Galactrum: Community Controlled Autonomous Digital Currency

Shensu (Developer)

Iwasaki (Developer)

Tiangou (Community Manager)

March 2018

Abstract. Galactrum (ORE) is an autonomous digital currency, forked off of the Dash platform. In this paper the improvements Galactrum has implemented over its predecessors, including improved ASIC resistance, user experience and democratic controls, are discussed. The philosophies and motivations behind creating a self-funded, decentralized, community controlled digital currency that demonstrates the applications and developmental freedoms of a democratic proposal and voting system will be explored.

1. Introduction

Bitcoin is a revolutionary digital currency that emerged in 2009 and was hard pressed to gain public acceptance. Over time Bitcoin has been more openly accepted and implemented into an increasing number of applications. This has mainly been a result of its practical use and value as a medium of exchange. Bitcoin has provided us a baseline demonstration with great practicality and security, as well as paving the road for blockchain technology[1]. On the downside, Bitcoin's technology is becoming outdated. With much faster and more reliable systems already competing for the market space, Bitcoin has a slow and difficult time adapting to changing conditions[2]. Additionally, Bitcoin has lost its integrity as being a decentralized currency due to Application-Specific Integrated Circuit (ASIC) mining equipment that has created a monopoly over the minting of coins. This erosion of fairness has grown for multiple proof-of-work (PoW) algorithms, including SHA256 and X11, used by Bitcoin and Dash, respectively[3].

Dash was founded on January 28, 2014, under its original name Xcoin. XCoin, which was rebranded as Darkcoin 10 days later, eventually took the final name Dash in March 2015. Dash achieved many of its goals and quickly grew into a highly valued digital asset[4]. One of Dash’s main features is an incentivized masternode network that requires locking 1000 Dash. The Dash masternode network was easier to join in its early stages. Dash witnessed a huge growth period as demand increased dramatically[5]. Over time Dash grew into a peer-to-peer network of thousands of nodes. While this imposing growth gave Dash compelling network stability, it came at a cost. Dash now faces the same issue it set out to solve; growth potential in the peer-to-peer network.

As demand for Dash grew, it became more difficult to acquire, to the point of being impossible for the general public to obtain the 1000 Dash needed for a masternode. This demand indicates future growth and development will be centralized towards institutional investors and ASIC mining monopolies[6], further undermining the goals of a “decentralized” currency.

Galactrum uses the ASIC resistant Lyra2v2 chained algorithm to secure block hashing. Combined with quick 2 minute

block times and the latest advanced Dark Gravity Wave difficulty targeting, Galactrum is a modern platform ready for usage by the masses.

2. Proposal and Voting System

Galactrum establishes community control through a transparent proposal and voting system. Anyone may submit a proposal pertaining to the current state and/or future development of Galactrum for a small fee, paid in ORE (the fee is burned, increasing scarcity). A proposal is to be outlined presenting the development or changes proposed in a clear and professional manner with a detailed plan. Proposals may request a budget.

Writing proposals and votes directly to the blockchain results in a decentralized and censorship resistant democracy. The first voting cycle begins at block 197,100. Votes are tallied and budgets paid every voting cycle, which is 21,900 blocks (approximately 30 days).

2.1 Decentralized Autonomous Organization

The Decentralized Autonomous Organization (DAO) consists of Galactrum masternode operators. Operating a masternode is the only requirement to holding a seat on the DAO. Each masternode on the network may cast 1 yay/nay vote per proposal. Proposals must receive 10% yay votes of the total possible votes. This gives Galactrum a decentralized and democratic approach to its structure and future development while also remaining fully transparent. Every vote is cast on the Galactrum DAO for public view in each cycle.

2.2 Galactrum Treasury

After the voting cycle begins 10% of every block is reserved in the treasury for proposals. Proposals can request one time payment or recurring payments. It is up to the masternode operators to examine the proposal and determine if the requested funds are reasonable. Masternode operators can revoke their vote at any time and funds are only awarded at the end of voting cycle.

2.3 Voting Platform

The Galactrum DAO lives inside its blockchain powered by its consensus algorithm. Accessing the underpinnings of the DAO core functionality are esoteric and cryptic to a non-technical user. Without a web-based voting platform tool, it would be extremely difficult to participate in the DAO for the average user.

The Galactrum voting platform will assist users in formatting their proposals into the appropriate bytecode needed to broadcast to the network from the wallet console. Additionally, the platform will track current proposals, display statistics, and serve a place for community discussion and debate.

3. ASIC PoW Consensus Resistance

Bitcoin was originally intended to be a decentralized and distributed currency where the security and integrity of the blockchain is not controlled by a single entity or group. The creator of Bitcoin, Satoshi Nakamoto, once wrote “One CPU, One Vote”[7]. However, the birth of specialized chips called Application-Specific Integrated Circuit (ASIC) that can mine Bitcoin thousands of times more efficiently than any desktop computer made mining inaccessible to the general public. Bitcoin mining is now dominated by a small group of people with the capital to develop or purchase these ASICs, and the ability to build and maintain large mining farms[6]. This gives them a disproportionate amount of influence, making it easier to mount a successful 51% attack.

Galactrum’s PoW (proof-of-work) hashing algorithm, called Lyra2REv2 (often shortened to Lyra2v2), is designed specifically to resist the development of custom mining hardware and multi-pool mining. This resistance ensures that all transactions are verified by a widely distributed network.

3.1 Lyra2v2 Technical Advantages

Lyra2v2 is a more efficient password-based key derivation scheme that allows legitimate users to fine tune memory, processing costs and parallelism according to the desired level of security and resources available in the target platform. It employs the use of cryptographic algorithms that allows the generation of a pseudorandom string of bits from the transaction message and private key provided by the sender. This process employs a one-way function, so that recovering the private key from the output string of bits is computationally infeasible, making it almost impossible to reverse engineer the private key. To achieve this, Lyra2v2 uses the concept of reduced-round cryptographic sponges, creating a strictly sequential process. These sponge functions are an iterated mode of operation that uses a fixed-length permutation and a padding rule. Additionally, Lyra2v2 brings the following important improvements:

- It allows a significantly higher security level against attack venues involving time-memory trade-offs.
- It allows legitimate users to benefit more effectively from the parallelism capabilities of their own platforms.
- It includes tweaks for increasing the costs involved in the construction of dedicated hardware to attack the algorithm.
- It balances resistance against side-channel threats and attacks relying on cheaper storage devices.

The combination of a strictly sequential design, the high costs of time-memory trade-offs, and the ability to raise the memory usage beyond what is attainable with similar solutions security levels and processing time, make Lyra2v2 a powerful solution for an efficient and secure cryptographic hashing.

4. Masternode and Mining Network

A P2P (peer-to-peer) digital currency is comprised of full nodes, partial nodes and miners. The masternode network is a network of full nodes facilitating connectivity, transaction relays, privacy protection, and instantaneous transaction locking. Masternodes play a paramount role in network stability, security and usability, and as such, are compensated with a portion of the block reward. Additionally, Galactrum masternode operators earn a vote in Galactrum DAO.

Blockchain full nodes require a significant amount of resources to operate, namely hard disk space, to maintain a full copy of the blockchain and relay transactions. This increasing demand for resources ultimately birthed a decline in the number of active nodes across the Bitcoin network[8]. With its advanced and innovative code, Galactrum is able to reliably transfer large amounts of data, in less time, all while using considerably fewer resources. With a target block time of 2 minutes combined with a block size limit of 8Mb, Galactrum is prepared to scale for generations.

4.1 Masternode Stewardship

To operate a Galactrum masternode, 1,000 ORE is needed for collateral. This collateral is used to prevent Sybil attacks[9]. Once the masternode has been set up and operational, your wallet will lock the 1,000 ORE in place. This ensures the masternode collateral is unaffected and the masternode is granted access to the network. This collateral is not forfeit. It is held as a bond which allows a masternode to participate on the network to receive a portion of the block reward. This collateral may be recovered whenever the operator wishes to terminate their masternode.

Masternodes must maintain a consistent uptime and not go offline for more than an hour. Doing so will require the masternode operator to rebroadcast a signed start message to reintegrate to the network, and as such, will lose their current place in the block reward queue.

4.2 Block Rewards

Masternodes are identical to full nodes on the Bitcoin network. However, Bitcoin nodes lack the incentive to operate. With costs far outweighing any benefits, over time the number of nodes has decreased substantially on the Bitcoin network. This has led to the masternode reward system being implemented across many new digital assets.

The consensus algorithm offers node operators a pre-determined share of newly generated ORE as well as a share of the transaction fees on the network. Like many other blockchains, Galactrum's block reward decreases over time to combat inflation. When the maximum supply has been generated, miners and masternodes will no longer generate new

coins, instead, they will be rewarded from the transaction fees on the network.

Galactrums block reward starts at 10 ORE and decreases by 50% every 5 years. The reward is distributed as follows:

Block Height	Miner	Masternode	Treasury
1-89999	50%	50%	0%
90000-99999	40%	60%	0%
100000-109999	30%	70%	0%
110000-197099	20%	80%	0%
197100-Infinity	15%	75%	10%

Only one masternode is paid in each block creation. Masternodes are paid in a round-robin fashion, scaling to any number of masternodes (note that the current ORE supply is the only limiting factor to the number of active masternodes). This method of scaling leads to fluctuations in masternode rewards and can be calculated using the following formula:

$$\frac{n}{t} r * b * a$$

Where the terms are defined as:

n	# of masternodes operator owns
t	Total number of masternodes
r	Current block reward subsidy
b	Daily create block average
a	Percent of masternode payment

4.3 Deterministic Block Reward Ordering

Masternodes are paid in a pseudorandom order to avoid any possibility of manipulation. The hash from each proof-of-work block is used to secure this algorithm for selecting a winner from the network.

Psuedocode which selects a masternode block reward payee:

```
// blockHashes maps height->hash
// masternodeVins maps
//     masternode->vin
// HEIGHT is current block number

top_score = 0
For(m in masternodes) {
    hash = blockHashes[HEIGHT]
    vin = masternodeVins[m]
    score = abs(hash - vin)
    if(score > top_score){
         top_score = score
         payee = m
    }
}
```

4.4 Trustless Network Consensus

Incentivization of operating a masternode creates a decentralized network of nodes that are difficult to manipulate. To control 51% of the network, an attacker would need to acquire at least 1000 ORE multiplied by

the number of masternodes. If the majority of the circulating supply is locked into existing masternodes, the attacker would be unable acquire enough ORE to carry out a 51% attack. Ultimately it becomes impossible for any one person to control 51% of the network because the required supply is not available when a high number of nodes are active on the network. Newly mined coins become more valuable as the supply decreases and it becomes financially unviable to obtain and sustain 51% control.

A large decentralized masternode network enables Galactrum to execute highly sensitive tasks on the network in a trustless manner, where no single entity can manipulate the results. For each task assigned, a selected amount of pseudorandom masternodes from the network perform the same task. Randomizing the work distribution to multiple nodes ensures there is no way to manipulate the results of the task. Similar to the manner in which a fork is corrected on a blockchain, in the event of a conflict, the results of the task are determined by the majority influence.

5. Advanced Transaction Technology

Building on the principal of a strong masternode network, we are able to establish critical functionality that is lacking in many other coins, such as Bitcoin. Bitcoin's slow block time leads to a slow transfer confirmation rate and the only privacy transactions have is based on obscurity. Two critical things a currency needs to be applicable are secure quick transactions and the option for privacy. Galactrum implements both cloaking for privacy and transaction locking for immediate transfer confirmations.

5.1 Cloaking ORE

Cloaking works by breaking ORE into standard denominations, similar to many fiat money currencies, and making the ORE owners indistinguishable from one another. Multiple parties can safely submit their ORE to be queued by the masternode network for cloaking. Masternodes are responsible for facilitating the cloaking process by creating sessions between parties anonymously.

The chance of cloaking being deanonymized are low when there is a large and distributed masternode network. The *probability* of a single transaction to be tracked calculated with the equation:

$$100\left(\frac{a}{e}\right)^{r}$$

Where the terms are defined as:

a	# of masternodes attacker owns
e	# of masternodes on network
r	# of cloaking rounds

5.2 Instant Transaction Locking

To be applicable in modern transactions between merchants and users, Galactrum features instantaneous transaction locking. Every block, 10 masternodes are derived in a pseudorandom fashion, similar to how masternode payments are determined. The entire network knows which 10 masternodes are selected through the consensus algorithm. These 10 nodes all vote if a transaction is valid for locking. If they all agree, a message signed by each of the 10 selected masternodes is broadcast to the network. This message signals to all wallets and miners that the inputs and outputs for the transaction are locked.

It is possible to determine the likelihood of an attacker being able to execute a double spend attack against the locking mechanism. The probability of an attacker compromising instantaneous transaction locking is very low and can be expressed with the equation:

$$\prod_{i=0}^{s} \frac{(a-(i-1))}{(m-(i-1))}$$

Where the terms are defined as:

s	# of selected masternodes
a	# of masternodes attacker owns
m	# of masternodes on network

6. Wallet Platforms

At the core of Galactrum is a family versatile and user friendly wallet GUI (graphical user interface) programs. It attempts to forge a balance between implementing the complex features of Galactrum while maintaining usability and comfort. It is essential, from a decentralization standpoint, to extend the reach of Galactrum to as many platforms as possible.

6.1 Desktop Wallets

To be applicable for a wide range of use cases, Galactrum has developed desktop wallets for Windows, Mac OSX, and Linux/Unix environments. Core features such as cloaking, instant transactions, and masternode management are available across all desktop platforms.

The main philosophy behind the design of the Galactrum desktop wallets is simplicity and usability. Using a low-contrast theme and minimizing the amount of extraneous windows, the Galactrum desktop wallets achieve a succinct and pleasant user experience.

6.2 Mobile Wallets

As the digital world rapidly advances, many actions on the internet are carried out by mobile phones. To preserve relevance and increase usability, Galactrum is developing wallets for all the major mobile platforms, such as iOS

and Android. Mobile wallets bridge a key gap between consumers and merchants. With mobile wallets, Galactrum suddenly becomes useful in situations where use of a desktop computer is not available or desired. This is a key stepping stone in the proliferation of ORE.

7. Conclusion

This paper has discussed the core concepts and motivations of Galactrum. Based on advanced cryptographic tools and methods, Galactrum establishes a robust and advanced system for commerce and self-governance. Decentralized democratic processes make up the core components of Galactrum's design. By implementing forward thinking practices, such as an internal treasury for development voted on by masternode owners, the Galactrum platform is positioned for long-term success and relevancy.

Leveraging on the success of its predecessors, Bitcoin and Dash, Galactrum lays out a concrete and precise strategy for self-expansion and developmental growth. As a consequence of using an ASIC-resistant mining algorithm, Galactrum ensures that monopolies around block mining cannot occur. Featuring essential innovations such as instantaneous transaction locking and fungibility of ORE makes Galactrum applicable to a wide range of uses. P2P digital currencies offer an exciting new frontier. Galactrum strives to be at the forefront of this new wave of thought.

Bibliography

1: Empson, Rip, "Bitcoin: How An Unregulated, Decentralized Virtual Currency Just Became A Billion Dollar Market",
2: Jonald Fyookball, https://medium.com/@jonaldfyookball/why-does-bitcoin-have-ridiculously-high-fees-and-slow-confirmations-e3fd58258a6d, 2017
3: Darryn Pollock, Bitmain's Mining Monopoly Compromises Bitcoin's Decentralized Nature, 2017
4: Theo Tsihitas, Dash vs Bitcoin: Has Dash Successfully Overcome Bitcoin's Shortcomings, 2017
5: Payments Journal, Dash Now an Easy Payment Option at 40 Million Merchants Accepting Visa, 2017
6: Joon Ian Wong, China's Bitmain dominates bitcoin mining. Now it wants to cash in on artificial intelligence, 2017
7: Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, 2008
8: Luke Parker, , 2015
9: John (JD) Douceur, The Sybil Attack, 2002