Blocks & Chains Decentralized Exchange

A Peershare for exchanging cryptoassets

by Jordan Lee

with contributions from Tom Joad and Michael Witrant (aka sigmike)

The arrival of a decentralized exchange has been eagerly anticipated within the cryptoasset community. Exchange hackings and defaults have been a major problem discouraging use of cryptoassets.

We will present the design for Blocks & Chains Decentralized Exchange (B&C Exchange), a decentralized exchange where native blockchain assets are traded directly, without the use of proxy assets. The chances of theft and default will be dramatically lower than traditional centralized exchanges because handling of funds will be coordinated via blockchain messages between multisig signers whose reputations are adjusted every minute by shareholder voting. A web based interface that will be familiar to users of centralized cryptoasset exchanges will be offered. Unlike centralized exchange websites, exchange operators will have zero access to funds and zero responsibility for customer account information. If an exchange website disappears suddenly, a user can simply go to another site that uses the same open source exchange software, or use another application that supports B&C Exchange and continue using the same account without interruption. This is because all account information is stored on the blockchain.

First, let's take a brief look at the system from a user perspective:

> *Let's assume a user named Sam wishes to sell 8 Bitcoins (BTC) for 2000 NuBits (NBT) on B&C Exchange, using a website running the open source exchange software that will be developed.*
>
> *Sam clicks a Signup button which simply creates and displays a BlockCredit (BKC) key pair locally in the browser. Sam signs in using only the BKC private key. BKC are required as transaction fees for all exchange actions, so Sam requests 1 BKC and is asked to send 0.00455 BTC to a particular address. He does so and immediately receives 1 BKC. Next Sam requests a Bitcoin deposit address and then specifies a*

> *NuBit withdrawal address he has stored in a wallet. He places an order for 2000 NuBits at a price of 250 NuBits per BTC using the BTC/NBT trading pair. The highest BTC buy offer on the order book is 245, so the order is placed on the sell side of the order book and does not fill yet. Later in the day the price rises and Sam's order is filled. He immediately receives 2000 NuBits at his chosen withdrawal address when the order is filled.*

Sam's experience was similar to using a familiar centralized exchange. However, the architecture supporting his trade is completely different and offers compelling advantages.

Summary of Architecture

The infrastructure required for the exchange to function are B&C Exchange peers with reputed multisig signers also needing to run clients of foreign blockchains for which they sign. There are no privileged nodes, although certain BlockShare (BKS) addresses will be assigned a reputation score by minters, and those with the best reputation will be chosen as deposit address signers. Deposited funds will be protected by a network configurable number of reputed multisig signers.

In order for funds to be lost in the case of a 8 of 15 multisig deposit address, 8 reputed pseudonymous signers would need to conspire to steal funds or 8 signers would need to fail to sign valid transfers. A good reputation score permits a future and ongoing income doing nothing more than running a B&C Exchange client and in most cases one or more foreign blockchains, so signers will have incentive to act in a responsible, predictable and reliable manner to maintain their reputation, which is adjusted every minute. Reputed signers may place a security deposit of funds held by other reputed signers, typically in BlockShares. If shareholders felt a reputed signer engaged in misconduct, a motion could be passed to burn part or all of their security deposit. Before having their security deposit returned in the event of winding down operations, the reputed signer would need to prove the signing keys have been transferred to another reputed signer. A highly responsive reputation system combined with security deposits and a tolerance of up to 7 rogue reputed signers in the case the network is configured to use 8 of 15 multisig addresses means the chance of exchange default is exceedingly low.

There will be eleven types of new messages placed on the blockchain. Each of these will be accompanied by a transaction fee (which is burned as network revenue) except the fill message (which is unsigned):

1. Reputed signer deposit public key list
2. Non-reputed signer deposit address request
3. Non-reputed signer withdrawal address request
4. Order
5. Order validation
6. Fill (not signed and no transaction fee)
7. Fill validation
8. Fund transfer
9. Cancel order
10. Withdraw from deposit address
11. Pairing of BlockCredit and BlockShare addresses

In order to sign for foreign blockchain deposit addresses, a client must be connected to the foreign blockchain. One signer may choose to sign for Bitcoin deposit addresses, which means his client must be able to connect to a Bitcoin client. Another signer may choose to only sign Litecoin deposit addresses, which means his client must be able to connect to a Litecoin client. People who just want to use exchange services don't need to have their B&C Exchange client connect to any foreign blockchain, such as Bitcoin or Litecoin.

The B&C Exchange code base will be a fork of the Nu 2.0 code base. The only features of Nu that will be disabled completely are park rate voting and parking.

The following voting will be added:

- number of confirmations required by blockchain ID
- number of total reputed signers of deposit addresses by blockchain ID
- number of required reputed signers of deposit addresses to effect a transfer by blockchain ID
- maximum trade size permitted by asset ID
- number of reputed signers eligible for reputed signer block rewards
- Reputation voting will also be added, which consists of up to three upvotes or downvotes, each associated with a BlockShare address. Details are included in the Reputation voting section.

All of the new voting types will apply a protocol rule that an abstention will be interpreted as the value currently enforced by the protocol. This means if a shareholder likes the current network settings, they should abstain from voting to prevent blockchain bloat. The median vote in the last 2000 blocks will be used. Like Nu 2.0, the protocol values applied to the current block should be the consensus 60 blocks deep, so that there is a time window in which the applied values can be predicted.

There will be a second block reward (in addition to the minting reward) given to reputed signers in proportion to their reputation.

Transaction fees will be adjustable like Nu 2.0 but charged on a per byte basis instead of per kilobyte.

With these limited changes to the Nu code base, it is expected implementation of B&C Exchange will be easier than the original Nu network implementation. The majority of coding work will consist of processing the eleven new message types listed above.

Funding

In addition to the B&C Exchange solution being a fork of the NuBit code repository, the Nu production blockchain will also be forked. This will have no impact on the Nu network. All NuShare holders will receive BlockShares in proportion to their NuShare holdings. By doing this it is hoped that NuShare holders will have incentive to provide initial funding for B&C Exchange development via the NuShare auction custodial grant mechanism, due to the expectation that BlockShares will have value and B&C Exchange will lower the cost of NuBit liquidity operations. Specifically, we will ask that NuShare holders pass a motion to authorize auctioning 100 million NuShares. The auction will have a minimum bid price of 0.002 USD per NuShare and minimum bid size of 1000 USD. Bitcoin, Litecoin and Peercoin will be accepted in addition to NuBits. If valid bids do not total a minimum of 200,000 USD, the auction will be canceled. In the event of a successful auction, NuShares will be distributed within three days upon bid settlement. All Bitcoin, Litecoin and Peercoin proceeds will be converted to NuBits. This will ensure the development funds will have a stable value.

Ongoing B&C Exchange development would be funded with grants of BlockShares, which will work the same as NuShare or NuBit custodial grants. This means initial distribution of BlockShares is fully automated and very straight forward. It is really just a separate copy of the Nu network, communicating on different ports with a substantially modified protocol.

The B&C Exchange blockchain will be created when the network is ready for exchange operations as a fork of the Nu blockchain, with NuBits on the blockchain at that time invalidated. So, the best way to receive the first BlockShares will be to purchase NuShares. It is expected that the initial B&C Exchange market cap will be priced into the NuShare market cap prior to the creation of the B&C Exchange blockchain. For example, if the market prices the value of B&C Exchange at 5 million NBT at the time of launch, then we could expect that entire valuation to be contained in the NuShare market cap just prior to launch. The NuShare market cap may fall a little after B&C Exchange is released, but its enduring value will be tremendously enhanced as B&C Exchange provides an extremely cheap and secure way to provide NuBit liquidity and defend the peg.

Distribution to Bitcoin holders

To maximize the number of people who have a stake in B&C Exchange 20 million BlockShares will be offered to all who hold Bitcoin by having Bitcoin holders sign and broadcast a message signed by their Bitcoin address, which could be verified by the reputed signers that process Bitcoin deposit addresses. 100 BlockShares would be created for each Bitcoin up to 10 Bitcoins per Bitcoin address and 20 million BlockShares in total (for all Bitcoin addresses) will be distributed this way. This will be done to enlarge the B&C Exchange community by providing a monetary incentive to all Bitcoiners to promote and use it. In this way initial share distribution will be completed according to verified proportional Bitcoin ownership, as opposed to centralized decision making.

Here is the manual process for distributing BlockShares to Bitcoin holders. Making the process amenable to automation is undesirable (so no RPC method for this):

1. Use the integrated Shapeshift (or similar service) interface to purchase BlockCredits with nearly any cryptoasset.

2. Sign a blank message with a Bitcoin address using the Satoshi client or any other application that permits signing messages with cryptoasset keys.
3. Copy the resulting signature and the Bitcoin public address into a dialog in the B&C Exchange client made specifically for this purpose. Specify a BlockShare address to receive BlockShares at. Click a Receive BlockShares button.
4. From a user perspective, steps 1 through 3 are all that is needed. However, in the background the client creates a transaction including the Bitcoin address, message signature, BlockShare address and standard transaction fee.
5. Validations will be sent by top reputed signers that have Bitcoin deposit public key lists on the blockchain. When the validations received represent the majority of weighted reputation of eligible top reputed signers, the BlockShares will be created and considered valid by the protocol.

Exchange Accounts

An exchange account is simply a BlockCredit address used for signing. No reputation is needed to effect trades. Deposit address requests, withdrawal address requests, orders, etc. (which are detailed below) are all signed using this key.

Deposits

In order to prepare the way for deposits, some individuals must decide to become reputed signers for deposit addresses on one or more blockchains. Initially, it is expected that the Bitcoin, B&C Exchange and Nu blockchains will be supported, though many others will be added iteratively. A particular individual might choose to be a reputed signer for the Nu blockchain. To do so effectively, he will need to make sure his B&C Exchange client is always running and always able to connect to his Nu client. He will need to convince shareholders to upvote his reputed BlockShare signing address. This reputed address will be used to sign reputed signer deposit public key lists, or deposit key lists to be brief. This is a blockchain record subject to transaction fees that contains the following information:

- reputed Blockshare public address of signer
- signature using reputed address

- blockchain ID
- asset ID
- a list of public addresses of the asset type referenced

When a reputed signer posts such a message, he is promising to keep the addresses listed in a wallet connected to the blockchain client referenced, which can in turn be contacted by his B&C Exchange client at all times in the future, except if he transfers the keys to another reputed signer as described in the Signer Incentives section. Each address in the list may be used once and only once in a non-reputed signer deposit address request, or deposit address request to be brief.

When making a deposit address request, depositors cannot choose which reputed signers will handle their deposits and how many signers are required to move their funds. By protocol, they must choose the most reputed signers with an available deposit address for the asset type they are requesting a deposit address for. Shareholders will vote on the number of signers and the number required to move funds (such as 4 out of 7 or 6 out of 10), up to 15. The signers will be the ones with the highest reputation score (derived from upvotes and downvotes placed on the blockchain) that have an unused deposit address in a deposit key list of the same asset type. The more signers there are the higher the fee will be and the more blockchain space is required.

A request for a deposit address will need be to broadcast through the network accompanied by a fee. The request will contain the public keys of the proposed signers. So through blockchain voting, shareholders may define 8 signers to move funds, 15 signers total. These m of n quantities in effect will be determined by ongoing shareholder votes.

So, from a user perspective a new deposit address for a specific exchange asset such as Bitcoin or NuBits is requested. That is all the end user needs to be aware of. The client can build the multisig deposit address locally using the public keys of the signers chosen, which are all on the blockchain. The deposit address request is broadcast and placed on the blockchain. It contains the following data:

- multisig deposit address
- public address of each reputed signer selected for one time use from a deposit key list (these addresses will be of the relevant asset type such as Bitcoin or NuBits)

- blockchain ID
- asset ID (Bitcoin, NuBit)
- signer address (BlockCredit) controlled by entity requesting the deposit address (used to sign orders); may be multisig; this represents the exchange account
- signature using the exchange account address
- transaction fee

To construct this, a client must first determine which reputed signers it will use, which will be the ones with the highest reputation score. Once these signing candidates are determined, the blockchain must be searched for a deposit address list published by a particular signer which matches the asset ID of the deposit address request. An address must be confirmed to have not been used before, which means it does not appear in any other deposit address request on the blockchain. If a reputed signing candidate does not have an eligible and valid address the requester can use, another signer should be chosen (the one with the next best reputation).

The deposit address request will then be broadcast and the deposit address will be displayed in the local client. Reputed signers who have a key to sign the multisig address will broadcast a signed acknowledgement to be placed on the blockchain with a fee that they have received the deposit address request (using their key for the deposit address, not their reputed address). The number of acknowledgements received will be displayed in the client next to the deposit address. Deposit address requests should be stored in the appropriate wallet of all reputed signers using the addmultisigaddress RPC. Once the deposit address request is broadcast and an acceptable number of acknowledgements have been received, the user can feel comfortable depositing funds to the multisig address. Discovering which reputed signers failed to acknowledge should be easy so they can be appropriately downvoted.

The protocol must ensure that each exchange account (BlockCredit address) is associated with at most one deposit address. Later iterations of B&C Exchange will allow the account holder to change the deposit address.

Orders

Order messages should contain the following data:

- signature using the exchange account (BlockCredit) address
- exchange account public address
- numerator asset type
- denominator asset type
- numerator asset quantity
- denominator asset quantity
- buy or sell, in reference to the numerator asset type
- order ID as random GUID (not subject to transaction malleability)

The protocol will ensure that the necessary deposit and withdrawal addresses to complete the order are associated with the exchange account. Protocol requires that an order is not valid until it has associated order validations from enough signers to move funds plus two backup signers. For instance, for an 8 of 15 deposit address, 10 signers must broadcast an order validation (these are detailed in the Order Validation section below). The protocol should be rigorous in requiring complete and valid order data as described above. Once an order is deemed valid it will be placed on the blockchain. The order will not be eligible to be filled and will not be placed on the order book until the order has the number of confirmations voted for by shareholders for the B&C blockchain.

Order Validations

Order validations should contain the following data:

- signature using reputed address
- transaction fee
- order ID being validated
- whether verified funds are the denominator or numerator asset of the trade

When an order is received, sufficient funds must be verified. Nodes that are signers of the appropriate deposit address (for buy orders it will be the denominator deposit address, for sell orders it will be the numerator asset) will broadcast a signed message confirming or denying sufficient funds for the order. This message will contain the standard transaction fee and be placed on the blockchain. They must check the deposit address for sufficient funds on the appropriate blockchain using the RPC for its client, but they must also check the orders already in their memory pool and on the B&C Exchange blockchain and subtract the amount of those orders from available funds. Submitting multiple orders based on the same deposit is similar to double spends, and the same established techniques must be used to defend against it. Verification must be received from enough signers to accomplish the appropriate transfers from deposit addresses plus two signers to be valid.

Fills

Of the eleven new types of messages included in B&C Exchange, fills are the only message type that isn't signed. This is because fills are merely the consequence of matching orders. Each node has all the information (from the blockchain) it needs to determine an order fill is occurring, so order fills do not need to be broadcast. They should simply be added as a message to the memory pool by all clients. The protocol should permit zero transaction fees for valid order fill messages. This won't allow for abusive overuse of blockchain space because orders must be paid for, which are the only thing that can result in order fills.

Order fills need to be placed on the blockchain because they impact the validity of orders. The network is unable to rigorously track the validity of orders without a blockchain record of order fills.

Each time an order on the blockchain receives the required number of confirmations, the order book will be checked to see if there is a matching order on the books. If one is detected, then an order fill transaction will be created by the client. An order fill message references exactly two signed orders and contains exactly two transfer messages. A transfer message consists of the following data:

- asset ID
- source order ID
- destination order ID
- transfer quantity
- sender address

- receiver address

A fill message consists of:

- limit order ID (sat on the order book aka liquidity maker)
- market order ID (matched an order on the order book at the time placed aka liquidity taker)
- exactly two transfer messages as detailed above

There is a risk that not enough signers for one transfer will be available at a particular time, but enough will be available for the complimentary transfer. This would result in one exchanger receiving value without paying the other exchange partner. To prevent this, signers must confirm they are ready and prepared to sign just before an order fill is considered valid. Therefore, when matching orders are detected the appropriate wallet must be checked to see if the client is a signer for the order fill. If they are, they must sign an order fill validation message (described below) indicating they are prepared to sign the transfer and broadcast it which will be placed on the blockchain with the appropriate fee. For an order fill to be considered valid, the client must have received signed order fill validations from enough signers to transfer plus two alternate signers. No block confirmations are required for fills. As soon as the required fill validations are received, reputed signers will begin signing fund transfers.

Fill Validations

These are quite similar to order validations in that they verify funds are available and that signers are ready to sign transfers. While order validations and fill validations are mostly redundant, they do both provide unique protections. Only order validations can prevent fraudulent orders from appearing on the order book. There is a chance that if an order remains on the order book for a very long time that sufficient signers will no longer be available to handle the fund transfer. Fill validations ensure this is not the case. Like order validations, fill validations must be sent by enough signers to effect the transfer plus two. They also appear on the blockchain.

Fill validations should contain the following data:

- signature using reputed address
- transaction fee
- limit order ID (sat on the order book aka liquidity maker)
- market order ID (matched an order on the order book at the time placed aka liquidity taker)
- whether verified funds are the denominator or numerator asset of the trade

Fund Transfers

Signed multisig messages that do not yet have enough signatures will be broadcast through the network and placed on the blockchain with the appropriate fee. This message should include:

- the signed raw transaction
- the multisig deposit address
- a list of all addresses that have signed it
- the signature of the reputed address

Cancel order

A cancel order is broadcast, placed on the blockchain, and requires a fee. It contains the following data:

- order ID of the order to be cancelled
- signature of the exchange account used to sign the original order
- transaction fee

Withdrawal address request

The withdrawal address request is broadcast and recorded in the blockchain. It contains the following data:

- withdrawal address (may or may not be multisig)

- blockchain ID (Nu, NXT)
- asset ID (Counterparty, NuBit)
- public address of exchange account; may be multisig
- transaction fee
- signature using the exchange account address

The protocol must ensure that each exchange account (BlockCredit address) is associated with at most one withdrawal address. Later iterations of B&C Exchange will allow the account holder to change the withdrawal address.

Withdrawal from deposit addresses

An exchange account address can be used to broadcast a withdrawal request from the associated deposit address if a withdrawal address request with the same asset ID has been successfully included in the blockchain. While it is not really necessary for it to be in the blockchain, it is necessary for there to be a fee charged to prevent denial of service attacks, and the fee must be assessed on the blockchain. Therefore, a blockchain record with the following elements should be made:

- transaction fee
- address of exchange account
- signature of exchange account
- asset ID
- blockchain ID
- amount to be withdrawn

No confirmations are needed as the relevant blockchain can successfully handle multiple withdrawal requests that would constitute a double spend.

Pairing of BlockCredit and BlockShare addresses

There is a need to associate BlockCredit and BlockShare addresses when they are used as reputed signing addresses. There is a need for reputed addresses to be BlockShare addresses so they can receive block rewards of shares. There is also a need to have reputed addresses be BlockCredit addresses so that transactions can be signed and paid for. The protocol prohibits transactions that use both BlockCredits and BlockShares for important reasons. So, a reputed signer will at times need to identify himself using a BlockShare address while at other times being identified using a BlockCredit address. A simple message associating a BlockShare and BlockCredit address with the following information will suffice for this purpose:

- BlockShare address
- BlockCredit address
- transaction fee
- signature of BlockCredit address

Reputed signer incentives

Each block will have a reputed signer reward given to a single signer. The reward should be given in proportion to the reputations as they were 60 blocks deep. Here is an example using small numbers for clarity: Let us suppose that shareholders have voted to reward 3 reputed share addresses. Let us suppose that reputed share address A has 20 weighted reputation points, share address B has 50 weighted reputation points and share address C has 30 weighted reputation points. Over a period of 2000 blocks, the total rewards for each reputed address can be calculated. If A has received 19.9% of the reward, B has received 50.3% of the rewards, and C has received 29.8% of the rewards, the block reward must be awarded to C, because his reward over the last 2000 is the farthest below what it should be, according to his reputation score.

It is expected that some shareholders will choose to vote to give reputation to an address under their control, just to receive the reputation based block reward. This is contrary to the interests of the network. Such attempts will be thwarted by a combination of the total number of rewarded address allowed by voters, and by downvotes given by other shareholders. If only 20 addresses are being rewarded, rogue shareholders trying to reward themselves will have trouble getting their address in to the top 20. This is especially the case because other shareholders will be downvoting them. Reputed signers are expected to make public appeals for upvoting. So, a particular entity may make a community forum post, saying vote for me because I have built a reputation with past actions in the community, have posted a 3 million share deposit, have a VPS to process messages with a failover node set up, and promise to transfer keys to a top ten reputed signer in the event I later choose to cease operations. Shareholders would expect that the address associated with this entity would be upvoted. However, if an unknown address began to be upvoted, it should be downvoted by other shareholders, as shareholders should suspect it is just a single shareholder attempting to receive the reputed block reward himself without providing any service. It is expected that most shareholders will have their reputation votes set by a data feed provider so they don't need to individually monitor these things.

If a signer wishes to cease operations, their private keys can be sold (they have value in proportion to the block reward it will earn). The new operator could then continue operations, although it would be possible for the original operator to also sign requests. Selling a signing key will accordingly reduce its value as it is likely to have its reputation reduced as a result. Signing key sales are likely to occur in secret as a result. If the original owner signs in addition to the new owner, this can be detected and shareholders will likely down vote the signing address. The risks involved in covert signing key sales are modest and are mitigated by the distributed trust model of using many signers.

Minting and reputed signing nodes

Minting nodes are such because they have BlockShares eligible for minting. Reputed signing nodes are such because they are capable of signing transactions on deposit addresses. A client may be neither a minting nor signing node, one or the other, or both. Furthermore, being a signing node will only be in reference to a specific non-native blockchain. So, a particular node may a Bitcoin signing node, but not a Peercoin signing node, while another node may play the role of a Bitcoin signing node, Peercoin signing node and minter.

Share wallet conversion

A dialog that can be invoked by selecting File...Convert NuShare wallet should allow users to specify a local NuShare wallet to be converted to a BlockShare wallet. A BlockShare wallet will be created in the same location as the NuShare wallet and will be named wallet8.dat. There is no need to convert NuBit wallets.

Protocol changes regarding currency

Because NuBits will be in the copied Nu blockchain used by B&C Exchange, transactions with NuBits in blocks below the fork block height will be prohibited by protocol. Currency outputs recorded in blocks higher than the fork will be interpreted as BlockCredits. NuBits on the original Nu blockchain will be handled just like any other blockchain such as Bitcoin or Litecoin.

Reputation voting and scoring

When a block is minted, the minter may enter up to three upvotes or downvotes, each associated with share address, presumably that of a reputed signer. What the user may place in his client from which these three upvotes or downvotes will be derived is a bit more complex. The user may place as many pairs of addresses and numbers as they like. This way it is possible for the user to express what the relative reputation of any number of addresses should be. Consider this example user entry as the basis for determining a reputation vote:

8RW7kF2bGhq175ipJWor8aTjM5LBUdZi2D	5
86BqkZdb79W2CT79o84j1pqnhs1R3w3QsB	10
8TgryZQ1dQNJYMjm74K3ajdRnDfsCjh3c3	1
8LMMdCqZYZSj48e8dZLci5kK7h7iMPrJ36	-5

Only three pairs can ever be selected for inclusion in a block, and the quantity of upvote or downvote cannot be specified: it is always understood as one upvote or one downvote. The absolute value of the number beside the share addresses indicate how likely (relatively) each is for inclusion in the block. Whether it is negative or positive corresponds to being an upvote or downvote. So, the first address above is just as likely to be selected for inclusion as the last address, but the first address will always be upvoted and the last address always downvoted. The second address is ten times as likely to be chosen for inclusion as the third address.

Voting would be weighted most heavily toward recent votes. The last 5000 blocks of votes would receive full weight, the next most recent 10000 blocks would receive half weight, and the 20000 before that would receive quarter weight.

Transaction fees

Transaction fees will be variable and subject to shareholder voting, just as in Nu version 2.0. Transaction fees will be priced per byte, not kilobyte as in Nu. This creates the incentive to keep transactions small, even when below 1 kilobyte. Deposit address requests and multisig transactions are large in size, but typically under 1 kilobyte, so an incentive needs to be provided to use a more compact 3 out of 5 multisig rather than 10 out of 15 if it is demonstrated that the counterparty risk is similar. All of the new messages defined in this paper must be signed with a BlockCredit address and offer a transaction fee in BlockCredits. Just as in Nu, a transaction fee in shares will be used to transfer BlockShares.

Dividends

It is expected that all proceeds from the sale of BlockCredits will be distributed to shareholders as Bitcoin dividends. Custodial grants of BlockCredits should be given to custodians for the sole purpose of placing sell walls and using the proceeds to distribute Bitcoin dividends. These sell walls would be particularly well suited for a BlockCredit / NuBit trading pair, though it is possible NuBot could be adapted to offer them on a BlockCredit / Bitcoin pair at a floating rate. In any case they should always be sold for one US dollar. While BlockCredits are the same as NuBits to the code base, they have a completely different purpose. They are solely for use as transaction fees and are not intended for general trade as NuBits are. Accordingly, a peg for BlockCredits will not be maintained. They are comparable to postage stamps in many ways. They are sold with the promise you will receive one US dollar worth of transactions on the B&C Exchange. Just as you wouldn't expect to be able to sell postage stamps to a third party at face value, there shouldn't be an expectation that BlockCredits can be sold for one US dollar, although a resale market may appear. BlockCredits should only be purchased with the intent of consuming them to pay transaction fees on the B&C Exchange. Care should be taken not to approve custodial grants of BlockCredits for any purpose other than sale and subsequent dividend distribution. If grants of BlockCredits were used to fund development or other expenses, the sale of BlockCredits by developers as they cash out to local currency might outpace the demand for BlockCredits at times and distort the sale price. Instead, development should be funded with BlockShares. Stable value of granted funds will often be important. In those cases, granted BlockShares should be sold for NuBits, for which there is good liquidity at a stable price. While this is our opinion about the best use of BlockCredits, it should be noted that the protocol permits shareholders to grant BlockCredits as they see fit. As with all

Peershares implementations, shareholders will have their way and no one is in a position to promise how they will behave in the future.

Future business applications

The B&C Exchange architecture is well suited to provide reversible or escrowed transactions on any supported blockchain. It can do this without any protocol changes on the blockchain in question. Non-reversibility of transactions is desirable in some contexts, but has been identified as a serious flaw of Bitcoin and other cryptoassets in other contexts. A reversible payment could be made to a multisig deposit addresses. A contract and dispute resolution organization could be associated with specific deposits. Their edict, expressed with signed messages, could automatically control where reputed signers send escrowed funds. While pursuit of this type of business won't be the first thing done with B&C Exchange, the door is open to this kind of expansion if it is successful.

Future optimizations

Some observers may have concerns about the scalability of the solution. The initial design can scale to handle approximately 10 orders per second, along with all the other transactions needed to support orders. There are many changes that can be made in the future to improve scalability. They require additional development, so it doesn't make sense economically to implement them at this time. As network latency reduces over time due to hardware improvements block intervals can be collapsed, validation messages can be merely broadcast but not placed on the blockchain, a derivative of Cryptonite's mini-blockchain can be employed, delegates can be employed, etc. The solution proposed here can be evolved to scale far beyond 10 orders per second.

Risks

The biggest risk of using the exchange may be that deposited funds will not be transferable at a certain point in time due to signers of the multisig deposit address not being available. This risk can be mitigated in a number of ways. First, this risk increases as the amount of time since a deposit address was created increases. This means that getting new deposit addresses with new signers regularly would mitigate this risk. Second, using more total signers and fewer required signers mitigates this risk. Using 6 of 12 signers is safer than 3 of 6. Likewise, using 6 of 12 is safer in this regard than using 9 of 12, though decreases in the required number of signers increases the risk of rogue signers stealing funds. Experience will demonstrate an optimal ratio of required to total signers to provide optimal protection from both failure modes.

If something goes wrong

While no one could ever guarantee that if a loss is experienced due to a network defect shareholders will compensate the loss, because no one could compel shareholders to do that, it can be said it would be possible and in the interest of shareholders to compensate the loss via BlockShare grant. BlockShare grants could be made directly, or if there were too many parties involved they could be granted to a custodian, possibly exchanged to the asset the loss occurred in, and distributed by the custodian to those affected by the network defect.

Changes to the design

It is inevitable that some design changes will need to be introduced as more is learned in the process of implementation. Major design changes prior to completion will be approved by NuShare holders. In order to grow and prosper, the design will need to continually evolve after initial implementation. Such design changes will be determined via BKS shareholder motion and funded via BKS grant as directed by shareholders.

Use case: Minter and shareholder

First, BlockShares must be acquired. They can be acquired by owning NuShares at the time the production B&C Exchange is created, by purchasing them on an exchange such as B&C Exchange thereafter, or by proving Bitcoin ownership. If they are acquired by owning NuShares when B&C is created, then the shareholder will use the B&C client to convert his NuShare wallet to a BlockShare wallet by selecting File...Convert wallet to BKS. Acquiring them by proving Bitcoin ownership is described above in the section titled "Distributing to Bitcoin holders".

In order to be eligible for minting, at least 10,000 BKS must be transferred to an address in a single transaction. If BKS were acquired through purchase or proving Bitcoin ownership, 7 days must pass before any minting can be done. Once eligible for minting, the chances of minting does not change over time, nor does the reward for minting a block. If the same number of BKS shareholders mint as in the Nu network presently, someone minting constantly with 10,000 BKS could expect it to take 32 days on average to mint a block and get a vote in the network (including the seven day initial waiting period). If your wallet is only open and processing half the time, it will take 57 days on average. If you have 100,000 BKS, you can expect to find an average of 10 blocks every 32 days (25 days + 7 day waiting period). When a block is found, you will be awarded 40 BKS.

Prior to beginning to mint, it is important to select a data feed to configure your vote dynamically using the Data Feed button the Voting tab. You should pick the data feed operator you feel has voted in the best interest of shareholders in the past. You can switch which data feed to have configure your vote at any time. Advanced users can configure their own vote manually if they are following developments very closely (nearly every day) on the B&C public forum and have a good understanding of how the network operates. **Minting without any manual or automatic vote configuration is quite injurious to the network, as it is a 'No' to every proposed course of action.**

While the quantity of mint rewards received varies based on the percentage of shareholders minting, NuShare holders constantly minting currently receive between 2.5% to 3% additional NuShares over the course of a year.

Use case: BlockCredit custodian

BlockCredits are used solely to pay transaction fees on B&C. Community members with excellent reputations may propose to become BlockCredit custodians subject to shareholder approval. While the protocol permits shareholders to elect anyone to become a BlockCredit custodian for any purpose, it is expected that shareholders will elect BKC custodians that will make the BKC they receive available for sale at a variety of exchanges and venues. A BKC custodian may be a single entity or a group of entities using a multisig address to jointly control BKC they receive. Once sold, a BKS custodian will use the funds received to purchase Bitcoin and distribute it as dividends to all shareholders in proportion to their holdings.