IOC

Ethereum Smart Contract Compatible Blockchain Ecosystem

IOCoin -Ticker: IOC

Whitepaper

v.2022

SCAN ME

I/O COIN

I/O DIGITAL Foundation

IOCOIN.IO / IODIGITAL.IO

CHAMELEON

IOC Specifications

EST 2014

Symbol: IOC

Coin Algorithm: POS Cipher

Encryption For All Services: AES 256

Block Confirmations: From 60 to 16 Seconds

4MB Block Capacity

POS Reward 1.5 IOC per block

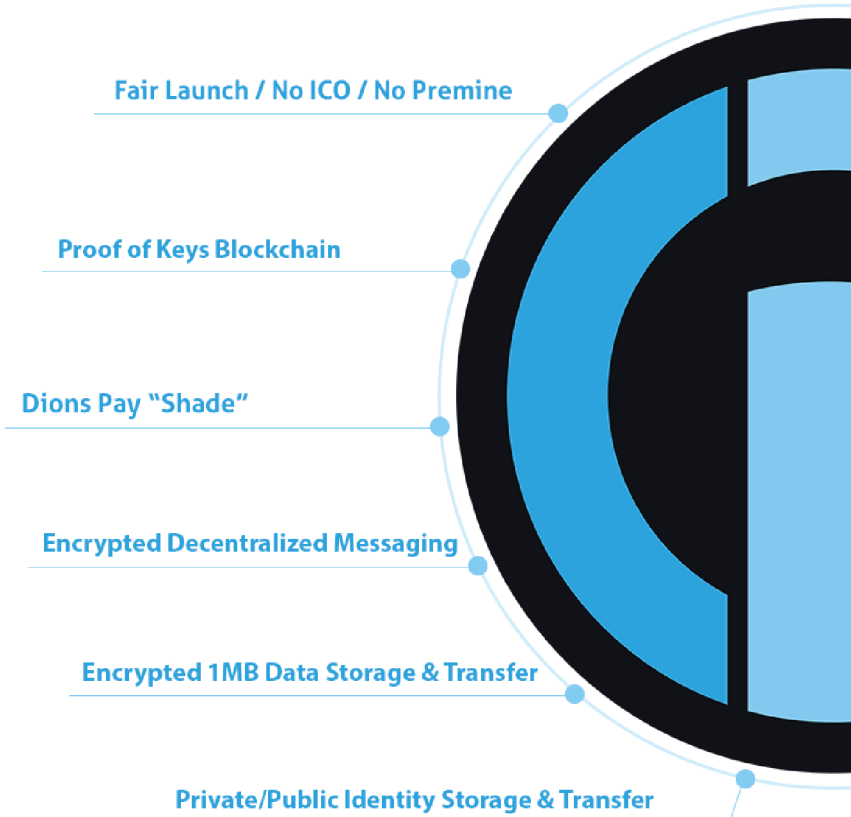
Fee for Services: Weighted from .01 iOC

All fees are distributed back to Stakers

No governance Model

19M IOC in Circulation

On Chain Services accessible via API for DAPPS



GitHub IOCoin/DIONS

2016 FINTECH100

Leading Global Fintech Innovators

H2 VENTURES KPMG

FINTECH AWARDS benzinga FINALIST NYC 2016

EUROPEAN FinTech 100 100.FINTECH.NL | 2016

TokenInsight

Project Rating Report

I/O Coin

B Stable Outlook

Analyst | Pei Zhou

Feb 2019

Table of Contents

Mission Statement

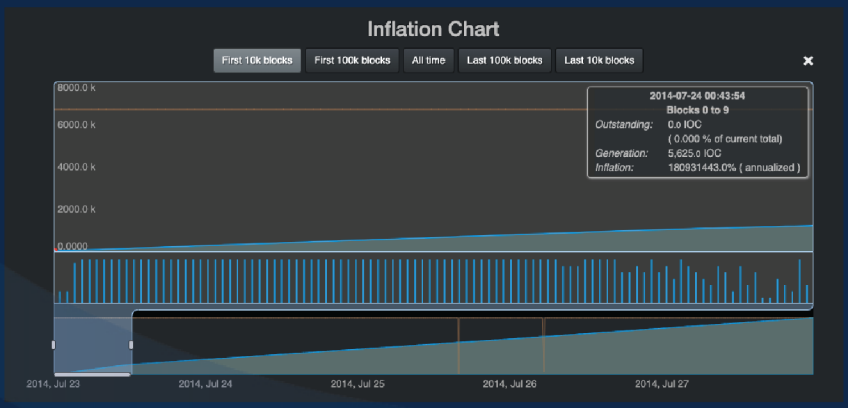
Our ultimate goal is to provide a secure, fast and user friendly Blockchain Ecosystem in order to advance adoption of decentralized services around the world

Introduction

Since the rise of the Bitcoin network in 2009, countless developers have embarked on creating competing peer-to-peer digital currencies/assets. Many of these were rebranded copies of Bitcoin with no 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 for power to mine new coins was one problem some wished to solve. In April 2013, the estimated Bitcoin mining power consumption cost worldwide was $150,000 per day.

In January 2018, the Bitcoin mining power consumption cost worldwide was estimated at around $5,287,349 per day. Looking to improve the problem of excessive power consumption due to Bitcoin consensus algorithm; Scott Nadal and Sunny King in 2012 released the whitepaper, "PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake". This paper led to Peercoin development and resulted in a coin that used roughly 30% of the power consumption used by Bitcoin and introduced several other improvements such as the reduced risk of a monopoly held by mining pools and the possibility of a 51% attack. Following this and other enhancements within the blockchain technology, The I/O Coin team, led by its founder Joel Bosh (lead developer), devised a unique approach and developed POS V2. In POS V2, among other things, "coinage" was removed to promote early incentivisation to stakers joining the network. The I/O Coin genesis block was mined via POW X11 on July 24, 2014.

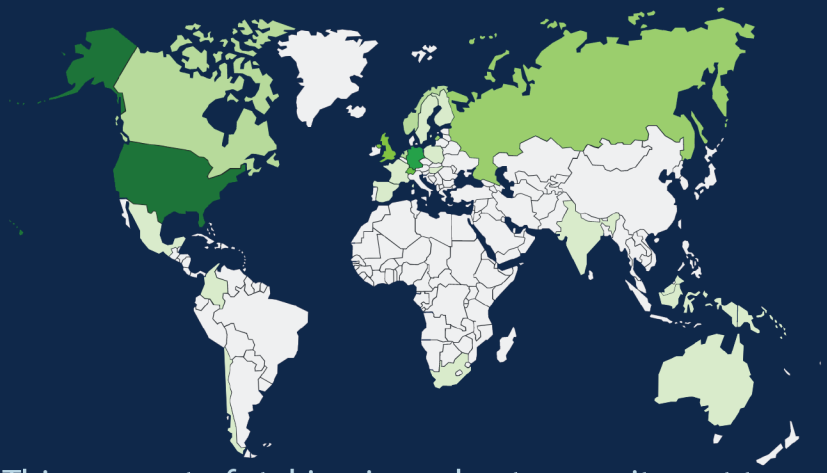


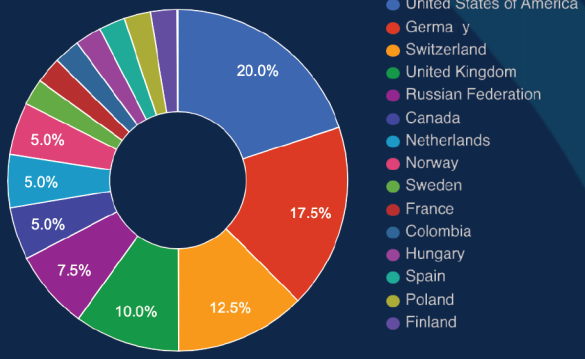
The IOCoin development team launched IOCoin (IOC) without any Initial Coin Ofering (ICO) or pre-mine. IOC was fair launched via POW mining. To ensure fair and balanced distribution. The team added to its source code a sophisticated cryptographic hash in Proof of Work (POW) X11 algorithm before switching to Proof of Stake (PoS I/O).

The IOCoin team has since then added further improvements/user-friendly features to its blockchain with a focus on security, privacy, 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 43 thousand hours of POS computation. At no time the IOC blockchain has ever been close to a 51% attack. The IOC community has maintained over 20% staking since it's genesis block.





This amount of staking 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 worldwide. In 2016, IOC won the "Blockchain" category in the European Fintech Awards, a Benzinga Fintech award and was a finalist in the same year for the European Fintech Awards. The I/O Coin development team's goal is to secure, game-changing, user-friendly blockchain frameworks. The team's passion and determination drive us to focus on our goals.
We have always put development priority first. For that reason, the team formerly formed a non for profit foundation to further educate on the use of the I/O Coin public blockchain. To push awareness to companies and individuals to adopt the I/O Coin blockchain's application-based services. In the same year, community members formed a non-profit foundation named the I/O Digital Foundation.

Problem Statement

In 2014 IOC minted 16 million coins during a two week pow x11 mining period to fairly distribute and switch its security to proof of stake. An early switch from Proof Of Work to Proof of Stake was essential for the long term viability of a POS blockchain complete, healthy node sync, and ensuring that the network was less node dense, further avoiding unnecessary chain splits. In late 2017, the dev team deployed DIONS. A constant 1.5 IOC reward per block to maintain stakers incentivized in perpetuity. It was imperative to incentivize network security further and as a continuous inflation control mechanism, and a constant reward solves issues relating to human-induced coin losses.

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. It allows for 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 all redistributed to all active stakers in the network. All IOC fee rewards enhance IOC distribution by incentivizing users to stake while further securing the network. Along with staking and security enhancements to its core platform, advances on encrypted data, messaging and aliases to the Blockchain. With all of these live features alongside our decentralized GPG-like system, DIONS proved to be successful in combining these three major components for an open, user-friendly and advanced Blockchain platform.

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 IOCoin POS chain, codenamed Chameleon. The sidechain will further decentralize and enhance POS shortcomings via an entropy-based graph ledger. Chameleon is slated for release in early 2023.

In 2021, the IOC Dev team proposed a new project codename, "DVM" (DIONS Virtua Machine), to launch Chameleon and enhance further adoption. The DVM will enable Ethereum compatible smart contracts via solidity and fixes to gas fees and network delays while also opening the door to further its interoperability between IOC, Ethereum and Bitcoin.

coindesk®

"The proposal represents one of the latest efforts to build on existing PoS models, as well as make the technology more resistant to network threats. Past events, including the hard fork of the Vericoin network, have raised concerns that proof-of-stake systems are too risky for broader adoption. The new I/O proof-of-stake system is set to go live on September 26th, 2014 beginning with the 100,000th network block."

IOC - DIONS (Decentralized DNS)

The alias key-value pairs provide a means of indirection concerning the naming of IP network nodes. DIONS may be the basis for a blockchain-based DNS like name resolution service. DIONS are also aliases and provide human-readable names uniquely ascribed to an ordinary IOCoin public hex address. DIONS provide a means of mapping names to resources on the internet or private networks, which can be resolved directly from the blockchain.

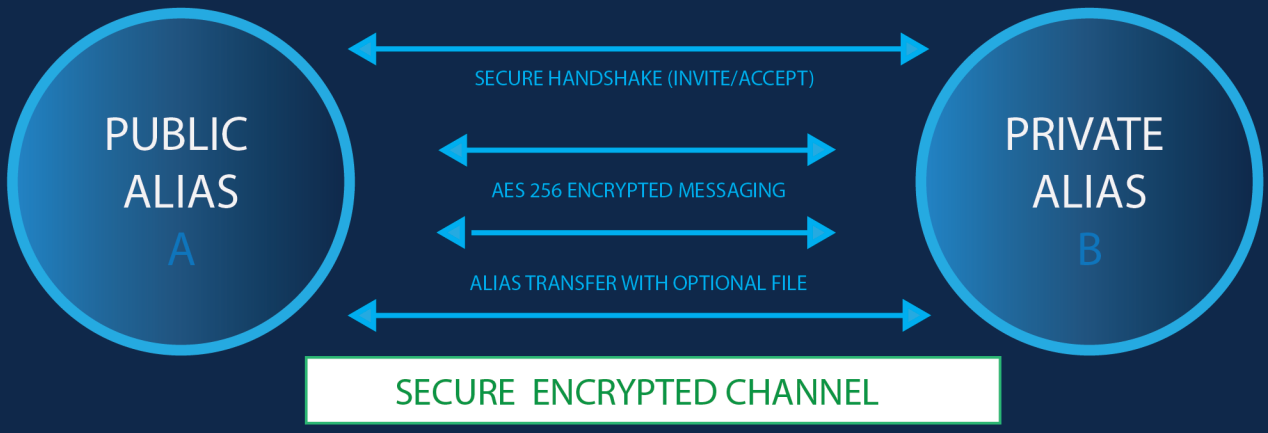
Aliases Private & Public

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 255characters. At any given time, an alias is identified with one unique IOC address. Private aliases are for private use. Once created, the resulting key-value pair will be encrypted, private and nonviewable on the blockchain. This allows mitigating alias squatting. A private alias stays private within the user's registration and cannot receive IOC while encrypted. Users can only use private DIONS for file storage & secure file transfer. Once created, a user can paira particular file or transfer the alias to another user in the application blockchain. In IOC, data transfer is achieved by constructing an encrypted channel over which the private alias is encrypted for the recipient and 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 as keys are said to lapse after a so-called 250K blocks expiry, where no updates occur.

Private Alias	Upload 1MB Encrypted File	Transfer Alias or file ownership	X
Public Alias	X	X	Send & Receive IOCoin

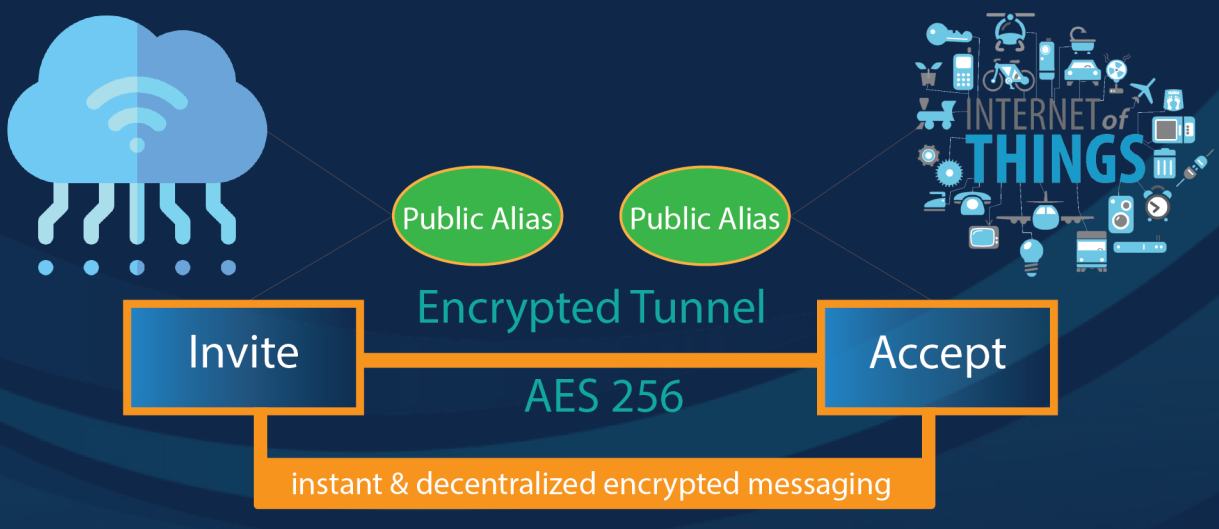
Aliases Private Transfer

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

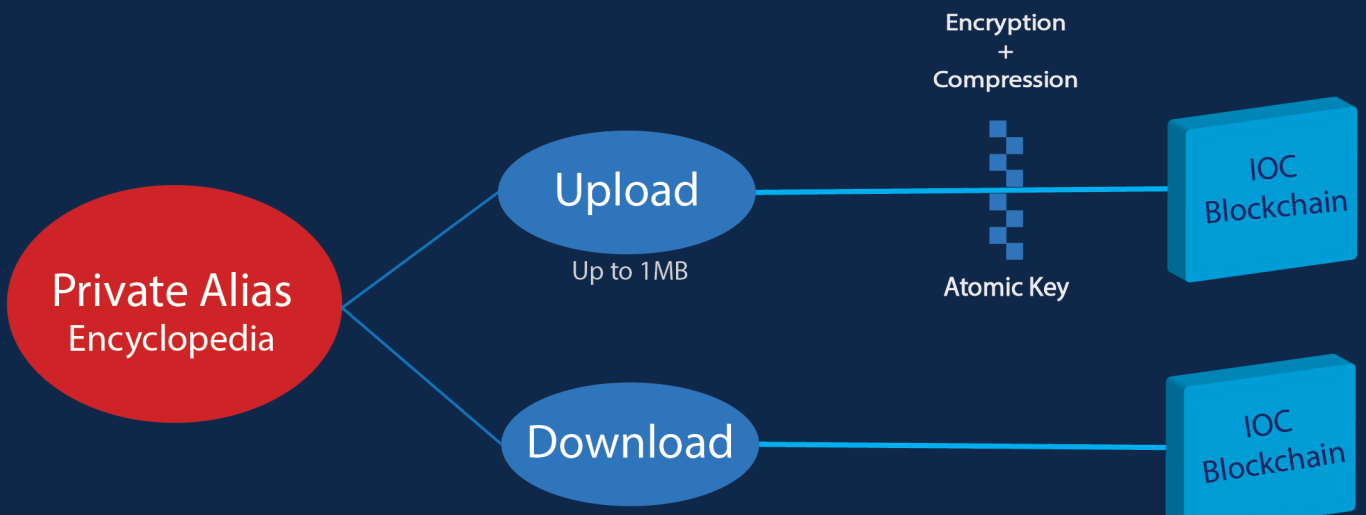
Peer to Peer encrypted messages can be sent and received after an encrypted channel is established between public aliases. Similar to the negotiation of, for example, an ssh session, the channel is first negotiated using RSA encryption thereafter; all payload encryption is by means of the established symmetric key, which is more efficient. Following asymmetric key exchange over RSA, users can converse instantly over encrypted communication channels. Confirmations are not needed for the message to be transferred, making them instant. The message encryption relies on AES 256 bit keys, one per channel, along with a per-message 128-bit initialization vector.



Encrypted Data Storage

With DIONS there is the option to store encrypted content. The content is base64 encoded, and the underlying data may be, for example of the form ASCII, PDF, JPEG, PNG, MP3 or any binary data.

With each DION alias, there is an option to upload a data value that is currently restricted to 1 MB. Once a user has uploaded an encrypted file, he may 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. Thus encryption of data may be private whether or not it is over a channel or shared the encryption used for transfer.




```
[
    {
        "alias" : "encyclopedia/mathematics/algebraic geometry/algebraic variety",
        "encrypted" : "false",
        "value" : "An algebraic variety is a reduced <<scheme>> of finite type over a <<field>> K",
        "address" : "muUDC2D7sJaYoJXFQ9sXfhX6dAH3XRTn9x",
        "nHeigt" : 264
    },
        "address" : "mn1BPyW5rMHZ1pfczPoeCFh8coA5nfpbxA",
        "nHeigt" : 256
    },
    {
        "alias" : "encyclopedia/mathematics/field theory/field",
        "encrypted" : "false",
        "value" : "A field is any set of elements that satisfies the <<field axioms>> for both addition and multiplicatio
n and is a <<commutative>> <<division algebra>>.",
        "address" : "mkQj4q41ka9vm9sMcebeeg9nBauiA5hbPc",
        "nHeigt" : 267
    },
    {
        "alias" : "encyclopedia/mathematics/field theory/scheme",
        "encrypted" : "false",
        "value" : "Scheme - A <<local-ringed>> space which is locally <<isomorphic>> to an <<affine>> scheme.",
        "address" : "moh4CsGgVC5wxBswMVW5LTeyFJceLBMxnQ",
        "nHeigt" : 268
    }
]
argosy:>
argosy:>
```

Encrypted Group 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 clampdowns, 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 naturally generalize our channel negotiation using the invite procedure already discussed 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 all messages in the group in sequence.

The extension of the present AES 256 bit message system of I/O Coin will provide a safe means for entirely decentralized group discussion. In addition, we will be adding phase-modulated decryption for a one-time message view.

POS CiPher

Proof of stake cipher is the process for securing the blockchain. The staking mechanism was also reviewed, along with the recent implementation and launch of the preceding sections. Since November 2017, coinage was completely removed from the staking model. The new model ensures to reward early stakers for keeping nodes running, therefor maximizing staking rewards. Also, block confirmation times speed up based on transaction count.

Coinage & Shuffle

There is no longer any notion of latency of rewards. Nodes will only be rewarded if they are connected and compete for blocks. We also took a further step in shuffling coin stake addresses to prevent the issue of seeing significant wallet stake rewards mostly going to a single address. 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 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 retargeting 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 associating two endpoints with an asymmetric 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 to allow backup and management of secret keys in a separate storage location.

Atomic Keys

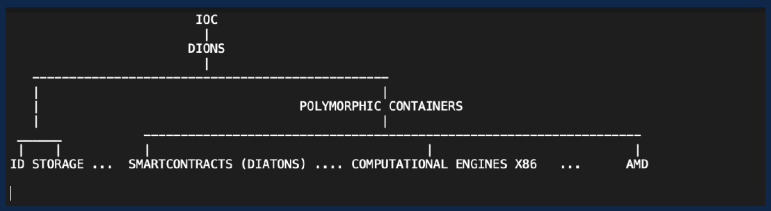
Channel Keys

Bip 165

Before 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, and this enables the corresponding outputs to be locked until the specified time threshold is reached.

DVM (Ethereum Compatible) Smart Contract Platform

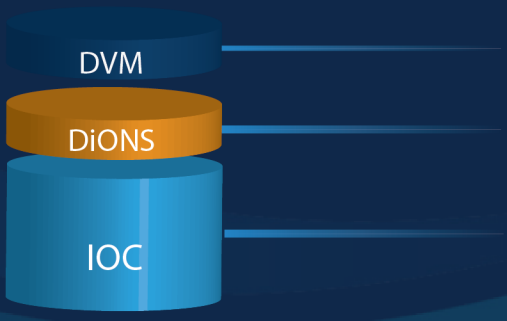
Proof of Stake Since 2014



The IOC Dev Team is currently working on an ambitious proposal to enable a virtual machine fully integrated into its DIONS layer. Specifically taking use of its "Dions payload" to deploy a fully compatible Ethereum Smart Contract platform. Code name "DVM" for Dions Virtual Machine. The Dvm will process all of the Bytecode for example;

cycle — create — call functions

In essence, as development moves along "ide tools" will be added so that the Dvm will be able to handle solidity compiles within the "Dions" ecosystem. This approach will provide the IOC Blockchain with the same user appearance as the smart contracts in Ethereum, but the mechanism under the Dvm hood will be the IOC's Dev team own unique code work. Once fully deployed it will be fully compatible with all current Ethereum dapps. Current Ethereum developers will be able to take advantage of the DVM to be able to launch ERC20 tokens. The launch of DVM will come with many upgrades to the core IOC Blockchain including Cold Sig (Offline Signatures) Orphan Pruning tool, Graduated Staking, Gas fees and block confirmation.



DiONS Virtual Machine | ETH SMC Compatible

Decentralized Input Output Name Server

Core Blockchain

Graduated staking

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

The enhanced benefits for strong staking will involve gradation, including 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 ballots reserved by consensus, which may be more appropriate for the domain of public and general elections.

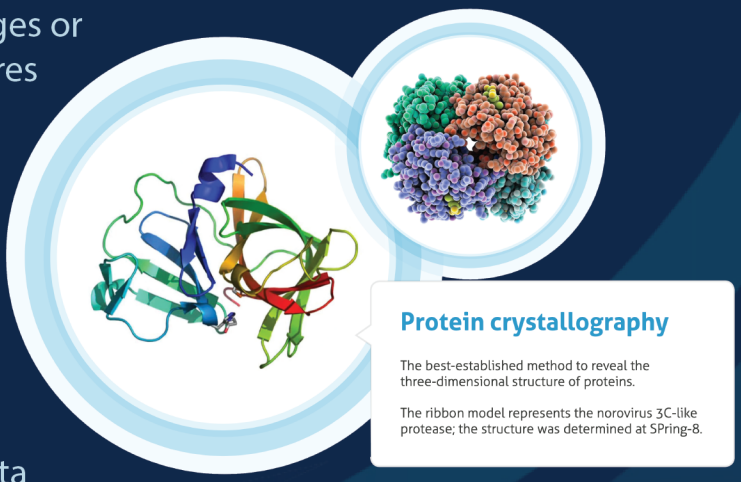
It is advantageous and to the benefit of the entire network to have a graduated staking reward policy.

Gettxout & Checklocktimeverify

Gettxout and Checklocktimeverify have been implemented in the code. Both return information on a given output, including the block hash, number of confirmations and value. This addition enabled IOC to be ready for any decentralized exchange mechanisms.

Scientific computation

One area of interest that we are currently investigating is helping to improve understanding of cancer development and possible treatments. 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, and 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 analyzing 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.

CHAMELEON

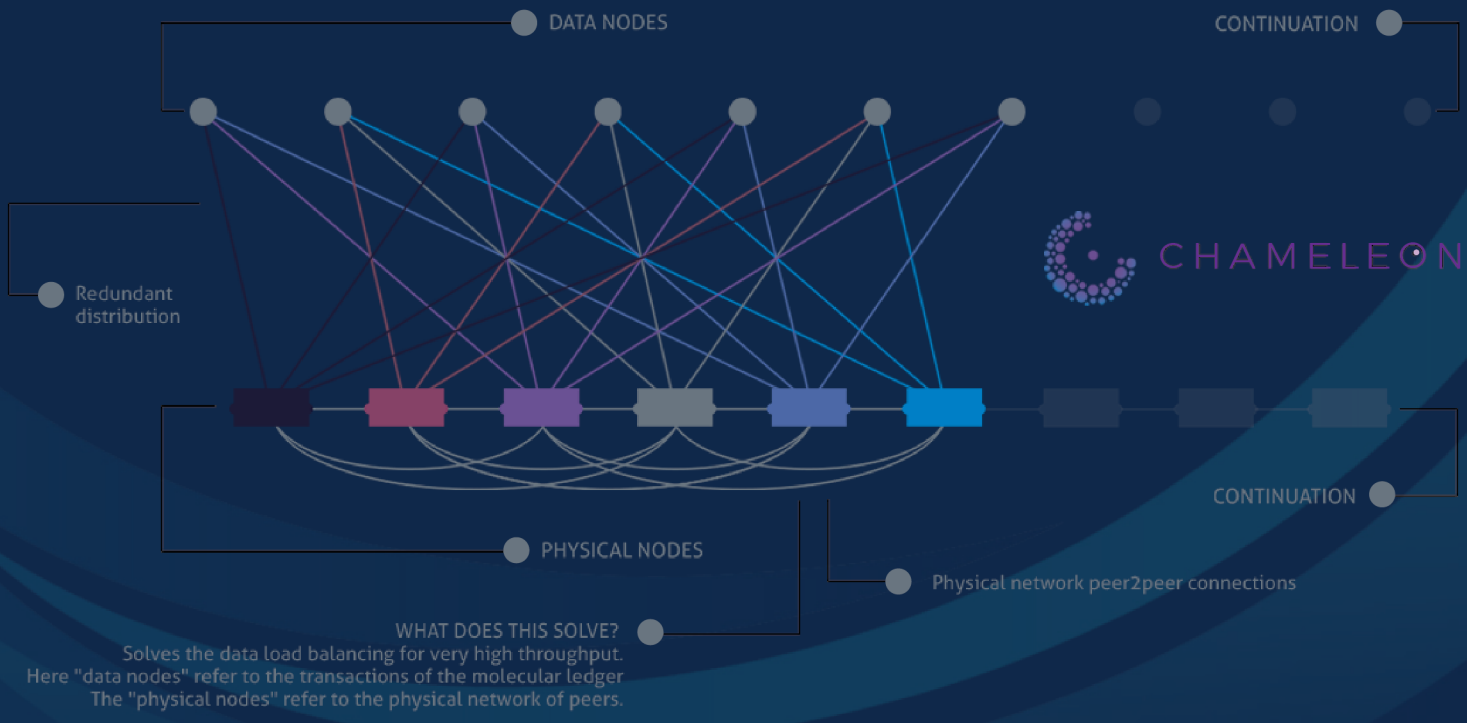
Research and prototyping of a mechanism allowing heterogeneous networks of entities with different protocols and API specifications, allowing them to interoperate transparently without the need for central provisioning. What we termed a connection patch was developed allowing transaction information 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 resulted 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 more networks could be added by using the network adapter API.

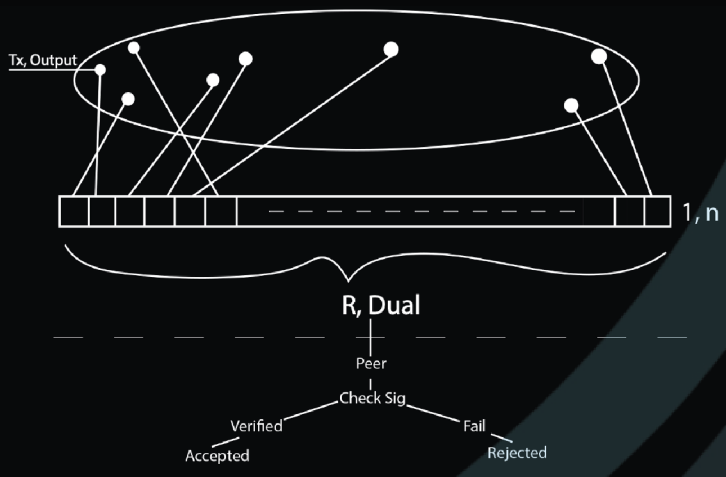
We investigated the potential for further services within the connection patch itself, such as being able to handle more data-oriented networks for example, which would provide a effective demonstration of service specialisation and interoperability as well as policy voting within the connection layer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

The first results of this led us to investigate refining and extending what began as a proof of concept, and the result grew into the Chameleon project. We will launch aside, entropy-based molecular graph ledger to scale, increase transactions per second, and deploy Non-Turing complete abstract smart contracts.

Chameleon is planned for initial release in 2022.



Nighthawk Zero-Knowledge Stealth addresses will be added to a stand-alone sister chain to IOC. Ring signatures (first introduced by Rivest, Shamir & Tauman in 2001 [1]) are planned for 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 linearly with the number of keys.
However, recent algorithms have been proposed that involve sub-linear and 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 determine who from the ring signed the transaction feasibly. Thus the system will provide a powerful resource for complete document transfer anonymity.



For a given stealth address, say (P, Q) a a one-time address can be generated using a 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 know the resulting one time address feasibly.

The addition of the component public Q results in only the receiver spending 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).

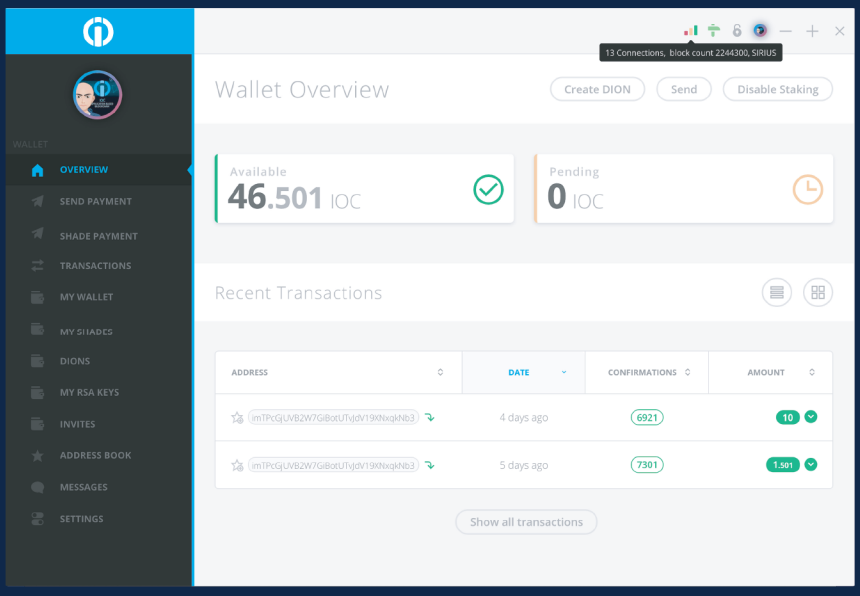
How to use these features

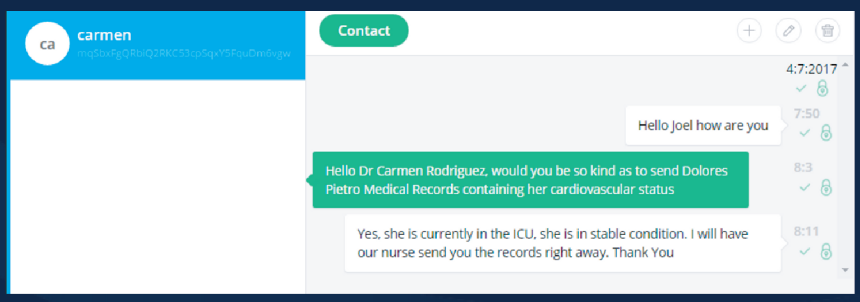
We created a fully functional HTML5 electron-based wallet system that incorporates all features described in the earlier sections in a transparent and easy to use way.

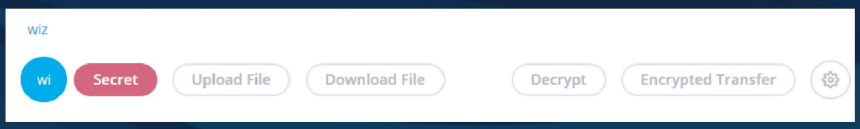
All features - ranging from alias creation and decryption - encrypted file upload as payload and encrypted file content decrypt / download - secure channel negotiation via a single Invite - Accept button sequence - secure file transfer - secure instant message communication. All of this made transparent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

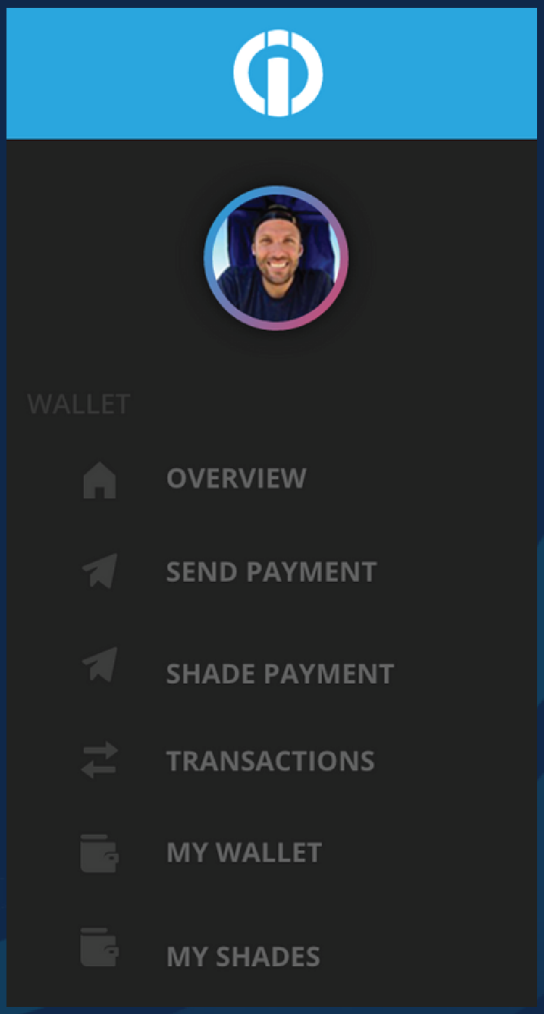
Thus our graphical layer may be regarded as a canonical implementation of an interface to the full spectrum of features that we right now provide via our API. Businesses or institutes can use the I/O Coin Blockchain API to build custom interfaces to fit their domains, use cases, and preferred look and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

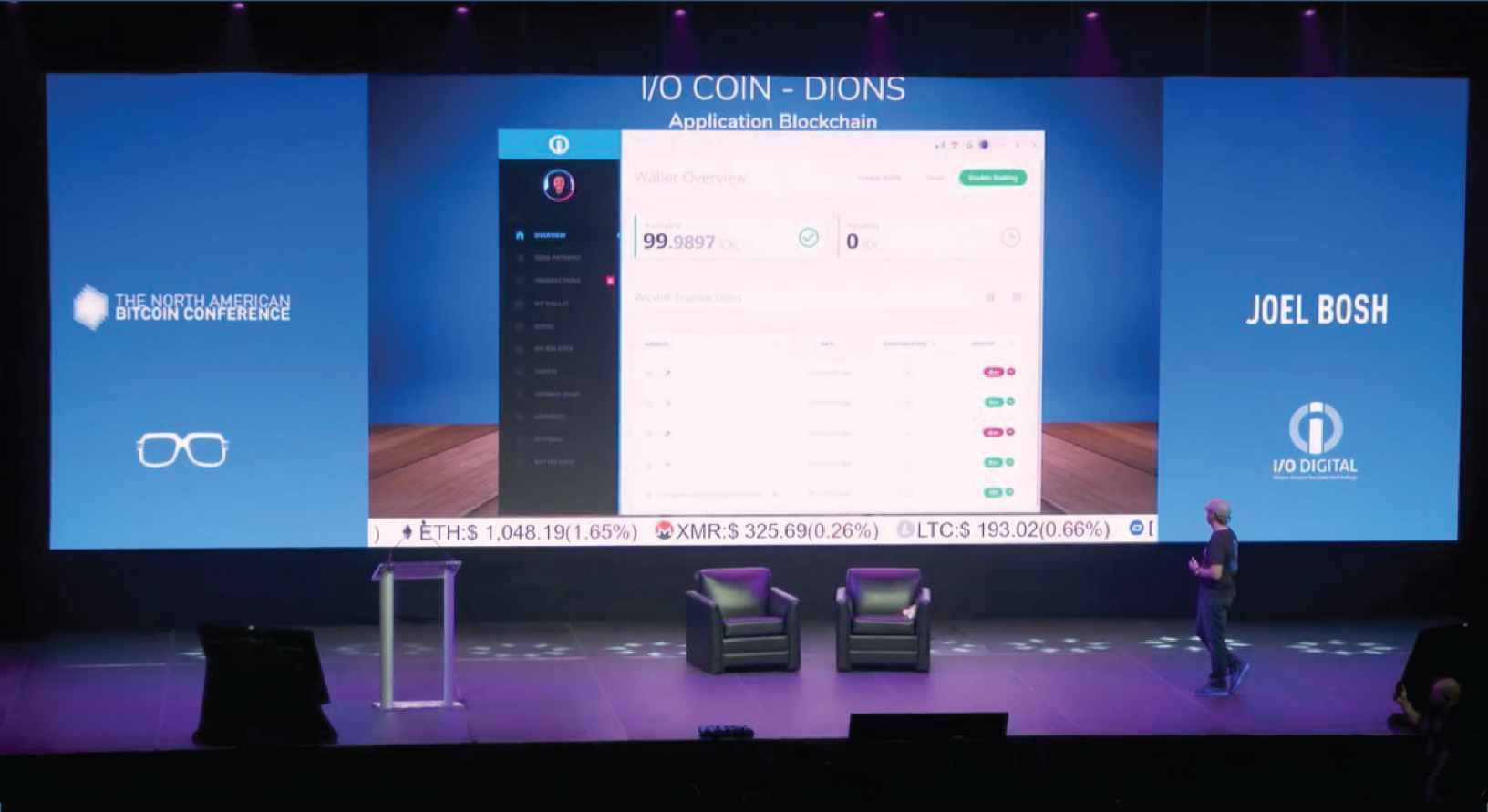
Through the daemon, all the features described in the preceding sections are accessible unless explicitly stated.











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
Sep 15, 2021
Document revision 4.0

I/O DIGITAL Foundation & IOCoin Community
www.iocoin.io / www.iodigital.io

IOCoin WiKi
https://i-o-digital-foundation.gitbook.io/ioc/

Latest Github developments
https://github.com/IOCoin/DIONS