Interwallet Operability Protocol White Paper

Pawel Mastalerz & David Gold

August 2019

Abstract

Interwallet Operability Protocol (IOP) is a decentralized public blockchain, which acts as a service layer to native blockchains and aims to improve wallet usability. It is not an intermediary to transactions on those blockchains and offers its users privacy and security. Its incentive structure ensures the viability of the network and accelerates adoption among wallets and exchanges. Key elements of IOP are 1) Wallet addresses - human-meaningful identifiers on IOP, which can be used for sending or requesting funds and which do not publicly map to user's public address on other blockchains; 2) Request for Payment - error-free and secure ability to request funds from another wallet using Wallet address; 3) Metadata - ability to attach metadata to any blockchain transaction.

Background

The purpose of a White Paper is to inform readers concisely about a complex issue and present our philosophy on the matter. That context has been lost in the world of blockchain as White Papers have often become marketing documents. As co-founders of the company that is building a specific implementation of the Interwallet Operability Protocol (called the FIO Protocol[1]), we offer this White Paper to accomplish that goal.

Throughout this Whitepaper "wallet" refers to the primary user interface to blockchains. It may include self-sovereign wallets where private keys are stored, but also centralized or exchange-based wallets which act as the interface, but do not technically store user's public keys.

Introduction

Over 10 years after the publication of the Bitcoin White Paper[2] the process of interacting with blockchains continues to be complex and risky, leading to a considerable barrier to broad user adoption. Not unlike other information technologies, the initial versions necessarily focus on core operations and functions. In many instances, the layers of usability in information technology come not as part of the underlying technology infrastructure or protocols, but, rather, as a layer that stands besides, or on top of, the core operational technology. This enables the underlying technologies to excel at what they are good at while relinquishing usability to a layer or protocol that is specifically designed for that purpose. For example, the first computers had text only command lines with complex command structure and it wasn't until graphical user interfaces enabled broader adoption. The Internet was a protocol that required users to initially be technically savvy until the Hypertext Transfer Protocol (HTTP) enabled ease of use through web browsers.

We propose that at the highest level, blockchains uniformly have two core usability issues today. First, are the risks and challenges associated with the security of a user's private key. Second, are the risks and challenges associated with moving blockchain value from one party to another and the various methods by which different blockchains enable this. The focus of this white paper is this second challenge. We present the need for and concept of a decentralized Interwallet Operability Protocol (IOP) that acts as a service layer enabling homogeneous usability across all other blockchains. The IOP enables wallets and exchanges to very easily enhance user experience with industry-standardized features like wallet names and request flow, while at the same time not encumbering underlying

[1] https://fio.foundation/
[2] https://bitcoin.org/bitcoin.pdf

blockchains with complex integration projects and allowing those teams to focus on core blockchain technology instead.

Key Usability Challenges When Moving Blockchain Value

When value is to be moved on a blockchain today in a decentralized manner, a number of complexities and risks face users.

Complex public addresses or other identifiers. When interacting with blockchains, a public address[3] is typically required as the identifier of the recipient of funds. On most blockchains it is a hashed representation of the public key resulting in a long alpha-numeric string. This virtually guarantees that it will not be human-meaningful. It is also not practical to type nor even recognize one.

Send only functionality. Most transactions of value in the world today begin with a request for payment, an invoice, a bill, an order cart, etc. Today blockchain transactions begin with "send" and users are typically forced to initiate it using information (amount, destination public address, metadata, etc.) obtained from emails, websites or by scanning QR codes. This significantly increases the chances that transactions will be sent to the wrong address, include the wrong amount or will not be properly reconciled due to lack of associated metadata. Being immutable and without a centralized third party that could correct issues, this approach leads to greatly increased risk of errors and, on some blockchains, errors can result in a complete loss of funds.

Security risks. The most common way to exchange public addresses today is copy-pasting or scanning a QR code (1). Both options are fraught with usability and security issues. Users are often susceptible to man-in-the-middle (MITM) attacks[4] as they exchange addresses over less secure channels such as email, text or other plain text transfer. QR code scans are not any more secure and only work in specific scenarios, such as when the payer uses a mobile wallet and payee QR code is not on that device, which rules out mobile commerce.

Limited metadata. Transactions of value in the fiat world typically include transaction metadata such as a memo, order cart, invoice, etc. While some blockchains support the concept of transaction metadata, the implementation varies making it a unique wallet integration activity for each blockchain and almost impossible for a wallet to provide a unified homogeneous user experience. As a result, very few wallets support the metadata constructs of blockchains that support them.

Refunds are difficult. In the world of commerce, the ability to issue refunds to customers is critical. With fiat accounts a refund is simply processed back to the same account typically in an automated fashion. In blockchain, refunds are often complex and may require customer's public address be obtained before a refund is issued. This usually requires manual intervention, which increases costs.

Growing Number of Blockchains. Each underlying blockchain endeavors to provide different capabilities and each has different strengths and weaknesses. As a result, it is probable that the world will continue to have multiple blockchains providing various capabilities to the market. Each will be architected differently meaning that a user directly interacting with those blockchains will face differences in the manner of interaction and the differences of each respective blockchain's capabilities. As a corollary, users of the Internet don't even need to know what software, database or architecture a website utilizes to easily interact with them in a common manner that they understand.

With such significant usability issues, it is not surprising that the vast majority of users do not feel comfortable sending and receiving crypto and nearly one in five report having experienced failed transactions or having lost funds not due to hacking but do to user errors in the transaction process (1).

[3] https://en.bitcoin.it/wiki/Address
[4] https://en.wikipedia.org/wiki/Man-in-the-middle_attack

Previous Attempts to Solve Key Challenges

To date, the attempts to solve these challenges fall into two categories: 1) Off-chain standardized structures for passing information to wallet; 2) Wallet names.

Off-chain standardized structures. These solutions attempt to make it easier to pass certain information to a wallet. The two most notable examples are QR Codes[5] and the BIP-21[6]/70[7] standard for the Bitcoin blockchain.

QR code scans allow a user to scan a code, typically on mobile device, which embeds key transaction information such as the public address of the recipient, the amount and type of token/coin to be sent. QR codes fall short in several ways. First, they require the recipient to be able to generate such a code and present it to the sender. If the two parties aren't physically together, the QR code must be sent, typically through unsecure means like email where it becomes subject to man-in-the-middle attacks. In fact, even on a device to device interaction the device generating the QR code could be attacked to replace the QR code with one that would send the payment to the attacker. In addition, QR codes require access to two devices. Yet, already today over 53% of all ecommerce[8] is transacted by mobile users who are on a single device where they often do not have access to a second device in order to scan a presented QR code, essentially eliminating the ability for mobile commerce.

The BIP-21 is a URI scheme[9], similar to "sendto:" used in email. Clicking a properly structured link on a supported device will open a program, typically a wallet, and pre-fill send information including the public address and amount of bitcoin to be sent. BIP-21 currently supports only Bitcoin and is subject to man-in-the-middle attacks since the information is transferred in plain text. An attacker could intercept such a transfer and replace the public address. BIP-70 has enhanced that by introducing X.509 certificates, but those are issued by centralized authorities that must be trusted and have security risks of their own including known vulnerabilities, such as Heartbleed[10]. In addition, in both cases, the wallet that will send the payment must be on the same device as the referring link. In a business use case where an employee needs to make a purchase with payment coming from a company wallet, that the company would not want stored on that individual's device, these standards would not work.

Although these partial solutions are being attempted, none incorporates them with sufficient security, workflow and UX quality for the problem to generally be resolved.

Wallet Names. The second category of attempts have been human-meaningful wallet names that replace the need for users to know or interact with complex public addresses. Those attempts do not address any of the other key challenges facing blockchain usability. To date, none of these have been broadly adopted nor utilized to any meaningful degree in blockchain transactions. It is our belief that all of these attempts have fallen short for one or more of the following reasons:

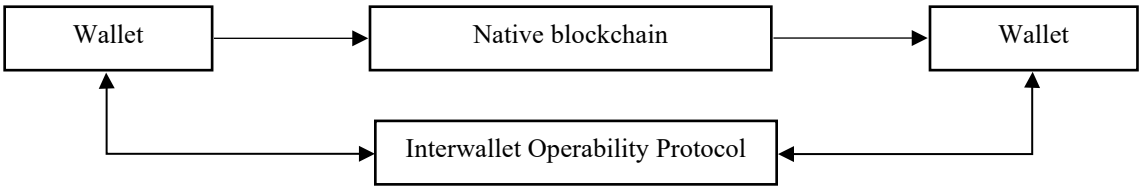
- **Blockchain Specific.** Ethereum Name Service[11] is probably the most well-known attempt at a blockchain-specific naming convention. The challenge with any blockchain-specific solution is that unless that blockchain becomes the only blockchain, users are faced with having a wallet name for some tokens/coins, different ones for others and none at all for ones beyond that. A horribly confusing and unusable construct. While some blockchain specific solutions could eventually be extended to include public addresses for other blockchains, all the other issues in this section would also need to be addressed to enable a system that had the performance, privacy and path to adoption necessary for success.

[5] https://en.wikipedia.org/wiki/QR_code
[6] https://github.com/bitcoin/bips/blob/master/bip-0021.mediawiki
[7] https://github.com/bitcoin/bips/blob/master/bip-0070.mediawiki
[8] https://www.statista.com/statistics/249863/us-mobile-retail-commerce-sales-as-percentage-of-e-commerce-sales/
[9] https://en.wikipedia.org/wiki/Uniform_Resource_Identifier
[10] https://bitcoinmagazine.com/articles/wallet-developers-express-security-concerns-over-bitpays-payment-protocol-policy
[11] https://ens.domains/

- **Conflation with Decentralized TLDs.** Zilliqa Name Service[12] and Handshake[13] both have the noble goal of creating decentralized top level domains (TLDs) for the Word Wide Web and corresponding uncensorable websites. In some cases, these projects then also attempt to solve the Wallet Naming issue. The challenge here is that decentralized web domain directories must, by nature, be open text so that any user can get to any website. However, information about a user's public addresses is generally not something that most users prefer to have publicly known especially if a Wallet Name corresponds to multiple blockchains as others can then learn how much value that Wallet Name has on different chains. Decentralized web domain platforms must be open by design whereas any usable effort at blockchain Wallet Names must be private by design.
- **Centralization and Walled Gardens.** Some attempts have included centralized elements of the implementation. In no scenario can a Wallet Naming solution have centralized aspects as these will become huge honey pots for hackers wanting to redirect funds. Other projects created walled gardens requiring all users to use their software platforms to get the naming benefits. Such a strategy will never succeed unless such a company becomes essentially the only provider which we believe is very unlikely.
- **Difficult to Use.** Many attempts at Wallet Names ironically are very challenging to use themselves. The process of obtaining such a name and associating it with a wallet needs to be seamless and easy for the everyday user.
- **No Economic Model.** For Wallet Names to work, wallets must spend the time and money to integrate the capability. To date, every wallet naming solution requires such a cost to be incurred with no path for a direct economic return, creating huge friction in adoption.
- **Only Wallet Names.** Finally, these attempts only solve the issue of complex public addresses and do not have a means to address the other critical usability issues facing blockchains.

Interwallet Operability Protocol

We propose that a decentralized Interwallet Operability Protocol (IOP), which acts as a service layer to native blockchains is the best approach to solving usability problems. To ensure swift adoption, the protocol must work seamlessly with all blockchains without requiring them to integrate it. It cannot be an intermediary to native blockchain transactions, and it must offer its participants privacy and security. Finally, it needs a proper incentive structure to ensure the viability of the network and to accelerate adoption among wallets and exchanges that act as the user interface for sending and receiving transactions and are most committed to enhancing the user experience. One might draw a loose analogy to SWIFT[14] which sits alongside interbank transactions providing a layer of messaging and information about transactions of value, but which does not actually send any currency itself. IOP moves information and does not integrate with nor interact directly with the underlying native blockchains. However, the comparison ends there as the IOP is fully decentralized, operates only with blockchain transactions and enables usability for any user whether they are a business or individual.1



We propose the first generation of the IOP could provide three core capabilities: Wallet Addresses, Requests for Payment and Transaction Metadata.

[12] https://github.com/unstoppabledomains/zns
[13] https://www.handshake.org/
[14] https://en.wikipedia.org/wiki/Society_for_Worldwide_Interbank_Financial_Telecommunication

IOP Blockchain

To ensure that no single central authority has control over IOP and to enable unrestricted access, IOP has to run atop a blockchain. In theory, it could run atop existing blockchain such as Bitcoin or Ethereum. However, for the following reasons we believe it's best implemented on a public blockchain utilizing Delegated Proof of Stake (DPoS)[15] consensus algorithm:

- Wallets and exchanges are the primary participants in the IOP and need to have both substantial economic incentives as well as large share of voice in the governance. Neither would be easy if IOP was running on another chain with its own network economic model.
- To deliver required functionalities and adequate performance and security requires greater access and control than typically allowed by smart contract platforms running code from many system participants.
- A protocol running on purpose-built blockchain has a much higher chance of being adopted by the community than a protocol running on any one smart contract platform which is often seen as competing with other platforms.

Wallet Addresses

The concept of creating human readable "wallet names" which we refer to more appropriately as "addresses" (e.g., like an email "address") is on the surface the simple matter of creating an index between the human readable Wallet Address and the various blockchain public addresses with which it is associated. But that is a simplistic view that neglects critical issues of security and privacy.

In IOP, a user can create a human-meaningful name and let that name act as their identifier on the network. The name is controlled via the user's IOP private key which resides securely in their wallet and signs all transactions on the IOP blockchain. The wallet address ledger itself lives on the IOP blockchain ensuring no single central authority has control over it.

IOP Wallet Addresses' key differentiator is that they cannot be mapped by an observer to private data such as public address on another blockchain or metadata stored on IOP blockchain. Furthermore, IOP obfuscates the connection between Wallet Addresses, which would have otherwise been established if one party sends a request to another on the IOP blockchain. These concepts are described in more detail further in the document.

IOP a wallet address consists of a name and a domain delimited by a colon. Example: **purse:alice**. The use of colon is intended to clearly differentiate the wallet address from a web address or email address. The concept of IOP domains allows for 2 types of wallet addresses. Users can register their own IOP domain and create various usernames on it. In addition, enterprises, like blockchain wallets, can enable third parties to register a username on their IOP domain, enabling cheap or even free wallet addresses to their customers, akin to Gmail or Hotmail. This is facilitated by IOP enabling anyone to register a name for anyone else, simply by providing their public key during registration.

Owners of domains have limited ability to control wallet addresses on their domains:

- By default, only domain owners can register usernames on their domains. However, they can also make their domain public, which would allow anyone to register a name on that domain.
- Domain owners can choose to prohibit transfers of usernames registered on their domains.
- Wallet addresses are always in total control of their owner (i.e., the user with the associated private key). However, a domain owner can burn any wallet address on their domain irrespective of who owns it.

Both usernames and domains are non-fungible tokens (NFT)[16], allowing them to be easily transferable. To enhance the experience of selling NFTs, IOP supports a smart contract-based transfer functionality. When enabled by the

[15] https://en.bitcoinwiki.org/wiki/DPoS
[16] https://en.wikipedia.org/wiki/Non-fungible_token

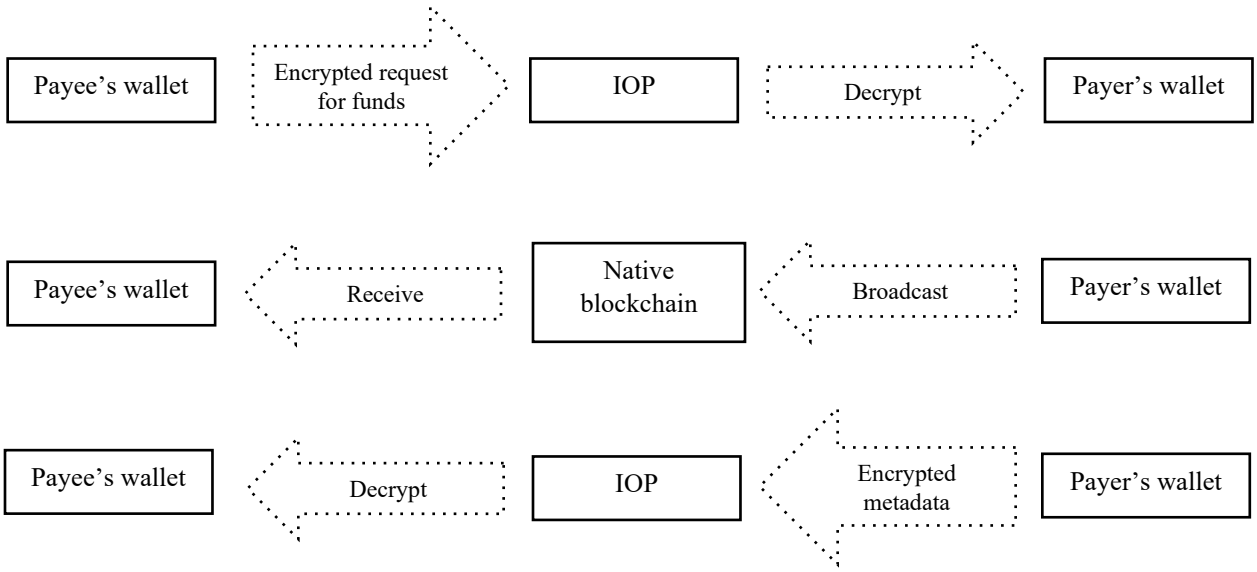
owner, it allows for automatic transfer of the NFT to the new owner upon payment of a specified amount to a default address. This functionality eliminates the need for an off-chain escrow.

Wallet addresses and domains are subject to annual fees. If the fee is not paid before expiration date, the name/domain is locked for a period of time when only limited transactions are supported. After that time, if not paid, it is burned and can be re-registered by any user. In addition, after domain expires, all wallet addresses on that domain will be locked and if domain fee is not paid, all wallet addresses on that domain will also be burned. Anyone, not just the owner, can renew a wallet address or domain by paying the required fee.

Requests for Payment Using Wallet Addresses

Ability to request funds is a critical element of IOP. Combined with wallet addresses, it enables easy, error-free and secure way to transact. When a payee requests funds using a wallet address, they first encrypt all sensitive metadata (e.g. currency, amount, public address of payee, memo, etc.) using Diffie-Hellman key method[17], which derives a shared secret from the payee's private key and the payer's public key and combines it with initialization vector. Then they place the transaction on the IOP blockchain with intended recipient obfuscated, as described in more detail further in the document. The payer polls the IOP blockchain, decrypts the payment request inside their wallet and uses the information to pre-populate the send transaction, which is broadcasted to the native blockchain without involving IOP.

In addition, the payer may choose to place metadata about the native blockchain transaction (e.g. native blockchain transaction id, refund address, memo, hash of off-chain metadata, etc.) on the IOP blockchain. Just like the request, the metadata would be encrypted using Diffie-Hellman key exchange method and hence only readable by payer and payee.



Sending Funds Using Wallet Addresses

The process of sending funds without first requesting them is also made easier and more secure using wallet addresses. The owner of the wallet address can associate public addresses for different currencies to their IOP wallet address and publish those associations to the IOP Blockchain. For example, **purse:alice** can simultaneously map to:

[17] https://en.wikipedia.org/wiki/Diffie%E2%80%93Hellman_key_exchange

• 1A1zP1eP5QGefi2DMPTfTL5SLmv7DivfNa on Bitcoin's blockchain.

• 0xAb5801a7D398351b8bE11C439e05C5B3259aeC9B on Ethereum's blockchain.

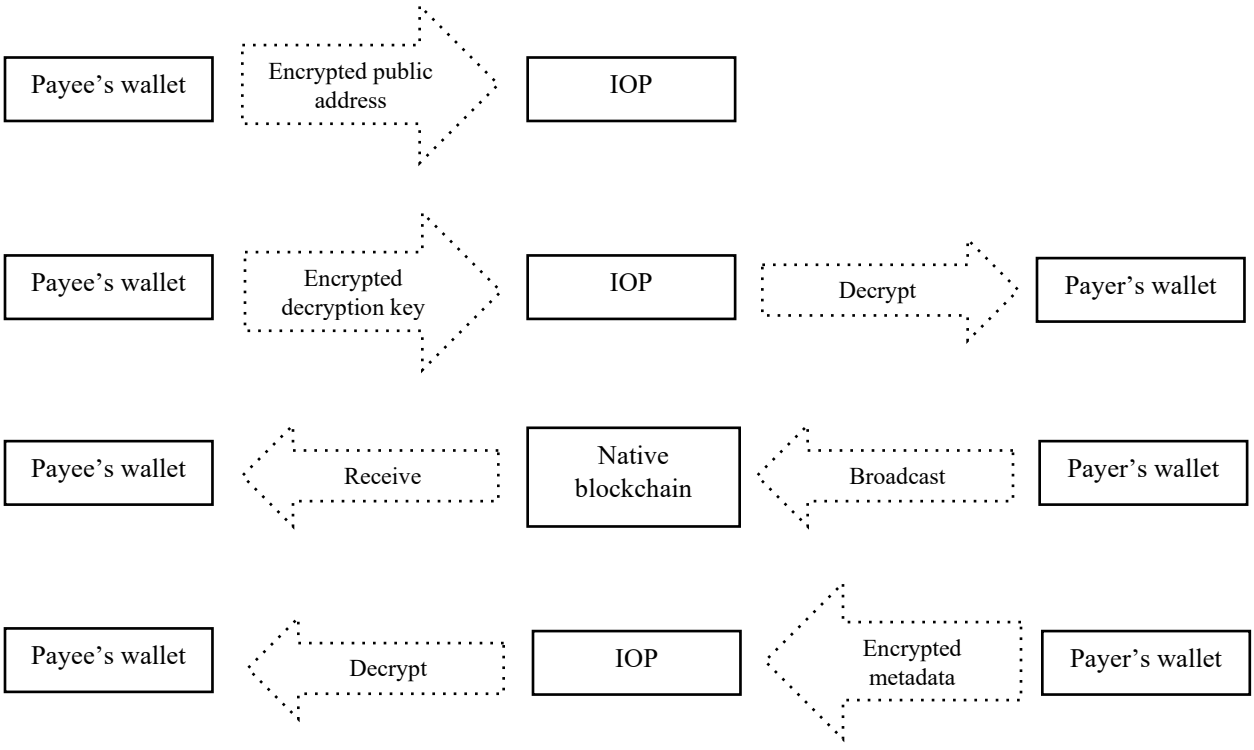
• A public address on any other blockchain.

The mappings can be updated at any time. Deterministic wallets[18] can choose to automatically update the mapped address when unspent output (UTXO)[19] from a transaction is sent to a new address.

We believe that, unlike DNS for the internet, public address mappings cannot be publicly available on IOP blockchain, as it would compromise the privacy of users by allowing anyone to link public addresses across multiple blockchains. Following privacy by design principles[20], the wallet address owner will decide when to place public addresses on IOP blockchain and they will always be encrypted and readable only by approved parties. In order to offer the most flexibility to users and to reduce the amount of content stored on IOP blockchain, each public address is encrypted symmetrically three separate times using different secret key each time:

- Address level secret key – only used to encrypt one public address.
- Blockchain level secret key– used to encrypt all public addresses for a particular blockchain (i.e. Bitcoin).
- Wallet level secret key – used to encrypt all public addresses in that wallet.

Address level secret key can decrypt just one public address. Blockchain level secret key can decrypt current public addresses for specific blockchain and all future addresses for that blockchain published by the owner. Wallet level secret key can decrypt all addresses published by that wallet. The wallet address owner can then decide which of those decrypt keys to make available to which user by placing it on the IOP blockchain encrypted asymmetrically with the approved user's public key. It is assumed that wallet address owners will add approved users using their wallet addresses or as part of the request flow. Users less concerned about the privacy issues may also make any of their secret keys public by placing them unencrypted on IOP blockchain.



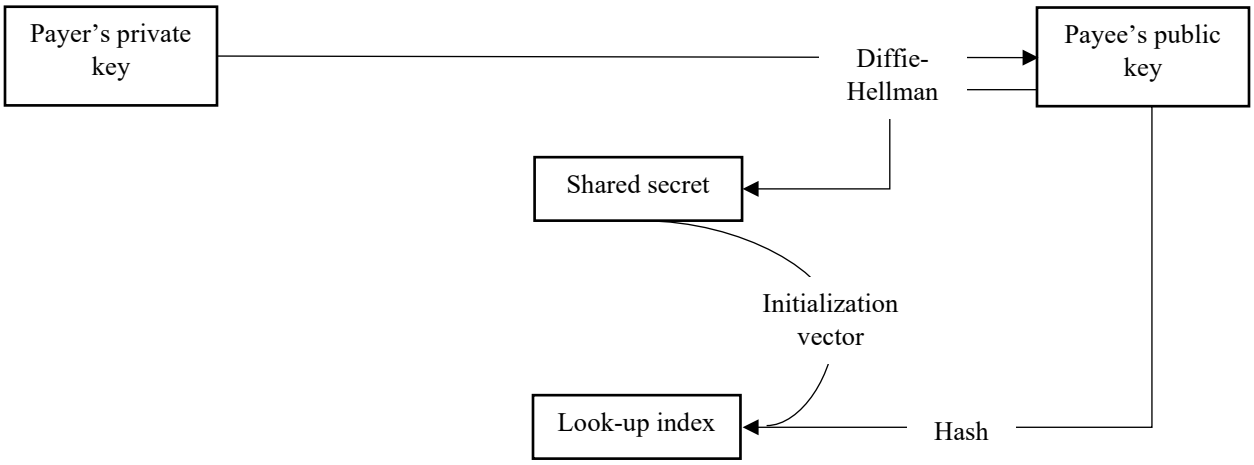
[18] https://en.bitcoin.it/wiki/Deterministic_wallet
[19] https://bitcoin.org/en/glossary/unspent-transaction-output
[20] https://en.wikipedia.org/wiki/Privacy_by_design

As a middle ground between having to pre-approve individual users and making the secret keys public, IOP will support stealth wallet addresses. The owner can place any of the decryption keys on IOP blockchain encrypting them using human-meaningful secret. That secret can be prepended to their wallet address: **secret:purse:alice**. The sender's wallets will know to use the prepended value as a secret to decrypt the keys obtained from IOP blockchain using the second part of the wallet address.

Obfuscating Connection Between Counterparties

In addition to encrypting request for funds transaction and send transaction metadata, it is important for IOP to obfuscate the connection between counterparties exchanging transactions on the IOP blockchain. If left unaddressed, when a payee placed a request for funds transaction with payer as the intended recipient, it would become public that those parties were interacting with each other. To address this privacy issue, in IOP request for funds, the payee is always public, but the payer is hidden behind a specially constructed look-up index unique to each party.

It is required that the payer first add the payee to a whitelist of approved parties. To accomplish this, the payer first derives a shared secret from the payer private key and the payee public key using Diffie-Hellman key method. That secret is then hashed and placed on the blockchain by the payer.



Since the payee can derive the same secret, they can easily and privately check the IOP blockchain to see if they have been whitelisted. When a payee sends a request, aside from encrypting it, they also create a unique look-up index by hashing payer's public key using derived secret and the public key itself as initialization vector. Payer knows to look for that unique index when querying the blockchain, because the payee is in their whitelist.

Similarly, if payer wants to "respond" to the payee (e.g. reject the request for funds), they will create a unique look-up index by hashing payee's public key using derived secret and the public key itself as initialization vector.

This concept allows both parties to place transactions on the IOP blockchain without an observer knowing that the parties are interacting with each other.

It is also possible to allow any user to publicly state, e.g. as part of their Wallet Address setting, that they are not concerned with obfuscating the connection between counterparties, i.e. they want to be public. This way if another user, with that same setting wants to initiate a request for funds transaction, they should be able to do so without the need for whitelisting.

There are additional benefits of the whitelisting concept:

- It virtually eliminates the risk of spam transactions (e.g. spammer sending random requests in hopes of getting users to send them funds), as the recipient of such transaction must first add the sender to the whitelist and can just as easily remove them.
- In case of a Byzantine Fault[21], if an attacker was to transfer ownership of a Wallet Address to themselves, they will not be able to interact with others, as they would not be in their whitelists.

The recommended approach for deriving look-up indexes results in the same pair of indexes being used for any two users indefinitely. This may increase the probability of associating two users as interacting with each other or associating their Wallet Address to transactions on other blockchains. The obvious solution would be to incorporate a unique initialization vector for each transaction between parties. It should be considered vis-à-vis the performance implications of using expanding number of look-up indexes. In addition, users should be allowed to opt-out of recording send transactions on the IOP blockchain in order to increase the level of privacy.

Network Economics

A viable network economic model is critical to IOP adoption and long-term sustainability. IOP is constructed with two core economic principles. First, that users which benefit from the usability will provide a form of economic input either by directly paying fees or indirectly by economically benefiting a service they utilize (e.g. a wallet). Second, that portion of the economic value created by the IOP needs to return to the entities that must integrate IOP into their products and who are providing the user interface solutions, thereby incentivizing them to support IOP.

For most individual users, this will primarily come in the form of an annual fee to register a wallet addresses or a domain. It is likely that some businesses will cover the annual cost of the wallet addresses for their users, in exchange for their use of that product, akin to email services such as Gmail which are "free", but which monetize users through other means such as advertising.

To avoid the friction of having to pay every time a request for payment is sent or address mapping updated, wallet addresses will come with bundled transactions, which should be high enough so that most users will never exhaust their limit. This greatly simplifies user interaction and avoids layering a second blockchain transaction fee on top of the underlying transaction they are engaging. However, we anticipate that frequent business users will pay nominal per transaction fee typically for a payment request as they will exceed their bundled transactions.

As IOP is a decentralized public blockchain, most of the cost to run and secure the network will be borne by the validators. Therefore, they should receive a major portion of the collected fees.

Wallets and exchanges should have an active role in governing IOP and therefore should be encouraged to become validators on the network. To make that possible and to give industry participants with more users a louder voice, IOP implements default proxying of votes. Absent a specific user vote or proxy, tokens held by wallets originating IOP transactions are automatically proxied to the entity that built the wallet and registered it with the IOP blockchain. Wallets and exchanges should also receive a meaningful portion of tokens distributed at launch.

Extending the Protocol

IOP may be extended to further enhance usability. Here are some concepts requiring further research.

- **Verified wallet addresses**. In order to further enhance the security when interacting with wallet addresses, trusted community participants may administer verification programs and issue "verification seals" to wallet addresses, which have passed their checks.
- **Wallet address aliasing**. Once validated by trusted community participants, identifiers from other communication channels (e.g. email, cell phone number, telegram handle) may be attached as an alias to the

[21] https://en.wikipedia.org/wiki/Byzantine_fault

wallet address on IOP. This would allow users to use existing identifiers instead of, or in addition to, IOP's wallet address.

- **Wallet address look-up**. For users who want to use their wallet address to identify themselves on other blockchains, IOP may enable a look-up of their wallet address using any other blockchain's public address. This could be desirable for users who want to publicly disclose that their public address is associated with an NFT, a high score in a game, or any other action they want others to know about.
- **Multi-signature transaction[22] routing**. Due to their complexity, most wallets today do not support multi-signature transactions. IOP's request can make those types of transactions much easier to implement and use. When a multi-signature send transaction is initiated, the other users required to sign the transaction will receive a request to approve the transaction with all information already pre-populated. If the blockchain requires partially signed transactions to be exchanged between users, such as a Partially Signed Bitcoin Transaction as defined in BIP-174[23], those could be stored off-chain with a hash recorded on IOP blockchain.
- **Recurring payments**. IOP's request can also enable recurring payments, which are not easy today when using cryptocurrencies. IOP users would only provide their wallet address and the merchant will trigger a request on a regular schedule. The user will approve each request with a single click inside their wallet.
- **Pre-approving requests**. In order to improve frequent interactions with DAPPs[24] (e.g. playing a game), the integrating wallets may implement the ability to pre-approve requests based on sender, amount, and frequency. When enabled, the wallet will automatically approve a request from an approved sender if it is below a designated amount threshold or frequency. This could greatly improve the usability of DAPPs, which today typically require every action to be manually approved.

Further Reading

The FIO Protocol[25] is a specific implementation of the concept described in this White Paper. Those desiring to understand the more detailed roadmap and long term vision should also read the FIO Roadmap[26].

References

1. **Foundation for Interwallet Operability.** Blockchain Usability Report. [Online] February 2019. https://fio.foundation/blockchain-usability-report-2019

[22] https://en.bitcoin.it/wiki/Multisignature
[23] https://github.com/bitcoin/bips/blob/master/bip-0174.mediawiki
[24] https://en.bitcoinwiki.org/wiki/Decentralized_application
[25] https://fio.foundation/
[26] https://fio.foundation/roadmap