I/O DIGITAL

IOCOIN.IO / IODIGITAL.IO

Application Based Blockchain

I/O COIN - Ticker: IOC

WHITEPAPER

Table of Contents

Mission Statement

Our ultimate goal is to provide a secure, fast and user friendly Blockchain Ecosystem in order to advance adoption of decentralized services around the world

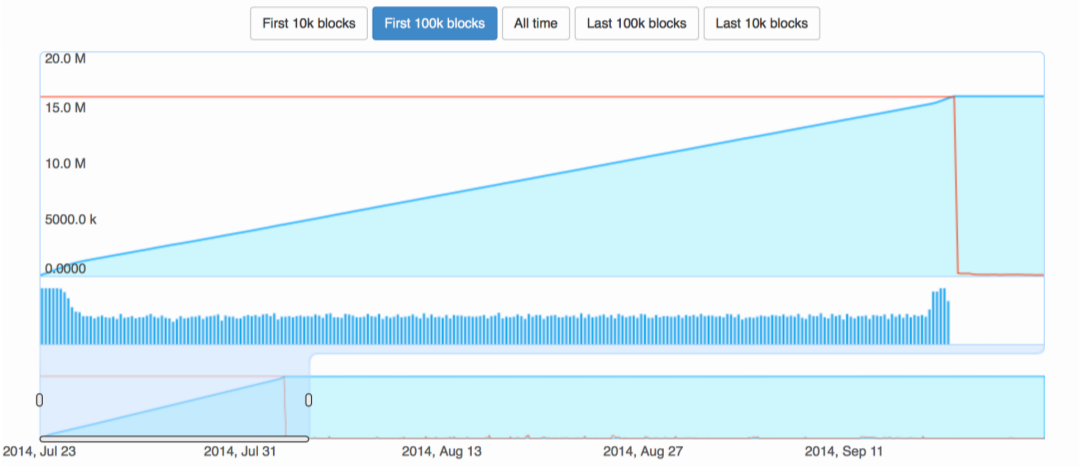
Introduction

Since the rise of the Bitcoin network in 2009, countless developers have embarked in the creation of competing peer-to-peer digital currencies/assets. Many of these were rebranded copies of Bitcoin with no to little difference in purpose, design or features. Some others attempted to improve on the path that Satoshi had proposed within his white paper, "Bitcoin: A Peer-to-Peer Electronic Cash System".

Major and viable proposals to improve on this technology have since emerged. Bitcoins constantly expanding need of power to mine new coins was one problem some wished to solve. In April 2013, a $150,000 USD per day in power consumption cost was the estimate given to Bitcoin mining world-wide.

In January 2018, a $5,287,349 USD per day power consumption cost was the estimate given to Bitcoin mining world-wide. Looking to improve the problem of exorbitant power consumption due to Bitcoin mining; Scott Nadal and Sunny King in 2012 released the white paper, "PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake".

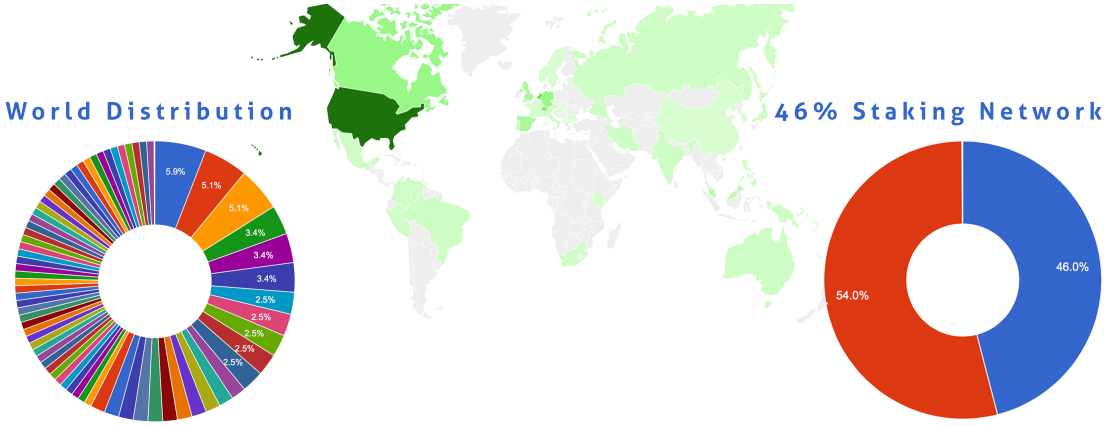
This led to Peercoin and resulted in a coin that used roughly 30% of the power consumption used by Bitcoin and introduced a number of other improvements such as the reduced risk of a monopoly held by miners and the possibility of a 51% attack. Proof of Stake minting has the effect of making a monopoly more costly, and separates the risk of a monopoly from proof-of-work mining shares. Following this and other improvements within blockchain technology, The I/O Digital team lead by it's founder Joel Bosh, devised a unique approach to PoS and the first I/O Coin Genesis block was mined on July 23, 2014.



I/O Digital development team launched I/O Coin (IOC) without any Initial Coin Ofering (ICO) or pre-mine. IOC was fair launched via mining. To ensure fair and balanced distribution, the team added to it's source code a sophisticated cryptographic hash in Proof of Work (POW) X11 algorithm, before switching to Proof of Stake (PoS I/O). I/O Digital team has since then added further improvements/user friendly features to its blockchain with a focus on security, global adoption and scalability.

State of the I/O Coin Blockchain

The importance of I/O Coin's initial fair launch, allowed for a healthy growth period while achieving synergy through features, support and trust. The I/O Coin blockchain has maintained 100% uptime in over 32 thousand hours of POS computation. At no period of time the IOC blockchain has ever been close to a 51% attack. The IOC community has maintained over 46% staking since it's genesis block.



This is a robust commitment to securing the chain. The community has achieved 100% consensus on upgrades and public nodes have been active in over 65 countries around the world. IOC recently won the "Blockchain" category in the European Fintech Awards in 2016, the Benzinga Fintech award in 2016, and was a fnalist in the 2016 European Fintech Awards.

The I/O Digital development team's goal is to secure, game changing, user friendly blockchain frameworks. The team's passion and determination is what drives us to focus on our goals. We have always put development priority frst. For that reason the team formally formed a non-proft foundation, to further educate on the use of the I/O Digital public blockchains. This is to push awareness to companies, individuals and to gain adoption for the I/O Coin blockchain's application based services.

Problem Statement

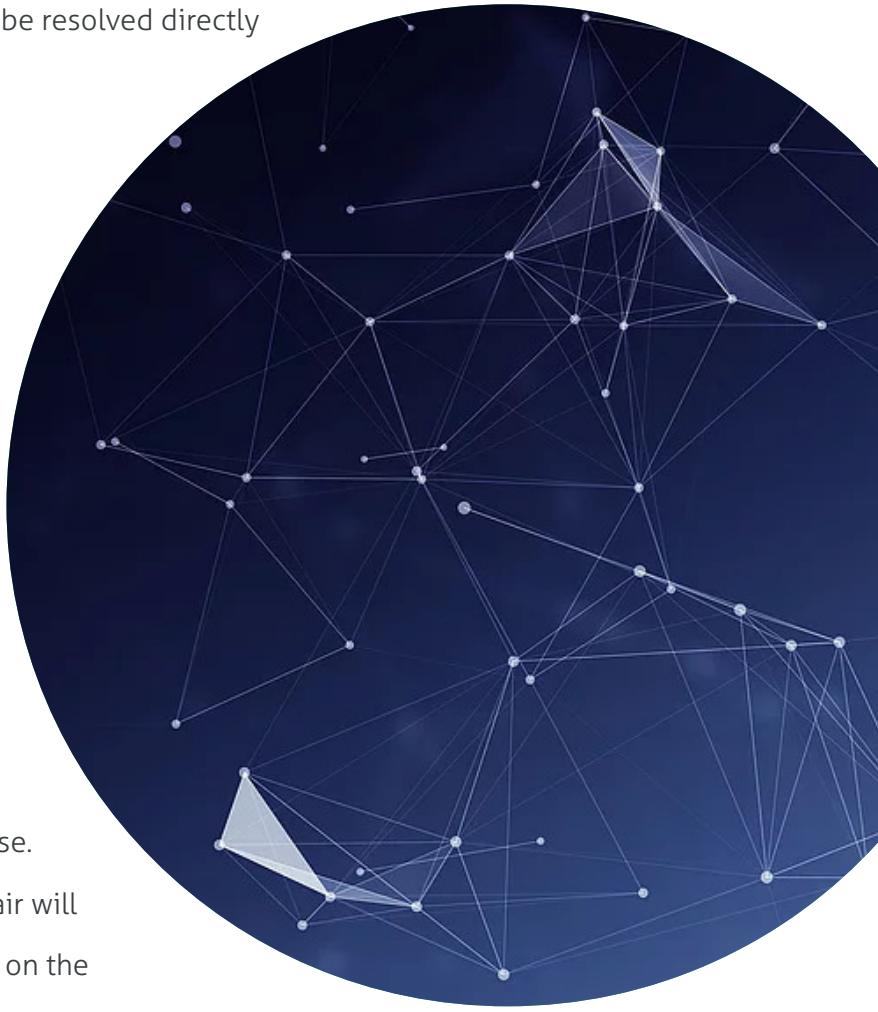
Following in the steps of Satoshi Nakamoto, IOC minted 16 million coins, with a maxcap of 22M to be reached by 2052 through POS rewards. After successfully delivering on our initial roadmap, the team embarked on the second blockchain upgrade named DIONS (Decentralized I/O Name Server). DIONS enables data on the blockchain, with capabilities of document and identity storage. DIONS also allows for AES 256 encrypted messaging, along with a complete Alias system. The IOC data, messaging / alias system fees are redistributed to all active stakers in the network. This ensures further IOC distribution and incentivizes users to stake while securing the network.

Considering the risk of data bloating, security breaches and the lack of user friendly features, the development team knew that it would only be a matter of time before a single Blockchain would be a thing of the past. The team deployed a roadmap with aggressive goals and quickly proposed an upgrade to the main I/O Coin chain, codenamed DIONS. The upgrade focus was to serve as an entry point registrar to the team's proposed Chameleon sidechain. To make this all possible the core platform algorithm was upgraded to a new Proof of Stake (PoS) algorithm codenamed "CiPher".

Along with CiPher, we have enhanced the platform with staking and security enhancements, decentrilized encryption for data, messaging and the new alias system. With all of these features being deployed alongside our decentralized GPG-like system, DIONS will prove to be successful in combining these three major components for a true user friendly and advanced Blockchain platform. Users who help secure the I/O Coin Blockchain will earn IOC at an annual rate of 4% for Staking, with additional rewards for transactions and registration fees that are redistributed to stakers..

IOC - DIONS (Decentralized DNS)

The alias key value pairs provide a means of indirection with regard to the naming of IP network nodes and may be considered as providing the basis for a blockchain based DNS like name resolution service. DIONS are aliases and provide a human readable name, which can be resolved directly from the blockchain. Alias can uniquely ascribe to an ordinary I/O COIN address. DIONS provide a means of mapping names to resources located on the internet or private networks. Which can be resolved directly from the blockchain.



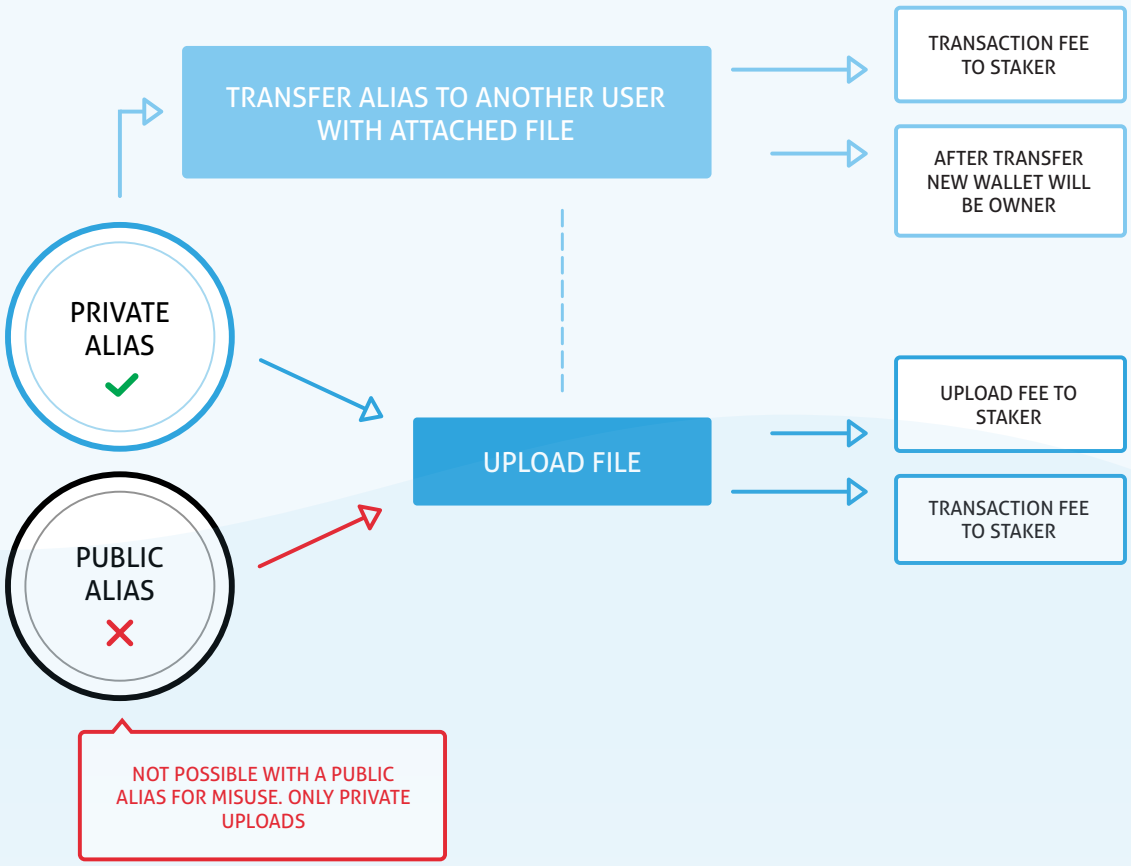
Private & Public Aliases

There are two types of Aliases; public (unencrypted) and private (encrypted). An alias is an identification of an IOC hex address with a plain text key of up to 255 characters. At any given time an alias is identified with exactly one IOC address. Private aliases are for private use. Once created, the resulting key-value pair will be encrypted, private and non viewable on the blockchain. This allows to mitigate alias squatting. A private alias stays private within the users registration and is not able to receive IOC while encrypted.

Users can only use private DIONS for file storage & secure file transfer. Once created a user can pair a particular file or transfer the alias to another user in the application blockchain.

Transfer of data is achieved by construction of a channel, over which the encrypted alias is encrypted for the recipient along with any associated data. As a result the net data payload size (and transaction size) may change as a result of the double encryption procedures.
In order to receive IOC, a private alias can be made public by simply decrypting it.

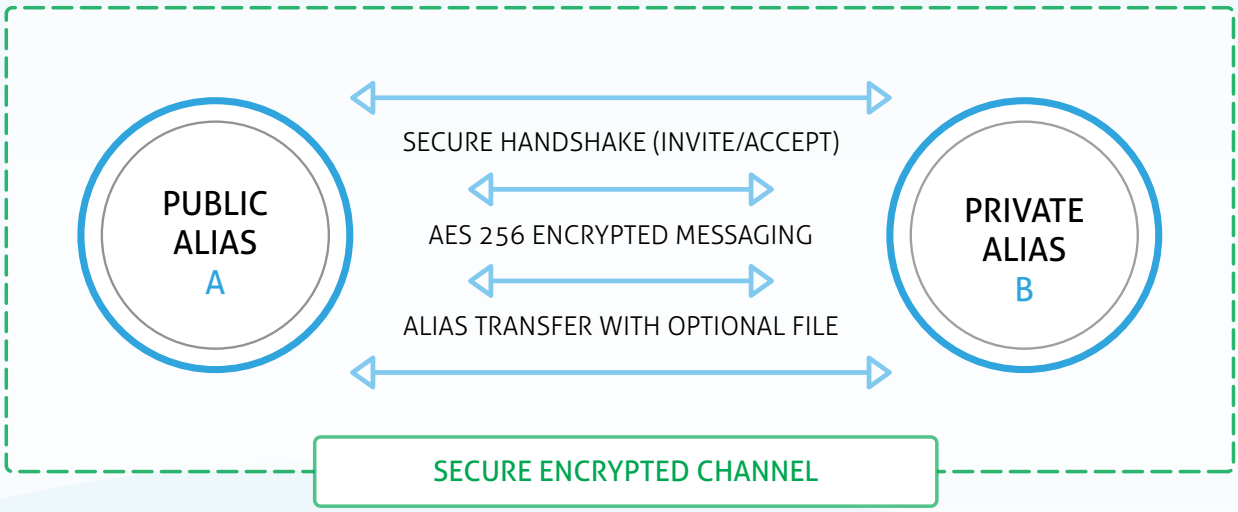
Once an alias is made public, the alias is attached to a public address and able to receive ioc. Subsequently all aliases are said to lapse after a so called 250K blocks expiry interval, where no updates can occur.



Aliases Private Transfer

Private aliases are transferable. In order for users to send or receive an alias users would have to send an invite From Public alias (A) to Public alias (B) as in an rsa key exchange. This would initiate an encrypted tunnel, giving the ability to transfer aliases, but also initiate messaging between users.

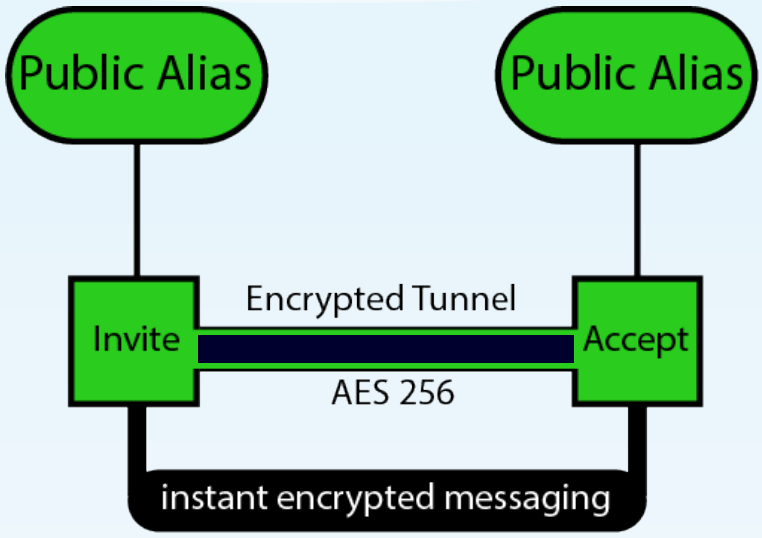
As described above, we construct a channel between endpoints associated with two aliases, in this case the alias for transfer is private i.e. encrypted. If there is any payload data this is encrypted using the symmetric key.



AES 256 Encrypted Messaging

Peer to Peer encrypted messages can be sent and received after a channel is established between Public aliases. Similar to the negotiation of an ssh session the channel is first negotiated using RSA encryption. Thereafter all payload encryption is by means of the established symmetric key which is more efficient.

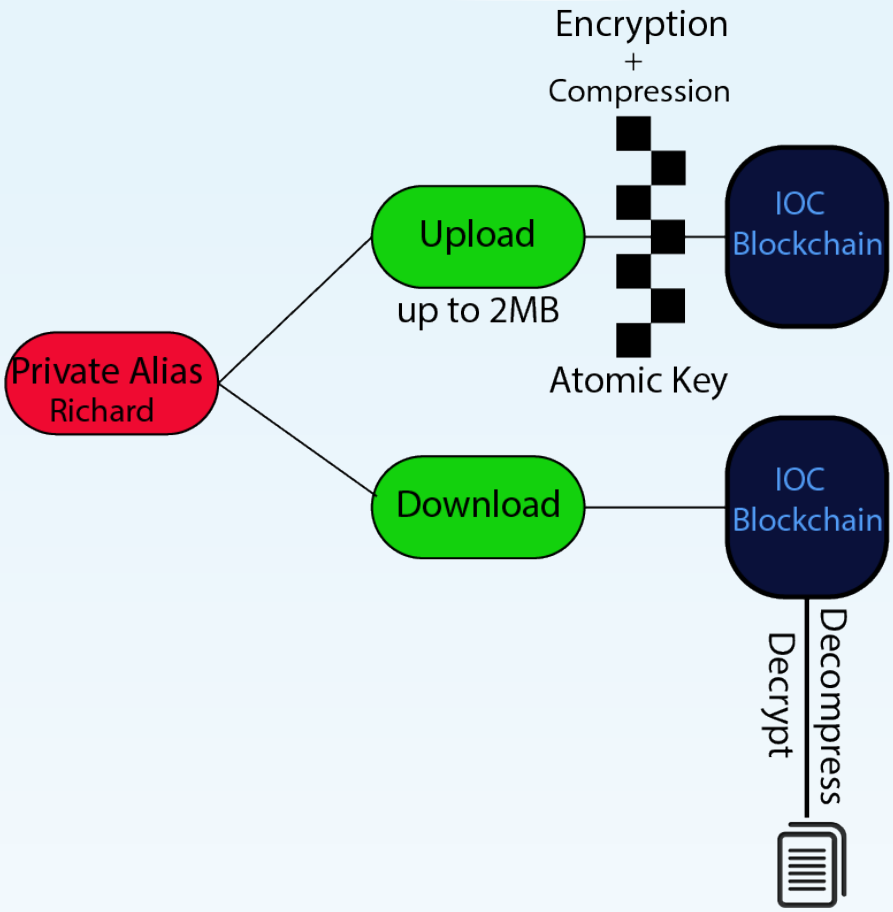
Following exchange of a symmetric key over RSA, users can converse instantly in encrypted communication channels. Confirmations are not needed for the message to be transferred, therefore making them instant. The message encryption relies on AES 256 bit keys, one per channel along with a per message 128 bit initialization vector.



Data storage

With DIONS there is the option to store encrypted content as referred to earlier. The content is base64 encoded and the underlying data may be (for example) of the form ASCII, PDF, JPEG or any binary data.

With each DION alias there exists the option to upload a data value which is currently restricted to 1 MB. Once a user has uploaded an encrypted file he may choose to send it to a second party. For this purpose an encrypted channel is established between the users and the data transmitted using AES 256 bit encryption. Once data is uploaded and encrypted by a user it is permanently available for download and decryption by the user. Thus encryption of data may be private whether or not it is over a channel or shared encryption used for transfer.



POS CiPher

This is the process for securing the blockchain. Along with the recent implementation and launch of the foregoing sections the staking mechanism was also reviewed. Since November 2017, coinage was completely removed from the staking model. The new model ensures that it is in the best interests of stakers to keep nodes running constantly in order to maximize staking rewards.

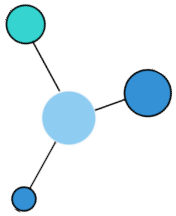
Coinage & Shuffle

There is no longer any notion of latency of rewards. Nodes will only be rewarded as long as they are connected and competing for blocks. We also took a further step in shuffling coin stake addresses to prevent staking rewards from being skewed in favour of larger addresses. This has shown itself to be effective in operation in smoothing out the distribution of rewards among addresses.

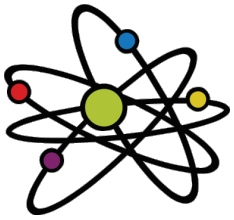
If a wallet has ioc it can begin to stake immediately and receive rewards and only be able to receive rewards while the wallet is actively running and staking. The rewards are fixed at 1.5 IOC per block plus any fees resulting from transactions including DIONS transaction fees. Rewards and fees are due to retarget in future upgrades to code in intervals per governance consensus. (As of the time of writing DIONS fees are 0.01 IOC plus 0.01 IOC for each kilobyte of data.)

Channel & Atomic Keys

A channel is initiated by means of associating two endpoints with a symmetric encryption key. Channels are central to the data storage and communications infrastructure.
The establishment of a two way channel involves "inviting" another alias target, which if accepted, establishes the necessary key exchange allowing encrypted communication as well as encrypted data transfer. All encryption private keys are stored in the wallet.dat. In Q1-Q2 a parallel API option will be created in order to allow backup and management of secret keys in a separate storage location.



Channel Keys



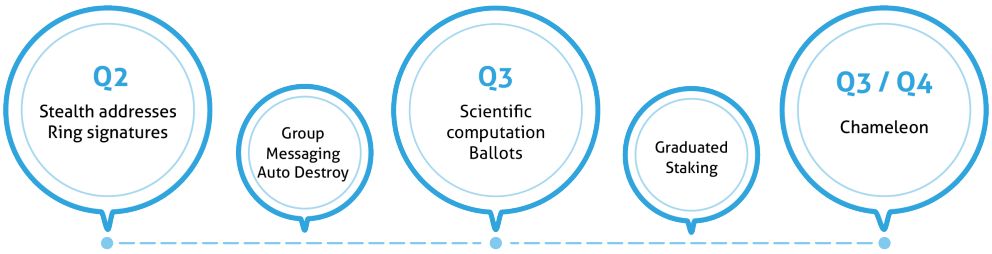
Atomic Keys

BIP65

Prior to our November 2017 release we took the step of implementing bip65. The purpose of this is to allow transaction outputs to be checked against a lock threshold which may be either a block height or block time. This enables the corresponding outputs to be locked until the specified time threshold is reached.

DIONS V.2

Stealth addresses



In the second quarter stealth addresses will be added to the system. Stealth addresses are a convenient method of protecting the privacy of data and ioc receivers. For example, medical records could be uploaded and transfered without trace or a vendor may put his address for payment on a website or some other public site, but this may be an issue for the vendor with money payments to that address being on display for anyone to see. Stealth addresses protect privacy in this sense. It works by getting the payment sender to generate a one time address based on a single public Stealth address.

For a given stealth address say (P, Q) a one-time address can be generated using essentially a large random number r to produce the product r.G = R. The fact that r.P = r.p.G = p.R is the reason why the sender can generate the one time address and the receiver can independently check whether the address is his without any third party being able to feasibly have knowledge of the resulting one time address. The addition of the component public Q results in only the receiver being able to spend any funds sent to the address. In this way we term P the stealth address inner component and Q the outer component of the stealth public address (P, Q).

Ring signatures

Ring signatures (first introduced by Rivest, Shamir & Tauman in 2001 [1]) are planned for Q2 in conjunction with stealth addresses allowing for any collection of public keys a signature to be created such that it is not feasible to determine which key was used in the construction of the signature. A restriction on the practical use of ring signatures is the way that the ring signature grows in size in many algorithms essentially linearly with the number of keys. However recent algorithms have been proposed which involve sub-linear and also constant size growth.

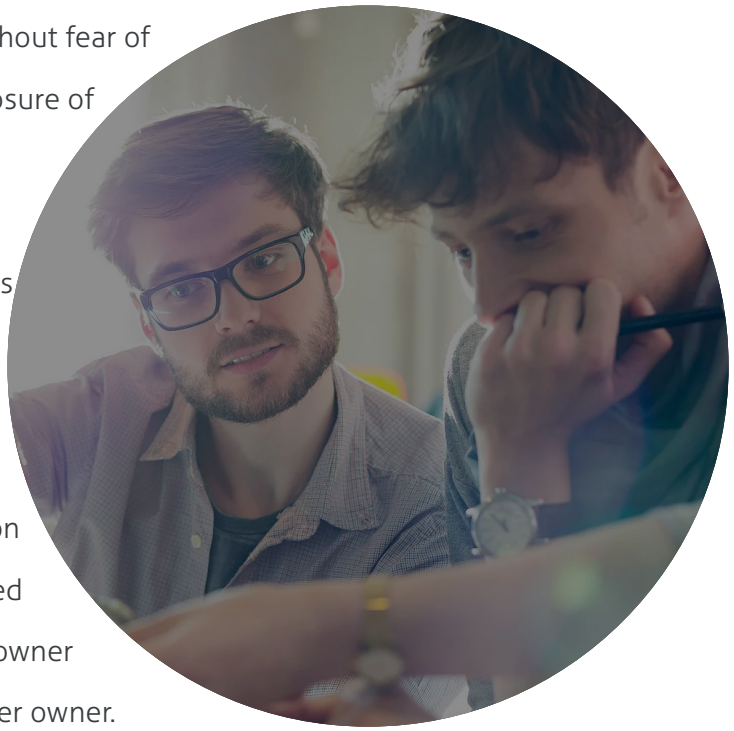
Ring signatures can be viewed as the complement to stealth addresses in that a user may sign a transaction and any observer will not be able to feasibly determine who from the ring signed the transaction. Thus the system will move towards providing a powerful resource for complete ioc and document transfer anonymity.

Ballots

With our secure channel mechanism comes the possibility for secret voting. Ballots may be called by anyone with regard to anything at all from potential new projects and directions in the peer to peer network to matters relating to private groups. A vote may be called by establishing what we term a Ballot box alias. Which may be functionally an alias or designated group.

Group encrypted message channels & auto destroy

The current system provides encrypted peer to peer communications. The next important step in this direction is the extension to groups of members. Recent events concerning some well known encrypted group message platforms have proven yet again that it is essential that more and better alternatives are created to provide a means for people to discuss political or technological views for example without fear of clamp downs, repression or unauthorized disclosure of the messages to state governments or regimes.



The extension to encrypted discussion groups, is a natural and logical progression of our already fully operational peer to peer encrypted messaging. The implementation will involve a natural generalisation of our channel negotiation by means of the invite procedure to a designated alias. As is natural with groups there will be an owner and this owner may transfer the group to another owner.

As members are accepted, multiple sessions are established with a single symmetric key giving group members access to all messages in the group in sequence.

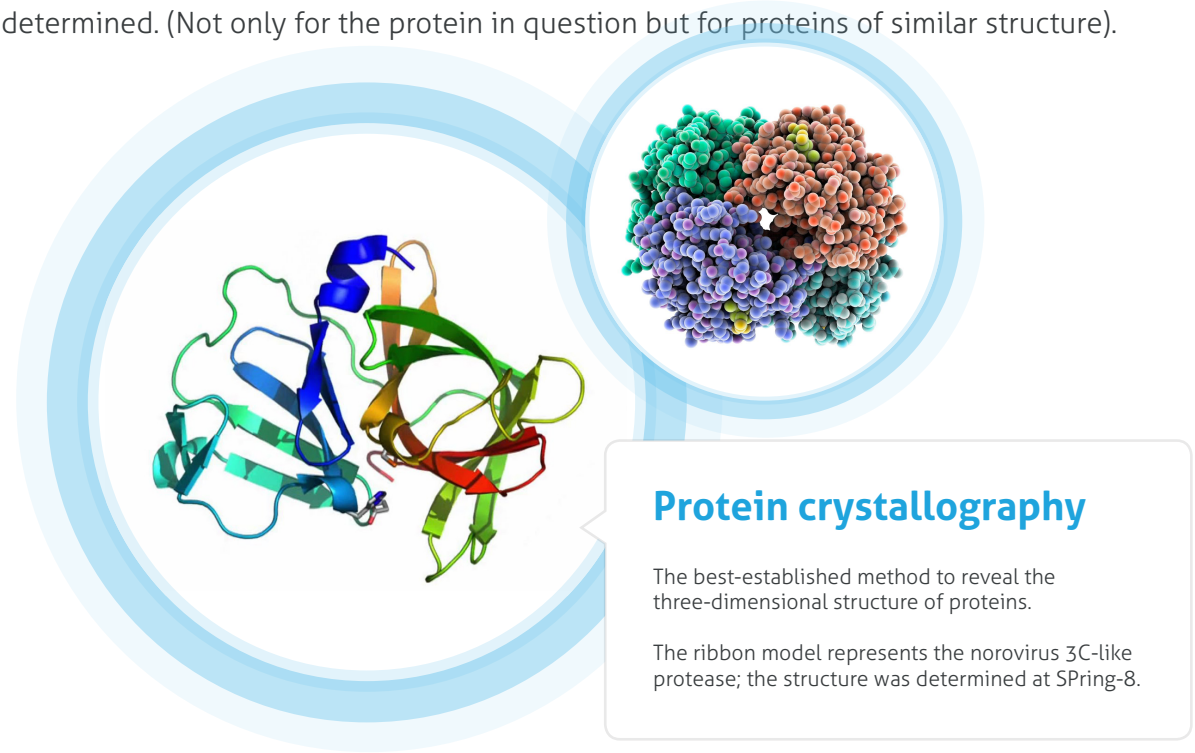
The extension of the present AES 256 bit message system of IOCoin will provide such a safe means for group discussion that is completely decentralized. In addition we will be adding phase modulated decryption for one time message view.

Scientific computation

One area of interest that we are currently investigating is that of helping to improve understanding of cancer development and possible treatments, by using spare computational cycles from IOC staking nodes. Of particular interest are proteins that have marked distribution changes or mutations in cancers.

Studying these structures involves X-Ray crystallography. The proteins must first be crystallized. This is a very complex procedure involving many different parameters and combinations. The type of solution, acidity level, temperature, hydrophobicity, isoelectric point, etc thousands of possible conditions.

Further, different proteins have different parameter sets. By analysing the resulting data sets from millions of crystallization experiments effective methods of crystallization can be determined. (Not only for the protein in question but for proteins of similar structure).



Protein crystallography

The best-established method to reveal the three-dimensional structure of proteins.

The ribbon model represents the norovirus 3C-like protease; the structure was determined at SPring-8.

Graduated staking

Along with the desire to promote network security comes the need to recognize nodes with consistent high levels of long term staking commitment. By means of enhanced rewards directed at the behavioural characteristics of such peers we strongly encourage other peers to aspire to follow suit, in turn to the benefit of all of the network.

The enhanced benefits for strong staking will involve graduation which will involve a policy of enhancing alias and communication related fees accrued on the network to reward these Sentinel nodes. Potential rewards will involve block voting rights awarded again in a graduated manner. As described above Ballots are already a feature we have. We anticipate certain types of ballot reserved by consensus which may be more appropriate for the domain of public and general elections.

It is clearly advantageous and to the benefit of the entire network to have a graduated staking reward policy. This is currently under test and will be introduced and fully documented in Q3 or Q4.

Gettxout

Gettxout is currently being implemented in the code, expected in Q1. Gettxout returns information on a given output including the blockhash, number of confirmations and value. The completion of the gettxout addition will then enable IOC to be listed on an exchange utilizing decentralized exchange mechanisms.

CHAMELEON

We have been researching and prototyping a mechanism allowing heterogenous networks of entities with different protocols and API specifications allowing them to transparently interoperate without the need for central provisioning. What we termed a connection patch was developed allowing transaction information to be published directly between different peer to peer networks that were integrated using a minimal API.

In practice we tested with two different networks, together with the connection patch. Transactions were published to an address in the connection patch and matches from the other network result in funds being exchanged with the connection patch. As a result, services were available for each user in the other's network. Again, the test took place for two heterogeneous peer to peer networks but by using the network adapter API more networks could be added.

We investigated the potential for further services within the connection patch itself such as being able to handle more data oriented networks which would provide an effective demonstration of service specialisation and interoperability as well as policy voting within the connection layer itself.

The first results of this led us to investigate refining and extending what began as a proof of concept. The result grew into the Chameleon project. This is currently under development and planned for initial release later this year.

How to use these features

We created a fully functional HTML5 electron based wallet system that incorporates all features described in the earlier sections in a transparent and easy to use way.

All features - ranging from, alias creation and decryption - encrypted file upload as payload and encrypted file content decrypt / download - secure channel negotiation via a single Invite - Accept button sequence - secure file transfer - secure instant message communication. All of this is made transparent in the easy to use HTML5 graphical interface.

Thus our graphical layer may be regarded as a canonical implementation of an interface to the full spectrum of features that we now provide via our API. Businesses, governments and institutions can use the I/O Digital API to build custom interfaces to fit their own domains, their own use cases and with their own preferred look and feel.

Through the daemon all the features described in the foregoing sections are accessible unless explicitly stated.

References

[1] "How to leak a secret", Rivest, Shamir, Tauman, ASIACRYPT 2001. Volume 2248 of Lecture Notes in Computer Science, pages 552–565.

https://link.springer.com/chapter/10.1007%2F3-540-45682-1_32

Author: *Derek Hatton, Joel Bosh*

January 09, 2018

Document revision 1.0

I/O DIGITAL Foundation

www.iocoin.io / www.iodigital.io

Latest Github developments

https://github.com/IOCoin/DIONS/releases

IOCOIN.IO / IODIGITAL.IO