IOV: a Blockchain Communication System

December 2017 - February 2018

Antoine Herzog[a], **Serge Karim Ganem**[b], **Isabella Dell**[c], **and Florin Dzeladini**[d]

[a]antoine@iov.one; [b]karim@iov.one; [c]isabella@iov.one; [d]florin@iov.one

Abstract

A Blockchain Communication System would allow users to store and exchange multiple types of values without the need to download an electronic wallet each time a new blockchain is being created.

The decentralization of blockchains has created a diversified ecosystem of autonomous blockchains, with each system requiring different protocols to access coins and values. The lack of standardization makes it very difficult for a typical electronic wallet to send a transaction or to query several different blockchains.

We propose a solution to empower the end-user and remove the need to download multiple wallets, by providing a system that includes:

1. Blockchain Communication Protocol: a set of standards that each participating blockchain implements.

2. IOV Wallet: an application to interact with an unlimited number of token's blockchain state.

3. Blockchain Name Service: a special blockchain that tracks each participating token to enable the interaction with the IOV Wallet.

In 2009, Bitcoin created the first decentralized digital currency, introducing a new way to exchange a value token between two Internet users. The problem of "double spending" (1) was solved, without the need for a third-party bank or financial institution.

In 2015, Ethereum created an alternative protocol for building decentralized applications (dapps) via scripted transactions and autonomous transactional agents. Ethereum has utilized the technology underlying blockchains to create what are now called "smart contracts" (2), which have become a way to facilitate, verify, or enforce the negotiation or performance of a contract.

In 2016, Cosmos created the first network of distributed ledgers. Cosmos became the first player working to eliminate the dependence on exchanges and create a decentralized network that allows the free flow of digital currencies. (3).

Over the past year, interest in blockchain technology and its underlying usability has been rapidly increasing. The blockchain industry has reached a tipping point where thousands of blockchains will be issued. The majority of them will be decentralized and independently operated.

There are two main options for building a system that is able to track millions of different tokens; the creation of one global blockchain where transactions of all the tokens are stored; or the creation of one blockchain per token.

Ethereum approach and the ERC20 Token

In November 2015, Ethereum published the initial specification to store and exchange many different tokens on the Ethereum blockchain. It provided dapps and wallets to handle tokens across multiple interfaces/dapps. This specification also allowed projects to be funded via ICOs (Initial Coin Offerings).

Current limitations. Unfortunately, this specification only exists for use with the Ethereum blockchain. Additionally, the Ethereum blockchain is about 160GB. While the size is manageable, the blockchain contains deprecated tokens or tokens attached to projects that have been abandoned.. This phenomenon has become commonplace because most tokens have a limited lifespan due to human factors. The case is similar with shares of a company. A company's shares are created and their associated stock token is created, exchanged and at some point is no longer active when the company ceases to function.

The lifetime of most of the tokens issued on blockchains will be limited use and unique. Therefore, only tokens of active projects need to be tracked in order to be exchanged.

Bitcoin approach

Greater efficiency for each specific use case is created with one blockchain per token. As a result, the lifetime of the blockchain is associated with the

lifetime of its own token. When the token's purpose becomes invalid there is no need to maintain that specific blockchain.

Current limitations. This approach has several limitations as well. In 2017, many different blockchains exist to track value, such as Bitcoin, Litecoin, etc. However, each time a user wishes to use one, that user needs to create a wallet for that specific blockchain. This can be problematic if a user wants to own tokens related to many blockchains, as a result the user needs to create a seperate wallet for each token. Furthermore, it is challenging to deploy a new blockchain, and the consensus of a single blockchain can be more vulnerable than a global multi-assets blockchain.

Below, we propose a system that solves all these problems.

Description of the Blockchain Communication System

The goal of a Blockchain Communication System is to allow any value or asset to be stored, or exchanged from a unique electronic wallet.

The key elements of our system that will allow for the exchange of these values are:

- **Blockchain Communication Protocol**: a set of standards that each blockchain implements;
- **IOV Wallet**: an application to interact with an unlimited number of token's blockchain state;
- **Blockchain Name Service**: special blockchain to interact with the IOV Wallet.

All blockchains adhering to the Blockchain Communication Protocol will be directly compatible with the IOV Wallet. Anyone wishing to create their own token only needs to follow the Blockchain Communication Protocol.

A. Blockchain Communication Protocol. A BLOCKCHAIN TOKEN is a simple blockchain that implements the Blockchain Communication Protocol. Its only purpose is to track the transaction of its token. The blockchain could utilize proof of work, proof of stake, or proof of space and time. We began by defining the external properties (A.1 TO A.4), which will bring standardization among blockchains before defining the internal properties the blockchain should also fulfill (A.5 TO A.8).

A.1. Public Address of Value & Signature. We define an abstract format for the public address of value that needs to be implemented by all BLOCKCHAIN TOKENS. This standardization is necessary for the IOV Wallet to be able to send several transactions on different BLOCKCHAIN TOKENS from the same public address of value. A public address of value is composed of 2 parts:

- A delimited string which specifies the type of curve for the signature (Initially, we plan to support 2 types: ed25519 and secp256k1)
- A public address derived from the private key.

A.2. Standard API to query or submit a transaction. We define a standard API and associated routes to query or submit a transaction on any BLOCKCHAIN TOKEN.These mechanisms are necessary to allow external interaction with the system.

A.3. Hashed Timelock Contracts. This feature is needed for the IOV Wallet to exchange Coin A against Coin B easily without the need of a third-party exchange. As each BLOCKCHAIN TOKENS implements the same protocol for the public address of value, then it is trivial to provide Atomic cross-chain trading (4).

A.4. Token Definition. Each BLOCKCHAIN TOKEN should be able to keep up to date some important data on its ledger. This information is called TOKEN DEFINITION and it is required for the Blockchain Name Service to operate.

- Genesis file. The BLOCKCHAIN TOKEN should save the genesis file in the TOKEN DEFINITION. The genesis file is immutable and will never change once committed.
- Human name for the token. A human readable name for the BLOCKCHAIN TOKEN is a required definition. If a user wanted to register Bitcoin, this would be stored with the name Bitcoin, and include potential abbreviations, such as BTC or XBT.
- Unique identifier for the token. In order to differentiate BLOCKCHAIN TOKEN, each must

provide a unique identifier or prefix. This prefix may mirror the abbreviation for the token, for ease of identification. For example: BTC.

- Pictogram for the token. The pictogram for the BLOCKCHAIN TOKEN is a digital representation of the token's image. One example can be seen with Bitcoin here.

- Bootstrap nodes. The BLOCKCHAIN TOKEN should agree on which nodes are safe and secure to receive transactions and queries from outside. This list of bootstrap nodes must maintain high uptime or have the potential to be updated over time.

A.5. Blockchain Token consensus.

- Consensus made by the BLOCKCHAIN TOKEN itself. The consensus on a BLOCKCHAIN TOKEN could be proof of work, proof of stake, delegated proof of stake or proof of space and time.

- Shared Consensus provided by a third party consortium (Consensus as a service). The BLOCKCHAIN TOKEN could also choose a public consensus ready to run this specific BLOCKCHAIN TOKEN. In this case, the blockchain creator doesn't have to set up his own BLOCKCHAIN TOKEN nodes. As mentioned before, this is how Ethereum based tokens operate and must be used carefully.

A.6. Objectivity & Determinism. The BLOCKCHAIN TOKEN needs to be deterministic and to be objective, or at least weakly subjective. The Blockchain Name Service needs this feature to be able to keep in its ledger a valid copy of the TOKEN DEFINITION of the BLOCKCHAIN TOKEN.

A.7. Transaction. Transaction fees and inflation for validators should always be paid in the token value.

A.8. Intra Blockchain Token. Optionally, a BLOCKCHAIN TOKEN can also include some sort of intra tokens, not visible, and not tradable from the outside.

B. IOV Wallet.

B.1. Wallet feature. The IOV Wallet is similar to most cryptocurrency wallets with a few important differences. It can:

- Store: create a value address with a private key.
- Observe: Query multiple balances from multiple blockchain tokens.
- Transfer: send a transaction to any blockchain token.
- Exchange: Exchange tokens between blockchains.

C. Blockchain Name Service. The Blockchain Name Service is the backbone of the IOV Wallet. It is a special BLOCKCHAIN TOKEN (i.e. fulfilling the Blockchain Communication Protocol, see above). The main function of the Blockchain Name Service is to maintain a valid copy of each TOKEN DEFINITION and provide an accurate listing for all accepted definitions. The Blockchain Name Service is very similar to DNS, as it provides the ability to look up related blockchains and its hosts. We designed a simple process for anyone to copy a TOKEN DEFINITION on the Blockchain Name Service, based on the information available on its BLOCKCHAIN TOKEN.

C.1. IOV Token. The Blockchain Name Service has a native token called the IOV Token. The IOV token is the participation token of the Blockchain Name Service.

C.2. Consensus. The consensus of the Blockchain Name Service is a proof of stake. IOV Token is used as the staking token of the Blockchain Name Service.

C.3. Registration of a Token Definition on the Blockchain Name Service. Any user can register or update a TOKEN DEFINITION of a BLOCKCHAIN TOKEN on the Blockchain Name Service. This procedure needs to be done at least once a year. Otherwise the BLOCKCHAIN TOKEN is marked as inactive by the Blockchain Name Service. By requiring this update process, a user is able to discover if the BLOCKCHAIN TOKEN is active and maintained.

The Blockchain Name Service truly allows anybody to report a TOKEN DEFINITION on the Blockchain Name Service. A mechanism is therefore needed to prevent any malicious actors from

Fig. 1. Schematic representation of the Blockchain Communication System. 1. IOV Wallet requests to the Blockchain Name Service the list of active BLOCKCHAIN TOKEN. 2. Blockchain Name Service sends the list including the IP address of the bootstrap nodes for each BLOCKCHAIN TOKEN. 3. IOV Wallet sends a transaction or query to the BLOCKCHAIN TOKEN via a Bootstrap Node.

adding false information to the Blockchain Name Service. Below, we below such a mechanism.

I. Registration request. In order to update or register a TOKEN DEFINITION, the user needs to send a special transaction, which is called a Registration Request. This transaction includes the current TOKEN DEFINITION available on a BLOCKCHAIN TOKEN, a fee in IOV coin and escrow amount in IOV.For initial registrations, the Blockchain Name Service makes sure that the unique human identifier for the token is available, otherwise the transaction is rejected.

II. Challenge phase (7 days). During this phase, other users may challenge the request by sending another specific transaction, called a Registration Challenge. The transaction includes a fee in IOV Token and escrow amount in IOV and its correct version of the TOKEN DEFINITION.

III. Settlement phase (optional). If another user challenges the request, then the Blockchain Name Service will settle the case. A user called a moderator elected by the governance of the Blockchain Name Service will be in charge to rerun the actual state of the BLOCKCHAIN TOKEN. The moderator can determine without ambiguity the actual state of the token registry. If the request is legitimate, the challenger loses their escrow. If the request is not legitimate, the user who initiated the request loses their escrow instead. The escrow is then distributed among the moderators of the Blockchain Name Service.

IV. Registration phase. If no one challenges the request or if the settlement phase proves that the request was legitimate, the Blockchain Name Service update its ledger accordingly.

D. Human Address Name Links. The ultimate goal of the Blockchain Communication System is to provide an easy, human readable, value address. This feature is needed in order to allow easy exchanges between end-users. However, there are still some open security issues remaining regarding its implementation. Research about the Human Address Name Links is still active and another paper will be published to solve specifically these issues.

Example of Human Address Name links A user will be able to register a human name for a value address.

All value addresses can be linked to an understandable. Potential human names for a value address:

- antoine*iov.value
- isabella*iov.value
- mycompany*iov.value

Example of use cases

Send a token from user A to user B. User A can send any token to user B by simply submitting a transaction via the IOV Wallet.

Exchange 2 different tokens from user A and user B. If user A wants to exchange value A against value B, atomic cross-chain trading is the easiest solution as each BLOCKCHAIN TOKEN implements a shared protocol.

ICO. In the case of an ICO, a user via their IOV Wallet holds a Token A and wants to trade to a new fancy token B. In this example, atomic cross-chain trading or an exchange should be responsible to escrow the token A and B and send it back to the correct value address. The immediate benefit is that the user can get the new token immediately in its IOV Wallet. Another very interesting aspect brought by the IOV Wallet is that there is an uniformity between using one or an other token to participate in the ICO. Currently, this is a problem to the ICO organizer, who has to implement different mechanisms in order to allow users to participate in his ICO using different coins.

Conclusion

The diversification of isolated consensus requires a global and universal solution. We believe that the Blockchain Communication System as we have outlined will create the foundation needed for a unified protocol for exchanges of all values between blockchains. This protocol would not only solve the problems of multi-chain disjunction, but would also empower end-users by providing them with a secure and single access e-wallet to inventory and exchange all their digitals assets and values. In addition, it offers solutions to the problems of digital asset registry, inventory and exchange in an environment of constant multiplication of autonomous and heterogeneous blockchains. We believe this will be a true game-changer for the way people and businesses share values and assets. And we believe that it has the potential to fundamentally transform economic dynamics from micro and local economies to global interconnected exchanges. We see this upcoming transformation as a revolution. If value can meet values, this revolution could also be a way to empower people worldwide and to embrace a mindset of abundance in our collective exchanges.

www.iov.one

ACKNOWLEDGMENTS. We would like to thank our friends from Cosmos for their continuous support. We would like also to thank the community for developing amazing projects such as Ethereum, Litecoin, Dash, Lisk, Stratumn, Aragon, Zeppelin, Iexec, Algorand, Epicenter. We are looking forward to continuing this journey with all of you.

1. Nakamoto S (2008) Bitcoin: A peer-to-peer electronic cash system (https://bitcoin.org/bitcoin.pdf).
2. Buterin V, , et al. (2014) A next-generation smart contract and decentralized application platform. *white paper*.
3. Buchman E, Kwon J (2016) Cosmos: A network of distributed ledgers.
4. (2016) Atomic cross-chain trading (https://en.bitcoin.it/wiki/Atomic_cross-chain_trading). Accessed: 2017-03-12.