Gravium

Community Driven Cryptocurrency

Contents

Introduction 2

Key Features 3

- Governance 3
- Real World Application 3
- ASIC Resistant Proof of Work 4
- Hashing Algorithm (X16r) 4
- PrivateSend 5
- InstantSend 5

Gravium Network 6

- Masternode Network 6
- Masternode Rewards 6
- Mining 7
- Pre-Mine 8

Platforms 8

- Wallet 8
- One-Click Miner 8
- Masternode Installer 8

References 9

Introduction

Gravium is a community coin project that has arisen from a community driven to create a blockchain technology that is easily integrated into everyday life.

With the introduction of Bitcoin[1] and the 2011 recession, the world has changed the way it thinks about alternative currency. Bitcoin was developed from a desire to decentralise the market of payment. To achieve this, the creators of Bitcoin implemented a technology where there is no government or institution controlling the funds. Instead, it was governed by individuals with a computer and for this, the people helping the network through mining received a reward in Bitcoin. Since then, ASIC[2] miners have been developed that mine Bitcoin at a rate that an individual cannot compete with. Large factories of ASIC miners have been set up, which in turn has caused a centralisation of Bitcoin.

While Bitcoin has gained popularity, there has also been issues within the cryptocurrency world. Primarily, the exploitation of the newly created market to gain profits. This is achieved either by seizing the majority percentage of a particular cryptocurrency's mining hash power or starting as the majority coin holder.

Many newer cryptocurrencies have tried to implement a system of governance that would once again form a decentralised network of currency, but with the increasing sophistication of technology, many have been centralised by ASIC mining. A prime example is DASH and the X11 algorithm it implemented (the first of the X series algorithms), which operates using multiple algorithms, but in a sequential order. This in-line algorithm allows the ASIC miner to anticipate which algorithm will be calculated next. This resulted in X11 being dominated by ASIC's shortly after DASH gained popularity and compromising the decentralised network DASH was aiming for.

Gravium has implemented the latest mining algorithm, X16r[3], to ensure the longevity and decentralised nature of the blockchain industry. X16r does this by not just changing the algorithm used, but through alternating and randomising the pattern. The integration of this algorithm making it extremely difficult for an ASIC miner to be developed to mine Gravium.

Having a democratic voting system within the cryptocurrency network helps to ensure the active development and management of Gravium. The first vote ever cast was to select the hashing algorithm, which resulted with the deployment of x16r as the hashing algorithm to prevent possible market-share domination through mining the majority of coins through ASIC miners.

Along with an ASIC resistant algorithm, Gravium has implemented a masternode network, to ensure that the currency stays secure, decentralised and has the ability for InstantSend and/or PrivateSend functions. In the future, these masternodes will be used in Gravium Governance to assure an uncompromised environment for voting.

Gravium is working from the ground up, by focusing on being implemented into every day businesses and personal use functionality. While it would be ideal to obtain a large corporation for backing, this would go against the decentralised nature of cryptocurrencies. We are aiming to have a platform that is user friendly and easily accessible to both individuals and small to medium businesses, so they can start trading Gravium. In the initial phases, the developers have used a familiar wallet that many people have used with other cryptocurrencies. Looking to the future, Gravium will implement both Android and IOS based software for easy, instant transactions, along with an electrum-based wallet and a paper wallet.

Gravium is proposing a new cryptocurrency with a long-term ASIC-resistant hashing algorithm and a community based decision-making system in order to stay decentralised throughout the life of the currency. By giving the community the power to determine their own destiny, Gravium will truly be a decentralised cryptocurrency, as Satoshi Nakamoto once envisioned.

Key Features

The key features for the Gravium network are community voting and an ASIC-resistant hashing algorithm (X16r). These features are of utmost importance in securing the network from centralisation of mining and to ensure the voting community has a say in the direction and governance of Gravium and its' potential functionality.

Governance

A common trend in the cryptocurrency market is to create a coin that has a designated amount of pre-mined coins. This is to assure that the developers of the currency keep a majority stake, as well as being able to have funds for investment, marketing and development of the cryptocurrency to grow its' exposure and value. While it is a solution to prevent a dominant stake in the currency especially at early stages of the blockchain, as the market value of the pre-mined coins grow, self-control can become an issue because of the human factor. To ensure the longevity of Gravium, a multi-signature protection of pre-mine coins will be developed.

Creating a cryptocurrency has never been easier since all of the code base is open-source and a person with no prior knowledge of computer science or software development can fork[5] an already working cryptocurrency and label it their own. This creates issues of trust within the crypto-community.

Gravium has put systems in place, before the beginning of blockchain, to ensure the community gets their say in all major decisions in the development. By giving the power back to the community who invest in Gravium, no single person can decide to move in a direction that may be detrimental to its' future prospects. Everything from future software developments, community management and marketing policies can all be voted on by the community for the long-term interests of the whole community.

The management team, software development and marketing can all be subject to a vote and any stakeholder can request a vote on any reasonable topic. This helps to remove the parts that are depressing the progression of Gravium. The community will always assist in determining the operations and goals of Gravium by proposing an idea, discussing the feasibility of the concept with the community and developers, and putting it to a vote. Constructive criticisms are encouraged in the Gravium community since it provides different perspectives and in-depth thinking.

Gravium plans to adopt governance by the end of 2018 (Q4), which will add yet another task to masternodes. Masternodes will have a right to vote through a platform developed by the team to ensure the voting is fair. The use of masternodes in governance will not only encourage the masternode operators to take part in determining the future of Gravium, but will also serve as a protection against any outsiders altering the outcome of voting.

Real World Application

Gravium's focus is on ensuring every individual is able to transfer funds, without any prior experience in transferring payments through desktop wallets. Gravium will focus on getting onto multiple wallet platforms that are currently being used and if need be, develop its' own ease of use application. Gravium's aim is to build a community that will not only spread the word about Gravium, but start using Gravium as a means to pay for items and services in daily life.

Businesses are constantly looking for ways to simplify their systems, whether it be personnel, day to day operations or financial processes. When using any computer based system, the number of 'clicks' that are necessary to complete a task is important in ensuring efficiency. To achieve integration of our system into small and medium businesses, Gravium is focused on developing the infrastructure to make payment processes require as few clicks as possible, ensuring an easy-to-use, efficient process.

ASIC Resistant Proof of Work

Proof of work (PoW) makes it extremely difficult to alter any aspect of the blockchain, since such an alteration would require re-mining all subsequent blocks. ASIC miners have created a concern for blockchain technology through centralising the hashing power mainly to large companies who can afford to purchase mining specific hardware in large quantities. Smaller investors that make up the majority of the community are excluded due to losingthe majority market shares and hashing power to a single person or a group, which compromises decentralisation and the PoW[4] system which is the main purpose of most cryptocurrencies.
Gravium uses the latest ASIC resistant algorithm, which uses an alternating algorithm based on the X16, but constantly disrupting the order based on the previous eight bytes of the last block created. This makes it difficult for an ASIC miner to determine the following hash sequence.

Hashing Algorithm (X16r)

Most of today's popular cryptocurrencies have used or created newer algorithms to prevent ASIC miner dominance[6] through creating ASIC resistant algorithms. Many of the algorithms currently available are now nothing more than a marketing tool as most of the allegedly ASIC-proof algorithms can be compromised [7]. Many of the cryptocurrencies that use algorithms that have not yet been compromised by ASIC is because they are not yet profitable. It costs a lot in research and development for the production of a new ASIC miner and the algorithm needs to become profitable for a shift of production in manufacturing facilities. This means that these cryptocurrencies will struggle to both grow in value and stay ASIC resistant which makes these cryptocurrencies prone to fail in long-term.

The first community voting was to choose the best and latest algorithms available. The community of Gravium voted the X16r hashing algorithm as it has the most promising algorithm to potentially remain uncompromised by ASIC manufacturers in the long-term. This hashing algorithm uses 16 different algorithms at the same time while changing the sequence of the algorithm being used, thus making it difficult for ASIC manufacturers as there are easier and more profitable targets.

This algorithm works as a defence against ASIC producers, not because it is new and not yet compromised, but because it uses multiple hashing algorithms simultaneously while alternating the sequence of the algorithms being used and constantly disrupting the order based on the previous 8 bytes of the last block created. This system is totally against the nature of “Application Integrated Circuits” because these “developed circuits” were created to work exceptionally well performing one single task. This means that ASIC’s simply cannot work well under the circumstances created by X16r which uses 16 different algorithms at the same time in a changing sequence, requiring different tasks to be accomplished simultaneously.

Algorithms used by x16r are shown below:

blake	keccak	shavite	fugue
bmw	skein	simd	shabal
groestl	luffa	echo	whirlpool
jh	cubehash	hamsi	sha512

Difficult, however, does not mean impossible. The Gravium community is committed to maintaining ASIC resistance and will continue to be vigilant and innovative in this area of development.

PrivateSend

PrivateSend is an additional feature to the regular transactions as it has a higher level of privacy. Powered by the masternode network, the sent coins are mixed together and separated again, while repeating the mixing process according to the amount of coins sent in order to ensure the highest level of privacy possible. Three users are gathered in a queue for the PrivateSend, then the coins that they are going to send get mixed. The mixing is done by breaking down the amount to denominations of 10 (0.01GRV, 0.1GRV,1GRV,10GRV). Each time the coins are mixed according to the denominator is called a round. The segments of coins then are combined again and sent to the designated address. Since the division of coins are according to the amount of the coin using denominations of 10, the larger the transaction amount, the more break down of denominations will occur. In this way, the level of privacy is kept the same along the process whether the transaction amount is large or small.

The probability of a PrivateSend transaction being traced can be calculated with the formula as follows:

$$100 * (\frac{a}{m})^r$$

Where the variables are
a : Number of attacker masternodes
m: Total number of active masternodes
r : Number of rounds

InstantSend

InstantSend is yet another feature of Gravium, aiming to maximise the transaction speed by use of the masternode network. Everytime a block is mined, the hash is used to select 10 pseudorandom masternodes that will search for and perform the InstantSend transaction. The moment an InstantSend transaction is formed, 10 pseudorandom masternodes broadcast the InstantSend transaction to all masternodes and form a tunnel between the sender and receiver creating a fast and secure route for the coins sent. The coins reach the designated wallet instantly without confirmations necessary, while any other transactions broadcasted with the same input address and different output address will be rejected, preventing double spending.

Gravium Network

The network of Gravium consists of full nodes (masternodes)[8], partial nodes (wallets) and miners. The difference between full nodes and partial nodes is that full nodes store every single transaction that takes place in the blockchain and continues to verify them against the core consensus rules of the blockchain network, whereas partial nodes only download the necessary part of the blockchain to function. This puts full nodes in a very important role, as the whole blockchain system is based on loyal full nodes which form the backbone of the currency network, as these are the major contributors that maintain the nature of the blockchain network. Keeping an up-to-date ledger allows a healthy communication between the clients of the network. Operating a full-node is resource intensive and requires a significant amount of traffic. The growth of the cryptocurrency and its network increases the work done by the full-nodes over the years, thus making it even more resource intensive. Through the increase of network traffic, it is natural for full nodes to decrease over time if not incentivised. Another difference between full nodes and partial nodes is the incentive received by full nodes for providing services to the network as miners.

Masternode Network

Masternode network is the network of full nodes that keep the real-time ledger of all transactions taking place, while also utilising the resources of these masternodes to utilise additional features. Gravium will have a secondary peer to peer network in order to allow features like InstantSend and PrivateSend, as well as to maintain additional security to the network in order to prevent sybil attacks[9]. These nodes are kept active 24/7, as opposed to regular nodes, which creates a healthier network and prevents service shortages. For providing services these full nodes will earn an amount of GRV by splitting the block rewards with miners. 1000 GRV should remain as a collateral in the wallet in order to become a masternode. A masternode will be added to the masternode network after one hour, which requires the masternode to wait a maturing time before earning rewards.

Masternode Rewards

Keeping a healthy network is of utmost importance. Through maintaining a masternode network, a number of GVR coins are locked keeping them out of circulating supply, creating a more sustainable environment for the value of Gravium. For providing all of these services and keeping 1000 GRV locked, masternode owners are rewarded with a passive incentive to continue operating the masternode. Masternodes will be rewarded from the coins created by splitting the block reward with miners. The percentage of the rewards split will change relative to the current block number*. The percentage of rewards will increase in favour of masternodes throughout the years to incentivise the continued operation of masternodes ensuring a healthy network in the long-run.

Each hash of block will be used to select a masternode in partially randomised order, rewarded in a round robin[12] fashion. The reward received by masternodes is in direct proportion with the current active masternodes.

Masternode rewards can be calculated by the formula below:

Year	Masternode Reward	Miner Reward
1	55%	45%
2	60%	40%
3	65%	35%
4	70%	30%
5	75%	25%
6	80%	20%

$$S = \left(\frac{n}{t}\right) * r * b * p \qquad S = \left(\frac{n}{t}\right) * r * b * p$$

Where:

S = Daily income of masternode operator
n = Number of masternodes owned by the operator
t = Total number of active masternodes
r = Current block reward
b = Daily blocks created
p = Percentage of masternode reward

Mining

Gravium block time is set to be one minute. The block reward is seven GRV per block and will be reduced by one GRV once every two years, which is split amongst miners and masternode operators. Miners and masternodes will be rewarded according to the table below before splitting the reward with each other. Block rewards are significantly reduced within the first two weeks of the coin in order to prevent any unfair advantage.

Block Height	Block Reward	Coins Created	Circulating Supply
20,160	1	20,160	20,160
525,600	7	3,679,200	3,679,200
1,051,200	7	3,679,200	7,378,560
1,576,200	6	3,153,600	10,532,160
2,102,400	6	3,513,600	13,685,760
2,628,000	5	2,628,000	16,313,760
3,153,600	5	2,628,000	18,941,760

Pre-Mine

Gravium's pre-mine is a combination of a 1.42% (283,824 GRV) pre-mine for development and another 674,285.72 GRV for Gravium's swap process from a previous coin. All remaining GRV that were not used for the swap process, were burnt and sent to an unusable Gravium address. This can be verified on the block explorer.

In order to fund the project, Gravium sourced funds to keep operations running smoothly. The process of pre-mining the coin generated these funds to help bring on board qualified people such as designers, marketers, developers and many other talented personnel to assist with its growth to make Gravium viable. This will enable Gravium to maintain a core development team to work on the coin and ensure its continued success.

Platforms

Wallet

Gravium has developed a desktop wallet v1.2 qt that is accessible by Windows, Linux/Unix and macOS. Gravium has used an interface that is familiar to the crypto community to avoid any complications while using the wallet. The wallet can be used to send/receive coins, as well as monitoring masternodes via enabling the masternodes tab.

One-Click Miner

Gravium has developed a One-Click Miner for users that would like to participate in mining, but are looking for an easier and more straightforward method to do so through the application.

Masternode Installer

For people who do not wish to go through the cumbersome process or have no prior experience of setting up a masternode the team developed a masternode Installer that sets up a masternode in a few clicks.

References

[1] Satoshi, N. (2018, June 2). *Bitcoin. A Peer-to-Peer Electronic Cash System.* https://bitcoin.org/bitcoin.pdf
[2] (2015, May 29). *ASIC.* https://en.bitcoin.it/wiki/ASIC
[3] Black, T. Weight, J. (2018, June 4). *X16r, ASIC Resistant by Design.* https://ravencoin.org/wp-content/uploads/2018/03/X16R-Whitepaper.pdf
[4] (2018, July 12). *Proof-of-work system.* https://en.wikipedia.org/wiki/Proof-of-work_system
[5] Glazner, P. (2018, Feb 11). *An Explanation of Cryptocurrency Forks.* https://hackernoon.com/an-explanation-of-cryptocurrency-forks-65d79efe214c
[6] Hamilton, D. (2018, July 08). *A Short History of Antminer: Bitman's Road to Dominance.* https://coincentral.com/antminer-bitmain-dominance/
[7] Higgins, S. (2018, April 3). *Bitmain Confirms Release of First Ethereum ASIC Miners.* https://www.coindesk.com/bitmain-confirms-release-first-ever-ethereum-asic-miners/
[8] (2018, June 18). *Masternode.* https://decryptionary.com/dictionary/masternode/
[9] Murch. (2017, Feb 11). *What's a Sybil attack.* https://bitcoin.stackexchange.com/questions/50922/whats-a-sybil-attack