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 “immortal” 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. Infinium-8 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-8 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 block 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 — 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.

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_whitepaper.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 ди-джеев / 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.

Информацяи в блокчене

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 блокчейне, 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 биткойны 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 биткойны 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 блокчейне. 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. Infinium-8 - 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. Эта 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-8 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.

Исходные 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