limits were removed then the differences due to different consensus algorithms would start to show up. Networks that used proof-of-stake would be much faster than networks that used proof-of-work since the processing power of the node is not being used up by proof-of-work computation. Ideally the rate at which the network processes transactions should be proportional to the number of nodes in the network so that increasing throughput means increasing the number of nodes (horizontal scaling). This project will aim to build a network that is horizontally scalable.

High capacity means that the network should be able to provide persistent storage for very massive amounts of state data. Global-scale applications could require exobytes of state data. The current generation of blockchains and distributed ledgers appear to be functional only because they have not been stressed in this dimension. This project will aim to build a network that can horizontally scale not only throughput, but also capacity.

Low bandwidth means that the network should try to minimize the amount of data transfer needed when distributing transactions and achieving consensus. This does not imply just compressing the data or using binary formats; rather the more important factors are network architecture and algorithmic details of the consensus algorithm. In bitcoin-like networks, adding more nodes to the network actually increases the amount of bandwidth used to process each transaction. This project will aim to create a network where the amount of bandwidth consumed by a transaction is constant and does not increase proportional to the number of nodes.

Auto-scaling means that the network should be able to self-govern the number of nodes the network needs and properly incentivise node to achieve the desired size. This implies that the network is able to effectively use the available nodes to achieve desired tradeoffs; for example scaling of throughput proportional to the number of nodes available. Otherwise there is no benefit in a network trying to auto-scale. In bitcoin-like networks there are conflicts in the desired size of the network. The low bandwidth requirement would favor having as few nodes as possible, while the high security and decentralization requirement would favor having as many (unrelated) nodes as possible. This project will aim to build a network that can auto-scale.

Low latency means the total turnaround time between submitting a transaction to the network and knowing that the network has applied the transaction is short. In bitcoin-like networks, latency is the time between submitting the transaction and the transaction being included in a block. For such networks the fastest latency is no less than the average block production time. This project will provide latency of just a few seconds by processing each transaction individually and not grouping them into blocks.

Fast finality means having a quick turnaround time between submitting a transaction to the network and knowing that the transaction is irreversible. In bitcoin-like networks there is a probabilistic finality time such that the longer you wait the lower the chance that a transaction which has been confirmed in a block cannot be reversed. Thus, the finality time is not just the time for the transaction being included in a block, but rather a number of blocks being produced after it to reduce the probability of the transaction being reversed. For large value transfers on the bitcoin network, it is recommended to wait for at least 6 blocks (about an hour) to ensure irreversibility. This project aims to provide immediate finality meaning that finality time is the same as latency time of a few seconds.

High fairness means that a transaction which was received by the network earlier than another should be applied before the other. In a blockchain-based network, all transactions within a block are considered to have occured at the same time and the order in which they are applied does not matter. For some applications like games this does not provide sufficient time resolution. Also, it is possible for transactions that were received much later to be processed before transactions that were received much earlier. In bitcoin-like networks this is actually a feature by which transactions can receive priority processing by including a fee for the miner that includes the transaction in a block. This project will aim to create a network that processes and applies transactions in the order they were received.

Steady incentives means that all nodes which are providing resources to the network are paid on a regular basis, like once a day. In bitcoin-like networks, there is enormous variance in the payout frequency. It is possible that a node may not receive any payment for many years. This leads to nodes joining mining pools in order to receive steady payments, and pools have the negative effect of increasing centralization. This project aims to avoid this problem by giving active nodes in the network a steady incentive for providing resources.

No fees means that transactions do not have to include a small payment to be processed faster. However, there may still be valid economic reasons to have transaction fees which are burned in order to reduce the money supply. Such fees are not considered here. In blockchain-based networks, the maximum size of the block creates a scarcity of space in the block and transaction fees cannot be avoided. The low transaction fees on many blockchain-based networks are only possible because transaction rates are currently low. Even if the block size and block rate were increased, the transaction throughput of the average node would create scarcity and require transaction fees. Another reason that fees are used is to avoid spam transactions that transfer only very small amounts. A flood of such transactions could be used to slow down the processing of other transactions. Networks typically require a minimum transaction fee if the amount being transferred is below some threshold. However, this discourages microtransactions since the minimum fee could potentially be larger than the transaction amount. Microtransactions are a prime use case for such networks and should be encouraged. This project aims to replace transaction fees with variable just-in-time proof-of-work.

Decentralization means that the nodes providing resources to the network are unrelated. Ideally every node is provided by an independent entity and the entities are unknown to one another, such that they are not able to collude. A simple measure of the centralization of the network is the largest percentage of resources provided by a single entity or a group of related entities. Many security properties of decentralized networks fail if the centralization level of a network is 33% or more. Thus, it is crucial to maintain a very low level of centralization. If the resources required to run a node increases as the usage of the network grows, there will be a tendency for the network to become more centralized. Or if the cost of running a node is higher than the compensation provided by the network then there will be a tendency for nodes to leave the network and the few nodes that stay will tend to have a higher level of centralization. There is also the problem that if the compensation provided for running a node is too high, it could attract botnets which find joining the network to be more profitable than other options. This project will aim for a high level of decentralization by keeping the resources needed to run a node low even as the network usage grows; by compensating the nodes properly and by auto-scaling the size of the network to prevent a large number of nodes from joining the network at once.

Security means preventing a wide range of possible attacks on the network assuming the four common operational models; namely honest majority, uncoordinated majority, coordinated choice and bribing. Security in a trustless environment is closely linked to the level of centralization of the network. If the level of centralization increases beyond some threshold, the network will be operating outside the bounds of the common operational models and it's security is no longer guaranteed. The typical worst-case scenarios are a network partition, a malicious change in the state data, or denial of service. This project aims to provide the highest level of security possible under the common operational models by avoiding high levels of centralization in the consensus and network protocol.

Sustainability mean the network is able to provide funding for not only the nodes providing resources, but also future development and maintenance of the network software. The bitcoin network only provides funds for the nodes operating the network and the core developers of the network are supported by external funds such as contributions, or the developers contributing their time and effort at no cost. The Dash network was one of the first to establish a native fund to support future development and promotion of the network. This project will aim to provide a native fund to support future development and maintenance of the network.

Self-governance means that the community of coin holders can participate in the future direction of the network and not just leave this to the miners and developers. In bitcoin-like networks the miners tend to have the most control since they decide what version of the software to run. The user community and developers can provide the software, but it is eventually up to the miners to adopt it. This leads to a minority having more control than the majority. A recent innovation in bitcoin-like networks has been the introduction of User-Activated Soft Fork (UASF), whereby an economic majority can activate a change in the software without the involvement of miners. This project will aim to incorporate features similar

to UASF to allow the community of coin holders to participate in the future direction of the network.

Architecture

To provide the many features listed above, this project will use a blockless approach combined with both compute and state sharding. In blockchain-based networks, transactions are grouped into blocks that have a size and generation rate determined by the network. In a blockless network, the transactions are processed independently without being grouped into blocks.

A blockchain-based approach may appear to be more efficient since it groups transactions together and benefits from economies of scale. However, we believe that the blockchain-based approach also introduces many complications which are avoided by a blockless approach. For example, low latency and fast finality are limited by the self-imposed block generation rate. Also, blockchain-based networks cannot avoid fees since high transaction rates will mean competition for space due to the self-imposed block size limit. Sharding blockchain-based networks is not trivial. It can be done by creating multiple chains (often referred to as sidechains), but this creates additional complications. For example, transactions which modify data on two or more chains become quite complex and take much longer to execute than transactions which modify data only within one chain. The dimension on which to segregate data into different chains must be predefined and can cause transactions to become more complex if chosen wrong. For example, Ethereum plans to shard based on the contract address, whereas Cardano plans to shard based on industry or geography. Using sidechains also does not give the network any control on which sidechains to allocate available resources. Nodes will want to join the sidechain that is paying the most in fees. This leads to some blockchain-based networks sharding only the validation of transactions and not the state. In practice, this means that all nodes hold complete state data for the network, but transactions are routed to shards only to be validated. Once the shard has signed off on the transaction as being valid, it is propagated to all nodes in the network to be applied and update the local state data.

In blockless networks the transactions are processed (i.e. validated and applied) as soon as they are received. This results in low latency and fast finality. The fast finality of blockless networks allows transactions that cross shards to be much faster than blockchain-based networks where finality is probabilistic. Sharding in blockless networks can be done on various different dimensions, including account ID, so that there is a more even distribution of nodes across shards. This also lends to auto-scaling whereby the network can determine how many nodes are needed based on the load. The overhead of processing each transaction independently does mean that the number of transactions processed per time will be less than for blockless networks, but the more distributed sharding allows every node joining the network to be used more effectively and eventually achieve higher throughput with sharding. In time we believe networks that are blockless and completely sharded will prevail over blockchain-based networks using sidechains.

Project Comparison

The following table compares features of this project with other projects that provide or are developing peer-to-peer network software.

	Architecture	Consensus	Sharding	TPS	Capacity	Finality	Fairness	Decentralization
Bitcoin	blocks	PoW	no	3	full	1 hour	no	low
Ethereum	blocks	PoW	not yet	25	full	1 minute	no	high
Stellar	blockless	PoQ	no	2000	full	immediate	fair	low
Lisk	blocks	dPoS	sidechain	3	partial	immediate	no	low
EOS	blocks	dPoS	no	50,000	full	immediate	no	low
Cardono	blocks	PoS	sidechain	1,000	partial	1 minute	no	med
Nano	DAG	dPoS	no	10,000	full	immediate	no	low
Zilliqa	blocks	PBFT	yes	1/node	partial	immediate	no	low
IOTA	DAG	PoW	no	50,000	full	1 minute	fair	high
HashGraph	blockless	PoQ	no	50,000	full	immediate	fair	low
ULC	**blockless**	**PoQ**	**yes**	**1/node**	**partial**	**immediate**	**fair**	**high**

ULC is the only project which has a blockless architecture along with complete sharding. Nodes can process about 100 transactions per second and there are 100 nodes per shard. This gives 1 transaction per second per node. With a network of 10,000 node ULC will be able to scale to 10,000 transactions per second. However, the ULC network is designed to scale to millions of nodes and allow millions of transactions per second.

Project Funding

The project will be self-funded through a bounty program in which bounty participants are compensated with Unblocked Ledger Tokens (ULT). The bounty program will create and launch the Unblocked Ledger Coin (ULC) peer-to-peer network software. When the ULC network is operational, holders of ULT tokens will be able to obtain an equivalent amount of ULC coins directly on the network while still retaining their ULT. The transferable nature of tokens and coins on trustless networks will allow the bounty participants to exchange ULT and ULC for products and services as well as other tokens and coins. The key to the success of this project will be in finding bounty participants who share the same vision and goals of the project.

Unblocked Ledger Token (ULT)

- A max supply of 1,000,000,000 (one billion) ULT tokens are created in an ERC-20 contract.
- The tokens are only distributed as bounties to help create and launch the Unblocked Ledger Coin (ULC) peer-to-peer network software. Tokens are not sold.
- Bounties are awarded based on the ULT tokens having a nominal value of $0.10 USD each. For example if the project offers a bounty which it determines provides a value of $100 USD, then 1,000 ULT tokens will be the reward for completing this bounty.
- Although the project awards tokens for bounties based on the above price, the tokens cannot be redeemed with the project for any value. Nor does the project take tokens out of circulation once they have been distributed.
- The early contributors to the project are reimbursed with ULT for past efforts and expenses incurred due to the project. The total amount to be reimbursed is announced at the start of the project. The reimbursement is done with a limit of 2% per month. After the project is completed any amount remaining is reimbursed at once.
- A maximum of 10,000,000 ULT will be given freely as part of airdrops to members of cryptocurrency communities.
- A monthly report is published on the website of how many ULT were distributed that month. These numbers can also be verified by examining the ULT smart contract.
- Once the ULC software is developed and deployed, the excess ULT tokens in the ERC-20 contract not already distributed are burned. The maintenance fund from ULC will be used to provide future support for ULC and ULT.
- The holders of ULT tokens will be able to obtain coins on the ULC network after it is deployed at a 1:1 ratio. The ULT tokens are not lost when ULC is obtained.
- The ULC software will be released under a Creative Commons BY-NC-SA license.
- Non-commercial projects which use the ULC software will be asked to airdrop tokens for their project to ULT token holders. Doing so will help them gain an immediate community of users.
- Commercial projects which want to use the ULC software can obtain a license token by burning a percentage of ULT tokens through the ULT smart contract. The percentage will be determined when the ULC software is released and may subsequently be adjusted based on market conditions.
- After 10 years (from the excess burn event), the ULC software will be licensed under a Creative Commons BY license. The ULT in circulation will be converted to ULC at a 1 ULC per 10 ULT ratio and the ULT smart contract will be frozen.

Unblocked Ledger Coin (ULC)

- When the ULC software is released, the ULC peer-to-peer network is created by people around the world running the ULC node software.
- Each node in the ULC network is given a fixed amount of ULC on a daily basis for participating in the network.

- The coins on the ULC network serve the function of a cryptocurrency. They also provide the utility of User-Activated Software Forks (UASF).
- Each node in the ULC network will need to hold a fixed amount of ULC in a bond account in order to participate in the network. The amount held in the bond account is at risk of being lost if the node misbehaves. The bond amount can be adjusted by the community via UASF.
- A fixed amount of ULC is also given to a maintenance fund on a daily basis.
- The holders of ULT tokens will be able to obtain an equivalent amount of ULC once the network is started.
- There is a 0.01% transaction fee on transactions. The transaction fees are burned. This amounts to a fee of $0.01 for a $100 transaction. The purpose of the the transaction fees is to reduce the coin supply to benefit all users and not just the miners. The transaction fee rate can be adjusted by the community via UASF.
- The amount given to nodes, the amount given to the maintenance fund and the transaction fee are parameters that can be changed by the community via UASF every 3 months.
- UASF outcome is determined by amount sent to the option addresses. The amounts sent to option addresses are burned after the software fork is activated.
- The total supply of ULC is not fixed and can gradually fluctuate based on what the community chooses for the miner rewards and transaction fees. The ULC supply will initially be close to the ULT supply after the excess ULT is burned.
- Other projects which use the ULC software and want to gain an immediate community of users can airdrop tokens for their project to ULC holders.

Reimbursements

A total of 6,000,000 tokens will be distributed to 6 early contributors as reimbursement for sweat equity and other expenses related to the project over several years prior to the token launch and for ideas contributed to the project without further Intellectual Property right claims.

The tokens will be reimbursed at a rate of 2% per month. Upon final release of the ULC software and prior to the ULT to ULC distribution event any remaining amount that was not already reimbursed will immediately be distributed.

Project Reporting

Each month the project will report on the website ulcproject.com, the total amount of ULT distributed through the bounty program. Also, any amount that is distributed as part of reimbursements and airdrops will be reported. The total circulating supply information can also be verified by examining the Ethereum blockchain for the ULT smart contract.

Project Roadmap

Since 2011, Omar and Aamir Syed have been studying consensus algorithms and in 2016 began to focus on writing specifications for the Unblocked Consensus Algorithm and the Unblocked Sharded Ledger. The specifications were completed in mid 2017.

In late 2017

- The Unblocked Consensus Algorithm was implemented and tested across nodes running in different data centers in the USA. These tests did not exceed more than 100 nodes. Future tests with 100+ nodes running in data centers throughout the world are planned.

In Q1 2018

- Project funding model is determined.
- Legal opinion on the project funding model is obtained.
- Website developed.
- White paper written.

In Q2 2018

- The project is announced publicly.
- The core team is expanded with more developers.

In Q3 2018

- The project will develop the Unblocked Ledger Coin node software along with a command line interface to interact with it.
- The project will also be developing a web and mobile client to interface with the network.
- The project will also be developing an explorer for the ULC ledger.

In Q4 2018

- The project will file for defensive provisional patents. If a complete patent is not filed within one year of the provisional patent, the patent rights expire and become public domain. This ensure that others cannot obtain a patent for the same technology based on first to file and prevent the original inventors from using the technology.
- The test network for Unblocked Ledger Coin will be released along with the command line interface.
- Shortly after the release of the test net, the web and mobile client will be released.
- The ULC ledger explorer will also be released in Q3.

In Q1 2019

- The project will release the main net for ULC.
- Undistributed ULT will be burned. The maintenance fund from ULC will be used to provide future support for ULC and ULT.

- After the burn event, a snapshot of the balances of ULT will be taken and the holders of ULT will automatically obtain an equivalent amount of ULC by proving their ULT address.

In 2019

- The ability to perform cross chain atomic swaps with other coins that support this feature will be added.
- Also support for trustless, off-chain transactions, similar to the lightning network, will be added.
- The ULC software is designed to be forked and used for other open source public ledgers. Projects which use the ULC software are asked to provide tokens from their project to holders of ULT and ULC.

Project Team

The project is organized as an international association of multiple individuals working towards the same goal. As such we invite anyone who can add value to the project to get involved. We can be contacted at info@ulcproject.com. For a list of current team members please visit the project website at ulcproject.com.

Future Directions

The technology developed for ULC will serve to showcase the many features discussed earlier. We expect other project to fork the software and use it for their own needs. Additional coins with different economic models or greater privacy can be created as forks of ULC. Projects can also fork ULC to add a virtual machine and smart contract layer. Combining the ULC technology with a smart contract layer will allow for easy development of global scale decentralized applications such as a global identity and reputation network.