BitShares 2.0: Financial Smart Contract Platform

Daniel Larimer, Lance Kasper
Cryptonomex, Cryptonomex.com
Blacksburg (VA), USA
Email: {dan, agent86}@cryptonomex.com

Fabian Schuh
BitShares Europe, BitShares.eu
Erlangen, Germany
Email: fabian@bitshares.eu

***Abstract*—Ever since Satoshi Nakamoto released his whitepaper and corresponding software for bitcoin, the cryptocurrency ecosystem grew rapidly. Bitcoin created an ecosystem which everybody could use to *transfer* value without unnecessary middlemen, banks or counterparty risk. Having the blockchain and consensus technology established and proven stable, the question arose whether this technology could be applied to allow *trading* of multiple assets without the need for a broker or central entity. The aim of BitShares 2.0 is to innovate the term *decentral exchange* (DEX) and not only provide trading of assets but additionally offer classical financial instruments on the blockchain. Two of these instruments — market pegged assets and user-issued assets — are discussed here.**

I. Introduction

In todays world, crypto-currencies are unique in that they are the only digital currency that is not someone else's liability. They are *fungible*, *decentralized*, and as *valuable* as the network of users that support them. Unfortunately, they suffer from very high volatility, because their perception of value constantly changes as users enter and leave the ecosystem. Although many professional traders appreciate this volatility, it prevents its adoption as a *payment* solution.

The traditional approach to creating a *stable* asset is to accept deposits and issue a digital token as a *claim receipt* (i.e. "I Owe You"). Under this approach, the token is valued by the market as the underlying asset, discounted by any credit risk associated with the issuer. This can work well for transactions, but less well as a form of savings. Furthermore, history has repeatedly proven that issuers eventually go bankrupt due to fraud, incompetence, or government intervention.

More recent alternative approaches have used a crypto-currency as *collateral* in a *contract for difference* (CFD) [1]. Under this approach, two parties take opposite sides of a trade, where one party is guaranteed price stability, and the other party is granted leverage. This approach works as long as sufficient collateral exists, and the contract can be settled by an honest 3rd party with a price feed.

These contracts are *derivative instruments* and part of a wider definition of *financial instruments*. Since financial instruments is defined as *tradable* assets of *any* kind they can (in general) be cash, proof of ownership, or a contractual right to receive or deliver a financial instrument.

BitShares, as a decentral counterparty-trust-free platform for financial smart contracts which operates over the internet, offers a set of financial instruments including CFDs. Several other financial instruments are fully implemented, one of which can act as *derivative* with *cash* as underlying asset. These derivatives contracts derive its value from the performance of an underlying entity and are thus often referred to as *market pegged assets* (MPA) or "smart-coins", and will be presented in section II-B.

Additionally, the BitShares platform provides an abstract feature known as "user-issued assets" (UIA) to help facilitate as wide range of profitable business models for certain types of services. The term refers to a type of custom token registered on the platform, which users can hold and trade within certain restrictions. The creator of such an asset publicly names, describes, and distributes its tokens, and can specify customized requirements, such as an approved *whitelist* of accounts permitted to hold the tokens, or the associated trading and transfer fees. These tokens allow for diverse use-cases such as, for instance, ownership tracking, crowd fund raising, IOUs, coupons, and many more and will be discussed in section III

In order to *trade* financial instruments, BitShares provides a high-performance *decentral exchange* (DEX), with all the features expect from a trading platform (see section IV). Any two assets that are registered on the blockchain (MPA or UIA) may be traded against each other at any time. Orders can be settled almost instantly up to at least 100.000 transactions per second. With this kind of performance on a decentralized exchange, there is no more need to risk funds in centralized exchanges.

In the following we will discuss the financial instruments available in the BitShares network as well as the DEX. It is recommended to previously read through the basic technological components of BitShares in the other white papers [2], [3], [4].

II. Market Pegged Assets (MPA)

A crypto-currency, with the properties and advantages of Bitcoin, that is capable of maintaining price parity with a globally adopted currency (e.g. U.S. dollar), has high utility for convenient and censorship resistant commerce. This can be achieved by BitShares' market pegged assets (MPA), a new type of freely traded digital asset whose value is meant to track the value of a conventional underlying asset by means of contracts for difference (CFD).

This work was supported by Cryptonomex and honorable members of the bitsharestalk.org community.

A *SmartCoin* (synonym for MPA) is a crypto-currency that *always* has 100% or more of their value backed by the BitShares core currency (BTS), to which they can be converted at any time, as *collateral* in a CFD.

What makes MPAs unique is that they are free from counterparty risk even though they resemble a CFD backed by collateral. This is achieve by letting the network itself (implemented as software protocol) be responsible for securing the collateral and performing settlements as will be described in more detail below.

We will present SmartCoins as a viable open source alternative to the expensive banking system. Achieving price parity with a commonly used currency facilitates pricing and acceptance by merchants. Additionally it reduces the need to calculate capital gains and losses on volatile assets to determine tax liability. In short, BitShares brings *publicly* auditable open source banking to anyone with access to the internet. MPAs allow savers and spenders to choose preferred asset types. This brings flexibility and ease of use to the open source banking experience.

The subsequent paragraphs will explain how market pegged assets including (for instance) *BitUSD* (intended to track the value of the U.S. dollar) achieve price parity while minimizing risk to holders.

A. Price Stability

Ever since the bitcoin blockchain initiated the age of decentral public ledgers, economists and engineers are trying to achieve a *stable* or *price pegged* crypto-currency. The following two subsection want to discuss the meaning of a *stable* or *pegged* currency and show how BitShares fills the gap.

1) Definition of Price Stability : Before we discuss how BitShares achieves price *stability* we first need to define what properties make a currency *stable*.

In the U.S., for instance, the Federal Reserve (FED) has as a mandate of *stable prices* and it is almost universally accepted that this is a good mandate. The same holds true for the Euro with its stability being *controlled* by the European Central Bank (ECB). Mostly every country/nation or federation applies a similar concept.

It is also widely accepted among many crypto-currency fans that, in the case of the US dollar, the FED has failed at their mandate because of persistent rise in prices resulting in the dollar losing 99% of its *purchasing power* since the FED was founded in 1913. As a result people in the crypto currency space are attempting to provide an alternative currency that can achieve the FEDs mandate. The goal of price stability at its heart is the same as *price fixing* and this is a well known economic fallacy that crypto-currencies should avoid.

The goal of the FED price stability mandate is to mask the systematic theft of all increases in the production efficiency of the economy. Lets assume the FED managed to keep prices stable through their monetary policy with 0% price inflation over 20 years. Now lets assume that during this same 20 years the invention of the computer and Internet resulted in a 3x increase in efficiency and thus there are now 3x as much food, cars, phones, houses, etc. For the sake of this example we will assume the population is the same and everyone has the same amount of money in the bank. You would normally expect that everything would be 1/3 the price and that everyone would be able to afford 3x their prior life style. But because of FED intervention they have managed to also increase the money supply by 3x and distribute it to their friends. The end result is that some people get a 1000x increase in life style while everyone else stands still.

We can conclude from this that the mandate for price stability is a goal meant to mislead the general public and mask theft from the lower and middle classes on a massive scale even at 0% price inflation. It would be ridiculous to bring this same mandate to crypto currencies which aim to free us from monetary enslavement.

We also notice that the goals should not be *price stability* nor should we target a *stable value* or *purchasing power* (at least not yet). What we really want instead is

- a *predictable* price with reduced volatility
- a unit of account that doesn't have any meaningful capital gains or losses for tax purposes
- a somewhat reliable ability to predict the future value of a token.

Hence, price "stability" really means price *predictability* within some tolerance level. In the case of the U.S. dollar, a willingness to accept a 5% loss (in purchasing power) per year demonstrates that predictability is more important than stability [5].

2) It needs a Price Floor : The first proposal of the BitAsset system has evolved over the 9 months since it first launched as we learned how market participants reacted to various rules. Liquidity is critical to confidence in the value of the token. A system with unbalanced rules will tend to bias the price in one direction or the other. Early on, BitUSD was driven down to $0.85 as demand for shorting outstripped demand for BitUSD and shorts were not forced to cover. Then, after implementing 30 day forced covering rules, the price stabilized around $0.98 to $1.00. Later, as the bear market progressed, we now have BitUSD trading at $1.05 or more because everyone is scared to use leverage and those that have open positions look to cover their position while those who hold BitUSD are not looking to sell. Over the course of these past 9 months, we have seen 3 different markets and had an opportunity to better understand the behavior of market participants.

In order for BitUSD to be accepted as being equal to $1.00 for the purposes of setting prices and online shopping, it only needs to maintain a *floor* of $1.00. If it can maintain a floor of $1.00, then merchants can accept it and know their margins are safe and that they are not exposed to currency risk. In order to enable a guaranteed floor, all BitUSD can be force liquidated at a trustworthy price feed the hour. If this rule is present, then those who create the BitUSD must sell it at a price that properly accounts for this risk of so called *forced settlement*. This means that at almost all times new BitUSD

will only enter circulation when there is a buyer willing to pay a premium for a guaranteed floor.

As we will see, since USD holders can initiate so called *global settlement*, there is no need for artificial forced covering every 30 days. This relieves shorts of risk, helps increase short demand, and keeps the price of BitUSD near the floor.

3) Price Feeds : In order for settlements to convert any smartcoin into the core asset (e.g. BTS in the BitShares network) at a fair price, the blockchain needs to be aware of the external price of BTS.

In BitShares, this is achieved by means of a set of N trusted *delegates*. These delegates have to be elected by the corresponding BitShares shareholders (e.g. holders of BTS) and can be constantly reviewed as all prices are put on the blockchain in a public manner by means of transactions of a particular type.

Having a set of N prices $p_i,\ 1 < i < N$ for an arbitrary MPA on the blockchain, the protocol obtains a single price $\tilde{p}$ by the use of the *median* according to:

$$x = \text{sort}(p_i) \tag{1}$$

$$\tilde{p} = \begin{cases} x_{\frac{N+1}{2}} & N \text{ odd} \\ \frac{1}{2}\left(x_{\frac{N}{2}} + x_{\frac{N}{2}+1}\right) & N \text{ even.} \end{cases} \tag{2}$$

Hence, this price is resistant against misbehaving delegates in such as only majority of published prices (for a particular MPA) can manipulate the outcome of the median and hence the price from blockchain perspective.

Obviously, the shareholders are required to constantly monitor the published prices of their delegates and should make public note about discrepancies.

B. Issuance and Supply of Collateralized Smartcoins

A BitShares MPA can be viewed as a contract between an asset buyer seeking price stability and a *short seller* seeking greater exposure to BTS price movement. The open source BitShares software program implements a decentralized marketplace for MPA where all transactions are recorded on the shared block chain ledger and the software enforces the market rules. This block chain based marketplace is referred to as the *decentral exchange* or *internal market* (c.f., section IV) to distinguish from *external markets* such as websites that facilitate the exchange of government issued currencies with crypto-currency.

SmartCoins are tokens of a particular MPA (e.g. bitUSD), take the concept of a contract for difference, and make the long side fungible. For the purpose of this discussion, we will assume that the long side of the contract is BitUSD and that the backing *collateral* is BTS (the BitShares core asset).

In practice, bitUSD are created on the BitShares blockchain when a BTS holder asks the network for them by handing over *collateral* to the network essentially locking them in a contract for difference.

The collateral is only returned to the short seller when assets are purchased back from the market and effectively destroyed to fulfill the contract. This is referred to as *covering a short*. If the value of the collateral relative to the current price of the market pegged asset falls below a certain margin of safety the assets can be automatically repurchased from the market before collateral becomes insufficient. These rules create systemic demand for market pegged assets while allowing them to remain fungible. To protect your contract against *margin calls* (automated, network initiated force settlement of your contract at the price feed), you should at least maintain the so called *maintenance collateral level* at all times. Hence, the collateral only needs to be high enough to cover any slippage as a result of a short squeeze.

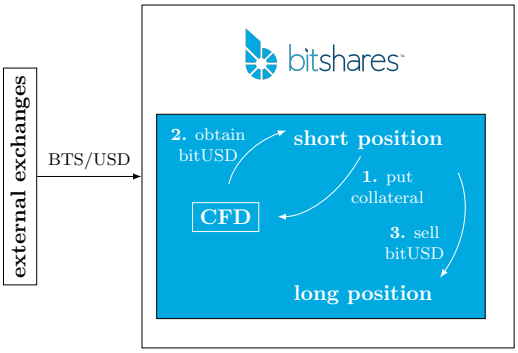

Fig. 1. Illustration of

Hence, at the moment of creation, the position of the *shorter* has not changed at all because he can directly cover the short position using the bitUSD to gaining back his BTS used as collateral.

In summary, the following set of market rules apply to all market pegged assets (for the sake of simplicity, we here focus on the MPA bitUSD):

- Anyone with BitUSD can settle their position within an hour at the feed price.
- The least collateralized short positions are used to settle the position.
- The price feed is the median of many sources that are updated at least once per hour.
- Short positions never expire, except by hitting the maintenance collateral limit, or being force-settled as the least collateralized at the time of forced settlement (see point 2).
- In the event that the least-collateralized short position lacks enough collateral to cover at the price feed, then all BitUSD positions are automatically force settled at the price of the least collateralized short.

A simple metric for testing the validity of our claim that 1.00 BitUSD is always worth at least $1.00 is to demonstrate that, if you can find someone willing to sell 1.00 BitUSD for $1.00, that it would be the cheapest option for buying BTS. This means that 100% of the buying demand for BTS would be available to give liquidity to BitUSD holders as a priority over BTS holders.

C. Perspectives of Participants

While the rules are simple, the consequences are less obvious. Let's analyze this from the perspective of the various players and attempt to prove that this condition is met.

1) The Short Position : When deciding a price at which to enter a short order, a trader must consider the risk of forced settlement. In this case, no trader will attempt to short at or below the price feed, because they could be forced to settle at the price feed. In fact, a smart trader would allow enough of a spread to account for the risk of being forced to settle at a feed price that was off by a small amount. In practice, the risk posed by the feed error is balanced equally between being in the favor of the short and in the favor of the long, leaving only the risk of being forced out of their position at an inopportune time.

A short can minimize their exposure to the feed by providing enough collateral to keep far above the least collateralized positions, and thus very unlikely to be forced to settle at the feed or at an inopportune time.

In practice, the only way new BitUSD enters circulation is if there is someone willing to pay enough of a premium to convince a short to provide guaranteed liquidity at the price feed on demand, while also covering the cost of exchange rate risk. This premium will be higher for the backing crypto-currency in a bear market, and will be lower in a bull market.

Someone who is short has only one way to exit their position: by buying BitUSD off the market. This means that a short must also factor in the risk that the premium may change. If a short position is entered in a bull market with a 0.1% premium, it may be forced to exit during a bear market with a 5% premium. In this event a short position is exposed to both exchange rate of the dollar vs. BTS and the premium risk. On the other hand, a short entered during a bear market with a 5% premium may get to cover during a bull market with a 0.1% premium.

For all intents and purposes, the premium is expected to move in the same direction as the price, and thus speculators who only care about relative price changes can ignore the premium.

2) The Long Position : The very first buyer of BitUSD will have to pay the lowest premium set by the shorters. For the sake of discussion, let's assume the first BitUSD was created in a bear market and cost $1.05 to create. The holder of that BitUSD has two options: sell it on the market for $1.04, or request forced settlement for $1.00. Clearly, the forced settlement option would only be used in situations where there was a decrease in total demand for BitUSD and there were no offers to buy it above $1.00.

As a trader only looking to trade back and forth between BitUSD and BTS, this premium doesn't matter. Such as trader is exposed to volatility in the premium, but that risk is limited to $0.05 in this example. In practice, the premium is expected to be relatively stable and predictable.

3) The Customer's Perspective : A customer looking to buy goods and services with BitUSD finds himself paying a premium to acquire BitUSD from the market. This means that customers will prefer merchants that offer a discount equal to the premium paid. On the other hand, the premium is a wash for a customer that earned BitUSD at a nominal value of $1.00. In fact, the only people to whom the premium matters are those who are looking to enter or exit the ecosystem. Once a customer or merchant is within the ecosystem, it is easy to simply trade BitUSD at parity, even if it is theoretically worth slightly more outside the ecosystem.

Customers use BitUSD because it provides them the convenience and freedom of a crypto-currency, and has the lowest transfer fees of any other payment platform besides being significantly more convenient than fiat.

Of course, merchants and customers are free to negotiate the best way to split the premium, and the free market will take care of the rest. In the mean time, all participants can rest assured that BitUSD is always worth *at least* $1, and can consider the premium for entering the ecosystem as a one-time fee comparable to fees required for the exchange of foreign currencies.

4) The Merchant's Perspective : A merchant wants to be able to price merchandise in BitUSD, and obtain real USD in the bank account, in a reasonable time, with minimal risk. In this case, a merchant would place BitUSD on the market at $1 per BitUSD. As discussed, BTS buyers fight for the opportunity to buy BitUSD at that price.

A smart merchant might recognize that 1 BitUSD can actually fetch $1 plus a variable premium, and start preferring that customers pay them in BitUSD at face value. An even smarter merchant might offer a discount to customers that pay in BitUSD.

Any way you slice it, merchants have a financial incentive to advertise BitUSD as the preferred payment mechanism, because they know that $1.00 is the lower bound on what BitUSD is worth.

5) BTS Shareholders and Investors : A buyer with dollars, looking to buy BTS, knows that 1 BitUSD can be used to buy $1 worth of BTS (plus the current premium). He also knows that this premium can never be negative, because of the option to force-settle at the price feed. In this situation, he can know with certainty that if he can convince someone with BitUSD to sell for $1.00, he can buy more BTS than if he simply buys BTS with his dollars directly. The higher the premium, the more incentive exists to buy BitUSD for $1.00.

This means that, in a BTS bear market, the BitUSD price gives the highest premium of the BTS price, and BitUSD becomes the easiest to sell. In practice, the BitUSD:USD market will reflect the premium, and traders will usually be unable to find anyone willing to sell for exactly $1.00.

If a buyer is looking to purchase a large quantity of BTS without moving the price, he can start by buying up BitUSD with dollars. This will slowly raise the BitUSD:USD price, which is a signal to other market participants. A careful buyer might be able to avoid signaling the market. Then, after acquiring the position in BitUSD, the buyer can request forced-settlement all at once and get the price feed on the entire purchase.

Because all positions and trades are visible on the blockchain, all of this trading activity can be factored into the price, minimizing any potential profits to be made by attempted manipulation.

D. Price Manipulation

There is always concern of price manipulation. Someone with a large amount of money on both sides of a trade can use their funds to manipulate the markets and thus the price feed. If the amount of money they lose manipulating the markets is less than the amount of money they can gain by manipulating the price feed, then it will be profitable to manipulate the market at the expense of either the BitUSD longs or the shorts. A low-collateralized short that sees a large force-settlement order requested can attempt to manipulate the markets and thus the feed against the BitUSD holder.

The risk of price manipulation is priced into the premium on BitUSD charged by the shorts, and thus should already be priced into the market. If price manipulation became a serious problem that caused very high premiums, then it could be addressed by the price feed producers, who can adopt a moving average over wider time windows to increase the difficulty of short-term manipulation. A variety of algorithms could be used to estimate a *fair price* that keeps BitUSD valued at least $1.00.

In practice, a feed producer can observe the BitUSD-to-USD market as an indicator on which way to adjust the feed. Generally speaking, the strategy that the feed producers adopt for controlling the feed should be public knowledge, because the shorts will ultimately rely on it. For the feed producers to change strategies in unpredictable ways could cause losses to both longs and shorts. Fortunately, it is assumed that shareholders primarily approve complying and quickly fire misbehaving feed providers.

E. Undercollateralization and Black Swans Events

All guarantees of SmartCoins are subject to the caveat that a SmartCoin can never be worth more than the collateral backing the least-collateralized short position. All collateral above the maintenance collateral limit is effectively meaningless when it comes to enforcing the peg. In normal market conditions, the value of the collateral is always more than sufficient, but, from time to time, markets can rapidly revalue the collateral.

If this revaluation happens faster than the short positions can be forced to cover, then all SmartCoins are liquidated at the exchange rate of the least collateralized short position. At this point, all positions are force settled and any additional collateral maintained by the shorts is returned to them. This is similar to an insolvent bank converting its deposits to equity.

F. Risks

The current implementation of market pegged assets in the BitShares system is designed to minimize risk of loss to market pegged asset holders. The collateral requirements and margin triggers were chosen conservatively to protect the holders of market pegged assets from volatility of the underlying collateral. Control over the price feed is distributed among N separately elected feed producers who compile information from multiple exchange sources. Despite such precautions, it is important to carefully explore risks of using the system. Risks can be broadly categorized as value risk, counterparty risk, or systemic risk.

1) Collateral Risk : Market pegged assets maintain their price parity due to being backed by collateral that has an established real world value. When the value of the collateral falls, the system is designed to react by driving the internal asset exchange to match the new real world exchange rate and trigger force settlements (i.e. margin calls) as necessary.

All collateral above the maintenance collateral limit is effectively meaningless when it comes to enforcing the peg. Maintenance collateral only needs to be high enough to cover any slippage as a result of a short squeeze.

However, there exists a possibility that the underlying collateral (BTS) drops in value so quickly the market pegged assets become under-collateralized. Often termed a *black swan event* (c.f., section II-E), a sudden crash of BTS value could prevent the system from adjusting in time. In this event, the full amount of collateral is no longer sufficient to purchase the market pegged asset back at the new real exchange rate. In such an event, assets may settle at the price fees and are converted back into the underlying collateral (BTS). This may expose costumers at the volatility risk of BTS. Under normal conditions, short term market movements, spreads, and fees charged by exchanges may also affect the potential cost of conversion into and out of market pegged assets.

2) Market Depth Risk :

3) Counterparty Risk : Unlike many attempts to create a digital asset that tracks the dollar, market pegged asset are not an *I owe you* issued by any entity. For this reason, it does not rely on a specific counterparty to honor its value (unless a software protocol is seen as entity).

Although manipulation risk occurs in any market, it is minimized by the open source and auditable nature of the BitShares system and carefully considered market rules. BitAssets stored on a *centralized* exchange become IOUs and are subject to counter party risk [6]. This risk is not a property of the BitAssets themselves. We recommend that users never deposit BitAssets on an exchange and instead only use gateways that issue their IOUs onto the BitShares network. This way you can trade your BitUSD against gateway IOUs without exposing your BitUSD to counter party risk while in the order book (more details in section IV-C1).

4) Systemic Risk : Systemic risk is a catch-all for other risks required to utilize the system. The primary risk is individuals are responsible for protecting the cryptographic private keys that sign transactions proving ownership of assets. These keys must be protected from theft or loss. This risk can be greatly reduced and virtually eliminated by following best practices.

Systemic risk also includes the possibility of an overlooked fatal flaw in the open source software or the possibility of

large scale failure of global network infrastructure and should reduce over time.

G. Privatized SmartCoins

Alternatively to regular MPA like the bitUSD, BitShares offers entrepreneurs an opportunity to create their own SmartCoins with custom parameters and a distinct set of price feed producers.

User-issued SmartCoin managers can experiment with different parameters such as collateral requirements, price feeds, force settlement delays and forced settlement fees. They also earn the trading fees from transactions the issued asset is involved in, and therefore have a financial incentive to market and promote it on the network. The entrepreneur who can discover and market the best set of parameters can earn a significant profit. The set of parameters that can be tweaked by entrepreneurs is broad enough that SmartCoins can be used to implement a fully functional prediction market with a guaranteed global settlement at a fair price, and no forced settlement before the resolution date.

Some entrepreneurs may want to experiment with SmartCoins that always trade at exactly $1.00 rather than strictly more than $1.00. They can do this by manipulating the forced settlement fee continuously such that the average trading price stays at about $1.00. By default, BitShares prefers fees set by the market, and thus opts to let the price float above $1.00, rather than fixing the price by directly manipulating the forced settlement fee.

III. User-Issued Assets (UIA)

In addition to the aforementioned market pegged assets, BitShares allows individuals and companies to issue their own tokens for anything they can imagine. The potential use cases for user-issued assets (UIA) are innumerable, and the regulations that apply to each kind of token vary widely, and are often different in every jurisdiction. BitShares provides the tools to allow issuers to remain compliant with all applicable regulations when issuing assets.

A. Deposit Receipts

Before discussing a subset of potential use-cases in this paper, we first present the tools and optional administrative rights given to the issuers of a given (user-issued) asset.

For instance, banks are simply companies that maintain a database of customer account balances and facilitate the transfer of these assets among their depositors. Companies like Dwolla and Paypal essentially issue deposit receipts, and then offer cheaper transfers among their users than between banks. The deposit receipt example is probably one of the most important, and yet most heavily regulated, use cases of user-issued assets.

With BitShares, it is now possible to move company-internal databases onto the blockchain where deposits can be used with smart contracts such as the internal markets, escrow, or bonds. In order to make traditional banking more profitable (through a decentral account balance database) and incorporate services like Paypal and Dwolla to their business model while offering more freedom to the costumers we were talking to many different banks and exchanges, and have learned a lot about what the law requires of those who wish to issue deposit receipts. The following shall briefly discuss how BitShares can assist to comply with those rules, technically.

1) Know Your Customer : First and foremost the issuer must know every single customer. BitShares supports this by enabling both *whitelists* and *blacklists* on the block chain. Rather than requiring every issuer to whitelist every customer separately, an issuer may specify a set of identity verifiers that they trust to do this job. This allows issuers to benefit from the network effect of validated users without having to do any direct identity verification themselves.

When an asset enables whitelists, no account may send, receive or trade that asset without being on an authorized whitelist. With this feature, account funds can effectively be frozen by removing them from the whitelist. Of course this only affects those tokens of that particular UIA.

2) Asset Seizing : From time to time, an issuer may be required to seize funds as a result of a court order. While this may be unappealing to crypto-currency purists, it is an unavoidable reality of trust-based assets. An issuer can determine whether or not they wish to revoke this privilege, but it may be a requirement in some jurisdictions. Once again, this privilege only affects tokens of a particular UIA and does not apply to market pegged assets as the bitUSD.

3) Market Restriction : An issuer who offers both USD and EUR deposits may need to restrict direct trading between their USD and EUR assets to avoid being subject to foreign currency exchange regulations. Some crypto-currency exchanges allow trading between fiat and crypto-currencies, but not between two fiat currencies. Without this feature, many exchanges would be unable to issue their assets on the BitShares blockchain. Hence, an issuer may chose to also white- or blacklist trading partners for their user issued assets (i.e. IOUs). Fortunately, MPAs, such as the bitUSD are not fiat and hence need not be blacklisted.

4) Transfer Restrictions : A transfer-restricted asset allows the holders of the asset to trade it in the markets but not transfer it from person to person. Only a few crypto-currency exchanges allow user-to-user transfer of funds outside the market, because this particular activity is often subject to a different set of money transmission regulations. For that reason, known exchanges make use of so called coupon codes if costumers demand for user-to-user transfers.

B. Profiting from UIAs

There are many ways to profit from issuing an asset. As the issuer you have complete control over market fees and can tune parameters such as the percent of each trade that is collected as a fee. This percentage can be bounded by a minimum and maximum fee. The combination of these parameters give issuers great flexibility in pricing.

C. Use-Cases

Having discussed the administrative possibilities of UIAs, we now list and briefly describe a few example use cases.

1) Company Shares : Corporate shares are heavily regulated in most countries by their corresponding exchange authority, such as the *Securities and Exchange Commission* (SEC) in the U.S.

However, none of those regulations prevent them from being issued or traded on an alternative trading system [7]. The regulations in many jurisdictions require all shares to be registered (a.k.a. held by known identities).

Since the BitShares network offers whitelisting for costumers of UIA according to section III-A, corporate shares can certainly be issued and traded in the BitShares Decentralized Dex (see section IV).

2) Event Tickets : Event tickets are a largely unregulated use case for user-issued assets. Tickets to a school play could be issued as digital tokens that are auctioned off to the highest bidder, who would then resell them. This ensures that the ticket issuer raises as much money as possible up front, while transferring the risk of ticket sales on to speculators. On the day of the event, the issuer can freeze all trading of the asset and then allow users to cryptographically check in.

Furthermore, the blockchain maintains the database of tickets which drastically reduces the organizational overhead.

3) Rewards Points : Merchants around the world offer rewards points for loyal customers. These points are accumulated to earn discounts on future purchases. Rewards systems are a prime opportunity to add value by making them available to BitShares smart contracts.

Furthermore, because the issuer can set a trading fee for their UIA, merchants can have an additional revenue stream from people trading their rewards points.

4) Crowd Funding : With BitShares, decentralized crowd funding never was easier. Technically the process breaks down to as few as two steps: (a) Create a new token that should represent your project, and (b) issue and sell your shares on the DEX. The issuer is now free to choose to sell them for bitUSD, bitEUR, or any other token and free to define the price for each share.

Whether being used as a transferable coupon for a pre-sale, or doing an IPO on a small company, issuing an asset is one of the most effective means of raising money for a cause.

5) Digital Property : Software and music licenses can be made transferable by issuing them as a digital asset. Every copy of a program can check to make sure that the user has control of a token before running. Software implementing such a licensing scheme can remain functional even if the company that produced the license goes out of business.

Trading cards can be simulated by creating many limited issue assets. Online games can use these assets to represent game items.

Further related possibilities include (but are not restricted to): ownership tracking, authorization, membership identifications, ...

6) Privatized SmartCoins (Stable Cryptocurrencies) : Price-stable crypto-currencies (a.k.a. SmartCoins) were the inspiration for BitShares. Now, users can create their own price-stable assets with custom parameters designed to track the value of any asset they can imagine. The benefit of price-stable crypto-currencies is that they are fully collateralized, and the issuer only needs to be trusted to appoint an honest set of independent (non-collusive) feed producers. Unlike deposit receipts, the value of a Privatized SmartCoin is secured even if the issuer disappears.

Bitshares provides many parameters that an issuer may tune. In addition to account whitelists, market restrictions, and transfer restrictions, the issuer of a private SmartCoin has control over:

1) Collateral Type
2) Initial Collateral Rate
3) Maintenance Collateral Rate
4) Forced Settlement Fee, Delay
5) Price Feed Update Rate
6) Global Forced Settlement
7) Trading and Withdrawal Fees

With these tools it is possible to emulate a pure contract for difference with periodic global forced settlement (i.e., monthly, yearly, etc), or to emulate BitShares 1.0 BitAssets by having a 30 day delay on forced settlement.

Arbitrary financial indexes can be used for the price feed to mimic all manner of exotic assets. In addition with publicly auditable accounts even mixed asset funds can be modelled with the advantage of verifiable ownership claims by the fund manager.

7) Information/Prediction Markets : A prediction market [8] is a specialization of SmartCoins where there is no need for margin calls or forced settlement because all positions are fully collateralized at any price. A prediction market has a price between 0 and 1 and the issuer settles all positions after the event occurs and the final price is known.

Prediction markets are quickly implemented with BitShares and the DEX. All that is needed a proper prediction criteria in the description of a newly created asset that anybody can issue by putting up collateral. While the event has not occurred, the price of this asset reflects the probability of an event to occur. Participants that have voted correctly will be able to settle their shares back to the network at a higher price and make a profit. This feature, in combination with the bitUSD, allows to reimplement most binary prediction and information markets currently established in a decentralized and trust-less manner.

These prediction markets can be very secure if the issuer is a multi-sig account with many independent and trustworthy parties involved.

D. Fee Pools

Issuers may optionally maintain a so called *fee pool*. The fee pool is a pool of BTS and an exchange rate at which the issued asset may be converted into BTS. This allows users to pay transaction fees in form of an asset even though the network requires fees to be paid in BTS.

When a user wishes to pay a network fee with the asset, the fee pool will step in to convert the asset into BTS at the rate that the issuer has specified. This means that issuers may charge a premium every time users opt to use their asset to pay network fees rather than paying them directly with BTS.

The purpose of the fee pool is to provide a convenience to users that would like to use an asset without concerning themselves with the details of acquiring BTS. Anyone may fund the fee pool, but only the issuer may specify the exchange rate. This exchange rate is automatically set to the settlement price if the asset is collateralized by BTS.

IV. Decentralized Exchange

Throughout history, centralized exchanges have repeatedly proven unreliable and untrustworthy. Whether it is MF Global, Mt. Gox, or BitStamp [9], [6], [10], many people have been cheated because they allowed a 3rd party to hold their funds. It doesn't matter how big they are, or how many auditors, regulators or insurers are involved, every kind of fraud, abuse, and theft can occur. In the modern financial system, these transgressions happen all too frequently within centralized banks and exchanges operating across the world.

Hence, in the following paragraphs, we introduce the decentralized exchange (DEX) within the BitShares network and discusses the benefits of using it.

A. Core Features of the DEX

A decentral exchange has a very particular set of advantages over traditional centralized exchanges and we would like to address some of them briefly below. The BitShares DEX comes with all of them. However, it is up to the reader and costumers to leverage those features in full or only partially.

1) Global Unified Order Book : Because BitShares can be access through an internet connection and there exists only one source of truth, namely *the blockchain*, there can only exist one global order book for one particular market. The impact of such a global unified order book is to improve market efficiencies (hence reduce all arbitrage opportunities), minimize spreads, and maximize liquidity. By having the trades executed on the BitShares network, we also eliminate high-frequency trading and front running because everyone has the same chance of filling an order. High frequency trading and front running depend upon centralized exchanges with high volume and deep markets. When the vast majority of trading activity moves to a decentralized, trust-free exchange with open order books, the remaining centralized exchanges become much less appealing to traders.

2) Separation of Powers : There is no reason why the same entity needs to be responsible for issuing IOUs and for processing the order book. It is only because these two roles are combined that we have a tendency toward centralization in the Bitcoin exchange space. If we want to create a decentralized exchange then the first step is to move the order book on to the blockchain where everyone can see it.

In this model, exchanges merely become gateways that receive USD and issue GatewayUSD on the blockchain. Later, they receive GatewayUSD and then execute a wire transfer. They will make their money entirely on transaction fees and not from a percentage of market fees.

The blockchain allows users to trade, for example, BitstampUSD against BitfinexUSD, in order to easily move funds from one gateway to another. Users could even trade BitstampUSD against BitstampBTC or BitstampUSD vs BitfinexBTC.

Unfortunately, simply moving the order book to the blockchain is not enough, because the market will naturally centralize around a few gateway IOUs and the markets for them. BitstampUSD is not fungible with BitfinexUSD because they have different trust profiles and regulatory considerations. Any of these IOUs are subject to default just like the IOUs that currently exist on the exchanges' internal databases.

What we need to do is move the trust from individual issuers to the blockchain itself. Hence, we have the bitUSD which is backed by collateral and is independent of governments, and trades for $1 independent of any gateway. It is also universal as you don't need to register anywhere to use bitUSD (or any other market pegged asset).

3) Trade Almost Anything : Trade in Gold, Silver, Gas, and Oil in addition to your national currency and crypto-currencies. Few limits exists on what can be traded on the BitShares exchange, given enough interest. The exchanges allows any two pairs to be traded directly. There is no need to ask the exchange to open up an additional market. If costumers prefer to trade Silver:Gold directly, they can simply do it. The BitShares exchange can support assets that can track stocks, bonds, indexes, or inflation. Companies can issue their own stock on the BitShares network and allow easy, low-cost trading with complete protection against naked shorting.

4) No Limits : You can trade any amount, at any time, from anywhere, without withdrawal limits[1]. All other legally compliant exchanges have daily withdrawal limits. Those who wish to exceed standard limits must provide increasingly invasive levels of documentation. Some exchanges, such as Coinbase [11], even limit what you can do with your money after you have withdrawn it [12]. Other exchanges demand documentation of how you earned your crypto-currency.

With BitShares, no one must approve your account. You have complete financial freedom.

5) Decentralized : Decentralization gives BitShares robustness against failure. When a centralized exchange is compromised, millions of dollars and thousands of users are impacted all at once. In a decentralized system, any attack or failure impacts only a single user and their funds. Users are in control of their own security, which can be much better than any centralized entity.

There is a fixed cost associated with attempting to hack an exchange or an individual user. The difference is the size of the reward. If you place a multi-million dollar bounty on attacking a specific exchange, then you can expect a lot more effort to be put into compromising that exchange than would be put into attacking your individual account.

[1]Restricted access may only apply to user issued assets, but not to market pegged assets, such as bitUSD, bitEUR, etc.

Within a given company, multiple people usually have access to customer funds. Currently, all centralized exchanges end up depending upon multiple people who share the responsibility of guarding the secret key that controls the funds. If any one of them is compromised, everyone's funds are put at risk. Because of this, being individually responsible for maintaining your own secrets is the only safe option.

Accessing funds in BitShares can be even more secured by means of corporate accounts that implement threshold signatures [2], [13] and validate only those transactions which signature weights (e.g. the CEO has more say than a worker) surpass a pre-defined threshold.

6) Secure : Every Dollar, Euro, bitcoin and ounce of gold held as a SmartCoin on the BitShares exchange is backed by at least 100% of the reserves of traditional centralized exchanges. The traditional banking system has long practiced what is call *fictional* reserve banking, more commonly known as *fractional* reserve banking. In the Bitcoin ecosystem, we demand at least 100% reserve. A single hack, mistake, or theft can quickly turn a 100% reserve system into a fractional reserve system, or worse, a no reserve system. Without any reserves, it is unlikely that an exchange can give you the funds it owes you.

By always maintaining reserves, you can rest assured that BitShares is solvent in almost any market. All of the reserves are kept as BTS held in collateral on the blockchain, and they cannot be stolen, because there are no private keys that can be compromised to steal all of the reserves.

7) Fast, but not too fast : With BitShares your trades execute in seconds, just like any centralized website interface. Unlike centralized exchanges, there can be no prioritized trading, front running, or hidden orders. This puts all traders on a level playing field.

On Wall Street, traders go to great lengths to get as physically close to the exchange systems as possible, because their trading bots make decisions so quickly that the speed of light is a considerable factor. Thus distinct fiber cables are put in the ocean between London and New York to improve profitability in Europe. A decentralized exchange is *location-neutral*, and gives everyone equal opportunity.

8) Decentralization of Privacy : Crypto-currencies depend upon a public ledger ,which makes privacy challenging, because everyone can see every transaction. Bitcoin gives every user one or more account numbers, and that gives many people a false sense of security. People assume that as long as no one knows your account number and you use a new account number with every transaction that no one can tie all of your bitcoins to your real life identity.

This is where the large centralized exchanges become a problem. In order to comply with government regulations, exchanges must know everyone they do business with. Since many bitcoin transactions flow through an exchange, the exchange learns who everyone is and can start to track who is doing business with whom. Coinbase is already closing accounts [2] based upon who you do business with after withdrawing your bitcoins.

In order to have even the slightest bit of privacy, the exchange functionality needs to be divided among hundreds of parties who are unlikely to collude to compromise identity. This is not economically practical today, because the exchange order book creates market incentives that naturally tend toward centralization in just a few exchanges with the vast majority of market share.

In BitShares, your identify need only be verified by issuers of IOUs (e.g. ccedkUSD) in order to comply with fiat regulations. Once traded for bitUSD your link to ccedk can be removed quickly by means of *blinded transactions* that allow to publicly move funds without revealing the exact amount [2], [14]. If issuers approve, blinded transactions may even be performed for UIAs directly.

B. Order Matching

The old BitShares 1.0 protocol went to great effort to avoid market manipulation and eliminate the supposed evil of front running. To stop front running, all orders were matched at the exact price specified in the order. Any overlap in the market was captured as fees. This means that to get the best price, a client would have been forced to submit many orders manually matching each order. This had the side effect of slowing down how quickly someone could walk the book. This slow down effect was pitched as protection against market manipulation attacks on Smartcoins.

Experience has taught us that the lack of standard limit orders has harmed market liquidity and adoption. BitShares 2.0 matches orders on a *first-come, first-serve basis* and gives the buyer the best price possible up to the limit. Rather than charging unpredictable fees from market overlap, the network charges a defined fee based upon the size of the order matched and the assets involved. Each asset issuer gets an opportunity to configure their fees as described in section III-D.

In contrast to BitShares 1.0, there will also be limit-orders that allow to buy on the market up to a pre-defined price. This allows to instantly fill any order below or above your price at the cost of a single fee (c.f., section V).

C. Collateralized Smartcoins

The heart of BitShares is the SmartCoin system which enables the creation of collateralized IOUs from the BitShares network. A BitUSD has all of the properties of Bitcoin combined with the price stability of the US dollar. At any point in time you can sell a BitUSD for at least 1 dollar worth of BTS. If at any time the value of the collateral falls below a certain point the blockchain will automatically buy back the BitUSD with a dollars worth of BTS (force settlement, see section II-B).

When you hold BitUSD the value of your holdings will remain pegged to the dollar so long as BitShares have a value > 0. This means that BitUSD is secure against just about everything but an unfixable software bug in the BitShares protocol itself. By the time BitShares matures to the level Bitcoin is at today, we expect the probability of that kind of bug to be similar to that of Bitcoin having such an event.

[2]https://www.cryptocoinsnews.com/coinbase-bringing-big-brother-bitcoin-accounts/

1) Fiat Gateways : The roles that traditional exchanges perform today encompass:

1) Receiving crypto-currency and issuing IOUs.
2) Receiving fiat and issuing IOUs.
3) Redeeming IOUs.
4) Processing an order book.

Each of these stages requires a high degree of trust and direct counterparty risk, because they involve an IOU from the exchange. To get the best liquidity and lowest spreads requires a large and active order book, and this means that most people gravitate toward a few core exchanges, leaving everyone exposed to the same counterparty risk.

Moving money into or out of an exchange often incurs a significant time delay, which means that active traders must keep their funds on the exchange. This magnifies the amount of risk to users of the exchange. It also magnifies the risk to all users in the crypto-currency ecosystem. Each large security breach results in significant sell pressure, from both the thief looking to cash in their loot, and from regular users hoping to sell before the thief.

With the separation of powers, we only need gateways that perform item 1, item 2 and item 3 while order book processing and storage of account balances are managed by the BitShares protocol/network. An entity issuing and redeeming IOUs for an other asset in BitShares is called a *gateway*. In contrast to central exchanges, the IOUs are send directly to the wallet of the costumer directly and are his under full control (see section III-A).

Many gateways prefer the low-risk approach of one-for-one redemption and will simply allow the GatewayUSD to float against BitUSD with a small but variable spread in the market. Users then pay a small variable conversion cost as they exit from BitUSD to fiat USD through GatewayUSD.

On the other hand, many users will want a direct conversion from BitUSD to fiat USD. In this mode of operation, the gateway takes care of providing all of the liquidity within a fixed percentage transaction fee. The gateways then compete on offering the lowest possible spread.

Once this happens, BitUSD is effectively as good as USD with a small fixed conversion fee. This fee will likely be no more than the withdraw and deposit fees that current exchanges charge. At that point, BitShares will be a fully operational exchange with many banking partners and no limits. At no point in time will user deposits ever be subject to default or confiscation by an exchange or gateway. A truly decentralized exchange will have been realized, and the original vision of BitShares completed.

V. Fees

In the BitShares ecosystem every operation is assigned a certain fee. These fees are subject to change. However, the fees are defined solely by shareholder approval and, hence, every shareholder of the BitShares core asset (BTS) has a say as to what the fees should be. Hence, if shareholders can be convinced to reduce a certain fee and consensus is reached, the fee will be reduces automaticall by the blockchain.

The following fees are associated with the DEX and financial instruments: `transfer`, `limit-order-create`, `limit-order-cancel`, `call-order-update`, `fill-order`, `asset-create`, `asset-update`, `asset-update-bitasset`, `asset-update-feed-producers`, `asset-issue`, `asset-reserve`, `asset-fund-fee-pool`, `asset-settle`, `asset-global-settle`, `asset-publish-feed`. Some more fees are available on the protocol level but are not subject of this paper. Which fees currently apply can be extracted from the blockchain and will certainly be put on a distinct information page of most wallet software.

VI. Conclusion

The BitShares network offers financial instruments for everyone to use at a low fee. Not only is there a decentral exchange (DEX) but also smartcoins and user issued assets.

The DEX allows for trade of any arbitrary pair of assets issued on the BitShares blockchain. The order-matching algorithm is equivalent to most central exchanges and allows to directly fill a given order or walk-the-books up to a given price by means of a limit order.

SmartCoins are a powerful tool for everyone from speculators and savers, to traders and entrepreneurs. The BitShares platform provides a toolset with which innovators can experiment to find optimal currency solutions using free market discovery. It was shown that in order to achieve a price *predictability*, a price floor of $1.00 USD per bitUSD is most reasonable. Hence, any long position can be settled at the price feed.

Additionally, we have shown that user issued assets (UIA) offer countless opportunities to reduce costs. Not only can they be used to simply store a token on a decentralized database (the blockchain), but it was also shown that IOUs can be issued complying with regulations.

Thus, the foundations of the BitShares network have been laid out to shift the paradigm of classical banking towards peer-to-peer financing at large scale.

References

[1] Investopedia, "Contract for Difference," http://www.investopedia.com/terms/c/contractfordifferences.asp.
[2] "BitShares 2.0: General Documentation," *BitShares Whitepapers*, 2015.
[3] "BitShares 2.0: Growth Considerations," *BitShares Whitepapers*, 2015.
[4] "BitShares 2.0: Business Plan," *BitShares Whitepapers*, 2015.
[5] D. Larimer, "Stable currencies are impractical and undesirable," http://bytemaster.github.io/article/2014/12/31/Stable-Crypto-Currencies-are-Impossible/.
[6] "Mt. Gox," http://www.wired.com/2014/03/bitcoin-exchange/.
[7] Wikipedia, "Alternative Trading System," http://en.wikipedia.org/wiki/Alternative_trading_system.
[8] ——, "Prediction Market," http://en.wikipedia.org/wiki/Prediction_market.
[9] "MF Global," http://www.forbes.com/sites/francinemckenna/2012/07/16/auditors-all-fall-down-pfgbest-and-mf-global-frauds-reveal-weak-watchdogs/.
[10] "Bitstamp," http://www.coindesk.com/bitstamp-claims-roughly-19000-btc-lost-hot-wallet-hack/.
[11] "Coinbase," http://coinbase.com.

[12] Coinbase, “Coinbase case demonstrates the pitfalls of regulatory compliance,” http://cointelegraph.com/news/112319/coinbase-case-demonstrate-the-pitfalls-of-regulatory-compliance.
[13] Ripple Labs, “Multisig / Transaction Proposal,” https://wiki.ripple.com/Multisign#Transaction_Proposal.
[14] Oleg Andreev, “Blind signatures for Bitcoin transactions (second draft),” http://oleganza.com/blind-ecdsa-draft-v2.pdf.