BitShares 2.0: Financial Smart Contract Platform

Fabian Schuh, Daniel Larimer
Cryptonomex, Cryptonomex.com*
Blacksburg (VA), USA
{fabian, dan}@cryptonomex.com

Abstract—

Ever since Satoshi Nakamoto released his whitepaper and corresponding software for bitcoin, the cryptocurrency ecosystem has continued to grow at a rapid pace. In the beginning, Bitcoin created a platform that anyone could use to *transfer* value across the internet without middlemen, banks or counterparty risk. However, once bitcoin's basic blockchain consensus technology became established and stable, people began to discuss whether blockchain technology could also be applied to enable the *trade* of multiple assets without the need for a broker or centralized clearinghouse. BitShares has created such a technology, and has coined the term "*decentralized exchange*" (DEX) to describe our Bitcoin 2.0 platform. Currently, it supports trade not only in digital assets, but also traditional financial instruments and securities on the blockchain. The two main tools we provide for the creation of these instruments, market pegged assets (MPA) and user-issued assets (UIA), are discussed in detail in this paper.

1 Introduction

In today's world, crypto-currencies are unique because they are the only type of digital currency that does not represent a corresponding counterparty liability. Instead, they are *fungible decentralized* tokens, whose value is derived from the amount of practical utility (or potential future utility) perceived by the network of users that support and trade in them. Not surprisingly, most cryptocurrencies suffer from high levels of price volatility due to many complex factors, such as constantly shifting public perception and highly speculative and unregulated markets. Although professional traders tend to appreciate this volatility, so far it has hindered the widespread adoption of cryptocurrency as a *practical payment solution*.

One approach to creating a *price-stable* asset would be for an issuer to accept deposits in return for a digital token as a *claim receipt* (an "I Owe You"). With this approach, the token would trade in the market as having the same value as the underlying asset, minus any perceived credit risk associated with the issuer. While this approach may work well for settlements, it is far less secure as an instrument for long term savings. History has repeatedly proven that many issuers will eventually go bankrupt due to incompetence, government intervention or outright fraud.

BitShares has developed an alternative approach to creating price stable digital assets by using a cryptocurrency as *collateral* in a collateralized counterpartyrisk-free loan implemented as smart contract. With 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 works as long as sufficient collateral exists, and the contract can be settled by an honest 3rd party with a price feed

BitShares is a counterparty-trust free platform for financial smart contracts which operates over the internet, and offers a set of *financial instruments* that includes collateralized loans. These contracts are *derivative instruments*, and as such they fall under the wider definition of financial instruments. Financial instruments can be defined as *tradable* assets of *any* kind, including cash, proof of ownership receipts, or a contractual right to receive or deliver an underlying instrument, commodity, option, etc. Additionally, several other digital financial instrument tools are currently available on BitShares, such as Market Pegged Assets (MPA) or "SmartCoins" which represent a *derivative* with fiat currency, gold, or even other cryptocurrencies as the underlying asset. These SmartCoins derive their value from contracts based on the performance of the BitShares base token (BTS). Smart coins will be presented in detail in section 2.

The BitShares platform also contains an flexible feature called "user-issued assets" (UIA) which will help facilitate a wide range of profitable business models based around certain types of services. A UIA is a type of custom token registered on the platform, which users can hold and trade within certain restrictions. The creator of such an asset can publicly name, describe, and distribute its tokens, and can specify custom 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 ownership tracking, crowd fundraising, IOUs, coupons, and many more that will be discussed in section 3.

In order to *trade* financial instruments, BitShares provides a high-performance *decentralized exchange* (DEX), with all the features expected of a professional trading platform (see section 4). 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 at speeds of up to 100,000 transactions per second. With this kind of performance on a decentralized exchange, there is no longer a need for traders to

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

expose their funds to the risks of centralized exchanges.

In this paper we will discuss the financial instruments available in the BitShares network as well as the DEX. Before continuing, we recommend that you read through the basic technological components of BitShares in the other white papers [1] (more papers to be published shortly).

2 Market Pegged Assets (MPA)

A cryptocurrency that has the properties and advantages of Bitcoin, but is also capable of maintaining price parity with a globally adopted currency (e.g. U.S. dollar), would have incredible high utility for convenient and censorship-resistant commerce. This has been achieved by BitShares' market pegged assets (MPA), a new type of freely traded digital asset whose function has been designed to track the value of a underlying conventional asset by means of collateralized blockchain loan.

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

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

We will present SmartCoins as a viable open source alternative to the slow, restrictive, and expensive "legacy" banking system. SmartCoins that have price parity with a commonly used currency will enable merchant adoption with ease and efficiency. Also, they will reduce the need to calculate capital gains and losses on volatile assets to determine tax liability. In short, BitShares is bringing *publicly* auditable open source banking to anyone with access to the internet. MPAs allow savers and spenders to choose their preferred asset type, which brings flexibility and ease of use to the open source banking experience.

The subsequent paragraphs will explain how market pegged assets achieve price parity while minimizing risk to their holders.

2.1 Price Stability

Ever since the bitcoin blockchain initiated the age of decentralized public ledgers, economists and computer scientists have attempted to achieve a *stable* or *price pegged* cryptocurrency. The following two subsections will discuss our discoveries about the true nature of *stable* or *pegged* currency and explain how BitShares has solved this complex issue.

2.1.1 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 a mandate of *stable prices* and it is almost universally accepted by the market that this is a good mandate. The same holds true for the Euro, with its stability being achieved through the European Central Bank (ECB). Almost every country applies a similar methods to gain control over prices via monetary policies like quantitative easing and fixing of the interest rates for commercial banks that borrow money from the central bank.

As a very basic example, imagine that a central bank has managed to keep prices stable through their monetary policy with 0% price inflation for 20 years. Now let's assume that during this same 20 years the advances in robotics and automation 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 lifestyle. However, this is unfortunately not the case. Because of constant intervention by the central banks, they have managed to also increase the money supply by 3x. The newly created money is then lent to the commercial banks which then lend it again to the people at a profit.

Since this monetary inflation results in a sustained increase in the general level of prices, it is equivalent to a decline in the purchasing power of money. Hence, a dollar buys less and less over time. As a result, we see the dollar hast lost 99% of its *purchasing power* since the FED was founded in 1913 (see fig. 1).

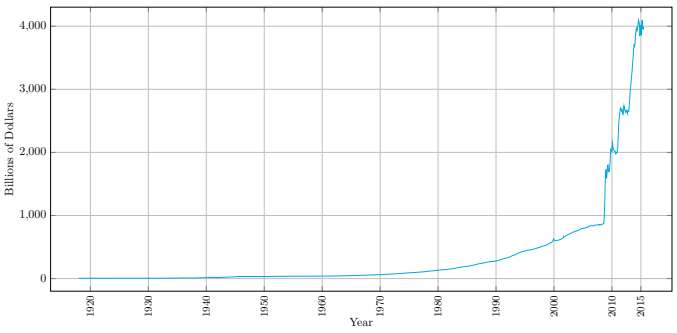

Figure 1: St. Louis Adjusted Monetary Base [2]

Of course, the goal of this paper is not to propose a replacement for central banks or their monetary policies, but we do wish to clarify some terminology, particularly as it relates to other "stable" cryptocurrencies. Other projects in the cryptocurrency space have attempted to provide an alternative currency that will ultimately achieve a similar mandate as the central banks, leaving the profits in the hands of only few institutional entities. BitShares *market-pegged* assets will not result in the centralization of power and control in this way.

Let us discuss the example above. Since the centralized bank policies have resulted in a steady decrease in purchasing power over time, we notice that price stability does not seem very important to them. Eventually, the ideal goal would be to achieve a currency with a long term *stable purchasing power*. However, for now we must be content to achieve *relative stability* by pegging SmartCoins to the dollar or euro or gold, etc. To summarize, what we want to achieve is:

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

Hence for us, price "stability" means price *predictability* within some tolerance level. In the case of the U.S. dollar, a willingness to accept a yearly loss in purchasing power via monetary policies demonstrates that predictability is more important than stability [3].

Alternatively, BitShares offers a decentralized solution to implement the Consumer Price Index (CPI) to peg to the changes in the price of a market basket of goods and services purchased by regular households. This is another way BitShares users can hold and trade a stable crypto token that will help them retain their purchasing power.

2.1.2 BitAssets 1.0: Historical Lessons

The first iteration of the BitShares bitAsset engine evolved for over 9 months as we observed how market participants reacted to various rules. We noticed that liquidity is critical to bring confidence in the value of the token, and that a system with unbalanced rules will tend to bias the price in one direction or the other.

Early on, BitUSD (BitShares SmartCoin pegged to the U.S. dollar) was driven down to $0.85 as demand for shorting outstripped demand for BitUSD and shorts were not forced to cover. Then, after implementing a *30 day forced covering rule*, the price stabilized around $0.98 to $1.00. Later, as the cryptocurrency bear market progressed, BitUSD was trading at $1.05 or more because everyone was scared to use leverage and those that had open positions looked to cover their position while those who held BitUSD were not looking to sell. Over the course of these past 9 months, we observed the dynamics of 3 different markets and thus had the opportunity to refine our understanding of the the behavior of market participants and improve the protocol accordingly.

While we saw that the idea of a market pegged crypto token was generally well accepted in the marketplace, we were not yet satisfied as that the system had been perfected. For that reason, we improved the BitAssets engine for the BitShares 2.0 protocol.

2.1.3 BitAssets 2.0: Evolving a Stable Crypto Currency

For BitUSD to be accepted as being equal to $1.00 for the purposes of setting prices, 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[1]. Since this rule is present, those who create the BitUSD must sell it at a price that properly accounts for this risk of *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 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.

[1] Price feeds are published by *witnesses* that have shareholder approval. See section 2.2.

2.2 Price Feeds

The blockchain needs to be aware of the external price of BTS in order for settlements to convert SmartCoins into the core asset (BTS) at a fair price.

In BitShares, this is achieved by means of a set of N trusted *witnesses*. These witnesses 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 certain type. Hence, misbehaving witnesses can be identified, "fired" and lose their reputation of shareholders.

Additionally, to prevent manipulation of the price feed, N witnesses have to be elected that can all produce their prices independently. 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:

$$x = \mathrm{sort}(p[i]) \tag{1}$$

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

Hence, the price is resistant against misbehaving witnesses in that only a majority of price publishers can manipulate the outcome of the median. In practice, any unintentional feed *error* is thus balanced around the true price.

Obviously, the shareholders are required to constantly monitor the published prices of their witnesses and should make a public note about any discrepancies. This is similar to traditional *quality management* for the *Smart Coin* products (e.g. bitUSD) and BitShares system can offer a paid position to perform this service.

2.2.1 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 or global settlement order requested can attempt to manipulate the markets and thus the feed against the BitUSD holder.

The risk of price manipulation should be 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*[2] that keeps BitUSD valued at least $1.00.

In practice, a feed producer can observe the BitUSD: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 feed producers and quickly fire misbehaving feed providers.

2.3 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 protocol 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 *decentralized exchange* or *internal market* (c.f., section 4) to distinguish from *external markets* such as websites that facilitate the exchange of government issued currencies with cryptocurrency.

SmartCoins are tokens of a particular MPA (e.g. bitUSD). They use the concept of a collateralized smart-contract supported loan, 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 a collateralized loan (c.f., *1)* in fig. 2).

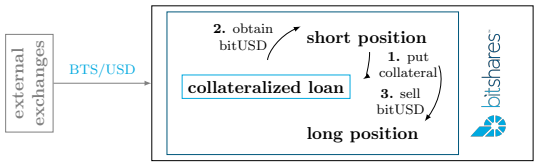

Figure 2: Illustration of external price discovery and a "short sell" to seek greater exposure for BTS price movements.

The collateral is only returned to the short seller when the corresponding amount of the asset agreed in the contract is handed over to the BitShares network again. The protocol will then effectively destroy these tokens and fulfill the contract. This is referred to as *covering a short*. At the moment of creation, the position of the *shorter* has not changed at all because he can directly cover his own short position using the bitUSD to gain back his BTS used as collateral.

If the short seller has sold the SmartCoins he has created, then he would be required to purchase them back from the market before closing his short position. Meanwhile, 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 (i.e. initiated by the protocol itself) repurchased from the market before the 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.

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 interval[3] at the settlement price (identical to the feed price).
- In this case, the *least* collateralized short positions would be margin called and their collateral would be 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 (black swan event, see section 2.5).

These simple rules enable a price floor of $1.00 for 1.00 BitUSD. A simple metric for testing the validity of our claim 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.

2.4 Perspectives of Participants

While the rules are simple, the consequences are less obvious. Let's analyze this from the perspective of the various players.

2.4.1 The Short Position

When deciding a price at which to enter a short order, a trader must consider the risk of being force settled. 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. Since feed errors are equally balanced between being in the favor of the short and in the favor of the long (c.f. section 2.2) this leaves only the risk of being forced out of their position at an inopportune time.

[2] "fair" for honest market participants.

[3] defined by the shareholder approval

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

In practice, the only way new SmartCoins enter 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 cryptocurrency 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 smartcoins 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.

2.4.2 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 a 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.

2.4.3 The Customer's Perspective

Customers use BitUSD because it provides them the convenience and freedom of a cryptocurrency, and has lower transfer fees compared to most other payment platforms besides being significantly more convenient than fiat.

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.

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 meantime, 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.

2.4.4 The Merchant's Perspective

A merchant wants to be able to price merchandise in BitUSD, and obtain real USD in their 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 are looking 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.

In any case, 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.

2.4.5 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 a global settlement 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.

2.5 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 this 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. This is called a *black swan* event since the least collateralized position is unable to buy enough BitUSD to cover. At this point, all positions are automatically 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.

2.6 Risks

The current implementation of market pegged assets in the BitShares system is designed to minimize risk of loss to SmartCoin 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.

2.6.1 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* (also known as margin calls) if necessary.

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 2.5), 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 customers 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.

2.6.2 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 you choose to view the software protocol itself as an independent "counterparty" 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. MPAs stored on a *centralized* exchange become IOUs and are subject to counter party risk [4]. This risk is not a property of the MPA themselves. We recommend that users never deposit their tokens 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 4.3.1).

2.6.3 Systemic Risk

Systemic risk is a catch-all for other risks required to utilize the system. The primary risk lies with individuals being 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. While some risk components should drastically reduce over time, such as implementation bugs and computational bottlenecks, others are constant and difficult to predict, such as politics (i.e. legislation, regulations, etc.) or natural catastrophes that may result in partial or global internet outages.

2.7 Privatized SmartCoins

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

Privatized SmartCoin managers can experiment with different parameters such as collateral requirements, price feeds, force settlement delays and forced settlement fees (see section 3.2.7). 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.

3 User-Issued Assets (UIA)

In addition to the aforementioned *market pegged* assets, BitShares allows individuals and companies to create and issue their own tokens for anything they can imagine. The potential use cases for so called user-issued assets (UIA) are innumerable. One example would be for UIAs to be used as simple event tickets deposited on the customer's mobile phone to pass the entrance of a concert. On the other hand, they can be used for crowd funding, ownership tracking or even to sell equity of a company in form of stock.

Obviously, the regulations that apply to each kind of token vary widely and are often different in every jurisdiction. Hence,

BitShares comes with tools that allow issuers to remain compliant with all applicable regulations when issuing assets, assuming regulators allow such assets in the first place. We will discuss the tools and optional administrative rights given to the issuers of a given UIA and provide a subset of possible use-cases in more detail.

3.1 Deposit Receipts

In principle, traditional 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 compared to banks. The deposit receipt example is probably one of the most important, and yet most heavily regulated, use cases of UIAs. For that reason we will describe the tools available in BitShares that allow for compliant deposit receipts on the blockchain.

With BitShares, it is now possible to move a company's internal databases onto the blockchain where deposits can make use of all the features that BitShares offers, such as smart contracts, internal markets, escrow, or (later) bonds.

In order to make traditional banking more profitable (through a decentralized account balance database), and enable services like Paypal and Dwolla while offering more freedom to the customers, we have identified (with extensive help from many different banks and exchanges) the relevant laws required to comply with when issuing deposit receipts. The following shall briefly discuss how BitShares can assist to comply with those rules[4].

3.1.1 Know Your Customer

To comply with Know Your Customer (KYC) laws the issuer must know every single customer's real world identity. BitShares supports this by enabling both *whitelists* and *blacklists* on the block chain.

When an asset enables whitelists, no account may send, receive or trade that asset without being on an authorized whitelist. 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.

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. Additionally, the issuer may take back his assets from any account, if required.

Note that these kind of administrative powers are available only for UIAs and not for MPAs. Additionally an issuer may choose to indefinitely give up partial of full control over each specific administrative power.

3.1.2 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 cryptocurrency enthusiasts, 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 MPAs like the bitUSD.

3.1.3 Market Restriction

An issuer who offers USD, EUR and other fiat deposits may need to restrict direct trading between their fiat assets to avoid being subject to foreign currency exchange regulations. Some cryptocurrency exchanges allow trading between fiat and cryptocurrencies, 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 choose to also white or blacklist trading partners for their user issued assets (i.e. IOUs). This way, the issuer can prevent customers from trading USD-IOUs for EUR-IOUs without restricting other pairs. Fortunately, MPAs, such as the bitUSD are not fiat and hence need not be blacklisted.

3.1.4 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 cryptocurrency 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 there is a customer demand for user-to-user transfers.

3.2 Use-Cases

Having discussed the administrative possibilities of UIAs, we will now list and briefly describe a few use cases. These serve as examples and only represent a subset of the possibilities.

3.2.1 Rewards Points

A use-case that can be easily implemented and with only minor regulatory hurdles are *reward points*, which Merchants already today offer to their 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. With an UIA, a merchant no longer needs to maintain a database of customers and their rewards. Instead, he simply transfers a crypto token to the customer (e.g. via a mobile phone application) and the public ledger of BitShares takes over the maintenance leaving all administrative power to the merchant (i.e. the issuer of the UIA).

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

3.2.2 Event Tickets

Event tickets are a largely unregulated use case for UIAs. Tickets to an event could be issued as digital tokens that are auctioned off

[4] This paper should not replace consultation of a lawyer

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 (e.g. with their smart phones).

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

3.2.3 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 limited to: ownership tracking, authorization, membership identifications, etc.

3.2.4 Crowdfunding

With BitShares, decentralized crowdfunding becomes an easy task. Technically the process breaks down to as few as two steps: (a) Create and issue a new token that should represent your project, and (b) sell your shares on an exchange. The issuer is now free to choose to sell them for bitUSD, bitEUR, or any other token and is free to define the price for each share. Not only can these shares be traded on traditional (centralized) exchanges but they can also be traded in the decentralized exchange that will be discussed in section 4.

Whether the UIAs are used as a transferable coupon for a pre-sale, or for holding an initial public offering (IPO) for a small company, issuing an asset is one of the most effective means of raising money for a cause.

3.2.5 Information/Prediction Markets

With BitShares and the decentralized exchange described in section 4, prediction markets [5] can be quickly implemented. A binary prediction market has a "price" between 0 and 1 representing the two possible outcomes of an event. All that is needed is a proper prediction criteria in the description of a newly created asset that anybody can issue by putting up collateral.

Hence, a prediction market 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.

While the event has not occurred, the price of this asset reflects the probability of an event to occur. After the event has occurred the issuer can settle all positions at final "price" depending on the actual outcome. Participants that have voted correctly will be able to settle their shares back to the network at a higher price and make a profit.

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

This feature, in combination with the bitUSD, allows anyone to implement most binary prediction and information markets currently established in a decentralized and trustless manner.

3.2.6 Company Shares

In most countries Corporate shares are heavily regulated by their corresponding exchange authority, such as the *Securities and Exchange Commission* (SEC) in the U.S. However, most of those regulations do not prevent them from being issued or traded on an alternative trading system [6]. 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 customers of UIA according to section 3.1, corporate shares can certainly be issued and traded in the BitShares ecosystem (see section 4).

When issuing a corporate share in BitShares, the company can decide who is able to hold, share, or transfer its shares and can restrict trading markets freely (e.g. only allow the market STOCK:bitUSD but not STOCK:bitGOLD).

3.2.7 Privatized SmartCoins

Wit BitShares 2.0, users can create their own derivatives (i.e. price-stable assets) with custom parameters designed to track the value of any asset they can imagine by means of collateralized loans. 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 (in this case, however, the asset may be declared non-complying by regulators since white and blacklists cannot be updated any longer).

To create a privatized SmartCoin, Bitshares provides several different parameters that an issuer may fine tune. In addition to account whitelists, market restrictions, and transfer restrictions, the issuer of a private SmartCoin has control over (a) Collateral Type, (b) Initial Collateral Rate, (c) Maintenance Collateral Rate, (d) Forced Settlement Fee, (e) Price Feed Update Rate, (f) Settlement Delay, (g) Global Forced Settlement, and (h) Trading and Withdrawal Fees.

With these tools it is possible to emulate a purely smart-contract based collateralized loan from the blockchain with periodic global forced settlement (i.e., monthly, yearly, etc), or to emulate BitAssets 1.0 by having a 30 day delay on forced settlement (c.f. section 2.1.2).

Hence, any arbitrary financial indexes can be used for the price feed to mimic all manner of exotic assets. Also, because accounts are publicly auditable, even mixed asset funds can be modeled with the advantage of verifiable ownership claims by the fund manager.

3.3 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 the 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.

3.4 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 bound by a minimum and maximum fee. The combination of these parameters give issuers flexibility in pricing.

For example, you could easily implement a centralized payment solution on top of the decentralized BitShares network and mimic the business model of Dwolla and Paypal. In BitShares, you simply issue your own IOUs for U.S. dollars or Euro and send them to the wallets of your customers. Whenever a customers buys a market items from another customer, they may choose to pay with your IOU and require a percentage or fixed amount as fee for your service. The major advantage for your business is that you are not required to maintain your own highly reliable database servers that contain your customers' balances since your customers maintain their wallets on their own and the public ledger securely stores the balances. This outsourcing increases security and profits, and improves competitiveness at no extra cost.

4 Decentralized Exchange

Throughout recent history, centralized exchanges have repeatedly proven unreliable and untrustworthy. Whether it is MF Global, Mt. Gox, BitStamp, or Bitfinex [7, 4, 8, 9], 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 and has occurred. In the modern financial system, these transgressions happen all too frequently within centralized banks and exchanges all around the world.

Hence, in the following paragraphs, we will outline the concept of the decentralized exchange (DEX) that powers the BitShares network and discuss the many benefits of using it has over traditional centralized exchanges.

4.1 Core Features of the DEX

A decentralized exchange has a very particular set of advantages over traditional centralized exchanges, and we would like to address some of them briefly below. Although the BitShares DEX comes with all of them, it is up to the reader and customer to leverage those features for their particular needs.

4.1.1 Separation of Powers

There is no reason why the same entity needs to be responsible for *issuing IOUs* and for *processing the order book*. In fact, this is is actually a disadvantage from a security standpoint. It is only because these two roles have been combined that there is a tendency toward centralization in the Bitcoin exchange space. Since both sides of any order book consist of amount/price pairs, it makes more sense to store this data on a public ledger such as a blockchain. Therefore, to create a decentralized exchange, the first step is to move the order book onto the blockchain so that anyone can see and audit it.

After this is done, *gateway services* can still be used to enter and leave exchange order book through IOUs, just like a traditional exchange uses. The blockchain can allow users to trade, for example, BitstampUSD against BitfinexUSD, and in order to easily move funds from one gateway to another. Users could even trade BitstampUSD against BitstampBTC or BitstampUSD vs BitfinexBTC.

With this model, traditional exchanges merely act as gateways that receive fiat and issue GatewayFiat as an UIA on the blockchain (In reverse, they would receive their own GatewayFiat token, execute a wire transfer and then burn the token). These gateways would make their money entirely on transaction fees and from a percentage of the trading fees similar to their current model.

But simply moving the order book to the blockchain is not enough, because the market would naturally centralize around a few gateway IOUs and the markets for them. Also, BitstampUSD is not fungible with BitfinexUSD because they have different trust profiles and regulatory considerations. Plus, any IOU carries the risk default similar to the the IOUs that currently exist on the exchanges' internal databases. If we only had gateway IOUs, it would prevent the possibility of having a single, unified order book for USD pairs (or any fiat pair).

Fortunately, BitShares has solved this issue with market-pegged assets. We have bitUSD which is backed by collateral and is independent of governments or centralized entities, and trades for $1 independent of any gateway. It is also universal because users don't need to register their identity with anyone to use bitUSD or any other market pegged asset. So bitUSD pairs can now act as the *universal order book*, where users are safe to keep their funds on the books without risking counterparty exposure. This core features sets BitShare apart from Ripple, because BitShares has this unique "*software protocol-based counterparty*" that can never cheat a user out of their funds.

4.1.2 Global Unified Order Book

Because BitShares can be accessed 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 would be to improve market efficiencies (reduce all arbitrage opportunities), minimize spreads, maximize liquidity and provide accountability and auditability.

By having the trades executed on the BitShares network, it would eliminate all 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 will become much less appealing to honest traders.

Furthermore, BitShares does not have restricted open hours, and is available for trading 24 hours a day and 7 days a week.

4.1.3 Trade Almost Anything

BitShares offers the tools to trade in Gold, Silver, Gas, and Oil in addition to several national currencies and cryptocurrencies. There are few limits on what can be traded on the BitShares exchange, if there are enough people interested to form a market. The DEX allows any two pairs to be traded directly. There is no need to ask the exchange to open up an additional market. If customers 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.

4.1.4 No Limits

Of course, you can trade any amount, at any time, from anywhere, without withdrawal limits[5]. 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 [10], even limit what you can do with your money after you have withdrawn it [11]. Other exchanges demand documentation of how you earned your cryptocurrency.

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

4.1.5 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 would impacts only a single user and their funds. Users are in control of their own security, which is generally preferable to trusting a centralized entity.

Furthermore, since KYC/AML verification can be outsourced via whitelists, a gateway that holds customers funds for fiat backed IOU's would not necessarily need direct access to the customers' identities. This was an issue with Mt.Gox [4], where thousands of customers' identities were stolen.

[5] Restricted access may only apply to user issued assets (e.g. IOUs of gateways), but not to market pegged assets, such as bitUSD, bitEUR, etc.

Since there is a fixed cost associated with attempting to hack an exchange or an individual user, the difference between a centralized exchange and the DEX is the size of the reward. If someone places 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.

Furthermore, within any centralized company multiple people usually have access to customer funds. Likewise, most 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 a much safer option.

Access to funds in BitShares can be further secured by means of corporate accounts that implement threshold signatures [1, 12] and validate only those transactions which signature weights (e.g. the CEO has more say than a worker) surpass a pre-defined threshold.

4.1.6 Secure

The traditional banking system has long practiced what is called *fractional* reserve banking, but in many cases the more appropriate term is "*fictional*" reserve banking. In the BitShares ecosystem, however, we demand at least 100% reserves. Every Dollar, Euro, bitcoin and ounce of gold held as a SmartCoin on the BitShares DEX is backed by at least, but often greater than 100% reserves. In a centralized exchange, a single hack, mistake, or theft can quickly turn a 100% reserve system into a fractional reserve system, or worse, a "fictional" reserve system. Without any reserves, it is unlikely that an exchange would ever be able to pay back the funds it owes to its customers.

Because the BitShares DEX always maintains a minimum of 100% reserves, users can rest assured that BitShares will be solvent in almost any market. Since all of the reserves are kept as BTS held in collateral on the blockchain, they cannot be compromised because there are no private keys that can be stolen.

4.1.7 Fast, but not too fast

On Wall Street, traders go to great lengths to get as physically close to the core computers as possible, because their automated trading robots make decisions so quickly that the speed of light is a formidable factor. This gives them an unfair advantage against other traders, and allows them to engage borderline unethical practices such as order frontrunning. They have even spent billions of dollars to lay transatlantic fiber optic cables between London and New York to shave milliseconds off of their trading times.

On the BitShares DEX, all trades execute in seconds, just like with any other centralized website interface. Unlike centralized exchanges however, there is *no prioritized trading*, front running, or hidden orders. This puts all traders on a level playing field.

4.1.8 Decentralization of Privacy

Crypto-currencies depend upon a public ledger or blockchain, 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 their account number and they use a new account number with every transaction, it is impossible to tie their bitcoins to their real life identify.

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 [13] 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 identity need only be verified by issuers of IOUs (e.g. GateUSD) in order to comply with fiat regulations. Once traded for bitUSD your link to the gateway or exchange *Gate* can be removed quickly by means of *blinded transactions* that enables users to publicly move funds without revealing the exact amount [1, 14]. If issuers approve, blinded transactions may even be performed for UIAs directly.

4.2 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 3.3.

In contrast to BitShares 1.0, there will also be *limit-orders* that allow to buy on the market up to a predefined price. This allows to instantly fill any order below or above your price at the cost of a single fee (c.f., section 6).

4.3 Collateralized Smartcoins

The heart of BitShares is the SmartCoin system which enables the creation of collateralized bitUSD from the BitShares network. A BitUSD has all of the properties of traditional cryptocurrencies like Bitcoin, with the additional features from BitShares 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 (forced settlement, see section 2).

When you hold BitUSD the value of your holdings will remain pegged to the dollar so long as BitShares have a value greater than 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.

4.3.1 Fiat Gateways

The roles that traditional exchanges perform today are:

1. Receiving cryptocurrency 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 cryptocurrency 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 does.

With the separation of powers, we only need gateways that perform the tasks 1, 2 and 3 of the list above while order book processing and storage of account balances are managed by the BitShares protocol/network. An entity issuing and redeeming IOUs for another asset in BitShares is called a *gateway*. In contrast to central exchanges, the IOUs are sent to the wallet of the customer and are under his full control (see section 3.1).

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.

5 Platform for Further Smart Contracts

In contrast Bitcoin that offers *Script* — a stack-based scripting language with a reduced set of instructions (called *OP codes*) — to allow for limited smart contracting capabilities, the BitShares network allows for arbitrary transactions types, in general.

However, in contrast to so called *Turing-complete* blockchain projects, such as Ethereum, adding new features or transaction types to the protocol requires shareholder consensus.

Hence, new features must be *proposed* to the shareholders who must reach consensus to approve them. Only after this happens is the protocol then upgraded to the next version which includes the new feature set.

6 Fees

In the BitShares ecosystem every operation is assigned an *individual* fee. These fees are subject to change. However, they are defined solely by shareholder approval, thus each and every shareholder of the BitShares core asset (BTS) has a say as to what the fees should be. If shareholders can be convinced to reduce a certain fee and consensus is reached, the fee will be reduced automatically by the blockchain[6].

7 Conclusion

In this paper, we have described the foundations of the BitShares network, which we hope will soon begin to inspire a paradigm shift from classical banking towards peer-to-peer financing. We have laid out the many features and benefits of the BitShares Decentralized Exchange, which offers financial instruments for anyone to utilize with low barriers to entry.

With SmartCoins, the BitShares ecosystem offers a powerful tool for everyone from speculators and savers, to traders and entrepreneurs.

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

The BitShares platform provides a toolkit with which innovators can experiment to discover optimal currency solutions using free market trading.

We also discussed how a price floor of $1.00 USD per bitUSD is the most reasonable approach to achieving price predictability.

Additionally, we have shown that user issued assets (UIA) offer countless opportunities to reduce costs. They can be used to distribute a token on a decentralized database (the blockchain), and can be programmed to comply with government regulations. Since the BitShares protocol handles order processing and storage of user balances, any implementation of business models around UIAs comes at very low cost to the issuer and will make expensive central server infrastructure a thing of the past.

[6] Changes of blockchain parameters are proposed by members of the committee. These members are voted by shareholders and improve the flexibility and reaction rate.

References

[1] "BitShares 2.0: General Documentation," *BitShares Whitepapers*, 2015.

[2] Federal Reserve Bank of St. Louis, "Dataset: St. Louis Adjusted Monetary Base (AMBSL)," https://research.stlouisfed.org/fred2/series/AMBSL/downloaddata?cid=124, Aug. 2015.

[3] D. Larimer, "Stable currencies are impractical and undesirable," http://bytemaster.github.io/article/2014/12/31/Stable-Crypto-Currencies-are-Impossible/.

[4] "Mt. Gox," http://www.wired.com/2014/03/bitcoin-exchange/.

[5] Wikipedia, "Prediction Market," http://en.wikipedia.org/wiki/Prediction_market.

[6] ——, "Alternative Trading System," http://en.wikipedia.org/wiki/Alternative_trading_system.

[7] "MF Global," http://www.forbes.com/sites/francinemckenna/2012/07/16/auditors-all-fall-down-pfgbest-and-mf-global-frauds-reveal-weak-watchdogs/.

[8] "Bitstamp," http://www.coindesk.com/bitstamp-claims-roughly-19000-btc-lost-hot-wallet-hack/.

[9] "Bitcoin Exchange BitFinex' Hot Wallet Hacked," https://www.cryptocoinsnews.com/breaking-bitcoin-exchange-bitfinex-hot-wallet-hacked/.

[10] "Coinbase," http://coinbase.com.

[11] "Coinbase case demonstrates the pitfalls of regulatory compliance," http://cointelegraph.com/news/112319/coinbase-case-demonstrate-the-pitfalls-of-regulatory-compliance.

[12] Ripple Labs, "Multisig / Transaction Proposal," https://wiki.ripple.com/Multisign#Transaction_Proposal.

[13] "Is Coinbase Bringing "Big Brother" to Bitcoin Accounts?" https://www.cryptocoinsnews.com/coinbase-bringing-big-brother-bitcoin-accounts/.

[14] Oleg Andreev, "Blind signatures for Bitcoin transactions (second draft)," http://oleganza.com/blind-ecdsa-draft-v2.pdf.