ENG

## A. Introduction

Over a long period of its existence, each country has accumulated extensive experience in various fields of science, technology, culture, and everyday life. There are a lot of smart and talented people in the world who pass on their knowledge from generation to generation, but much is lost or not available to others for various reasons. There are many people who want not only to pass on to their children but also to inform the whole world about something. Just as rare animals disappear in the world and the future generation will not even remember them and will not be able to see how they looked (for example, mammoths and dinosaurs). In history, we are constantly trying to recover information, but let's think about preserving information.

I think each of you thought about what will happen in the future, perhaps you wanted to transfer at least a part of yourself to the future. It is like sending a message to future generations, transmitting your thoughts, your creativity, and, in general, yourself. (for example, musicians, artists, thinkers, and inventors). We only know about them because we have carefully kept them.

At all times, there were different peoples and countries. There have always been borders and control between these countries. With the advent of the Internet, boundaries and control are slowly being erased. Nowadays, almost everyone uses the Internet to obtain new information and knowledge from around the world. Information is becoming more accessible to everyone.

People have always communicated with each other wherever they are. Used mail, telegraph, and e-mail to communicate with loved ones and for business communication. The importance of delivery and the issue of confidentiality has been and remains an important issue for everyone.

The Infinium project has been created to address these issues.

## B. Purpose

The main goal is to store information and transfer messages using advanced cryptography and blockchain technologies. Our project will be able to store information in an encrypted database, which will control the integrity of the stored data. When saving information, the block height will be fixed to track the time of information arrival. Safe transmission of messages from user to user. Using modern technologies (nodes) "Infinium" will be available in every corner of the world.

## C. The Problem - Infinite Coins and Database Size

This is not a problem, but an advantage. More precisely, infinity is our life. The life of mankind is endless as long as people are alive.

Gold has always been mined and continues to be mined to this day in exchange for other values. Gold can also be considered infinite, but it becomes more difficult to get it. The more workers mine gold, the more workers need to be paid. Our project uses a formula (log2(difficulty) * 2^40)/2 to reward workers (miners). The more employees, the more the block reward.

The number of coins will grow endlessly, but slowly. The total volume of coins will constantly decrease due to storage fees. For example, I am a musician and I want to keep my music and lyrics, so I have to spend a few coins for storage. These coins do not go into the total coin supply but are removed from the available coins. This will reduce the number of coins in circulation. At the same time, the non-material value is added to the database.

Nowadays, the volume of disks is huge and in the future, the size will increase, so you can not worry that the coin is endless. The volume will grow more slowly than the speed of technology development (hard disk size).

Since the coin is infinite, people in the future will always have the opportunity to add information to storage.

## D. Types of information to be saved

The main types of information for humans that are available with our technologies are text, photos, and music. Therefore, they will be saved in the database.

1.text
2.Photo
3.music

Also, space will be allocated in the block for recording text information. The specifics of this information will be discussed below.

## E. Scope

**Information in the database**

1. Text - Works of art, technical descriptions, poems, texts of your own composition, sayings of wise people, messages for future generations, and everything that can be described in text form.

2. Photo - Company logos, photos of celebrities and ordinary people, paintings by artists, and everything that is possible to photograph

3. Music - Works of your favorite composers, the music of your own composition, for DJ / musicians, and everything that can be recorded on audio.

When loading data, the date (block height) will be fixed. This is necessary to be able to see when the recording was made. For example, a musician has written music and wants to defend his rights as the original source.

**Information in blockchain**

1. Accounting for the number of coins
2. Control of the transfer of coins to another person or payment for storage of information
3. Encryption and decryption of data
4. Dedicated additional space for people who want to record any data. For example, I want to control the integrity of a database or any other information. I can save the hash function of my data directly to the blockchain to further verify the integrity of my personal data.

**Messaging**

Sending messages - relevant for everyone

## F. Options for access to information

1. Information is available to everyone without restrictions.
2. Information is available to everyone without restrictions, but after a certain date (block height).
For example, I wrote down the text and I want everyone to be able to see the text-only after block # 5,000,000.
3. Information is available to a person or group of people who owns the wallet. The wallet will be like a key to open information hidden from everyone. (encrypted with the private key of the wallet)
For example, a person/group of people can use it as a repository of confidential information. If a person/group wants to open it to everyone, they can publish their wallet to everyone or create a new message for everyone. Point 1. (To read sensitive information, it is enough to have a wallet/key even with 0 balance)
4. The information recorded in the blockchain is available to everyone since it is open. Only the creator of this record knows the true purpose.
5. The message can be read-only by the user to whom the message was intended. Encryption and decryption occur using the user's key.

## G. Difference from other types of blockchain/coins

For example Bitcoin - 21,000,000 pieces. Coins that have a limited amount. A lot of bitcoins were lost for various reasons. This means the real total will be much less. The price will rise in the future. Someone (bang/group of people/country) will eventually be able to get most of the coins and control the whole world if everyone uses only Bitcoin as a standard. Also, each transaction is tracked and it is possible to calculate the person with the coins. Bitcoin stores only transaction data and does not

provide any benefit to everyone.

Other coins have a large/infinite number of coins but are difficult for common people to use. Use of contracts and other technologies that only specialists in this field possess.

Unlike such species. Our variant is more secure from tracking and provides more privacy. Easy to use by people even without special education. An infinite number enables future generations to use technology as well as today. We do not limit our children, grandchildren, great-grandchildren to the number of coins or a narrow specialization ... we transfer our knowledge and experience ...

The value of our coin lies in the information itself that a person can write to the database and blockchain. Owning coins will allow a person to make an УimmortalΦ message for everyone in the present and future generations.

Nowadays, possession of any information/technology can cost 1000 bitcoins. Sometimes it happens that a person knows very important information and wants to share it with the whole world, but does not know who to tell it to so that everyone will know or keep it for many years. Our project "Infinium" will help to do this. The way of writing and reading will be easy for everyone to use. Over time, there will be more such information. Everyone will want to write or read something in our database and blockchain. The value of information and the ability to write it down will only increase over time.

## H. Communication to future generations

Be even with yourself and those around you, so you protect yourself from lying. You will quickly be able to discern truth from falsehood. 0-false 1-true - don't be zero in life. Even one unit can change everything. Seek and share knowledge. 313

## I. About the network and source code

### 1. Basic explanation

Infinium is a privacy-centric cryptocurrency with the ability to store data. It is based on cryptonote protocol. Cryptonote is the protocol for building decentralized blockchain networks with absolute anonymity, no one is able to see transaction details, only sender and receiver. This anonymity is done with ring signatures, ring signatures are a sophisticated scheme, which is more public keys needed for verification. In the case of ring signature, we have a group of individuals, each with their own secret and public key. The statement proved by ring signatures is that the signer of a given message is a member of the group. The main distinction with the ordinary digital signature schemes is that the signer needs a single secret key, but a verifier cannot establish the exact identity of the signer. Therefore, if you encounter a ring signature with the public keys of Alice, Bob, and Carol, you can only claim that one of these individuals was the signer but you will not be able to pinpoint him or her. This concept can be used to make digital transactions sent to the network untraceable by using the public keys of other members in the ring signature one will apply to the transaction. This approach proves that the creator of the transaction is eligible to spend the amount specified in the transaction but his identity will be indistinguishable from the users whose public keys he used in his ring signatures. It should be noted that foreign transactions do not restrict you from spending your own money. Your public key may appear in dozens of others' ring signatures but only as a muddling factor (even if you already used the corresponding secret key for signing your own transaction). Moreover, if two users create ring signatures with the same set of public keys, the signatures will be different (unless they use the same private key).

### 2. Double-spending proof

Many of you might think when you have completely anonymous payments, there might be a problem when the user will be able to spend the same coins multiple times which, of course, is incompatible with any payment system's principles. But the cryptonote protocol is ready for this. A ring signature is actually a class of crypto-algorithms with different features. Cryptonote uses a modified version of "Traceable ring signature" and transformed traceability into linkability. This property restricts a signer's anonymity as follows: if he creates more than one ring signature using the same private key (the set of foreign public keys is irrelevant), these signatures will be linked together which indicates a double-spending attempt. It was once exploited in cryptonote protocol, so users were able to make double-spend because key image in cryptonote is using elliptic curve ed25519 and it can be modified in a special way, that allowed to double spend. This bug was fixed in Infinium in version v2.0.0.

**3. Networking**

Infinium uses a P2P network to synchronize blocks between nodes. Blocks are part of the blockchain in which the transactions and data are stored. All blocks contain coinbase transaction that is an emission of new coins to PoW validators (in the modern era mostly mining pools) and other non-coinbase transaction that can be coin transfer or data store transaction. Infinium network is targeting to unlock blocks in about 90 seconds, so if more PoW validators join the network, the difficulty of unlocking blocks will increase. The network is calculating difficulty from the 720 blocks unlock time average. Every node saves p2pstate in which is written all connections with other nodes that the node had in its lifetime. When a node is started it will try to connect to nodes from its p2pstate. But when you are a completely new node you will use hardcoded seed nodes. These are nodes run by the Infinium development team that is meant to be the initial connection to the Infinium network.

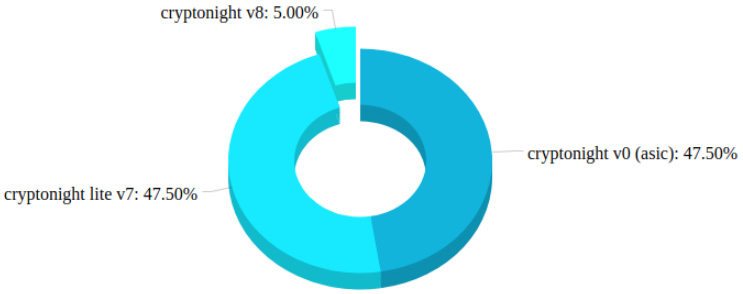
**4. Infinium 2.0.0+ Hardfork**

It is a hard fork from 4 November 2020, that changed everything in Infinium history. All older transactions were kept and old users were able to restore their wallets with old keys exporter that is able to export keys from your old wallet and use it with newer versions of Infinium. You need this exporter because the new version of Infinium uses the ChaCha8 algorithm for private and public key encryption in the wallet. Another change in the hard fork was halving the block reward because the Infinium block reward is controlled by the network hash rate, you can find the formula under C. But today there are much more powerful devices than back then when Infinium launched in the year 2014. Back then it was possible to mine Infinium with CPU, for example at the time the most top-of-the-line CPU Ч intel core i7 5820k has about 190 H/s of computational power on mining Infinium. But the times evolved and now we are using ASIC miner, which are devices with chips designed to mine that one specific algorithm and do it really fast. For example - antminer X3 has about 240,000 H/s, so this was needed. The next improvements were about the synchronization speed and calculating the Infinium total supply because the old codebase was badly written and variable with the total supply was overflowing. Also, support for BIP39 seed was added in the new Infinium to make easily rememberable seed to your wallet. The new hard fork is based on cryptonote protocol from Bytecoin v3.4.2, so thanks Bytecoin team.

**5. Infinium 3.0.0+ Hardfork**

This hard fork stole equality between miners and helped to secure the network for the future.

**1) Multiple PoW** mining algorithms are active on the Infinium network from this time. We wanted to populate all groups of miners (CPU, GPU, FPGA, ASIC) for maximal decentralization of the Infinium network. The percentile for each algorithm populated is in the chart on the right side of this document.




**1.1) How did we choose these algorithms?**

As I have written before we want equality between all miner groups, so we kept the original cryptonight v0 as an algorithm for ASIC mining. This algorithm is tested by time and it is known it is working without any unwanted bugs. As the second algorithm we have chosen cryptonight v8 for FPGA mining, this algorithm is also tested by time and it is known it is working without issues, it was implemented on the biggest cryptonote project (Monero), so its security is guaranteed. You might say why we only set 5% of the block to be mined with this algorithm. Great question, most of the time on other coins takeover of mining hash rate by few FPGA farms that are able to write bitstream for it is not much fun because only a few entities are getting newly generated coins and the rest of miners isn't able to have any chance of profitability. So we set it only to 5% because we don't want to miss out on a big hash rate from FPGA farms, but don't want to ruin the profitability for other miners. And last cryptonight lite v7, we use this algorithm for CPU and GPU mining, this algorithm was never mined on FPGAs in past, so there is little chance that bitstream for it will exist. By this algorithm, we are bringing mining Infinium to small miners at home to be able to earn newly created coins and secure the network.

**1.2) How are we able to set the percentile for each algorithm?**

We have gone up with a simple method of how to set the percentile of mined blocks to a specific algorithm. In normal PoW coin mining difficulty has been automatically retargeted to try to mine blocks in a specific time. INF (90 seconds), BTC (600 seconds). It is calculated most of the time by taking how much time it takes to mine a block on average and then the difficulty goes up or down to hit the target. We have marked 3 independent mining difficulties on Infinium for each algorithm to calculate from the

percentile of the specific block from each algorithm in the last 720 blocks and then we target for a specific time on each algorithm to get close to the percent. cn v0 - 189 seconds, cn v8 - 1878 seconds, cn lite v7 - 189 seconds.

**1.3) How is the block reward calculated after this change?**

Block reward is calculated from average difficulty from all difficulties.

**2) Merged mining** is allowed from this hard fork. And Infinium functions as the parent coin in merged mining. It is here to attract other miners from other coins with the same algorithm to mine their favorite coin + Infinium and secure both networks. It helps to stabilize the hash rate of Infinium, because of more miners, so the previously mentioned different algorithm difficulties will be more stable due to this in long term.

**Original links:**

**Website: https://infinium.space**
**Discord: https://discord.gg/jRQZMr9u84**
**Telegram: https://t.me/Infinium8**
**Github: https://github.com/Infinium-dev**

**Thanks to: CryptoNote developers, Bytecoin developers for maintaining cryptonote protocol before the Infinium team come.**

the whitepaper was written by Jacob & 313
**inspired by original cryptonote whitepaper:**
https://infinium.space/cryptonote_v2/cryptonote_v2_whitep7aper.pdf