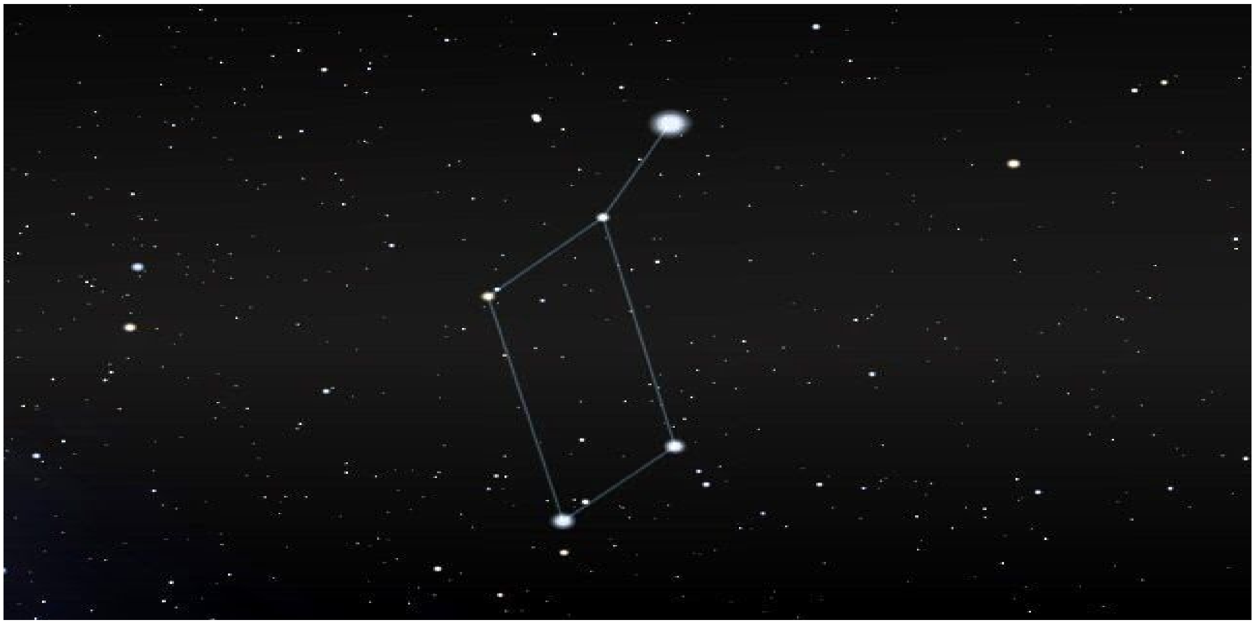

LYRA - DAG-style Tokenized Payments Blockchain Platform

FOR MERCHANT TOKENS AND BEYOND

Summary White Paper

Slava Gomzin, Dan Itkis, GRAFT Core Developers

Version 2.0 Draft

July 10 , 2019

Criteria for Lyra Blockchain **2**

LYRA Use Cases **4**
Issue Tokens 4

LYRA Principles **4**
Currencies vs Payment Platforms **4**
Token vs Currency **5**
Traditional Payment Systems vs Cryptocurrencies **5**
LYRA vs Traditional and Crypto Payment Systems **5**

LYRA Design Concepts **6**
Sharding **6**
Pruning **6**
Scalability **7**
Privacy **7**
Transfer and Pay Transactions **7**

Transactions with LYRA Brokers **7**

Special Applications **8**
Void, Pre-Auth, and Complete Transactions **8**
LYRA Plastic Payment and Cold Wallet Cards **8**
Proprietary LYRA Implementations **8**

Consensus Mechanism **9**
PoW vs PoS **9**
Delegated Proof-of-Stake **9**

Case Study - Shopify Loyalty Program **9**
Intro / Problem 9
Solution 10
How It Works 10

Conclusion **10**

References **10**

Goals of Lyra Blockchain

- Create a token payment blockchain that would keep and extend the main GRAFT project principals, proposals, and achievements such as privacy, real time authorizations, buyer-friendly fee structure, multi-currency support, special merchant transaction flows, custom merchant tokens, participating economy, and more (see original GRAFT white paper for more details) [1]
- Doesn’t rely on Proof of Work consensus
- Provides virtually unlimited scalability to enable TPS (transactions per second) rates competitive with traditional payment processing networks
- Is not subject to a prolonged locking of funds in user wallets (both payer and payee) caused by waiting for multiple “block confirmations”
- Low network latency
- Eliminates dependence on one large and continuously growing blockchain database
- Provides ability to generate any number of custom tokens
- Provides a conversion and utilization platform for the tokens
- Decouples the payment platform from any specific cryptocurrency

LYRA Functionality (high level)

Once a user created LYRA account and deposited Bitcoin, they can perform the following actions:

Issue Tokens

Anyone will be able to issue tokens on Lyra. There will be a cost to token issuance as determined by the blockchain setup. Depending how the blockchain is set up, there might or might not be an opportunity to issue additional tokens.

Grant and Redeem Tokens

The process of granting and redeeming tokens involves transferring tokens among users. Tokens can be set up as fungible or non-fungible, affecting the process of grant and redemption based on their nature.

Exchange Tokens

There is a process of token exchange which takes into consideration token internally or externally defined value.

LYRA Principles

The main goal of LYRA is creating a platform capable of issuing and collecting (redemption) of the tokens as payments alongside electronic fiat transactions. Such system has to be fast (point of sale fast), support unlimited throughput (TPS), be elastically scalable and eventually fully decentralized.

Currencies vs Payment Platforms

People often confuse between currency and payment system. Currency is Money. Payment System is a mechanism that allows currency to transact (change the owner).

US dollar is currency. Euro is currency. US dollar bills and coins (cash, banknotes) are a payment system that enables face to face transactions. Visa and Mastercard are payment systems that enable non-cash, electronic transactions. PayPal is a payment system that allows to safely transact online.

Bitcoin is native online currency (cryptocurrency, or simply crypto), with basic “built-in” payment system that allows to process Bitcoin transactions online. There are many other crypto in existence.

The world doesn’t need another currency, but it needs a permissionless, secure, private, fast, and convenient payment system that would be able to process payments and transfers both online and in brick-and-mortar stores, in various currencies and cryptocurrencies. Only decentralized payment system can provide absolute privacy, highest security, and undiscriminating access to buyers and merchants. Not to mention the fact that only decentralized payment system can operate decentralized cryptocurrencies without reducing the value of their fundamental properties.

Token vs Currency

Tokens have some properties of currencies: they have value and they can be exchanged to currencies or other tokens. But unlike currency, tokens typically have a specific niche, with limited applicability tailored for particular goals. For example, slot machine tokens are used to simplify and secure the operations of arcade games and casino slot machines. You cannot pay with slot machine tokens in a grocery store.

Traditional Payment Systems vs Cryptocurrencies

Traditional payment systems operate with existing, established currencies, which allows them to focus solely on payment processing domain. Crypto payment systems, in addition to payment systems, have a burden of taking care of their own underlying currency - something that is usually being taken care by national governments and financial corporations. As a result - inconvenient, insecure payment system, or illiquid, volatile currency, or both.

LYRA vs Traditional and Crypto Payment Systems

Unlike other crypto, LYRA is a pure payment system which does not have any “built-in” underlying currency or token.* Like traditional payment systems, it operates with existing currencies, so it is completely free of monetary policies, volatility, and other concerns not related to payment processing domain. As a result, LYRA has characteristics that are difficult or impossible to achieve using mono-cryptocurrency systems: high speed, virtually unlimited scalability, and versatility of payment methods. What differentiates it from traditional payment systems, however, is decentralization, which opens a pandora box of priceless features: undiscriminated permissionless access, security, privacy, low fees, open participating economy, and more.

LYRA Design Concepts

Nano was the first cryptocurrency that implemented “block lattice”, where transactions are recorded in individual accounts (blockchains) instead of single central blockchain.[2] LYRA introduces a similar concept of **chain collection** where transactions are also recorded on individual chains but *send* and *receive* blocks are not linked directly to preserve privacy.

Sharding

Each LYRA user maintains its own blockchain called **account**. Each block contains a single transaction. The network does not maintain a single chain of blocks, which allows to process transactions faster. Instead, there is a collection of individual accounts (chain collection) which effectively creates a **sharding** mechanism.

LYRA transaction consists of **send** and **receive** blocks. The sender wallet generates a *send* block and sends it to the authorizers for authorization. Once *send* block is authorized by the quorum of authorizers, it is broadcasted to the entire network and retained by all full nodes in *chain collection*. The *send* block is added to the sender account’s blockchain.

When a recipient receives the broadcasted authorized *send* block, it generates *receive* block and sends it to the authorizers for authorization. Once authorized, the *receive* block is added to the recipient account's blockchain (which is also a part of chain collection)

Comparing to traditional payment processing flow, *send* block processing is similar to authorization phase, while *receive* block corresponds to the settlement phase of the payment transaction processing. Once *send* block is accepted by the network, transaction is considered irreversible, even before the *receive* block is created by the recipient. Once the receive block is authorized, the transaction is considered fully settled.

Pruning

Both send and receive blocks contain the updated **account balance** (for sender and recipient account respectively), which enables **pruning**, i.e. all nodes don't have to store the entire chains but can only store the last blocks. Thus, wallets and other applications don't need to scan the entire blockchain in order to retrieve the current account balance, which enables real time financial transactions and dramatically reduces system requirements for CPU, memory, and disk space. This feature also solves the problem experienced by most crypto with single blockchain - continuously growing transaction database, which continuously increases the cost of operation of every network node.

Scalability

High scalability is achieved by using a chain collection of individual accounts, where transactions belonging to different accounts can be added simultaneously, without the need to accumulate them in blocks and maintain a single continuous chain of blocks. Thus, LYRA has virtually unlimited scalability, which is only limited by authorization nodes performance, and can achieve TPS (transactions per second) numbers competitive with traditional payment processing networks.

Privacy

Both send and receive blocks are protected by using the methods defined in CryptoNote white paper and its subsequent enhancements, such as unlinkable payments (aka stealth addresses) and ring confidential transactions.[3, 4] The amounts and the wallet addresses are obfuscated, i.e. an observer cannot establish a link between the sender and the recipient, or determine any transaction and account balances.

Transfer and Pay Transactions

Although Transfer and Pay are both spending transactions which use the same mechanism described above (send/receive blocks), they are processed in a slightly different way. Since Pay transaction is intended for merchants to collect payments from their customers in real time, it is prioritized over regular transfers when processed by the network.

Transactions with LYRA Brokers

Unlike basic LYRA transactions such as transfer and pay, LYRA Broker transactions involve third-party entities in addition to the LYRA nodes. LYRA Broker is a LYRA between a fully decentralized LYRA network and the rest of the (centralized) world. LYRA Broker is an element of decentralized system. Every network user with a positive account balance can vote for a broker. The voting allows to participate in broker dividends. Similar to authorizers, brokers belong to specific owners, but removal of one or several brokers from the network does not interrupt the function of the entire network as other brokers move up in the list.

Brokers provide liquidity to the network by accepting deposits of cryptocurrency or fiat currency and returning an equivalent of their deposit in LYRA notes. The network (authorizers) and all account holders can monitor deposits in real time.

The Broker's deposit guarantees that LYRA notes are backed by actual redeemable funds. Thus, LYRA does not generate any currency, and all LYRA accounts are 100% liquid and always redeemable for the original cryptocurrency or fiat currency.

Special Applications

Void, Pre-Auth, and Complete Transactions

The fact that every LYRA transaction consists of two blocks (send and receive) enables very important functionality which is not available on regular blockchain while widely used by payment card industry for years. Pay transaction can be either accepted by the recipient (by generating a complementary Receive block) or rejected (by generating special Void transaction).

LYRA can also easily implement pre-authorization and completion mechanism which is absolutely required for hospitality, gas stations, and other segments of payment processing industry.

Pre-auth/Complete is essentially a hard-coded smart contract. Pre-auth transaction is a send block of Pay transaction with special flag. Pre-auth must be followed by Complete, which is another transaction issued by the merchant with the change amount that cannot exceed the original pre-auth amount. Complete can be issued with zero amount which means that the entire amount of pre-auth is charged by the merchant. If Complete is not issued by the merchant within predefined time interval (7-30 days), the sender's wallet can issue a reverse transaction cancelling the pre-auth.

LYRA Plastic Payment and Cold Wallet Cards

The fact that LYRA updates the recent account balance for each block/transaction allows very lightweight implementation of spending card. The smart card has to store only one recent transaction in order to be able to create a new spending transaction and trace the account balance correctly. The card does not need to use any external "help" in order to be able to construct the spending transaction since there is always only one input (the recent balance) used in transaction. Also, the most recent incoming transaction (receive block), if the card is "bi-directional", can be easily requested through the payment terminal without any violation of privacy as all the account's blocks/transactions are encrypted.

Proprietary LYRA Implementations

Since LYRA does not have underlying cryptocurrency, it can be easily adopted by proprietary player. Proprietary implementation of LYRA software may help centralized payment processors rapidly enter the crypto business, and/or prepare themselves for participating in the public LYRA. Since authorization nodes also become proprietary, there will be no need in voting process. However, the system will still retain the performance, fault tolerance, privacy of transactions, and security of deposits - if authorization nodes are maintained properly, in isolated environments, with appropriate key management.

Consensus Mechanism

PoW vs PoS

The continuous emission and rapidly growing supply of "mineable" coins contribute to high volatility of those coins. Continuous emission is required for proof-of-work blockchains in order to keep them going. The miners receive significant incentives in a form of block rewards, even if transaction volume is insignificant. Therefore, a mineable blockchain becomes "self-sufficient" even if it does not carry a significant payment function. In absence of voracious miners, the proof-of-stake systems can be sustainable without inflation.

Delegated Proof-of-Stake

Several successful attempts have been made to eliminate proof-of-work and fully replace it with proof-of-stake. Several "high-ranking" crypto projects (EOS, Tezos, Lisk, BitShares, Nano, Ark) have implemented a **delegated proof-of-stake (DPOS)**, or based their consensus mechanism on DPOS principles (Cardano). [5] In DPOS all participants can vote for a few nodes by delegating their coin balances to the nodes they trust. The more votes (the greater stake balance) the node receives, the higher its position and the possibility of being elected as an authorizing node.

LYRA uses DPOS as its consensus mechanism applied to chain collection with separate send and receive blocks. Transactions are authorized within milliseconds because of the limited number of authorizers pre-selected by account holders, and compact blockchains consisting only of the blocks that belong to particular account.

Case Study - Shopify Loyalty Program

Intro / Problem

Shopify provides an ecommerce platform for small merchants to sell their differentiated product. While it provides a very effective, diverse, and streamlined payment options, the customers (merchants) are left to their own devices when it comes to implementing any sort of loyalty or store credit programs, resulting in very inconsistent and often missing experience for their client. Options exist in the Shopify appstore from 3rd party solution provides that utilize centralized databases to store the loyalty points, however it forces the merchant to permanently be at the mercy of said 3rd party to maintain their program once it has started.

Solution

Using a token payment blockchain like Lyra it's possible to create a loyalty / store credit program that's both portable and persistent. A blockchain-based solution doesn't depend on the 3rd party being operational, is inherently omni-channel, and survives transitions among e-commerce platforms, providing the merchant with much needed flexibility.

How It Works

Conclusion

As you can see from this white paper, LYRA is attempting to combine the best ideas and technologies currently available in crypto space, such as delegated proof of stake, sharding, and CryptoNote, and apply them to the tokenized financial payment network space. We operate with concepts like "accounts" (both regular and saving) to maximally resemble the existing financial system paradigms, while “authorizers” resemble payment network methods and workflows, which enables faster adoption by mainstream users

Given the limitations of PoW, a proof of stake blockchain with chain collection is ultimately a better approach for the “merchant token” functionality - faster, requiring less storage, consuming less resources, and providing more level playing field.

References

1. GRAFT: A Decentralized Payment Processing Blockchain Network. Slava Gomzin, Dan Itkis. https://www.graft.network/wp-content/uploads/2018/10/Graft_White_Paper_3.0_October_2018.pdf

2. Nano: A Feeless Distributed Cryptocurrency Network. Colin LeMahieu. https://nano.org/en/whitepaper

3. CryptoNote V2.0. Nicolas van Saberhagen. https://cryptonote.org/whitepaper.pdf

4. Ring Confidential Transactions. Shen Noether, Adam Mackenzie and Monero Core Team. https://lab.getmonero.org/pubs/MRL-0005.pdf

5. Delegated Proof of Stake: Features & Tradeoffs. Myles Snider, Kyle Samani, and Tushar Jain. https://multicoin.capital/wp-content/uploads/2018/03/DPoS_-Features-and-Tradeoffs.pdf