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.

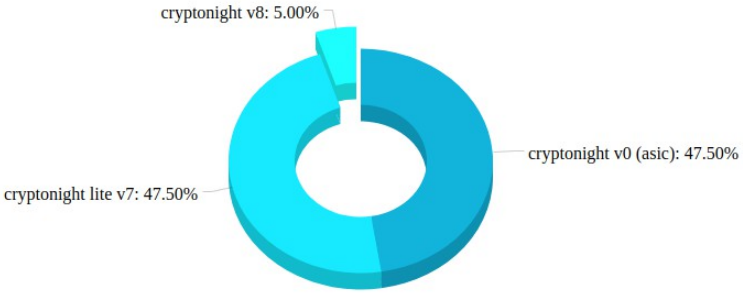
4. Infinium 2.0.0+ Hardfork

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 Ц 189 seconds, cn v8 Ц 1878 seconds, cn lite v7 Ц 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

RUS

A. Вступление

Каждая страна за длительный период своего существования накопила большой опыт в различных областях науки, техники, культуры и повседневной жизни. В мире много умных и талантливых людей, которые передают свои знания из поколения в поколение, но многое потеряно или недоступно другим по разным причинам. Есть много людей, которые хотят не только передать своим детям, но и рассказать о чем-то всему миру. Так же, как в мире исчезают редкие животные, и будущее поколение их даже не вспомнит и не сможет увидеть, как они выглядели (например, мамонты и динозавры). В истории мы постоянно пытаемся восстановить информацию, но давайте подумаем о ее сохранении.

Думаю, каждый из вас задумывался о том, что будет в будущем, возможно, вы хотели перенести в будущее хотя бы частичку себя. Это как послать сообщение будущим поколениям, передать свои мысли, свое творчество и, в целом, себя. (например, музыканты, художники, мыслители и изобретатели). Мы знаем о них только потому, что бережно их хранили.

Во все времена были разные народы и страны. Между этими странами всегда были границы и контроль. С появлением Интернета границы и контроль постепенно стираются. В настоящее время почти каждый использует Интернет для получения новой информации и знаний со всего мира. Информация становится доступнее для всех.

Люди всегда общались друг с другом, где бы они ни находились. Использовал почту, телеграф и электронную почту для общения с близкими и для делового общения. Важность доставки и вопрос конфиденциальности был и остается важным вопросом для всех.

Для решения этих вопросов создан проект «Infinium».

B. Цель

Основная цель - хранить информацию и передавать сообщения с использованием передовых технологий криптографии и блокчейна. Наш проект сможет хранить информацию в зашифрованной базе данных, которая будет контролировать целостность хранимых данных. При сохранении информации высота блока будет фиксированной для отслеживания времени поступления информации. Безопасная передача сообщений от пользователя к пользователю. Используя современные технологии (узлы) «Infinium» будет доступен в любом уголке мира.

C. Проблема - бесконечного количества монет и объем базы данных

Это не проблема, а преимущество. Точнее, бесконечность - это наша жизнь. Жизнь человечества бесконечна, пока живы люди.

Золото всегда добывали и продолжают добывать по сей день для обмена на другие ценности. Золото тоже можно считать бесконечным, но получить его становится сложнее. Чем больше рабочих добывают золото, тем больше рабочим нужно платить. В нашем проекте для вознаграждения рабочих (майнеров) используется формула ($\log_2$(сложность)*2^40)/2. Чем больше работников, тем больше вознаграждение за блок.

Количество монет будет расти бесконечно, но медленно. Общий объем монет будет постоянно уменьшаться из-за платы за хранение. Например: я музыкант и хочу сохранить свою музыку и тексты, поэтому мне нужно потратить несколько монет на хранение. Эти монеты не переходят в общий объем монет, а удаляются из доступных монет. Таким образом уменьшит количество монет в обращении. В то же время в базу данных добавляется нематериальная ценность.

В настоящее время объем дисков огромен и в будущем размер будет увеличиваться, поэтому вы можете не беспокоиться о том, что монета бесконечна. Объем будет расти медленнее, чем скорость развития технологий (размер жесткого диска).

Поскольку монета бесконечна, у людей в будущем всегда будет возможность добавить информацию в хранилище.

D. Виды информации для сохранения

Основные виды информации для человека которые доступны с нашими технологиями это текст, фото и музыка. Поэтому в базе данных будут сохраняться именно они.

1. текст
2. фото
3. музыка

Также будет выделено место в блокчен для записи текстовой информации. О специфике данной информации будет рассказано ниже.

E. Область применения

Информация в базе данных

1. Текст — Произведения искусства, технические описания, стихи, тексты собственного сочинения, высказывания мудрых людей, послания для будущих поколений и все, что можно описать в текстовой форме.

2. Фото — логотипы компаний, фотографии знаменитостей и обычных людей, картины художников и все, что можно сфотографировать.

3. Музыка — Произведения ваших любимых композиторов, музыка вашего собственного сочинения, для диджея / музыкантов и все, что можно записать на аудио.

При загрузке данных дата (высота блока) будет фиксированной. Это необходимо для того, чтобы можно было видеть, когда была сделана запись. Например: музыкант написал музыку и хочет защитить свои права как первоисточник.

Информация в блокчейн

1. Учет количества монет
2. Контроль передачи монет другому лицу или оплата хранения информации
3. Шифрование и дешифрование данных.

Выделено дополнительное место для людей, которые хотят записывать какие-либо данные. Например: я хочу контролировать целостность базы данных или любой другой информации. Я могу сохранить хеш-функцию своих данных непосредственно в блокчейне, чтобы дополнительно проверить целостность моих личных данных.

Передача сообщений

1. Передача сообщений — актуально для всех

F. Варианты доступа к информации

1. Информация доступна каждому без ограничений.
2. Информация доступна каждому без ограничений, но после определенной даты (высоты блока). Например: я записал текст и хочу, чтобы все могли видеть текст только после блока № 5 000 000.
3. Информация доступна человеку или группе людей, владеющих кошельком. Кошелек будет как ключ к открытию скрытой от всех информации. (зашифровано закрытым ключом кошелька)

Например: человек / группа людей могут использовать его как хранилище конфиденциальной информации. Если человек / группа хочет открыть его для всех, они могут опубликовать свой кошелек для всех или создать новое сообщение для всех. Пункт 1. (Для чтения конфиденциальной информации достаточно иметь кошелек / ключ даже при нулевом балансе)

4. Информация, записанная в блокчейн, доступна каждому, поскольку она открыта. Истинную цель знает только создатель этой записи.
5. Сообщение может быть прочитано только пользователем, которому оно предназначено. Шифрование и дешифрование происходит с использованием ключа пользователя.

G. Отличие от других видов блокчейн/монет

Например Биткойн - 21000000 штук. Монеты ограниченного количества. Многие монеты биткоин были потеряны по разным причинам. Это означает, что реальная сумма будет намного меньше. Цена в будущем вырастет. Кто-то (группа людей / страна) в конечном итоге сможет получить большую часть монет и контролировать весь мир, если все будут использовать только биткоин в качестве стандарта. Кроме того, каждая транзакция отслеживается, и можно вычислить человека с монетами. Биткойн хранит только данные транзакций и не приносит пользы всем.

Другие монеты содержат большое / бесконечное количество монет, но их трудно использовать обычным людям. Использование контрактов и других технологий, которыми обладают только специалисты в этой области.

В отличие от таких видов. Наш вариант более безопасен от отслеживания и обеспечивает большую конфиденциальность. Легко использовать людям даже без специального образования. Бесконечное число позволяет будущим поколениям использовать технологии так же, как сегодня. Мы не ограничиваем наших детей, внуков, правнуков количеством монет или узкой специализацией ... мы передаем свои знания и опыт ...

Ценность нашей монеты заключается в самой информации, которую человек может записать в базу данных / блокчейн. Владение монетами позволит человеку сделать «бессмертное» послание для всех в настоящем и для будущих поколений.

В настоящее время владение любой информацией / технологиями может стоить 1000 биткойнов. Иногда бывает, что человек знает очень важную информацию и хочет поделиться ею со всем миром, но не знает, кому ее передать, чтобы все знали или хранили ее долгие годы. Наш проект «Infinium» поможет в этом. Способ письма и чтения будет простым для всех. Со временем такой информации будет больше. Каждый захочет что-то написать или прочитать в нашей базе данных и блокчейн. Ценность информации и способность записывать ее со временем только возрастут.

H. Сообщение будущим поколениям

Будьте четными с собой и окружающими, так вы оградите себя от лжи. Вы быстро сможете отличать истину от лжи. 0-ложь 1-истина — не будьте нулем в жизни. Даже одна единица может все изменить. Стремитесь к знаниям и делитесь ими. 313

I. О сети и исходном коде

1. Основное объяснение

Infinium - это криптовалюта, ориентированная на конфиденциальность, с возможностью хранения данных. Он основан на протоколе Cryptonote. Cryptonote - это протокол для построения децентрализованных сетей блокчейнов с абсолютной анонимностью, никто не может видеть детали транзакции, только отправитель и получатель. Анонимность осуществляется с помощью кольцевых подписей, кольцевые подписи представляют собой сложную схему, в которой для проверки требуется больше открытых ключей. В случае кольцевой подписи у нас есть группа лиц, каждый со своим секретным и открытым ключом. Утверждение, подтвержденное кольцевыми подписями, состоит в том, что подписавший данное сообщение является членом группы. Основное отличие от обычных схем цифровой подписи заключается в том, что подписывающей стороне требуется один секретный ключ, но проверяющий не может установить точную личность подписывающей стороны. Следовательно, если вы столкнетесь с кольцевой подписью с открытыми ключами Алисы, Боба и Кэрол, вы можете только заявить, что подписавшим был один из этих лиц, но вы не сможете точно определить его или ее. Эта концепция может использоваться для того, чтобы сделать цифровые транзакции, отправленные в сеть, не отслеживаемыми, используя открытые ключи других участников в кольцевой подписи, которая будет применяться к транзакции. Такой подход доказывает, что создатель транзакции имеет право потратить сумму, указанную в транзакции, но его личность будет неотличима от пользователей, чьи открытые ключи он использовал в своих кольцевых подписях. Следует отметить, что внешние транзакции не ограничивают вас от тратить собственные деньги. Ваш открытый ключ может присутствовать в десятках кольцевых подписей других людей, но только как фактор путаницы (даже если вы уже использовали соответствующий секретный ключ для подписания собственной транзакции). Более

того, если два пользователя создают кольцевые подписи с одним и тем же набором открытых ключей, подписи будут разными (если они не используют один и тот же закрытый ключ).

2. Доказательство двойной траты.

Многие из вас могут подумать, что при полностью анонимных платежах могут возникнуть проблемы, когда пользователь сможет потратить одни и те же монеты несколько раз, что, конечно, несовместимо с принципами какой-либо платежной системы. Но протокол cryptonote для этого готов. Кольцевая подпись - это класс криптоалгоритмов с различными функциями. Cryptonote использует модифицированную версию «отслеживаемой кольцевой подписи» и преобразовывает отслеживаемость в возможность связывания. Это свойство ограничивает анонимность подписывающего следующим образом: если он создает более одной кольцевой подписи с использованием одного и того же закрытого ключа (набор внешних открытых ключей не имеет значения), эти подписи будут связаны вместе, что указывает на попытку двойного расходования. Когда-то он использовался в протоколе cryptonote, поэтому пользователи могли совершать двойные траты, поскольку в ключевом изображении в cryptonote используется эллиптическая кривая ed25519, и его можно изменить особым образом, что позволило удвоить траты. Эта ошибка была исправлена в Infinium в версии v2.0.0.

3. Сеть.

Infinium использует сеть P2P для синхронизации блоков между узлами. Блоки являются частью цепочки блоков, в которой хранятся транзакции и данные. Все блоки содержат транзакцию coinbase, которая представляет собой эмиссию новых монет для валидаторов PoW (в современную эпоху в основном пулы майнинга) и другую транзакцию, не связанную с монетой, которая может быть транзакцией передачи монет или транзакцией хранилища данных. Сеть Infinium нацелена на разблокировку блоков примерно за 90 секунд, поэтому, если к сети присоединится больше валидаторов PoW, сложность разблокировки блока возрастет. Сеть рассчитана на сложность из 720 среднего времени разблокировки блока. Каждый узел сохраняет p2pstate, в котором записываются все соединения с другими узлами, которые этот узел имел во время своего существования. Когда узел запускается, он будет пытаться подключиться к узлам из своего p2pstate. Но когда вы полностью новый узел, вы будете использовать жестко запрограммированные начальные узлы. Это узлы, которыми управляет команда разработчиков Infinium, которые предназначены для первоначального подключения к сети Infinium.

4. Хардфорк Infinium 2.0.0+.

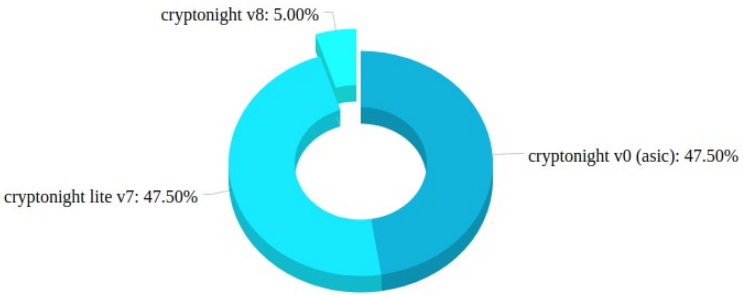
Это хардфорк от 4 ноября 2020 года, который изменил все в истории Infinium. Все старые транзакции были сохранены, и старые пользователи смогли восстановить свои кошельки с помощью экспортера старых ключей, который может экспортировать ключи из вашего старого кошелька и использовать его с более новыми версиями Infinium. Вам нужен этот экспортер, потому что новая версия Infinium использует алгоритм ChaCha8 для шифрования закрытого и открытого ключей в кошельке. Еще одним изменением в хардфорке было уменьшение вдвое вознаграждения за блок, поскольку вознаграждение за блок Infinium контролируется хешрейтом сети, вы можете найти формулу в C. Но сегодня есть гораздо более мощные устройства, чем тогда, когда Infinium был запущен в 2014 году. можно было майнить Infinium с помощью CPU, например, в то время самый топовый CPU в линейке - Intel Core i7 5820k имел около 190 H / s вычислительной мощности при майнинге Infinium. Но времена изменились, и теперь мы используем ASIC-майнеры, которые представляют собой устройства с чипами, предназначенные для майнинга этого одного конкретного алгоритма и делают это очень быстро. Например - antminer X3 имеет около 240 000 H / s, так что это было необходимо. Следующие улучшения касались скорости синхронизации и расчета общего предложения Infinium, потому что старая кодовая база была плохо написана, а переменная с общим предложением была переполнена. Кроме того, в новый Infinium добавлена поддержка семени BIP39, чтобы ваш кошелек легко запоминался. Новый хардфорк основан на протоколе cryptonote от bytecoin v3.4.2, спасибо команде Bytecoin.

5. **Хардфорк Infinium 3.0.0+.**

Этот хардфорк распределил равенство между майнерами и помог защитить сеть на будущее.

1. (Multiple PoW) Множественное доказательство работы.

С этого времени в сети Infinium активны различные алгоритмы майнинга. Мы хотим использовать все группы майнеров (CPU, GPU, FPGA, ASIC) для максимальной децентрализации сети Infinium. Проценты для каждого заполненного алгоритма указаны на диаграмме справа.



1.1) Как мы выбрали эти алгоритмы ?

Как я уже писал ранее, мы хотим равенства между всеми группами майнеров, поэтому мы сохранили оригинальный cryptonight v0 в качестве алгоритма для майнинга ASIC. Этот алгоритм проверен временем и, как известно, работает без каких-либо нежелательных ошибок. В качестве второго алгоритма мы выбрали cryptonight v8 для майнинга FPGA, этот алгоритм также проверен временем, и известно, что он работает без проблем, он был реализован в крупнейшем проекте Cryptonote (Monero), поэтому его безопасность гарантирована. Вы можете сказать, почему мы устанавливаем только 5% блока для майнинга с помощью этого алгоритма. Отличный вопрос, большую часть времени на других монетах хешрейт майнинга переходит на несколько ферм FPGA, которые могут писать битовый поток, потому что это не очень весело, потому что только некоторые объекты получают новые сгенерированные монеты, а остальные майнеры не имеют шансов на рентабельность. Поэтому мы установили его только на 5%, потому что мы не хотим упустить большой хешрейт от ферм FPGA, но не хотим разрушать прибыльность для других майнеров. И последний cryptonight lite v7, мы используем этот алгоритм для майнинга CPU и GPU, этот алгоритм никогда не майнился на FPGA, поэтому вероятность того, что битовый поток для него будет существовать, мала. С помощью этого алгоритма мы приносим добычу Infinium мелким майнерам дома, чтобы они могли зарабатывать вновь созданные монеты и защищать сеть.

1.2) Как мы установили проценты для каждого алгоритма?

Мы разработали простой метод, как установить проценты добытых блоков для конкретного алгоритма. В обычном режиме PoW сложность добычи монет была автоматически перенаправлена, чтобы попытаться добыть блоки в определенное время. INF (90 секунд), BTC (600 секунд). В большинстве случаев он рассчитывается исходя из того, сколько времени требуется для добычи блока в среднем, а затем сложность увеличивается или уменьшается, чтобы поразить цель. Мы создали 3 независимых сложности майнинга на infinium для каждого алгоритма, чтобы рассчитать проценты конкретного блока из каждого алгоритма в последних 720 блоках, а затем мы нацелены на определенное время для каждого алгоритма, чтобы приблизиться к процентам cn v0 - 189 секунд, cn v8 - 1878 секунд, cn lite v7 - 189 секунд.

1.3) Как рассчитывается вознаграждение за блок после этого изменения?

Награда за блок рассчитывается исходя из средней сложности по всем сложностям.

2. (Merged mining) Объединенный майнинг с этого хардфорка разрешен и Infinium функционирует как родительская монета в объединенном майнинге. Он здесь, чтобы привлечь других майнеров с других монет с помощью того же алгоритма, чтобы добыть их любимую монету + инфиниум и защитить обе сети. Это помогает стабилизировать хешрейт Infinium за счет большего количества майнеров, поэтому вышеупомянутые различные сложности алгоритмов будут более стабильными из-за этого в долгосрочной перспективе.

Оригинальные ссылки:

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

Наша благодарность: разработчикам CryptoNote, разработчикам Bytecoin за поддержку протокола cryptonote до прихода команды Infinium.

технический документ, написанный Jacob и 313
Вдохновленный оригинальным техническим документом cryptonote:
https://infinium.space/cryptonote_v2/cryptonote_v2_whitepaper.pdf

A. 介绍

在其存在的很长一段时间里，每个国家都在各个领域积累了丰富的经验科学、技术、文化和日常生活领域。世界上有很多聪明而有才华的人，他们一代一代地把知识传给另一代，但很多人失去了或得不到

因为各种各样的原因。有许多人不仅想传给他们的孩子，而且想让全世界知道一些事情。就像珍稀动物在世界和世界上消失一样下一代甚至不会记得它们，也看不到它们的样子（例如，猛犸象和恐龙）。历史上，我们一直在试图恢复信息，但让我们考虑保存信息。

我想你们每个人都在思考未来会发生什么，也许你们至少想把自己的一部分转移到未来。这就像给后代传递一个信息，传递你的思想，你的创造力，以及你自己。（例如，音乐家、艺术家、思想家和发明家）。我们只知道它们是因为我们小心地保存了它们。

在任何时候，都有不同的民族和国家。这些国家之间一直有边界和控制。随着互联网的出现，界限和控制正在慢慢被抹去。现在，几乎每个人都使用因特网从世界各地获取新的信息和知识。每个人都越来越容易获得信息。

无论身在何处，人们总是互相交流。用邮件、电报和电子邮件与亲人交流和商务交流。交付的重要性和保密问题一直是而且仍然是每个人的一个重要问题。Infinium项目就是为了解决这些问题而创建的。

B. 目的

主要目标是使用先进的加密技术和区块链技术来存储信息和传输消息。我们的项目将能够在一个加密的数据库中存储信息，这将控制存储数据的完整性。保存信息时，将固定块高度以跟踪信息到达的时间。用户之间信息的安全传输。使用现代技术（节点）“Infinium”将在世界的每个角落提供。

C. 问题- 无限硬币和数据库大小

这不是问题，而是优势。更确切地说，无限就是我们的生命。只要有人活着，人类的生命就无穷无尽。

黄金一直被开采，并一直被开采到今天，以换取其他价值。黄金也可以被认为是无限的，但它变得更加难以获得。开采黄金的工人越多，需要支付的工资就越多。我们的项目使用公式(log2(难度）*2^40)/2奖励工人（矿工）。员工越多，奖金越高。

硬币的数量将无休止地增长，但增长缓慢。由于保管费的原因，硬币的总量将不断减少。例如，我是一个音乐家，我想保留我的音乐和歌词，所以我不得不花一些硬币的存储。这些硬币不进入总的硬币供应，但被删除从可用的硬币。这将减少流通中的硬币数量。同时，非物质价值被添加到数据库中。

现在，磁盘的体积是巨大的，在未来，大小将增加，所以你不必担心硬币是无穷无尽的。容量的增长速度将慢于技术发展的速度（硬盘大小）。

由于硬币是无限的，未来的人们将永远有机会将信息添加到存储中。

D. 要保存的信息类型

我们的技术提供给人类的主要信息类型是文本、照片和音乐。因此，它们将保存在数据库中。

1.文本
2.照片
3.音乐

此外，将在块中分配空间用于记录文本信息。这些信息的具体内容将在下面讨论。

E. 范围

数据库中的信息

1. 文本 - 艺术作品，技术描述，诗歌，你自己的作品文本，智者的格言，给后代的信息，以及一切可以用文本形式描述的东西。
2. 照片 - 公司标志，名人和普通人的照片，艺术家的画，以及一切可以拍摄的东西
3. 音乐-你最喜欢的作曲家的作品，你自己创作的音乐，DJ/音乐家的作品，以及所有可以在音频上录制的东西。

加载数据时，日期（块高度）将是固定的。这是必要的，以便能够看到录制的时间。例如，一位音乐家写过音乐，想维护自己作为原始音乐来源的权利。

区块链中的信息

1. 计算硬币的数量
2. 控制向另一个人转移硬币或支付储存信息的费用
3. 数据的加密和解密
4. 为想要记录任何数据的人提供额外的专用空间。例如，我想

控制数据库或任何其他信息的完整性。我可以保存数据的哈希函数
直接到区块链进一步验证我个人数据的完整性。

信息

发送消息-与每个人相关

F. 获取信息的选项

1.每个人都可以不受限制地获得信息。
2.每个人都可以不受限制地获取信息，但必须在特定日期（街区高度）之后。例如，我写下了文本，我希望每个人都能看到文本后，才块 5000000.
3. 信息可供拥有钱包的一个人或一群人使用。钱包就像一把钥匙，可以打开隐藏在每个人面前的信息。（使用钱包的私钥加密）例如，一个人/一群人可以将其用作机密信息的存储库。如果某人/团体想向所有人打开钱包，他们可以向所有人发布钱包或为所有人创建新消息。第 1 点。（要阅读敏感信息，即使余额为 0，钱包/钥匙也足够了）
4.区块链中记录的信息是开放的，每个人都可以使用。只有这个记录的创造者才知道真正的目的。
5.消息只能由消息的目标用户读取。使用用户的密钥进行加密和解密。

G. 与其他类型区块链/硬币的区别

例如比特币 — 21000000 枚。数量有限的硬币。很多比特币由于各种原因丢失。这意味着真正的总数将少得多。将来价格还会上涨。如果每个人都只使用比特币作为标准，那么有人（bang/一群人/国家）最终将能够获得大部分硬币并控制整个世界。此外，每一笔交易都会被追踪，并且可以计算出持有硬币的人。比特币只存储交易数据，并不为每个人提供任何好处。

其他硬币的数量很多，但普通人很难使用。使用只有该领域的专家才能拥有的合同和其他技术。
不像这样的物种。我们的变种是更安全的跟踪和提供更多的隐私。易于使用的人，即使没有特殊教育。无限的数字使后代能够像今天一样使用技术。我们不限制我们的子女，孙子，曾孙.数量

硬币或一个狭窄的专业。 .. 我们传递我们的知识和经验 ..
我们的硬币的价值在于一个人可以写入数据库和区块链的信息本身。拥有硬币可以让一个人为今世后代的每个人传递一个“不朽”的信息

如今，拥有任何信息/技术都要花费 1000 比特币。有时候，一个人知道非常重要的信息，想与全世界分享，却不知道该告诉谁，这样每个人都会知道或保存多年。我们的“Infinium”项目将有助于做到这一点。写作和阅读的方式将便于每个人使用。随着时间的推移，这样的信息会越来越多。每个人都想在我们的数据库和区块链中写或读一些东西。信息的价值和记下来的能力只会随着时间的推移而增加

H. 与后代的沟通

对自己和周围的人要公平，这样你才能保护自己不说谎。你很快就能分辨真假。0-假 1-真-生活中不要为零。即使是一个单位也能改变一切。寻求和分享知识。313

I. 关于网络和源代码

1. 基本解释

Infinium 是一种以隐私为中心的加密货币，具有存储数据的能力。它基于 cryptonote 协议。Cryptonote 是构建具有绝对匿名性的去中心化区块链网络的协议，没有人能够看到交易细节，只有发送者和接收者。这种匿名性通过环签名，环签名是一个复杂的方案，需要更多的公钥进行验证。在环签名的情况下，我们有一组个人，每个人都有自己的秘密和公钥。环签名证明的声明是给定消息的签名者是组的成员。与普通数字签名方案的主要区别在于签名者需要一个单独的密钥，而验证者不能确定签名者的确切身份。因此，如果您遇到一个具有爱丽丝，鲍勃和卡罗尔公钥的环签名，您只能声明这些人是签名者，但你将无法确定他或她。这个概念可以用来使发送到网络上的数字事务不可追踪，通过使用环签名中其他成员的公钥，一个将应用于该事务。这种方法证明了事务的创建者有资格花费事务中指定的金额，但是他的身份将与他在环签名中使用公钥的用户无法区分。需要注意的是，对外交易并不限制你自己花钱。您的公钥可能会出现在许多其他人的环签名中，但这只是一个混淆因素（即使您已经使用了相应的密钥对自己的事务进行签名）。此外，如果两个用户使用同一组公钥创建环签名，则签名将不同（除非他们使用相同的私钥）。

2. 双重支出证明

很多人可能会认为，当你完全匿名支付时，可能会出现一个问题，用户将能够多次使用相同的硬币，当然，这与任何支付系统的原则是不兼容的。但是加密笔记协议已经准备好了。环签名实际上是一类具有不同特征的密码算法。Cryptonote 使用了“可追踪环签名”的修改版本，并将可追踪性转换为可链接性。此属性将签名者的匿名性限制如下：如果他使用同一私钥创建多个环签名（这组外部公钥不相关），则这些签名将链接在一起，这表示双重开销尝试。它曾经在 cryptonote 协议中被利用过，所以用户可以进行双倍消费，因为 cryptonote 中的密钥图像使用的是椭圆曲线 ed25519，并且它可以被复制 以一种特殊的方式修改，允许双倍的花费。此错误在 Infinium v2.0.0 版中修复。

3. 网络

Infinium 使用 P2P 网络来同步节点之间的块。区块是存储交易和数据的区块链的一部分。所有区块都包含**铸币库**交易，即向 PoW 验证器排放新硬币（在现代主要是采矿池）以及其他非**铸币库**事务，可以是硬币传输或数据存储事务。Infinium 网络的目标是在大约 90 秒内解锁块，因此如果更多的 PoW 验证器加入网络，解锁块的难度将增加。该网络正在计算 720 块解锁时间的平均难度。每个节点保存 p2p 状态，其中写入节点在其生存期内与其他节点的所有连接。当节点启

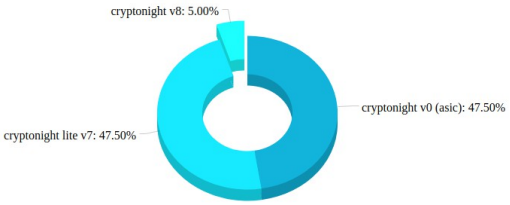
动时，它将尝试从 p2p 状态连接到节点。但是当您是一个全新的节点时，您将使用硬编码的种子节点。这些节点是由 Infinium 开发团队运行的，是与 Infinium 网络的初始连接。

4. 硬叉

Infinium 2.0.0+ 硬叉。这是一个从 2020 年 11 月 4 日开始的硬叉，它改变了英菲尼乌姆历史上的一切。所有旧的交易都保留了下来，旧用户可以使用旧密钥导出器还原他们的钱包，旧密钥导出器可以从旧钱包导出密钥，并与新版本的 Infinium 一起使用。您需要这个导出器，因为新版 Infinium 使用 ChaCha8 算法对钱包中的私钥和公钥进行加密。硬叉的另一个变化是将块奖励减半，因为 Infinium 块奖励由网络哈希率控制，可以在 C 下找到公式。但如今，Infinium 的功能比 2014 年推出时强大得多。那时候可以用 CPU 来挖掘 Infinium，例如当时最顶尖的 CPU — Intel Core i7 5820k 在挖掘 Infinium 方面的计算能力约为 190 H/s。但随着时代的发展，现在我们使用的是 ASIC 矿工，这是一种带有芯片的设备，专门用来挖掘一种特定的算法，而且速度非常快。例如，antminer X3 的速度约为 240000 H/s，因此需要这样做。下一步的改进是关于同步速度和计算 Infinium 总供应量，因为旧的代码基写得不好，并且随着总供应量的变化而溢出。此外，支持 BIP39 种子被添加到新的 Infinium，使容易记住的种子到您的钱包。新的硬叉基于 Bytecoin v3.4.2 的 cryptonote 协议，所以感谢 Bytecoin 团队。

5. Infinium 3.0.0+ 硬叉

这个硬叉偷走了矿工之间的平等，并有助于确保未来的网络安全。



1) 多个 PoW 从那时起，infinium 网络上的挖掘算法就非常活跃。 我们希望填充所有矿工组（CPU, GPU, FPGA, ASIC），以最大限度地分散 infinium 网络。本文档右侧的图表中列出了每个算法的百分位数。

1.1) 我们是如何选择这些算法的？

正如我之前所写的，我们希望所有矿工组之间相等，所以我们保留了原来的 cryptonight v0 作为 ASIC 挖掘的算法。 这个算法经过时间的检验，知道它没有任何不必要的错误。 作为第二种算法，我们选择了 cryptonight V8 作为 FPGA 挖掘算法，该算法也经过了时间的检验，并且在最大的 cryptonote 项目（Monero）上实现，安全性得到了保证。 你可能会说为什么我们用这个算法只能开采 5%的区块。很好的问题是，大多数情况下，在其他硬币上，少数能够编写比特流的 FPGA 农场接管了采矿 hashrate，因为这并不是什么有趣的事情，因为只有少数实体获得了新产生的硬币，其他矿商也没有任何盈利的机会。因此，我们只将其设为 5%，因为我们不想错过从 FPGA 农场获得的高额利润，但又不想破坏其他矿商的盈利能力。 昨晚的 CryptoLite V7，我们用这个算法来挖掘 CPU 和 GPU，这个算法在过去从来没有在 FPGA 上被挖掘过，所以它的比特流存在的可能性很小。通过这个算法，我们把采矿 Infinium 带给国内的小矿工，让他们能够赚取新创造的硬币，并确保网络的安全。

1.2) 我们如何为每个算法设置百分位数？

我们已经提出了一个简单的方法，如何设置百分位数的开采区块的具体算法。在正常的 PoW 硬币开采难度已自动重定目标，以尝试在特定的时间块开采。INF（90 秒），BTC（600 秒）。大部分时间是通过平均花费多少时间来挖掘一个区块，然后难度上升或下降以命中目标来计算的。 我们在 infinium 上为每个 algo 标记了 3 个独立的开采困难，从最后 720 个区块中每个 algo 的特定区块的百分位数计算，然后我们针对每个 algo 特定时间设定目标，以接近百分位数。cn v0 - 189 秒，cn v8 - 1878 秒，cn lite v7 - 189 秒。

1.3）这一变化后，积木奖励是如何计算的

方块奖励是根据所有难度的平均难度来计算的。

2) 合并开采 允许从这个硬叉。infinium 在合并开采中起着母币的作用。 它是在这里吸引其他矿工从其他硬币相同的算法来挖掘他们最喜欢的硬币+infinium 和安全的两个网络。它有助于稳

定 infinium 的命中率，因为有更多的矿工，所以前面提到的不同算法的困难将在长期内更稳定。

原始链接：

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

感谢：CryptoNote 开发者、字节币开发者维护 CryptoNote 协议
在英菲纽姆团队到来之前。

白皮书是雅各布和 313 写的
灵感来源于最初的 cryptonote 白皮书：
https://infinium.space/cryptonote_v2/cryptonote_v2_whitepaper.pdf