Valence: A Protocol for Trustless Decentralized Cryptocurrency Exchange

Karim Helmy
karim@valex.io

December 8, 2017

Abstract

Current systems for exchanging cryptocurrencies depend on a trusted third party, an inherent systemic flaw. The Valence protocol describes a system for trustlessly exchanging cryptocurrencies on different blockchains in a decentralized manner. By leveraging cross-blockchain atomic swaps and order-match-based mining to establish a decentralized exchange, the Valence protocol allows anonymous parties to exchange currencies without communicating. While Bitcoin and Ethereum, the two largest cryptocurrencies by market cap, are of particular interest, the proposed system is extensible, allowing the addition of arbitrarily many cryptocurrencies. The Valence protocol delineates a system that gives the advantages of a centralized exchange, namely providing liquidity and convenience, while eliminating counterparty risk.

Contents

Introduction

Centralized and Decentralized Exchanges

The function of an exchange is to act as an intermediary for parties wishing to trade assets, eliminating the problem of searching for a counterparty. In a centralized exchange, this function is performed by a single actor, who traders must trust to provide fair pricing information and faithfully execute the trade. Centralized exchanges dramatically decrease counterparty risk for traders by requiring only that they trust the exchange. This model has been carried over from traditional exchanges to those specializing in cryptocurrencies, forming the backbone for most large cryptocurrency exchanges including GDAX, Bitfinex, and Kraken.

Despite their advantages, centralized exchanges provide a single critical point of failure, even in interactions that would otherwise be trustless. This deficiency is not merely theoretical but practical, having been a factor in insolvency scares like the one experienced by Poloniex,[1] and more dramatically, economic crises such as the collapse of the Mt. Gox Exchange.[2]

To counteract the flaws of centralized exchanges, there is a growing movement to adopt decentralized exchanges as an alternative. Decentralized exchanges have no central clearing house, eliminating the risk associated with a centralized exchange. A prerequisite technology for such an exchange is the atomic swap, which enables trustless transactions. However, many of the existing decentralized exchanges, are not completely trustless and rely on a centralized actor for certain roles, such as the distribution of market prices.[3]

Furthermore, there is not yet a totally or even partially trustless cross-blockchain decentralized exchange. This paper outlines a stable and trustless decentralized cryptocurrency exchange leveraging atomic swaps as the primary transaction mechanism.

Atomic Swaps

Atomic Swaps: Concept and Current Status

The purpose of an atomic swap is to allow safe transactions between two parties who know of but do not necessarily trust one another. The first atomic swap between the Ethereum and Bitcoin blockchains was performed on October 7, 2017.[4]

There is already considerable financial infrastructure utilizing atomic swaps on the Ethereum blockchain.[5] However, a cryptocurrency exchange that leverages this technology does not yet exist.

Atomic Swaps: How They Work

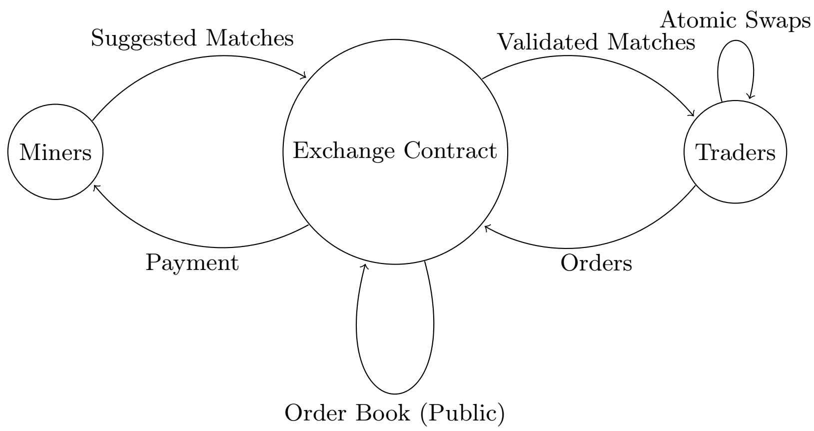
An atomic swap is a smart contract structured such that each party's ability to access the asset offered by their counterparty is dependent on the transfer of their own asset to either the contract or their counterparty.

Consider a case in which Alice wants to buy Ether from Bob in exchange for Bitcoin. She writes a smart contract specifying the terms of the swap. The contract requires Bob to send it the negotiated amount of Ether, which is only sent to Alice when she sends Bob the specified quantity of Bitcoin. If Bob does not receive Bitcoin from Alice within a specified window of time, his Ether is returned to him. In effect, the contract serves as an escrow who cannot defect from the agreed-upon terms.

Valence: General Architecture

The Valence protocol uses atomic swaps to allow the trustless exchange of cryptocurrencies on different blockchains. Orders are sent by prospective traders to the exchange. Miners on the network then match orders, and are rewarded for their matches by receiving a percentage of the transaction fees from that trade. Using an atomic swap, the matched parties then trustlessly exchange their respective currencies with a smart contract provided by the exchange. A visualization of Valence's process is shown below.

[1] https://cointelegraph.com/news/rumors-of-insolvency-circulate-among-users-of-bitcoin-exchange-poloniex-support-slow
[2] https://dealbook.nytimes.com/2014/02/28/mt-gox-files-for-bankruptcy
[3] https://kyber.network/
[4] https://news.bitcoin.com/altcoin-exchange-performs-first-atomic-swap-between-bitcoin-and-ethereum/
[5] https://www.airswap.io/



Order Matching

Orders contain specifications on the currencies to be exchanged, volume, addresses of the trader, and price limit. Orders are also sent with a predetermined amount of Ether to pay for gas and fees. The fees required are proportionate to the volume ordered, and partially refunded if the order is cancelled. These orders are submitted by traders to the exchange, which then stores them in a public order book. Miners can access this information to make matches, which are then executed as trustless trades.

The task of finding appropriate order matches is delegated to miners. These matches are then verified by the exchange. Matches are made such that the net exchange between currencies is within a specified margin as a percentage of the trade volume. The uncleared volume is reentered into the order book. Limits must also be non-contradictory. Matches found are rewarded according to the volume of currency exchanged in the transaction. To prevent attacks, miners will initially pay for any gas cost incurred in the network's verification of their proposal. This will be refunded on successful validation of the proposed match and instead paid for by the trading parties. Much like the factorization problem used in Bitcoin mining, the verification of a proposition is much less computationally demanding than the generation of a correct solution. This is because the matching problem used in the Valence protocol reduces to a subset-sum problem, which, like the factorization problem, is NP-complete.

Token

A key component of an implementation of the Valence protocol is an ERC20-compliant token issued on the Ethereum platform. The initial supply of this token is implementation-specific.

Each token grants its holder the right to a transferable vote on development decisions relevant to the platform. The inclusion of voting rights adds longevity to the system by allowing it to adapt to external changes. For example, a rise in popularity of a new cryptocurrency could be capitalized on by the addition to the exchange of transactions on that currency. Their transferability enables participation rates to remain sufficiently high by allowing miners who are less interested in the active development of the platform to transfer their voting rights to a more involved party. To prevent a majority coalition from abusing their amendment rights, all changes will be subject to a waiting period before being enacted. Token holders are also entitled to dividends, which come from the exchange's profits from collecting trading fees. Dividends are distributed at random intervals to reduce transactional costs and lower volatility.

Examples

Example 1: A Simple Transaction

Alice wants to buy 14 Ether for at most 1 Bitcoin. Bob wants to buy 1 Bitcoin for at most 16 Ether. Mary the miner's job is to match orders.

Alice submits her order, shown below, to the exchange:

Unit	ETH-BTC
Quantity	14
Unit Limit	0.07
Buy Address	0xFAc1f70C0f03Da4f67d...
Sell Address	1A1zP1eP5QGe...
Order ID	ALICE

Bob also submits his order to the exchange:

Unit	BTC-ETH
Quantity	1
Unit Limit	16
Buy Address	1XPTgDRhN8RFnzn...
Sell Address	0xACc1e6900d0eDE4fE8d...
Order ID	BOB

The exchange adds both orders to their order book, which already contains some orders:

Unit	BTC-ETH	ETH-BTC	ETH-BTC	BTC-ETH
Quantity	2	33	14	1
Unit Limit	16	0.07	0.07	16
Buy Address	1MCDMrgRyKnhnMhqiWC...	0xfbb1b73c4f0bda4f6...	0xFAc1f70C0f03Da4f67d...	1XPTgDRhN8RFnzn...
Sell Address	0x30caa9e296276...	1AMXYgrRgNnxnMNNi...	1A1zP1eP5QGe...	0xACc1e6900d0eDE4fE8d...
Order ID	CAROL	DAVE	ALICE	BOB

Mary sees that the order book has been updated and matches Alice and Bob's orders. She suggests this match to the exchange at a mutually acceptable exchange rate, 15 Ether per Bitcoin. The match is valid, so the exchange gives Mary a portion of the fees it receives from Alice and Bob. The exchange then creates an atomic swap contract for Alice and Bob, who trustlessly trade. Their entries in the order book are cleared.

Example 2: A Transaction with a Remainder

After Alice and Bob's transaction is cleared, only Carol and Dave's orders are still in the order book:

Unit	BTC-ETH	ETH-BTC
Quantity	2	33
Unit Limit	16	0.07
Buy Address	1MCDMrgRyKnhnMhqiWC...	0xfbb1b73c4f0bda4f6...
Sell Address	0x30caa9e296276...	1AMXYgrRgNnxnMNNi...
Order ID	CAROL	DAVE

As before, Mary suggests a match between Carol and Dave's orders at an exchange rate of 15 Ether per Bitcoin. There's a slight problem, though: this exchange rate leaves Dave's order with three remaining Ether on the order book. On validation of the match, however, the exchange finds that as a percentage of the total trade this deficiency is within its implementation-specific margin for error. Then the exchange rewards Mary for finding the match, and creates a smart contract for Carol and Dave to trade. Carol's order is cleared, while the remainder of Dave's order is reentered into the order book. The order book, shown below, now only contains the remainder of Dave's order.

Unit	ETH-BTC
Quantity	3
Unit Limit	0.07
Buy Address	0xfbb1b73c4f0bda4f6...
Sell Address	1AMXYgrRgNnxnMNNi...
Order ID	DAVE

Challenges and Resolutions

Latency and Scalability

A significant challenge faced by exchanges is maintaining low latency as the system scales. The system outlined by the Valence protocol should prove to be highly scalable. Updating the order book is inexpensive, and the on-blockchain operational cost is constant. Because few operations are performed on the blockchain by the exchange, the latency of transacting will be competitive with that of a centralized exchange.

To further increase efficiency at scale, we recommend the establishment of a convention whereby miners attempt to match trades of volumes proportionate to their computing power. This convention dramatically lowers the number of colliding suggested trades and decreases the latency with which orders are matched, increasing expected transactional value for both miners and traders. From a game-theoretical perspective, the strategy of adhering to the convention is evolutionarily stable, in that no party has an incentive to defect from the convention. Miners will not choose to match orders of lower value than their assigned bracket, because the yields will be lower. Similarly, they have no reason to match orders of a higher value than their assigned bracket, because they will be consistently be outpaced by competitors with more computing power.

Market Manipulation by Miners

Public order books have been criticized for enabling miners to front-run existing orders by placing their own orders and matching them.[6] Because orders are public, and not exclusively visible to miners, this analogy to classical front-running is fallacious. In reality, trading miners provide liquidity using only publicly available information, in a manner more akin to high-frequency traders on classical exchanges. Placing price limits on orders is always best practice, especially on an exchange with a public order book, but miners are in no way empowered to match orders that are not consensual for all parties involved.

Message Forgery

After making a match, miners diffuse their message to the exchange through the network. This presents an opportunity for other miners to take credit for making the match, rapidly diffuse this forged message, and receive payment for the match if the forged message is accepted by a majority of nodes. To counteract this potential abuse, we recommend the inclusion of a cryptographic nonce in the miners' message to the exchange, composed of a hash of the miner's public key and specifications for the trade. Creating this hash is a more complex operation than simply substituting the true key for the forger's key, so the inclusion of this nonce will slow down forgers, giving the true miner a more significant head start in diffusing the message and ensuring that the finder of the match is paid. The hash will be verified by the exchange on receipt of the message, and payment for the match will be withheld if the provided nonce is not equal to the hash of the relevant values.

Barriers to Entry

Atomic swaps do not support fiat currencies. Because the Valence protocol depends on atomic swaps, it cannot facilitate transactions involving a fiat currency. While this is a significant entry barrier for parties not holding cryptocurrencies, fiat currency transactions inherently require trust, so this deficiency is inevitable in a trustless system.

Additionally, because the exchange is implemented as an Ethereum smart contract, traders must possess a small amount of Ether to be able to pay transaction fees. This shortcoming is potentially problematic for smaller participants, but should not be an issue for more sophisticated traders, who tend to hold positions in both Ether and Bitcoin. To overcome this barrier, prospective traders with no Ether can perform a small transaction with a known broker, using information acquired from a Valence implementation's recent transactions for pricing data. They can then use the Ether acquired from this transaction to obtain a larger quantity using an implementation of Valence.

Because of its design as a completely trustless system, the outlined protocol does not require traders or miners to register. This removes a significant entry barrier faced by centralized exchanges.

Competition

An implementation of this protocol would also compete with other planned decentralized cryptocurrency exchanges such as KyberNetwork. Often, however, these exchanges primarily aim to

[6] `https://swap.tech/whitepaper/#order-books`

support trading Ethereum tokens, with cross-blockchain transactions as an afterthought. In the case of KyberNetwork, for example, there is no plan to support cross-blockchain trading until 2019.[7] Additionally, KyberNetwork depends on a reserve-management model, which poses significant security risks and is potentially prone to exchange rate fixing by malevolent reserve managers.[8]

Existing and planned token exchanges like AirSwap, Bancor, and 0x are orthogonal to Valence, and would not compete with a Valence implementation. Atomic swap contracts for exchanging tokens on the Ethereum blockchain are significantly different from those for cross-blockchain transactions, so for any of these exchanges to expand into competing with a Valence implementation would be a substantial undertaking.

Dark pools such as OmegaOne serve an adjacent but separate role from Valence.[9] Due to their high barriers to entry, they are largely inaccessible to even sophisticated traders without an agreement with a specialized broker. Furthermore, because OmegaOne is not a freestanding exchange, but rather splits up large orders it receives and distributes them among various exchanges, its relationship with Valence would actually be a mutualistic one, so the success of either would be beneficial to the other.

Conclusion

The Valence protocol outlines the creation of a decentralized cryptocurrency exchange using atomic swaps for trustless trades. this protocol has high value if faithfully implemented, and, utilizing technologies that are novel for an exchange, fixes the serious issue of counterparty risk in its domain.

[7]`https://kyber.network/#roadmap`
[8]`https://kyber.network/assets/KyberNetworkWhitepaper.pdf`
[9]`https://omega.one/`