Decentralized Bank & Exchange

by Daniel Larimer
dlarimer@invictus-innovations.com

February 14th, 2014

Abstract
Crypto-currencies such as Bitcoin have opened the door to an economic revolution in the information age as significant as the industrial revolution before it. BitShares X is the first experiment in taking the ideas introduced by Bitcoin to the next level by producing trust-free digital assets that have the potential to track the price of anything[1]. In this paper we share the details of how BitShares X is designed and functions.

1.0 Background

BitShares X is the first implementation of ideas first introduced by Daniel Larimer on May 24th 2013 in a post on bitcointalk.org. The ideas have evolved and been refined over time until a new metaphor for describing crypto-currencies was introduced in an article published on letstalkbitcoin.com titled "Overpaying for Security" first introduced the concept that crypto-currencies should be viewed as shares in businesses with an eye toward maximizing profits by producing the most value possible at the least possible cost. These businesses have come to be known as Decentralized Autonomous Companies (DACs).

Bitcoin can be viewed as a DAC where instead of 'coins' you have 'shares'[2]. The transaction fees are revenues and the miners are employees. In the case of Bitcoin, operating expenses exceed revenue earned from operation and therefore Bitcoin is operating at a loss of about $1 billion dollars per year[3] (as of this writing). The business model of Bitcoin is hardcoded into the block chain and will not break even for 100 years.

A DAC's goal is to maximize revenue from transaction fees by increasing the value provided by the transactions while minimizing the cost of operations. Instead of creating 'coins', DACs have shares much like a corporation. A share is nothing more than a percentage of a whole. There are many ways to allocate shares and historically crypto-currency (shares/coins) have been issued as needed to pay employees (miners) to secure the network with computational power.

[1] Any idea or concept for which there is sufficient market depth
[2] Shares are defined as a percentage of a whole and not as equity in a legal entity such as a coorporation
[3] Calculated as 25 BTC every 10 minutes for 1 year at a price of $800 per BTC

However, the issuance[4] of shares to new employees debases the value of shares held by old employees and is considered an expense by traditional businesses.

1.1 Security

There have been three primary ideas introduced on how to secure a network: proof of work, proof of stake, and consensus by voting. The goal of this security is to make it economically infeasible to change the transaction history or produce forged blocks. This is important because without protection against forgery no one can be certain that the shares they think they own will be recognized by others in the future. Additionally a network must be secured against denial of service attacks where someone has the ability to block some or all transactions from being processed by the network.

1.1.1 Proof of Work

Proof of Work was first introduced by Adam Bach as a means of preventing email spam. The idea is that certain computations are easy to verify but difficult to solve the first time. By requiring proof-of-work an attacker must consume significantly more resources to produce data than everyone else must spend to validate the data.

Bitcoin uses proof-of-work to accomplish several goals. The cost of producing a block in both time and money becomes increasingly expensive and thus harder to forge. Meanwhile the process also means that on average only one computer will find a block at a time. This naturally solves the problem of who should produce the next bock.

The theory is that this decentralizes block production and makes it economically inefficient for a single bad actor to do more work than all of the honest actors working together. This theory worked well for Bitcoin in the beginning because no one took it seriously, but upon closer inspection we find that this model of security is fundamentally flawed.

Proof of Work is done to earn a profit, and whoever can do the most work for the least reward will earn the most profit and put less efficient competitors out of business. This means that economies of scale will favor centralization of proof of work. In the case of Bitcoin, mining has already been centralized in the hands of a half dozen mining pools and increasingly in the hands of large private ASIC developers. It is now possible for one or two players to block transactions from being included in the network and in the future governments may compel certain balances to be frozen.

So while proof of work has significant costs, it ultimately undermines the value proposition of a DAC by creating the very situation it was intended to prevent, centralization. For this reason Proof of Work is not a suitable model for securing a transaction ledger.

[4] issuance is used as a metaphor for the creation of new bitcoins via coinbase transactions and the creation of a security backed by a corporation.

1.1.2 Proof of Stake

The concept of Proof of Stake was first introduced as a means to counter known attacks on the Proof of Work based networks, primarily the 51% attack. The 51% attack would enable denial of service and transaction filtering as well as double spends by the attacker.

Existing Proof of Stake systems such as Peercoin are based upon 'proof blocks' where the target the miner must meet is inversely related to the coin-days-destroyed[5]. Someone who owns Peercoins must choose to become a Proof-of-Stake miner and commit some of their coins for a period of time to secure the network.

The creators of Peercoin recognized that Proof-of-Stake in this form was insufficient so they rely upon a hybrid system whereby both Proof-of-Stake and Proof-of-Work are used to secure the network.

A recent entrant to the Proof of Stake scene is Nxt which claims to be 100% proof of stake and does so with a process they call transparent mining. With transparent mining the network deterministically selects who gets to produce the next block. If this person is online at the time then they get an opportunity to earn transaction fees. Otherwise a block is produced by the next in line.

The problem with existing proof of stake systems including Peercoin and Nxt is that they depend upon a subset of users that actually choose to dedicate computational power to mining in an effort to earn income from transaction fees. This creates two classes of users and significantly reduces the percentage of the money supply used to secure the network. Additionally both of these systems suffer from the potential that a large stake holder could perform a denial of service attack by refusing to include some or all transactions.

1.1.3 Consensus

The consensus process was first introduced by Ripple. Ripple made a very important and fundamental observation that in a market all that is necessary is for everyone to agree and that it is in the best interest of everyone to agree. They then combined this realization with the fact that with enough peers with diverse and competing interests it is almost impossible to conceive of them working together in an attempt to defraud you, especially if they have public reputations on the line.

The Ripple process builds a transaction ledger just like everyone else and a diverse group of nodes sign off on the ledger. Using a voting system biased toward agreeing with one another, the nodes are able to come to a consensus on what order to include new transactions. These nodes have no need to prevent forged transaction logs because they stay synced at all times

[5] A coin-day is the number of blocks a balance has been held times the amount of the balance

and simply trust the majority when they reconnect.

This process is not free. Nodes must exchange extra messages to reach consensus. Ripple nodes are not compensated with transaction fees, but instead transaction fees are destroyed reducing the number of XRP (the Ripple currency) in circulation. The act of destroying the transaction fees is the moral equivalent of paying a dividend. As such the Ripple network is the first profitable DAC.

1.1.4 Transactions as Proof of Stake

On November 28th, 2013 Daniel Larimer posted a paper on a new kind of Proof of Stake that leverages the fact that each and every individual making a transaction on the network has an interest in the current state of the network.

Transactions as Proof of Stake (TaPOS) operates on the principle that the shareholders of the DAC should decide and ratify the transaction ledger. Every shareholder is given one vote per share that they own every block. These votes accumulate and are automatically cast in favor of the current transaction ledger when the user makes a transaction. By voting for a transaction ledger that user is declaring that this is the state they saw at the time of the transaction and in their opinion is the legitimate public ledger. A public ledger with enough votes from interested shareholders cannot be changed or modified without getting all of the parties to agree to such a change. This is significantly more secure than other systems where a small minority of the stakeholders are actively involved in securing the network.

When a transaction is included in a ledger built off the state expected by the shareholder, the votes are counted toward securing the network. A transaction that votes for a an invalid ledger does not have its votes counted. This makes it impossible for hidden chains to leverage the transactions produced by the public network.

Every single block is required to have a minimal number of votes before it can be added to the ledger. This ensures that no one can produce a block without enough approval of the prior block and that votes are actively and consistently added to the network. As the transaction ledger grows more and more votes accumulate and it becomes immutable and thus secure.

The Proof of Stake solves the security issue, but does not solve the consensus on what the next block should be. This process can be achieved in many ways. One is to use a Ripple style consensus algorithm and the other is to use a Proof of Work style lottery system. Either system may be used and has its trade offs.

If a Proof of Work style lottery system is selected then the difficulty of producing the next block is infinite until enough votes are collected and then it uses a standard Bitcoin style difficulty adjustment to mine the block. Unlike Bitcoin the security isn't provided by the mining and miners that exclude transactions also exclude the votes required to produce the block. This property

makes denial of service attacks impossible as everyone must include as many transactions as possible to accumulate the votes necessary to start mining.

Nodes that have some of their own shares may choose to exercise some of their own votes to start mining a block that has insufficient votes from transactions and thus give themselves a edge over others. The motivation for a miner to use their own votes is so they can earn transaction fees. In a sense nodes are paid to vote regularly and provide predictable security for the network.

Regardless of how much hash power you have, it is impossible for someone to monopolize the production of new blocks that exclude 3rd party transactions for long. They would have to consume their own votes and once their votes are gone someone else will include the transaction.

To ensure the blockchain doesn't grow for ever, that balances of lost keys are recovered, and that voting power does not accumulate for ever, all balances must be moved forward in the block chain at least once per year or face a 5% fee.

2.0.0 Introduction to BitShares X

BitShares X is an experiment to test the economic theory behind a new kind of prediction market. This experiment creates a decentralized bank and exchange that uses a decentralized transaction ledger secured by TaPOS to create fungible digital assets that are market-pegged to the value of anything from dollars, to gold, to gallons of gasoline. Like all DACs BitShares X has shares that can be transferred between users in the same way as bitcoins. What makes BitShares X special is that it also implements a business model similar to existing banks or brokerages. For the purposes of this paper shares in BitShares X will be referred to as XTS and we will be using BitUSD, an asset pegged to the United States Dollar, as the example asset.

BitShares X can create BitUSD by lending it into existence backed by collateral in the same way that the banking system lends dollars into existence today. Whereas your bank uses your house as collateral, BitShares X uses XTS as collateral. If the value of the collateral falls relative to BitUSD then BitShares X will automatically cover your loan by selling the XTS held as collateral for BitUSD and giving the borrower what ever XTS is left over.

The reason someone borrows BitUSD is for the purpose of executing a short sell of BitUSD relative to XTS. This works in the same manner as shorting a stock. First, you borrow the stock, then you sell it at todays high prices. If all goes well then you can buy it back tomorrow for less than you paid today, pay off your loan, and keep the profit. However, if things go against you then you will have to pay more to buy back the stock than you sold it for in the first place and thus take a loss.

BitUSD is created when two people taking opposite positions can agree to a price and the only

price at which two people will agree is the current market price of USD to XTS otherwise one individual will start out losing money. The mechanics of the market peg are very similar to the mechanics of a prediction market. Once the market has reached a consensus that BitUSD should be valued the same as a real US Dollar no one will be able to trade against that consensus without losing money. Thus the value of BitUSD today is based upon the prediction of what market participants will value BitUSD at in the future. There is only one rational way to speculate, that the consensus will hold, and that creates a self-enforcing market peg.

With BitShares X all short positions (those borrowing BitUSD) must start out with enough XTS as collateral to purchase 2x the USD borrowed. Margin calls are executed when the value of the collateral falls to 1.5x the amount borrowed. This gives the market ample opportunity to cover the short position and pay off the loan before there is insufficient collateral. In the event that the market is forced to execute a margin call, a 5% fee will be assessed. This should encourage participants to be pro-active in maintaining sufficient margin.

In the rare event that the value of XTS falls by more than 50% in less than an hour resulting in insufficient collateral, 100% of the collateral will be used to cover as much BitUSD as possible leaving some BitUSD uncovered. The result of this price movement is that some BitUSD will be in circulation without any backing which may or may not impact the market peg of BitUSD to USD. We have two hypothesis as to the market response in this event: in one case the BitUSD will start trading at a discount proportional to the surplus BitUSD in circulation, in the other case the market expectation of a peg to USD will override any surplus supply and BitUSD will continue trading as before. This would be similar to how the dollar did not see an immediate fall to 0 value despite being removed from the gold standard.

3.0.0 Implementation Details

To implement BitShares X we utilize a blockchain structure similar to Bitcoin. In the case of Bitcoin every transaction takes inputs from prior transactions and produces new outputs that may be used as the inputs to future transactions. Every output may only be used once and when it is used certain conditions must be met. Every output contains a balance of bitcoins that can be added to future transactions. The value of all inputs to a transaction must be greater than the value of the outputs in order to preserve the property that no transaction can create coins from nothing.

Bitcoin uses a simple scripting language to evaluate the conditions upon which the balance of a transaction output may be spent; however, the vast majority of all transaction outputs simply require the cryptographic signature of their owner.

3.1.0 Transaction Types

BitShares X recognizes that having the flexibility of a scripting language is simply unnecessary overhead when all transactions use the same scripts. In the case of Bitcoin, the scripts are limited in their power and thus we were unable to build BitShares X using bitcoin scripts. Instead

we have defined a fixed set of seven claim conditions:

3.1.1 Claim by Signature

Allows the output to be spent provided it is signed for by its owner. This works just like a standard Bitcoin output script.

3.1.2 Claim by N of M Signatures

Allows the output to be spent provided it is signed by N of M owners. This works just like a Bitcoin Multi-Signature output.

3.1.3 Claim by Bid

Allows the output to be spent provided the specified asset type is paid to the owner of the Bid at the specified price. A bid may be partially filled so long as a new bid containing the change is also created at the same time. Bids can only be matched with other *Claim by Bid, Claim by Long or Claim by Cover* outputs in a deterministic manner when a new block is created according to the market matching algorithm. A *Claim by Bid* output can also be spent by its owner given a signature and in this manner the owner can cancel their order.

3.1.4 Claim by Long

Allows the output to be claimed provided a short position (*Claim by Cover*) is created for the owner at the specified price. The short position must be paired with a new *Claim by Signature* output that creates new BitUSD of the same amount. This output can also be spent by its owner given a signature and in this manner the owner can cancel their order.

3.1.5 Claim by Cover

Allows the collateral backing a short position to be accessed in proportion to the amount of BitUSD destroyed by the same transaction. BitUSD is destroyed by including it as an input without a corresponding output. This output can only be covered by its owner unless it is being used as part of a margin call during the deterministic operation of the order matching algorithm.

3.1.6 Claim by Option Execute

Allows the output to be spent by optionee before a given date provided they pay the specified amount to the optionor. After the specified date the output can only be claimed by the optionor.

3.1.7 Claim by Password

Used by cross chain trading, allows an output to be spent in one of two cases: two signatures are provided or one signature and a password.

3.2.0 Transaction Fees

BitShares X attempts to insure decentralization by minimizing barriers to entry. Bandwidth and disk space are two barriers to entry that must be kept low enough that the average individual can participate as a full node in the network. To achieve this we have settled on a maximum block

size of 1 MB every 5 minutes and a maximum life of an output of 1 year. This means that every node is only required to store at most about 100 GB of data per year (excluding indexes). However, while the maximum block size is 1 MB, the target block size is 512 KB and the transaction fees adjust automatically in an attempt to keep the block size less than 512 KB. Transaction fees are set as a price per byte to be paid in XTS.

The algorithm used to adjust the fees is as follows:

```
min_fee = .005 * total_shares  /  (512*1024 * 12*24*365)
next_fee_base = block_size * previous_fee / (512*1024)
next_fee = (99*previous_fee + next_fee_base) / 100
next_fee = max(next_fee,min_fee)
```

This algorithm should cause the price to rise while blocks larger than 512KB are being produced and fall toward the minimum fee while blocks less than 512 KB are being produced. Rising prices will reduce demand for transactions and falling prices will increase demand. Therefore the block chain has an automatic means of setting fees. This should reduce complexity and uncertainty around what kind of fee one should pay to get included in a block as experienced by Bitcoin users.

The minimum transaction fee is set such that if all blocks were 512KB then 0.5% of the share supply would be paid each year in fees.

3.3.0 Dividends

Because we view BitShares X as a DAC that seeks to make a profit, it should pay dividends to the shareholders. The dividends are paid from transaction fees which are destroyed. Reducing the supply of XTS is economically equivalent to dividing the transaction fees among all holders of XTS proportional to their ownership.

While many users may not feel like they are getting a positive return when dividends are paid by destroying shares rather than as a growing balance, this detail can be fixed in the user interface rather than in the block chain itself. BitShares X will display a users XTS balance as a percentage of the current share supply and therefore should see their balance grow each and every block.

When a user spends their XTS the user interface will convert the percentage specified back into actual shares before producing a transaction for the block chain.

3.4.0 Block Production

Blocks are produced using the TaPOS algorithm and combined with the Momentum Proof of

Work first introduced by BitShares PTS. The mining difficulty is adjusted based upon the average block interval of the past 24 hours with the goal to target one block every 5 minutes. There are no mining rewards and transaction fees are split with the miners proportional to the number of Proof of Stake votes provided by the miner relative to 3rd party transactions. A miner that doesn't include any Proof of Stake votes does not get any of the transaction fees. A miner that only provides 1% of the votes gets 1% of the transaction fees.

The timestamp on each block must be greater than the block before it and less than the current time or it will not be propagated across the network.

If two blocks are produced at the same time the block with the most votes will win. The miner who lost the tie break will have their votes included in the next block automatically.

4.0.0 Order Matching Algorithm

BitShares X uses a non-traditional order matching algorithm. The algorithm chosen always gives the buyer exactly what they ask for instead of traditional order matching which gives the buyer at least what they ask for and sometimes more. Any time a the highest bid is greater than the lowest ask the difference is captured as fees by the network. In the case of BitShares X there is no distinction between buyer and seller because someone buying XTS with USD is no different than someone buying USD with XTS. Both sides of the trade get the price they specified rather than using the same price for both parties. The difference is kept as fees for the network.

The reason for this algorithm is to penalize those that would attempt to manipulate the market by walking the book via fees charged proportional to the amount of the book they walk in a single go. This is designed to enforce value-based investing rather than technical trading. This is expected to reduce volatility and liquidity as trading noise is removed from the network.[6] No market participant should be able to complain about getting exactly what they ask for and thus they should only place orders they think are fair.

The result of this fee system is that some BitUSD will be taken out of circulation and effectively destroyed. This provides a growing base of support for the BitUSD price as there is now less BitUSD in circulation than the shorts require to cover their positions. In many ways this is like earning a dividend or interest on your BitUSD.

First all bids and asks are matched, then if the highest bid is above the margin call threshold of any *Claim by Cover* position, the collateral is used to accept the bids starting with the position with the least collateral.

[6] See Section 1 of "Noise" by Fischer Black (1986)
http://www.moneyscience.com/pg/bookmarks/Admin/read/49060/noise-fischer-black-pdf-1985

5.0.0 Hypothesis

BitShares X is an economic experiment where we believe the market can automatically reach a consensus that a digital asset lent into existence, backed by collateral, can maintain a high degree of correlation with arbitrary real world assets and thereby create a digital currency with the price stability of the dollar and all the other properties of Bitcoin. That said no systems have been created that have the unique properties of BitShares X. We would like to present some of our hypothesis below while making no promises that BitUSD will behave in any particular way.

5.1.0 1 BitUSD will track the USD / XTS ratio within a narrow range at all times.

This hypothesis is based upon the belief that the prediction market demand fundamentals will override any mismatch between the amount of BitUSD owed on short positions and the amount of BitUSD in circulation.

5.2.0 1 BitUSD will track the USD / XTS ratio with high correlation but with a relatively fixed premium or discount that may change occasionally during extreme market events.

This hypothesis is based upon the fact that there may be more or less BitUSD in circulation than is required to cover by shorts and that this mismatch will result in a proportional premium or discount. It is also based on the fact that the steady destruction of BitUSD to market fees may be perceived as a positive yield. On the other hand the risk of a rapid fall in XTS price resulting in under-collateralized BitUSD may result in a slight discount to USD. Whether there is a premium or discount is ultimately irrelevant so long as their is a high correlation with the price changes of USD vs XTS.