IDA Pay - Whitepaper

09.03.2018 - v0.9

Abstract

This whitepaper aims to bring to the public the vision of the development team, in relation to the very much fragmented world of cryptocurrencies. Many problems have been identified with the current ecosystem and this project proposes a path to an inclusive solution for many players in the industry. As more currencies are being released every day, each with their own objectives and use cases, investors and users are forced to choose and spend considerable time analyzing the advantages of one coin over the other. Next, starts the process of obtaining the respective coins, through ICOs, direct sales and other unofficial channels (eg. exchanges, person-to-person trades). IDA Pay wishes to bring to the industry a decentralized and reliable way of exchanging coins between organizations and people. In technical terms, the team will develop an easy to integrate atomic swap module, including an API and protocol for inter-blockchain communication. This module will be compatible with all cryptocurrencies having a Masternode implementation.

Introduction

IDA Pay is a peer-to-peer, decentralized cryptocurrency offering secure and private transactions as well as a governance voting system. The project's purpose is to lead the industry by constantly working towards the following four goals of our community coin; **community involvement, research and development, value appreciation** and **mass adoption**. We think that all these goals are closely interlaced and depend upon each other, we also think that the community will be first to decide which paths will be taken to achieve constant improvement.

IDA Pay provides an integrated Governance system that can be used to pass proposals; it is imperative to make use of such system for any direction that needs to be taken, be it the approval of funds for a new side projet or the nomination of a new core team member. This system is versatile and allows all types of proposals to be debated and voted upon.

The above mentioned feature is provided thanks to dedicated full nodes that share a specific stake; these are called Masternodes. They enable a set of functionalities available to the community; Governance, InstantSend and PrivateSend. In return for these services, they receive certain rewards on every block mined.

Lastly, as with any PoW coin, miners support the blockchain by creating its blocks. They also receive a reward in return, although this reward will decrease to leave place to Masternodes.

1.1 Technical Specifications

Ticker: IDA

Max Supply: 21 000 000

Coinbase maturity: 15 blocks

Target block time: 2.5 minutes

Block Reward = 18 IDA

PoW algorithm: X11

Masternode collateral: 1500 IDA

1.2 Problem

Invented by Satoshi Nakamoto in 2008 and popularized with the Bitcoin, the blockchain revolutionized the way we think of finances, it also brought a panoply of use cases. There is an outstanding adoption of the masses currently on going, every day we find new ways of utilizing the blockchain to make our processes more efficient, secure and decentralized. This has also brought a new supply of cryptocurrencies to the market; these coins all have different objectives and missions, we commonly call them altcoins (Alternate coins).

Although these altcoins are all different, they also share a common objective which is to achieve adoption and increase number of users. This brings many challenges to both the coins and the users. An individual or organization can only "join" the coin by buying its tokens; unfortunately this process can be far from easy and secure.

As the Bitcoin is the currently the currency of choice for trading altcoins, the process of obtaining a coin is commonly a two-step process:

1. Convert fiat or other coin into Bitcoin.
2. Convert Bitcoin into desired coin.

This process is not ideal, mainly because it brings risks and can be tedious.

1. Safe exchanges are not always available. People have lost access to their coins while trading in them.
2. Not all coins are available on all exchanges. A user might need to use two or more different exchanges to be able to obtain the desired coin.
3. New coins are not always available on exchanges, this forces users to go through different routes provided by the coin's community:
    i. Sale of coins by the owners.
    ii. Trading among community members. This requires outside escrow which is not always used, users have been scammed on both sides.

1.3 Proposed Solution

A decentralized, peer-to-peer, distributed atomic swap system can securely achieve this process in a single step: convert any coin into any coin.

There are three phases to the proposed solution, these can be considered evolutions of the product:

1. Alice contacts Bob to find an agreement on the price and amount of the trade. Users will need to manually exchange transaction information.
2. Alice connects to Bob's blockchain to find current offerings or post a new offer. Users still need to exchange transaction information.
3. Alice and Bob can now complete the trade without exchanging any information, by simply finding the right offer and initiating it.

2. Cross-chain atomic swap implementation

2.1 Background

Satoshi Nakamoto invented the Bitcoin with the vision that it would be a fully peer-to-peer system that would not use any centralization or third party regulation, almost all aspects of the Bitcoin (and other coins) do follow this requirement, except for trading platforms. An exchange is simply an entity that provides the service of connecting two people with matching trading objectives. The exchange then takes the amounts from each party into its own servers and updates the respective accounts with the new amounts. They commonly charge a fee for this service. Ideally, these two parties would simply connect with each other and proceed with the trade.

The atomic swap is not a new concept, this subject has been discussed for the past years with the rise of alternate cryptocurrencies (eg. Litecoin, DOGE, Ethereum). Some proof of concepts have been shown to work relatively well, although no concrete implementation has taken place yet. Also, it should be noted that discussions always seem to forget altcoins with lower market capitalization; a good example is Dash, the subject has only been seriously brought at the end of 2017 when price rose to new heights, although no steps have been taken publicly to bring a complete solution.

2.2 Implementation

An atomic swap is a trade between two users, a *cross-chain* atomic swap is a trade between two users from different blockchains, different crypto-currencies. The proposed implementation would require both

blockchains to run an additional module; although this module will not have any effect on consensus rules, thereby not needing a fork. The main reason for such an implementation is the requirement to dismiss any third-party interaction, everything can be done from within and in a peer-to-peer manner.

The main principle behind this solution is the generation of trustless smart contracts between both parties. A smart contract is a transaction agreement that is enforced by the blockchain itself, without the need for a central authority. These blockchain contracts include all the information to complete the trade accordingly, or refund the funds to each party if one of them does not follow the agreement in place.

Let's say we have two users, UserA and UserB, on different blockchains, ChainA and ChainB; UserA would like to sell X coins from ChainA and receive Y coins from ChainB. The terms of the agreement are already known and users will now proceed with the trade.

A) Contract Creation and Validation

1. UserA starts the transaction by creating and funding a contract on ChainA.
2. UserB receives the contract and verifies it.
3. UserB creates another contract on ChainB.
4. UserA receives the contract and verifies it.

As part of the verification, many parameters have to be validated; time limit, value and address. Then, the contract created by UserB needs to retain the same secret hash that was published by UserA's contract, this will guarantee, for instance, that a refund will be possible.

The contract transfer method between parties should be transparent, it should be done inside the solution itself. A discussion of possible channels will follow.

At this point, both users have paid into their contracts. The exchange needs to take place.

B) Contract Execution and Redemption

1. UserA withdraws the funds from the contract on ChainB using the secret.
2. UserA publishes the secret to UserB.
3. UserB withdraws the funds from the contract on ChainA using the secret.

UserA will always be first to withdraw the funds since only he has the secret, this is partly why a time limit (LockTime) is used; if UserA does not provide the secret, the transaction will be refunded. Same applies to UserB, if he does not create and fund his contract, the original transaction can be refunded.

2.3 Proof-of-concept

A working proof-of-concept is being developed and will be published. The underlying concepts behind the sequence of events explained above will be put into practice between IDAPAY and another chosen altcoin. This will be used to simply show that the ideas expressed are transferable to a technical form and that the project's main objective is feasible.

2.4 Product development

As soon as the proof-of-concept is completed, submitted and reviewed by all community members, the final product

development will make its debut, in an iterative manner.

Initial simple trading solution (v0.1)

The first iteration of the product will include facilities for simple trading between IDAPAY and a community chosen altcoin. This will include all CLI and GUI commands for successful exchange.

Initially, the parties will have to find each other through external systems and manually exchange data through other mediums (eg. email, discord, etc), notably the transaction hash. This data will need to be entered in the tools developed by the project for completion of the trade.

Peer-to-peer interchain trading listing solution (v0.2)

Upon release of this iteration, it will be possible to find current offerings by simply using the tools developed by the project. The user will be able to retrieve a list of real-time offerings (sell) available on the other coin's blockchain. The user will be able to communicate with the other party, through an external medium, and initiate the exchange of trade information.

Peer-to-peer interchain full trading solution (v0.9)

The user will be able to find offerings and proceed to a trade without the need to communicate with the trading party, all will be done automatically and a real-time status will be available throughout the process.

This is the final iteration to a fully functional inter-blockchain atomic swap solution, this release will integrate a fully capable transparent and peer-to-peer trading system, without the need of a third-party solution.

2.5 Inter-blockchain communication protocol

A key feature of the product will be the capability to transfer the important data between blockchains; this can all be encapsulated inside the smart-contract, although some required information is needed on both sides before a contract transaction can be created and submitted.

Data through current JSON-RPC protocol

Current Bitcoin Core and the majority of altcoins provide an RPC interface using JSON. By modifying the current API, it would be possible to quickly and easily provide the needed functionalities to implement most of the project's features. The downside to this would be the necessity to manually enter the IP address of the trading party as there would be no central server that would contain this information.

Data through Masternodes

Many new coins provide a Masternode feature; the project could capitalize on this as their main utility is to add new features to the network. Also, these communicate through their own network, we could make use of this by including our own messages to the protocol. The downside to this would be that not all altcoins will be compatible, but as most of these are based on Dash, a vast market could certainly be reached.

References

Nakamoto, S., 2009. bitcoin.org. [Online]
https://bitcoin.org/bitcoin.pdf

Hearn, M., 2011. Bitcoin Wiki. [Online]
https://en.bitcoin.it/wiki/Bitcoinj

Dash Whitepaper, 2017, [Online]
https://dashpay.atlassian.net/wiki/spaces/DOC/pages/5472261/Whitepaper

Atomic cross-chain trading, 2018 [Online]
https://en.bitcoin.it/wiki/Atomic_cross-chain_trading