0xBASE
Mobile-first dApp and instant payment infrastructure for the devices of today and the token economies of tomorrow

Boris Savic, Polona Remic, Klemen Kastelic, Martin Sirok,
Aljosa Praznik, Klemen Rupnik, Blaz Bregar

2018
March

Abstract

In the whitepaper current challenges of blockchain adoption are addressed, namely the ecosystem token economy fragmentation, relatively slow and costly Ethereum network transactions and lastly poor blockchain connected interactions with mobile applications whereas the majority of applications rely on desktop usage. Authors propose the new software and network infrastructure that intends to solve examined issues by providing an instant payment solution of periodical bulk settlement node network, software development kit for the network utilization, a secure wallet as a representation of the network gateway and a plugin to connect mobile and desktop experience along with secure private key handling.

Contents

1 Introduction

Blockchain technology has shown a great potential for disruption of multiple industries on a global scale. This is shown by the growing number of developer and business communities, which have sparked hundreds of new projects and ideas to life. But global adoption of the blockchain technology is still doubtful as the onboarding process imposes on users that wish to participate in the new economy a steep and unforgiving learning curve.

Research states that in the last few years smartphones are the primary device for going online instead of computers [10, 8, 9]. Comparing desktop computer, laptop and mobile device sales also shows that mobile device sales are growing with a far faster pace [5]. All this is happening while majority of the blockchain communities are building their products almost exclusively for the desktop environment.

The number of ERC20 tokens has also grown dramatically, each representing a local currency to be used by a respective community for payments of goods and services. But settling every and each micro-transaction on the blockchain separately can be extremely time and cost inefficient, thus slowing down the growth and adoption.

We believe that in order for the community to grow to a wider audience - a *base* for mobile platforms must be built first. The infrastructure, tools and SDKs developed by 0xBASE will enable dapp developers to grow and offer services with *instant* payments to their users on the devices they use the most - their mobile phones.

2 Existing work

The team at Aeternity [6] has recognized that the majority of the development in the blockchain space is focusing on other areas rather than mobile world. However, they've decided that the best approach is to build a completely new blockchain and bootstrap it from the ground up first. While they propose quite a few innovative solutions, the Ethereum[1] ecosystem is growing at a much faster pace [4, 7, 12, 3], hence we believe it is the logical platform to build upon.

There are several projects working on "layer 2" or "off-chain" solutions for the Ethereum blockchain such as Plasma[2] for scaling, Truebit[3] for complex computation and Raiden Network[4] using state channels for peer-to-peer secure off-chain payments. There has been also numerous attempts of mobile dapps, most notably the Trust Wallet[5], Ethos[6] and Stack[7].

Majority of computer browser based dapps rely on the user having installed Metamask[8] extension as it provides comfort, trust and security that would not be possible should the user be required to import his private key into every single dapp he uses. The importance of Metamask in the browser dapp landscape shows with over 1 million installs [11, 1]. Most of deployed dapps are now only accessible on desktop computers via Metamask as the only login and ETH wallet interaction plugin.

Web3js[9] and libraries for other programing languages (e.g. Swift[10] for native iOS and MacOS) are the go-to off the shelf solutions that most of the dapp developers turn to first. To access the Ethereum network the developers must setup either their own Ethereum node such as Parity[11] or Geth[12] or alternatively they rely on infrastructure provided by the Infura[13].

[1] https://www.ethereum.org/
[2] https://plasma.io/
[3] https://truebit.io/
[4] https://raiden.network/
[5] https://trustwalletapp.com/
[6] https://www.ethos.io/
[7] https://stktoken.com/platform-technology.html
[8] https://metamask.io/
[9] https://github.com/ethereum/web3.js/
[10] https://github.com/IndisputableLabs/Swiftheureum
[11] https://www.parity.io/
[12] https://geth.ethereum.org/
[13] https://infura.io/

3 0xBASE Platform

The 0xBASE platform consists of multiple layers of key infrastructure and tools that enable mobile dapp developers to develop native Android and iOS applications that support instant settlement of ERC20 token payments.

The following sub-chapters provide in-depth explanation of the 0xBASE architecture and the layers it provides:

- **0xINSTANT** - Secure and instant off-chain payment network
- **0xWALLET** - Wallet implementation sitting on top of 0xINSTANT payments network
- **0xSDK** - Android and iOS libraries providing services to mobile dapps
- **0xBRIDGE** - Bridge between the mobile wallet and the user's computer

3.1 Use-case

There are multiple cases when a payment of goods or services should be performed instantly in order to provide best possible user experience with as little friction as possible:

- Physical world
- Video streaming websites
- In-app and in-game purchases
- E-commerce and online stores
- Ticketing websites
- Payment systems
- Sharing economy

Each service or goods provider is a *merchant*. Merchants are, in order to provide their customers with a fast and secure payments, participating in the 0xINSTANT payment network. When a payment is required the merchant generates a payment request in their respective ERC20 token which the user has to confirm via the 0xWALLET application. The transaction fees are paid with BASE tokens and are set by the merchant or more specifically the settlement node provider. Merchants can also implement their own white-label wallets.

The confirmed payment is stored on the merchant's 0xINSTANT node. The node can periodically settle payments in bulk on the Ethereum network in order to save on gas fees. Upon successful settlement the merchant's node generates additional revenue by collecting payment fees in BASE token.

3.2 0xINSTANT

0xINSTANT is a Layer 2 scaling proposition for the Ethereum blockchain. Currently paying for goods and services with crypto-currencies is completely unoptimized for the fast paced world we live in. Paying with Bitcoin will take approximately 10 minutes for the transaction to be confirmed on the network, on Ethereum, new blocks are generated approximately every 15 seconds and this assumes user has paid a fee high enough to be included in the next block. During biggest congestion periods on the Bitcoin network users had to pay a fee of up to $ 50 to see a reasonable transaction times [2]. For some cases several block confirmations are needed to ensure the transaction was indeed settled. During congestion periods the confirmation time can be even longer thus making the crypto-currency based payments basically unusable in physical shops or environments where high throughput is extremely important.

We propose a new settlement mechanism that will enable new business models, reduce costs, eliminate the need for the middleman and trust in a central organization, while still providing the security and all benefits of the on-chain settlement. Additionally the proposed settlement mechanism will enable collection and payment of transaction fees in 0xBASE native token - BASE, meaning that the user initiating the transaction will not need to hold any Ether in order to perform purchases with any ERC20 token.

3.2.1 Protocol Overview

The Figure 1 depicts a protocol mechanics. User has to, in order to use ERC20 tokens in instant transactions, first make a deposit to the 0xINSTANT Smart Contract. For the ease of use, this deposit is masked to the user inside the 0xWALLET application as a simple toggle which enables any given ERC20 token to be used in instant payment transactions.

When a payment is required the merchants application first checks the balance of the users wallet in the 0xINSTANT Smart Contract and on the 0xINSTANT payment network. The public key was passed to the merchant via an arbitrary communication channel. If the user has sufficient balance, the merchant can proceed and generate a payment request which encapsulates the following data:

- ERC20 token to be used for payment
- Amount to be paid
- Customers public key
- BASE token amount to be paid as a payment fee - *optional*
- Merchants public address - where the funds will be routed
- Settlement node address - only that node is allowed to settle the transaction - *optional*

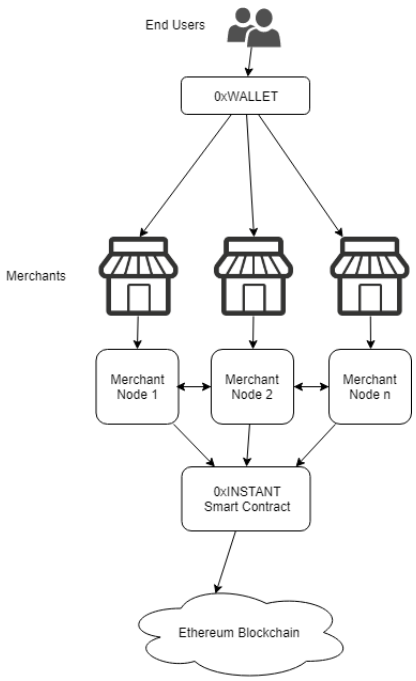

Figure 1: Protocol overview

The payment request can be passed to the 0xWALLET or any other wallet implementation through the arbitrary channel. User simply signs the transaction data through the wallet application with the private key and returns the signed data back to the merchant for settlement.

At this point the merchants has received a signed payment request, which is forwarded, after the signature has been verified, to the merchants settlement node. The settlement node periodically settles multiple payments via the 0xINSTANT Smart Contract.

The proposed payment flow enables new business models and disrupts the payment process entirely. It is giving the power of collecting payment processing fees to the hands of the merchant whereas usually the fees are taken either by the payment processor.

The payment process can be performed within a few seconds without the use of 3rd party trusted intermediaries and without providing additional stress on the Ethereum network - only the settlement is happening on-chain and it can be done periodically in bulk. Merchant keeps track of all the unsettled payments as he is the most incentivized party in the process to settle the transactions at some point in the future.

The key component in the whole process is ensuring that double spending is prevented. This is achieved as the nodes that participate in the network must share the unsettled payments within the 0xINSTANT payment network.

Mitigation of malicious nodes is described in the chapter Nodes.

3.2.2 0xINSTANT Smart Contract Overview

The 0xINSTANT Smart Contract will be written in Solidity[14] as it will be run on the Ethereum network. In general the Smart Contract will be split into two parts:

1. To be used by the Users
2. To be used by the Instant Nodes

The user faced smart contract will contain the implementation of the interface show in Code 1, while the 0xINSTANT nodes will contain several additional functions in order to settle transactions and handle network disputes in case of dishonest nodes. Please note that the code provided here should be basis for further development and research and only serves as a sign of general direction the research is heading.

```
1  contract InstantUsers {
2
3  function depositToken(address _token, uint256 _value) public
       returns (bool);
4
5  function requestWithdraw(address _token, uint256 _value) public
       returns (bool);
6
7  function completeWithdraw(address _token) public returns (bool);
8  }
```

Listing 1: Instant Payment Smart Contract Interface for Users

```
1  contract InstantNodes {
2
3  function depositStake(uint256 _value) public returns (bool);
4
5  function withdrawStake(uint256 _value) public returns (bool);
6
7  function settleTransaction( ...params ...) public onlyStakedNode
       returns (bool);
8
9  function settleTransactionBulk( ...params ...) public
       onlyStakedNode returns (bool);
10
11 function reportDispute(<TODO>) public returns (uint256) public
       onlyStakedNode returns (uint256);
12
13 function closeDispute(uint256 _disputeId)  public returns (bool);
14
15 function voteOnDispute(uint256 _disputeId, uint256 _vote)  public
       onlyStakedNode returns (bool);
16
```

[14] https://solidity.readthedocs.io/en/develop/

```
17  function defendDispute(...params...)  public onlyStakedNode returns
        (bool);
18  }
```

Listing 2: Instant Payment Smart Contract Interface for Nodes

3.2.3 Potential risks and mitigation

Replay attack: Replay attack is fully mitigated as the merchant cannot settle the same transaction twice since the Smart Contract stores a history of settled transactions or rather the hash of the settled transaction to a mapping.

```
1  // Mapping of already executed settlements for a given address
2  mapping(address => mapping(bytes32 => bool) executedSettlements;
```

Listing 3: Mapping of executed settlements

Stalled transactions: Merchant has a full control of the settlement node or at least in deciding who will perform the settlement if they wish to use a trusted intermediary. Since the merchant and both the node have the most incentive to settle a transaction in order to receive funds for provided goods and services, the number of unsettled or stalled transactions is controlled by the merchant himself.

User has no funds: All user funds are safely deposited in the 0xINSTANT Smart Contract, providing a secure way for merchants to assess whether the user has enough balance to cover the payment. Potential risk comes from the 0xINSTANT network in case a malicious node is not communicating it's pool of unsettled transactions to other participants in the network.

Such behaviour is detected by other nodes the moment the malicious node tries to settle a transaction it has not reported to others. The protocol defines a voting mechanism where honest nodes report a malicious node. If the vote passes the malicious node loses its stake and cannot participate in the network.

51% Attack Since nodes vote on each other there is a possibility for a 51% attack, where a bad actor controls 51% of the nodes and accuses an honest node of being malicious and can thus effectively steal its stakes. We propose to address this severe issue by giving an opportunity to a node to defend itself and win a dispute by proving that it has indeed shared the unsettled transaction within the network. When a node sends an information about new unsettled transaction to its neighboring nodes in the 0xINSTANT network, it is expected of those nodes to sign this information with their private keys and send it back to the source node as an evidence of receipt. With these signed replies the disputed node can prove that it has shared it's pool of unsettled transactions to other nodes in the network.

Since this same mechanism could potentially also be abused by the malicious cluster of nodes further research will be performed and voting mechanism will

also include the node scoring and vote weighting based on the number of settled transactions, node age and other parameters.

The 100% trust between the nodes cannot be guaranteed but we believe that this issue will be mitigated also by the fact that different merchants will use a variety of ERC20 tokens for payments and the only damage the malicious node can inflict is in case that the same user also performs a payment to a different merchant and the second merchant fails to settle the transaction before the malicious one - all this is accounting that user does not have enough balance to cover the second payment. Even in this case the honest merchant still holds the signed payment request which can be settled at any time in the future when the user deposits new funds. The financial effort to effectively cause damage to the honest nodes is growing dramatically with the size of the network and number of previously settled transactions as the attacker needs to deploy enough nodes with reputable history in order to cause relatively small damage since the general intention of the 0xINSTANT payment network is to provide the infrastructure that can handle micro-transactions effectively.

3.3 0xWALLET

0xWALLET serves as the starting point for end-users as a source of trust and familiarity. The wallet provides all the usual features of an Ethereum wallet and offers users the security similar to the hardware based wallets such as Ledger Nano S or Trezor through the secure chip (SC) available on both Android and iOS.

0xWallet supports:

- Ether token transfers
- ERC20 compatible tokens balance tracking
- ERC20 compatible tokens transfers
- 0xINSTANT protocol integration

The wallet will serve the community in a similar fashion as the Metamask or MyEtherWallet serves on the desktop environment - an easy to use and safe way to interact with the Ethereum ecosystem, while also providing a reference implementation of the 0xINSTANT payment protocol.

3.3.1 Security

In crypto, security is everything. Keeping your private key private is the first thing a wallet provider needs to take care of. The 0xWALLET securely stores your Ethereum private key with the platform's secure storage provider, on Android that is the *AndroidKeyStore* provider, which stores your private key in a secure chip. The same tactic is used on iOS with *Secure Enclave*.

The secure chip in mobile devices takes care of storing your key outside of user memory and unlocking it for use only when the user is authenticated with a

fingerprint, pattern, or a passcode; because of that, the user will be required to have his or her device locked. 0xWALLET will also provide with a screenshot protection and will put your device into Airplane mode for the duration of Ethereum wallet creation. Rooting or jailbreaking your device will make it vulnerable to many different vectors of attack, including the OS not being able to provide a secure storage for the private key, since we know that many power users will still want to have their device unlocked we will just display a warning, so the user can still use the wallet at his or her own risk.

3.4 0xSDK

0xWALLET provides a set of APIs offered to Android and iOS developers via an SDK written in their respective language - Java/Kotlin and Swift. APIs and SDKs provide developers with a set of tools that they can use to kickstart their project and move their community to the mobile devices at a faster pace. This new standard is needed as the current state of the art requires users to import their private key into each mobile dapp they intend to use, which brings several issues for both app developers and it's users as well as businesses trying to provide services on the blockchain:

- **Security**: Every app developer must solve the same set of issues regarding the security of storing and handling private keys. Users risk losing all their assets to a single malicious mobile dapp,
- **Transparency**: in order to prove the app handles the keys in a safe and secure manner code should be open source, which is not always preferable when there is some proprietary IP involved,
- **Barrier to entry**: since users must import their private key, the barrier to entry is quite high as the drop-off rate at this point is significantly high.

SDK libraries are developed and updated in tight cooperation with the feedback from the community and are divided into following categories:

- **Passive APIs**:
  - Obtaining user's public address
  - Standard Web3 API
- **Active APIs**:
  - Requesting user to sign data
  - Requesting user to perform a transaction of a desired token to a specific address

Developers are able to use passive APIs without disrupting user flow of the application unless explicitly a permission is needed - i.e. obtaining user's

public address as we deem this information should *not* be shared *without user's consent*, especially since the 3rd party app could also pair this data from other sensors such as GPS.

Active APIs always redirect the user from the current app to the 0xWALLET and require users confirmation of every transaction.

3.5 0xBRIDGE

We realize that power users prefer to use dapps on their desktop and laptop devices as well. The Chrome and Firefox plugin - 0xBRIDGE, will be as the name suggests the bridge between users mobile device and his browser.

0xWALLET on the mobile device will act in a similar fashion as hardware wallets like Ledger Nano S or Trezor act today. The private key is stored on the mobile phones Secure Chip. Dapp can request transactions or signatures to be made through the 0xBRIDGE APIs . User simply confirms or denies the transaction on the mobile device. The users private key never leaves the Secure Chip present on the mobile device.

This ensures additional layer of security compared to todays solutions, where the private key of the users wallet must be stored within the plugin.

4 0xBASE Token

0xBASE token is based on the ERC20 standard[15]. The token details are:

- **Total supply:** 1.000.000.000
- **Supply:** Fixed
- **Symbol:** BASE

4.1 Token Usage

The token serves as a fuel enabling fast, cost effective and secure off-chain instant payments through the 0xINSTANT payment network.

The token generates revenue for the merchants 0xINSTANT node. A certain amount of BASE tokens is required in order for the merchant to run a 0xINSTANT node - the security deposit made by the merchant enables him to participate in the network and serves as a stake that incentivizes the node to play by the rules and inform other nodes about it's activities.

[15] https://theethereum.wiki/w/index.php/ERC20_Token_Standard

References

[1] Firefox Add-ons. *MetaMask*. URL: https://addons.mozilla.org/en-US/firefox/addon/ether-metamask/?src=search. (accessed: 12.03.2017).

[2] BitInfoCharts. *Bitcoin, Ethereum Avg. Transaction Fee historical chart*. URL: https://bitinfocharts.com/comparison/transactionfees-btc-eth.html#1y. (accessed: 12.03.2017).

[3] State of the ĐApps Blog. *800 DApps! A non-stop Decentralized Growth!* URL: https://blog.stateofthedapps.com/800-dapps-a-non-stop-decentralized-growth-a8e5ac45e33e. (accessed: 12.03.2017).

[4] Gencer A. E. Basu S. Eyal I. Renesse R. e. G. Sirer. *Decentralization in Bitcoin and Ethereum Networks*. URL: https://arxiv.org/pdf/1801.03998.pdf. (accessed: 12.03.2017).

[5] Gartner. *Forecast: PCs, Ultramobiles and Mobile Phones, Worldwide, 2015-2021*. URL: https://www.gartner.com/newsroom/id/3816763. (accessed: 09.03.2017).

[6] Malahov Y. Hess Z. and J. Pettersson. *Æternity blockchain*. URL: https://aeternity.com/aeternity-blockchain-whitepaper.pdf. (accessed: 12.03.2017).

[7] Huffpost. *Rise of Ethereum: A New Blockchain Juggernaut*. URL: https://www.huffingtonpost.com/entry/rise-of-ethereum-a-new-blockchain-juggernaut_us_590b1229e4b05279d4edc304. (accessed: 12.03.2017).

[8] Ofcome. *International Communications Market Report 2017*. URL: https://www.ofcom.org.uk/__data/assets/pdf_file/0032/108896/icmr-2017.pdf. (accessed: 09.03.2017).

[9] Statista. *Percentage of all global web pages served to mobile phones from 2009 to 2018*. URL: https://www.statista.com/statistics/241462/global-mobile-phone-website-traffic-share/. (accessed: 09.03.2017).

[10] StatCounter Global Stats. *Desktop vs Mobile vs Tablet Market Share Worldwide*. URL: http://gs.statcounter.com/platform-market-share/desktop-mobile-tablet/worldwide. (accessed: 09.03.2017).

[11] Chrome Web Store. *MetaMask*. URL: https://chrome.google.com/webstore/detail/metamask/nkbihfbeogaeaoehlefnkodbefgpgknn. (accessed: 12.03.2017).

[12] TechCrunch. *How Ethereum became the platform of choice for ICO'd digital assets*. URL: https://techcrunch.com/2017/06/08/how-ethereum-became-the-platform-of-choice-for-icod-digital-assets/. (accessed: 12.03.2017).