IOV: A Browser of Value

Version 1.3

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

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

Abstract

A Browser of Value 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 current 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.

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 via scripting 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 to create a decentralized network that allows the free flow of digital currencies. (3).

Over the past months, interest in blockchain technology and usability has been rapidly increasing. The blockchain industry has reached a tipping point where, soon, thousands of blockchains will be issued. The majority of them will be decentralized and independent.

In building a system that is able to track millions of different tokens, there are two main options. 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 a first specification to store and exchange many different tokens on the Ethereum blockchain. It allowed 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 in the Ethereum blockchain. Besides, the Ethereum blockchain is about 160GB. Even if the size is manageable, the blockchain contains invalid tokens or tokens with dead projects. This phenomenon is very common because most tokens have a limited lifespan. It is similar with shares of a company, for example. A company is born, lives and dies and their associated stock token is created, exchanged and at some point is no longer active.

Because the lifetime of most of the tokens will be limited and unique, only tokens of active projects need to be tracked in order to be exchanged.

Significance Statement

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

1. A **Universal Value Specification (UVS)**: a set of standards that each blockchain implements;
2. A **Browser of Value (BOV)**: a graphical interface to interact with the token world from a computer or a mobile phone;
3. A **Value Name Service (VNS)**: a special blockchain to interact with the Browser of Value.

Bitcoin approach

Greater efficiency is created with one blockchain per token. This way, the lifetime of the blockchain is associated with the lifetime of its own token. As soon as the token has no more usability, there is no need to maintain that specific blockchain. It can disappear by itself, without causing any problems.

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 they are used, the user needs to create a wallet for that specific blockchain. This can be problematic if a user wants to own lots of different values, because the user needs to create as many wallets as tokens. Also, it is difficult to deploy a new blockchain, and the consensus of a single blockchain can be weaker than a global multi-assets blockchain.

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

Description of the Browser of Value System

The goal of a Browser of Value System is to allow any value or asset to be digitally initiated, monitored, stored, or exchanged from a unique electronic wallet.

Key elements of our system that will allow for the exchange of these values include:

- A **Universal Value Specification (UVS)**: a set of standards that each blockchain implements;
- A **Browser of Value (BOV)**: a graphical interface to interact with the token world from a computer or a mobile phone;
- A **Value Name Service (VNS)**: a special blockchain to interact with the Browser of Value.

All blockchains fulfilling to the Universal Value Specification will be directly compatible with the Browser of Value. Everybody can create their own token.

A. Universal Value Specification. A BLOCKCHAIN TOKEN is a simple blockchain that implements the Universal Value Specification. Its only purpose is to track the transaction of its token. The blockchain could be proof of work, proof of stake, delegated proof of stake or proof of space and time. We start by giving external properties (A.1 TO A.4), e.g. specification that will bring standardization among blockchains before giving 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 Browser of Value 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 (To start, we plan to support 2 types: ed25519 and secp256k1)
- Actual public address of the signature

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.

A.3. Hashed Timelock Contracts. This feature is needed for the Browser of Value to exchange Coin A against Coin B easily without the need of a third-party exchange. As each BLOCKCHAIN TOKENS implements the same specification about 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 needed for the VNS.

- Genesis file. The BLOCKCHAIN TOKEN should save the genesis file in the TOKEN DEFINITION. The genesis file should never change.
- Human name for the token. The BLOCKCHAIN TOKEN should agree on what the human name for the token is.
- Unique identifier for the token. The BLOCKCHAIN TOKEN should agree on what the unique identifier for the token is.
- Pictogram for the token. The BLOCKCHAIN TOKEN should agree on the image representation of the token.

- Bootstrap nodes. The BLOCKCHAIN TOKEN should agree on which nodes are safe and secure to receive transactions and queries from outside.

- Finality. The BLOCKCHAIN TOKEN should agree on what its finality is.

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.

A.6. Objectivity & Determinism. The BLOCKCHAIN TOKEN needs to be deterministic and to be objective or at least weakly subjective. The VNS 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. Browser of Value.

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

- Store: create a universal 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. Value Name Service. The Value Name Service (VNS) is the backbone of the Browser of Value. It is a special BLOCKCHAIN TOKEN (i.e. fulfilling the Universal Value Specification, see above). The main function of the VNS is to keep a valid copy of each TOKEN DEFINITION for each BLOCKCHAIN TOKEN. The VNS is very similar to Wikipedia. The VNS lists all valid token definition from all BLOCKCHAIN TOKEN. We designed a simple process for anyone to copy a TOKEN DEFINITION on the VNS, based on the information available on its BLOCKCHAIN TOKEN.

C.1. IOV Token. The VNS has a native token called the IOV Token. The IOV token is the staking token of the VNS.

C.2. Consensus. The consensus of the VNS is a proof of stake. IOV Token is the staking token of the VNS.

C.3. Registration of a Token Definition on the VNS. Any user can register or update a TOKEN DEFINITION of a BLOCKCHAIN TOKEN on the VNS. This procedure needs to be done at least once a year. Otherwise the BLOCKCHAIN TOKEN is marked as inactive. By doing this, a user is able to know if the BLOCKCHAIN TOKEN is active or not.

The VNS truly allows anybody to report a TOKEN DEFINITION on the VNS. A mechanism is therefore needed to prevent any malicious actors from adding false information to the VNS. We propose below such a mechanism.

I. Request phase. To update or register a TOKEN DEFINITION, the user needs to send a special transaction with the current TOKEN DEFINITION available on a BLOCKCHAIN TOKEN, including a fee in IOV coin and escrow amount in IOV as well. If it is the first registration, the VNS makes sure that the unique identifier for the token is available, otherwise the transaction is rejected.

II. Challenge phase (1 day). During this phase, anyone can challenge the request by sending another specific transaction fee in IOV coin and escrow amount in IOV and its correct version of the TOKEN DEFINITION.

III. Settlement phase (optional). If someone challenges the request, then the Value Name Service will settle the case. A user called a moderator elected by the governance of the VNS will be in charge to rerun the actual state of the BLOCKCHAIN TOKEN.

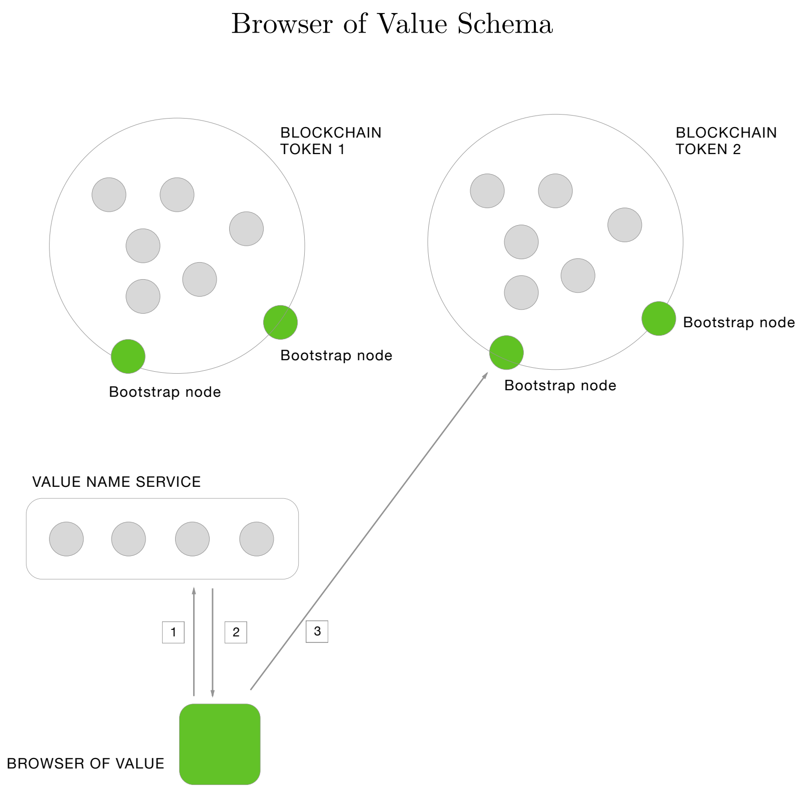

Fig. 1. Schematic representation of the Browser of Value. 1. Browser of Value requests to the Value Name Service the list of active BLOCKCHAIN TOKEN. 2. Value Name Service sends the list including the IP address of the bootstrap nodes for each BLOCKCHAIN TOKEN. 3. Browser of Value sends a transaction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

The moderator can determine without ambiguity the actual state of the TOKEN DEFINITION. If the request is legitimate, the challenger loses his escrow. If the request is not legitimate, the user who initiated the request loses his escrow. The escrow is then distributed among the moderators of the VNS.

IV. Registration phase. If no one challenges the request or if the settlement phase proves that the request was legitimate, the VNS update the copy of the TOKEN DEFINITION of the BLOCKCHAIN TOKEN on its ledger accordingly.

D. Human Address Name Links. The ultimate goal of the Browser of Value System is to provide an easy, human, universal 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 universal value address. All universal value addresses can be linked to an understandable, human name which starts with a prefix of these 4 characters:

- **iov:**

Potential human name for a human universal value address:

- iov:antoine.value
- iov:flodolphin.value
- iov:mynonprofit.value
- iov:mycompany.value

Example of use cases

Send a token between user A to user B. User A can send any token to user B by simply submitting a transaction via the Browser of Value.

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 it. There is also a second solution: standard exchange needs to hold value A and value B during the time of the trade. Current services like shapeshift can be used as well.

ICO. In the case of an ICO, a user via their Browser of Value 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 universal value address. The immediate benefit is that the user can get the new token immediately in its Browser of Value. Another very interesting aspect brought by the BOV is that there is a 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 Browser of Value 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 in the era of the Browser of Value. 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.