Autonomous cross-chain exchange

Secure realtime trading between all cryptocurrencies is now possible.

swopblock

WHITE PAPER

MORE INFO:
swopblock.org
info@swopblock.org
github.com/swopblock
@swopblock

ABSTRACT

Swopblock is an intermediate cryptocurrency providing a medium of exchange between other cryptocurrencies. Security has been a major problem with cryptocurrency exchange and since the beginning more than 800,000 bitcoins have been stolen. Today they would have a market value measured in billions of dollars. Swopblock offers a new and secure exchange protocol that enables it to perform as an intermediary cryptocurrency in exchange transactions that are secured in a blockchain. This avoids the need of placing unsecured deposits in the hands of a third-party exchange center. Swopblock is the medium used to conduct cryptocurrency exchange without the involvement of a third-party thereby locking the trade against theft.

INTRODUCTION

Mt. Gox was a bitcoin exchange based in Japan that launched in 2010 and three years later was handling over 70 percent of all bitcoin transactions worldwide as the largest bitcoin intermediary. Mt. Gox had been entrusted with hundreds of thousands of bitcoins, but they went missing; they were stolen over time starting in late 2011. Since then many other exchanges have also been the subject of crypto coin thefts worth hundreds of millions of dollars resulting in market value instability for the cryptocurrencies involved and giving the impression that the cryptocurrencies themselves are insecure. Forbes magazine reported for the year 2018 that nearly one billion dollars in cryptocurrency went missing.

INTRODUCTION

(continued)

Current blockchain technology provides security for cryptocurrencies, but this security only protects cryptocurrency holding and transfer and does not protect exchange. The primary security flaw in current cryptocurrency exchange is that in addition to the two parties involved in an exchange, there is an exchange center that is a third-party intermediary in the exchange. This third-party, holds value on behalf of customers wishing to make exchange between cryptocurrencies. The security of that value is not under the control of the exchange customers who own that value. This central exchange paradigm requires exchange customers to trust the exchange center with their funds until they receive funds back in the form of another cryptocurrency. This allows a window of time in which the funds could go missing. Even if these funds were secure against external hacks, they would not be safe from exchange center insiders transferring these funds elsewhere.

Yet nearly all exchange is conducted with centralized exchanges. What is needed is a distributed exchange system based on blockchain technology that provides security for the cryptocurrency exchange transaction, just as blockchain technology provides security to the individual cryptocurrency transactions. This requires a protocol that can be validated in a blockchain network that secures the cross-chain exchange.

PROTOCOL

The Swopblock protocol provides the means to conduct a secure and transparent multi-cryptocurrency exchange market.

Consider a current market order that will offer a quantity of BTC (b) in exchange for a protocol determined quantity of ETH (e).

Let a pool of BTC (B) be computed as the sum of all previous BTC offers still valid or potentially available for settlement of the current market order. Now the current market order will, upon completion, increase the pool of BTC and the available coin (B) will be increased to include the BTC offered in the current market order (B + b).

Let a pool of ETH (E) be computed as the sum of all previous ETH offers still valid or potentially available for settlement of the current market order. Now the current market order will decrease the pool of ETH and the available coin (E) will be decreased to exclude the ETH that will be used to settle the current market order (E - e).

(continued)

Now, the protocol requires that the ratio of (B + b) / (E - e) after the settlement of the current market order be equal to the ratio (b / e). This requirement makes the exchange fair because the price of the exchange equals the price of the liquidity pools, it sets up a stable feedback loop between supply and demand and allows anyone to freely participate in cryptocurrency exchange. The protocol deterministically calculates the protocol price as the optimal price for the current market order as follows:

Exchange ratio equality:

$$\frac{B+b}{E-e} = \frac{b}{e}$$

How a protocal exchange is calculated:

B, b and E are given, solve for e

$$e(B+b) = b(E-e)$$

$$eB + eb = bE - be$$

$$eB + 2eb = bE$$

$$e(B+2b) = bE$$

$$e = \frac{bE}{B+2b}$$

This calculation governs all exchange transactions and because anyone can participate in all aspects of the protocol, whether just a customer wanting to buy lunch or a financial interest suppling liquidity, the exchange is fair and no one party has a monopoly in the Swopblock exchange market. In most exchange markets the filling of orders is a function of the price of the bid and the price of the ask such that when the price of the bid is equal to or larger than the price of the ask the two orders involved are filled after an order match has been determined by the central exchange. However, here, the Swopblock protocol will operate for multiple cryptocurrencies at once and each trade will execute based on the volume of exchanges that develop overtime. This enables a completely deterministic trade price execution that is conducted on and between two Swopblock enabled blockchains.

Swopblock Takes are used to provide another cryptocurrency in exchange for Swopblock and Swopblock Gives are used to provide Swopblock in exchange for another cryptocurrency. This is the means by which Swopblock becomes the medium of cryptocurrency buying, selling and exchange.

SWOPBLOCK TAKE

A Swopblock Take is taking a protocol calculated amount (s) of SWBL and giving an amount (x) of one of the trading enabled cryptocurrencies in exchange. The amount taken is determined by a calculation that is a function of the Swopblock in circulation (S) and the amount of trading enabled cryptocurrency available (X). Because the amount of Swopblock in circulation is independent of a Swopblock Take the protocol liquidity price ratio is given as ((X + x) / S), which is given to be equal to the Take price ratio (x / s). Now use the price ratio equality and determine (s) as follows:

Take ratio equality:

$$\frac{X+x}{S} = \frac{x}{s}$$

How a protocal Take price is calculated:

S, X and x are given, solve for s

$$s\,(X+x) = Sx$$

$$s = \frac{Sx}{X+x}$$

SWOPBLOCK GIVE

A Swopblock Give is giving a protocol calculated amount (s) of SWBL and taking an amount (x) of one of the Swopblock enabled cryptocurrencies in exchange. The amount given is determined by a calculation similar to a Take except that there is a sign change in order to account for the removal from a liquidity pool of an amount (x) instead of the contribution to a liquidity pool.

Give ratio equality:

$$\frac{X-x}{S} = \frac{x}{s}$$

How a protocal Give price is calculated:

S, X and x are give, solve for s

$$s\,(X-x) = Sx$$

$$s = \frac{Sx}{X-x}$$

ATOMIC SWAPS ARE UNNECESSARY

Except for a possible startup sequence designed to stabilize startup exchange rates – atomic swaps (in the standard sense) are unnecessary! Cross-chain atomic swaps are slow and do not provide the high-speed exchange required to support many of the use cases envisioned for the Swopblock exchange and trade economy. Atomic swaps are unnecessary because from the perspective of the protocol, value does not move from one block chain to another. Value is persistent within each blockchain and who owns that value on any particular blockchain gets recycled within the same blockchain. Only the knowledge of who was involved creates the apparent cross-coin flow (see figure one below). This allows the exchange to complete quickly and yet retain exchange security.

figure one: