# BitShares

## A Peer-to-Peer Polymorphic Digital Asset Exchange

Daniel Larimer
dlarimer@invictus-innovations.com
www.tradebitshares.com

Charles Hoskinson
charles.hoskinson@invictus-innovations.com

Stan Larimer
stan.larimer@invictus-innovations.com

***note* the contents of this white paper are under active revision, comments are appreciated.**

## Abstract.

An ideal free market financial system [IFMFS] would allow parties to store, trade, and transfer value through time and space with minimal risk and cost. Starting with innovations first derived from the Bitcoin open source protocol[1], we have refined and extended a new protocol called BitShares that implements an IFMFS. Within the BitShares network, we have created a new type of financial product called a Polymorphic Digital Asset [PDA] that can track the value of gold, silver, dollars, or other currencies while paying dividends to holders and avoiding all counterparty risk. BitShares extends Bitcoin technology to provide many features of traditional currency, checking, savings, and brokerage instruments in a versatile new peer to peer network -- interoperable with Bitcoin and other commonly traded financial assets.

All value managed by the BitShares network is derived from the same sources as Bitcoin as well as several new sources. These sources include:

1. Demand for a trustless asset class that is digital, fungible, divisible, and anonymous.
2. Demand for a secure store of value.
3. Demand for a return on investment proportional to risk.
4. Demand for a free and open marketplace and exchange.

A critical ingredient to the success of BitShares as both a store of value and an efficient exchange is widespread adoption. BitShares attempts to assure this prerequisite by providing benefits with broad appeal to everyone that outweigh any technological, social, regulatory, or political risks associated with using the system.

[1] Please refer to Satoshi Nakamoto’s whitepaper: http://bitcoin.org/bitcoin.pdf

## Introduction

Bitcoin has revolutionized Internet commerce by enabling entities to exchange value securely and privately without counterparty risk. Bitcoin has proven that a decentralized digital asset can have an algorithmically limited supply, consistently increase in value and still serve as an effective means of exchange despite the absence of any physical or political backing.

Unfortunately, Bitcoin, like all existing crypto-currencies, suffers from both volatility and illiquidity compounded with the inability to easily exchange for other assets like gold or dollars on transparent global markets. These concerns have served to slow mainstream adoption and force consumers to use a patchwork of centralized exchanges and clearinghouses to exit and enter crypto-currency positions. Our goal is to embrace the innovations divined from Bitcoin while also implementing several evolutions capable of addressing both volatility and illiquidity without introducing the need for trust or dramatic changes to existing crypto-currency exchanges. Our solution is called Bitshares.

## Characteristics of an Ideal Free Market Financial System

We begin by discussing the nature of an ideal free market financial system [IFMFS] from first its motivation to the axioms required. Our goal is to develop a foundation that will serve as reference point for both BitShares and its competition.

### Motivation for an IFMFS

We require a digital free market financial system that can facilitate trade in any asset class without introducing valueless middlemen or centralized issuers of assets[2]. In effect, we desire to remove as many central points of failure and repositories of regulation and trust as possible while retaining their functionality. This effort would produce markets that transcend geography and sovereign manipulation while also allowing for traditional exchanges and financial service providers to integrate without concerns for localized issues such as specific laws or regulations.

[2] Bernard von NotHaus's Liberty dollar currency demonstrates the difficulties of centralized issuance of financial products regardless of apparent utility: http://www.nytimes.com/2012/10/25/us/liberty-dollar-creator-awaits-his-fate-behind-bars.html?pagewanted=all&_r=0

## Axioms of an IFMFS

After careful consideration and community review, the following axioms were chosen to define the characteristics of an ideal free market financial system (IFMFS) and thus defining the foundational goals for the Bitshare network:

### Axiom of Decentralization [AoD]

All parties in an IFMFS enjoy equal status, no special privileges are required, and at any point in time shall not require resources not already owned and used by over 50% of the population.

### Axiom of Trust [AoT]

No trust shall be required of any party in an IFMFS. No party has the ability to default and should have no contractual obligations as a prerequisite of use.

### Axiom of Liability [AoL]

No party in an IFMFS shall be required to engage in illegal or highly regulated activities or take any legal risks in excess of direct exchange of a cryptocurrency for fiat among friends and family.

### Axiom of Accessibility [AoA]

An IFMFS shall be easy enough to use that anyone who can handle email can successfully realize the benefits of trading and transacting within the system.

### Axiom of Scalable [AoS]

An IFMFS must scale to handle any volume without compromising the other axioms of the system nor shall the scaling require the introduction of centralized actors.

### Axiom of Asset and Trading Diversity [AoATD]

An IFMFS should support most common investment vehicles including, shorts, put and call options. It should enable trading in any tangible asset class.

### Axiom of Aggregation [AoAG]

A single bid within an IFMFS can be matched against many asks in an atomic exchange. Users attempting to exchange a large amount of money should be able to do so in a single transaction.

### Axiom of Atomicity [AoAT]

No exchange or transaction within an IFMFS is ever in a partial, incomplete, or reaches an invalid state.

### Axiom of Escrow [AoE]

Exchange of assets from systems outside the IFMFS for credit within the IFMFS shall not depend upon trusting any single party including the buyer, seller, or escrow agent. The escrow system should not be vulnerable to collusion of either the buyer or seller with the escrow agent.

### Axiom of Global Pricing [AoGP]

An IFMFS must not use any price information not derived from actual bids and asks provided by users of the system.

### Axiom of Zero Sum [AoZS]

An IFMFS must neither create nor destroy value and every profit by one party is matched by a loss of another party. No party is ever in debt to the system (see AoT)

### Axiom of Global Appeal [AoGA]

An IFMFS should offer compelling benefits which exceed the associated risks for everyone (regardless of their need to exchange currency) to participate, share, and promote. These benefits should generate the deepest possible market, most liquidity, broadest public support, and greatest demand when contrasted with any regulatory risks.

### Axiom of Privacy [AoP]

An IFMFS should provide at least as much privacy as afforded by Bitcoin for all users involved. Ideally providing complete anonymity[3].

### Axiom of Hermes [AoH]

An IFMFS should allow all users to deposit, trade, and withdraw as quickly as possible. Trades executed within the system should be confirmed as fast as possible.

### Axiom of Security [AoSEC]

An IFMFS must have a level of security on par with Bitcoin or better.

### Axiom of Open Source [AoOS]

All hardware and software components of an IFMFS must be open, auditable, and reproducible by any average developer.

### Axiom of Passive Order Execution [AoPOE]

Orders may be executed without the interactive participation of the user or their computer.

To the best knowledge of this paper’s authors, we have yet to find a system that fully implements all 17 axioms. Thus we have endeavored to develop one that can implement the axioms in both a simple and elegant manner. This paper will now describe our best efforts.

[3] We have had numerous discussions about implementing the Zerocoin protocol or some other implementation that would ensure a users privacy. For more information: http://zerocoin.org/

### Introducing BitShares

A BitShare is a Polymorphic Digital Asset, which means that it can morph into many different types of BitAssets. A BitAsset operates in a manner similar to Bitcoin with some optimizations and new rules that allow BitShares to provide the backing for its value. A BitShare has all of the properties of a Bitcoin with the additional property that dividends will be paid on BitShares and BitShare-derived BitAssets held for more than 24 hours. These dividends come from part of the mining rewards and transaction fees, are awarded every block, and are implemented in a manner that does not burden the network.

## Definitions

*Dividend* - a share of the mining reward and transaction fees proportional to the number of BitShares owned relative to the total number of BitShares in existence.

*BitAsset* - a collateralized, dividend paying asset backed by BitShares with 1.5 to 2x or more margin with all of the fungibility, divisibility, and transferability of a BitShare. All dividends are paid in BitShares from the dividends earned on the collateral.

*margin* - value held as backing in excess of the current market value of a BitAsset.

*BitUSD* - a BitAsset that is highly correlated *by self-enforcing market feedback* to the value of USD and backed by BitShares.

BitX - the general pattern used to name BitAssets based upon the value they are correlated with by self-enforcing market feedback (e.g. BitGold, BitAPPL, etc.).

Block-chain - A globally synchronized and ordered transaction ledger grouped into blocks.

*Output* - a balance in the transaction ledger with specific conditions on how it may be spent.

*Transaction* - links a set of unspent outputs to a new set of unspent outputs while satisfying the conditions of the unspent outputs and other blockchain rules.

## Block-chain Market

The purpose of a block-chain is to establish a global consensus on the order of events and current state of the a global transaction ledger. BitShares requires a global ledger that establishes the order of transfers, bids, asks, and market trades. Every 5 minutes the set of all bids and asks included in the previous block are deterministically matched.

Like Bitcoin, every transaction has a set of output balances that can be spent if certain conditions are met. The primary difference between BitShares and Bitcoin is the set of conditions that will allow an output balance to be spent. These conditions include:

1. Signed by N of M private keys.
2. Bid/Ask being filled at the specified exchange rate.
3. Margin being added to an existing position.
4. BitAsset being repurchased in order to spend remaining margin.
5. Call or Put option being exercised at the proper price.
6. Escrow transaction being released.
7. Escrow transaction being disputed.

8. Escrow transaction being resolved.
9. Cross-chain trade confirmation.

The block-chain market is how price information enters the chain and it is essential that this price information be accurate and free from artificial manipulation not founded on market forces. This price information is used to enforce margin requirements.

Users are free to agree on any exchanges they want and their transaction will be published in the blockchain, but trades between consenting individuals are meaningless for automated price discovery because the network has no means of identifying sham trades between two accounts owned by same individual. A successful trade only means that two people agreed, whereas an unsuccessful bid or ask means that everyone agrees that the bid is too low or the ask is too high.

User's who do not negotiate a trade 'off chain' can place their bids/asks on chain. After a miner has processed all transactions he has received, he will pair all compatible bids/asks in highest bid to lowest ask order. Once all trades that can be made are made, the block chain will be left with buy/sell spread of unfulfilled orders. These orders represent the market consensus that the true price is above the buy and below the sell. At this point, the buy price is checked against the margin requirements of all short positions and any short position with insufficient margin is forced to accept the current sell price with the lowest margin position being executed first.

The proceeds of any bids or asks that are paired by a miner may not be spent until after the blockchain forking window (24 hours) has passed because like coinbase transactions, all transactions generated by the miner without signatures of the owners are not movable to another chain during a reorganization. While you cannot spend the proceeds outside of the blockchain market for 24 hours, you can place new bids/asks within the blockchain market and have them executed by subsequent miners.

Canceling an open order is also subject to the 24 hour rule because a chain reorganization after you placed your order but before you canceled it could result in another miner executing your order.

## Creating BitUSD

BitUSD is a BitShares-derived BitAsset that must be created against a valid bid and post collateral in BitShares equal to the value of bid. If the bid is accepted, the collateral and purchase price are held by the network until the BitUSD is redeemed by repurchasing it. The block chain will then redirect the dividends of the collateral to all BitUSD holders. BitUSD is entirely fungible and all dividends from all BitShares backing all BitUSD are pooled to determine the dividends (in BitShares) paid to the holders of BitUSD.

The BitShares backing the BitUSD may be spent in two ways:

1. by providing BitUSD as input to the transaction and redeeming it.
2. by a miner who enforces a margin call when the value of the backing falls to less than 150% of the value of the BitUSD.

Margin calls are enforced by the miners when they put together a block. When a miner enforces a margin call, he uses the backing BitShares to repurchase the BitUSD and thereby redeeming it. After BitUSD is redeemed it no longer exists. Any leftover collateral is sent to an address owned by the short position (not kept by the miner).

If the miner is forced to exercise a margin call, the network assess a 5% transaction fee in order to motivate market participants to proactively manage their margin. If the market moves so fast that the margin is insufficient, then the market price of the BitUSD may fall slightly below parity for a short time if there is insufficient demand for BitUSD relative to the supply of sellers.

### Advanced Trading and Contracts

The infrastructure provided by BitShares with automated margin enforcement means that other types of contracts can be created and traded such as call and put options. The market and advertising for these options can occur off chain and once agreed upon can be enforced on chain with relatively simple output script rules.

## BitShare Dividends

Dividends are paid on BitShares based upon half of the mining rewards and transaction fees relative to the total number of BitShares in existence. The total number of BitShares in existence grows at a gradually reducing rate starting at about 50 BitShares every five minutes and reaching 0 after 12 years. This means that the dividend rate will also start out high and approach an amount proportional to the transaction fees paid.

BitShares has chosen to adopt a 12 year period for issuing the available units instead of the 128 years built into Bitcoin because inflation is not necessary for the proper functioning of a currency and within 12 years competition for space in the blockchain (which is limited to meet the decentralization and scalability axioms) should drive transaction fees / volume to a level that keeps mining profitable and fees in line with the level of security demanded by the market.

The network also has other means of generating fees/incentives for miners including: inactivity taxes, margin calls, and 'dividend dust'. Bitcoin suffers from the pricing of mining rewards entirely out of proportion of with the needed / desired security.

Based entirely on the mining rewards and ignoring any fees, the effective annual dividend rate by-month is shown to the right. You will notice that early miners have a lot to gain by mining and holding. This will create market demand that will push the net-present-value of the early BitShares to be much higher than the later BitShares and should drive prices higher early on and add to the price stability. Note that those holding BitUSD will earn twice this rate and therefore have the opportunity to earn over 20% APR for the first 10 years this new chain is in operation.

Because the dividend rate on BitUSD will be so high, it will be trading at a significant premium to actual USD. This premium will be the market's means of adjusting the effective APR on BitUSD based upon perceived risks and the relative demand to cover or short BitUSD. From an investment perspective however, if the price of USD doubles relative to BitShares then the value of BitUSD will also double which means that despite fluctuations in the premium there will not be exchange rate risk.

This dividend structure is zero sum in terms of value. Miners are paid through 'inflation' from all holders of BitShares and the dividends paid to holders of BitShares are also sourced from this same inflation. An analogy could be drawn to a stock which is undergoing a 1 to 1.0000001 stock split every 10 minutes. As a result, these dividends are really transferring no new 'purchasing power' to the holders of BitShares as the dividends paid to the holders of BitShares ultimately only cover half of the value lost via inflation to pay for the mining.

As a result, dividends sourced from the inflation (i.e. deployment) of the currency result in a *50%* lower inflation rate than experienced by the holder's of bitcoin. While initially dividends will be mostly sourced from inflation, they will ultimately represent true non-inflationary returns sourced entirely from transaction fees.

Dividends are necessary for several additional reasons:

1. They create opportunity cost for maintaining a short position (encouraging covering)
2. They create an incentive to hold and not sell (increasing the value)
3. They compensate longs for their risk
4. They turn BitAssets into revenue streams which enables price comparison and liquidity.
5. They cause BitUSD, BitGold, etc to go viral and appeal to anyone seeking a return on investment without exchange rate risk to buy in.

## BitShare Decimal / Divisibility vs Bitcoin

1 bitcoin is traditionally defined as 100,000,000 satoshi and as a result the community has started to see things priced as 0.0001 BTC or less. As the value of a bitcoin grows, prices will continue to have more and more leading 0's. This makes it challenging for users to both understand and compare prices and makes price tags on cheap items take a lot of numbers to

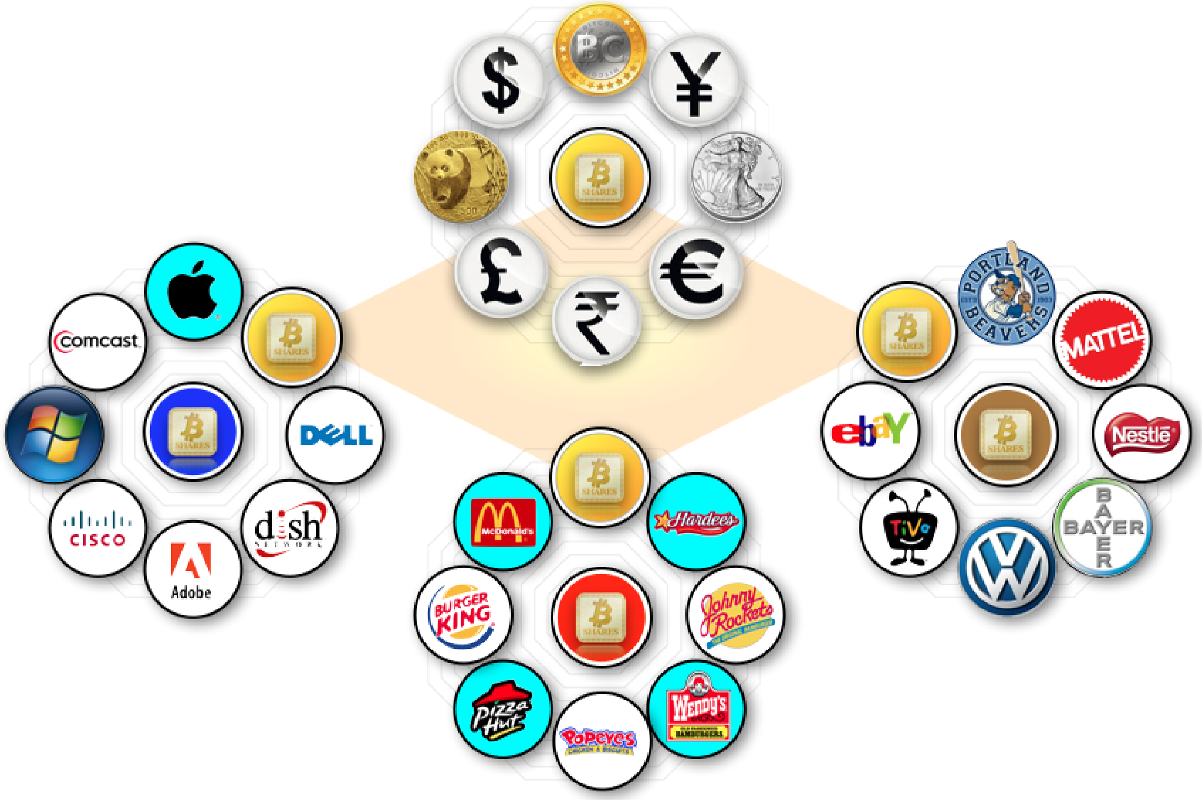
express. Furthermore, people are not as familiar with using milli, micro, or nano or other fractional units as they are with using thousand, million, billion. These large units are easier to 'round', 'talk about', and 'visually identify and compare'.

Throughout this paper we have referred to a BitShare as if it represented a similar percentage of the share supply as 1 bitcoin to the bitcoin supply. The reality is that the initial mining reward will be 5,000,000.000 BTS and 0.001 BTS is not any further divisible than a satoshi. Users will initially price things in terms of millions of BitShares and over time prices will fall to thousands, or even hundreds of BTS. By shifting the decimal point used in the BitShare network the effective BitShare supply with be over 15,000,000,000,000 (15 Trillion) and could support an economy with a $150 Trillion money supply with .001 BTS equal to $0.01. The US money supply (defined by the M2 metric) is about $10 Trillion which means that BitShares could support an economy 15 times larger than the current world economy with the price of 1 BTS equal to $10.

## Scaling

Block-chains have a fundamental limit on the rate at which transactions can be validated and confirmed based upon the proof-of-work and network latency. Attempts to increase the performance of a block-chain beyond a certain point will start to require high-end computers, disks and networks that ultimately start to centralize the network. To meet the demand for decentralization a BitShare block-chain will be limited to fixed limit of unspent outputs, and a total of 32 assets per chain.

Each such block-chain is called a *BitShares Exchange* (BSEx). Collectively, they are called the BitShares Free Market System (BSFMS). The BSFMS is designed to grow as independent competing/cooperating free market entities launch new BitShares-compliant BSEx's they hope will be profitable according to market demand. Four such BSExs make up the BSFMS shown in the figure. Each BSEx can have up to 32 crypto currencies -- plus local and global BitShare currencies. Each BSEx has its own block chain with its supported crypto currencies denominated in a local BitShare currency (represented as red, green, or blue BitShares.) These can be traded locally against the global (yellow) BitShares which also constitute the local standard on the currency BSEx.



**BitShares Currency Exchange (BSCurEx) and three other potential BSEx chains**

Unlike Bitcoin, BitShares can scale-wide and support multiple fully independent parallel chains. Because each chain can trade in BitAsset derivatives tied to other chains it is easy to move value between the chains. Some users could join both chains to arbitrage. The result of going parallel is that BitShares can scale to any volume without requiring the average computer to handle more than the one or two chains they wish to trade on. Native support for a new merged-mining technique will ensure that miners efficiently select which chains to mine for simultaneously without allowing 'free-loaders' to burden the network with larger than necessary proof-of-work caused by mining hundreds of chains at once.

Large players who wish to move billions of dollars at a time would likely join all chains with large data-centers and arbitrage the spreads between chains. These players would not have any centralizing effect because they are not necessary. Instead, large players will only serve to make the individual chains more stable.

## Fair Merged Mining

Merged Mining is a critical aspect for scalability of many different block chains. Unfortunately, merged mining requires a Merkle tree as the proof-of-work (POW) and thus takes more space in the block headers that must be stored for a year or more. So if you want to create a system like BitShares that will ultimately have 1000+ chains each trading in a subset of the potential BitAssets then merged mining will be critical. However, you do not want to 'artificially' limit the depth of the Merkle tree nor do you want to allow merged miners to get a 'free lunch' at the expense of everyone else by including every chain under the sun in their Merkle tree regardless of the potential value of that chain.

BitShares includes a new approach to natively support merged mining with proper profit incentives to minimize the size of the Merkel POW branch without placing any limits on the size. If there are two BitShare chains (Red and Blue) and each chain is trading in a different subset of assets then a miner who is doing merged mining for both chains has 3 options, mine red, mine blue, or do merged mining. If they opt for merged mining then both the Red and Blue networks experience a cost to accept the larger POW and yet the miner effectively doubles his payout. So the new approach uses the depth of the Merkle branch that proves the work to discount the percent of the reward that goes to the miner with the balance going to the dividends. Thus you can calculate your mining reward as block-reward / 2^(merkel-branch-depth). The end result is that if Red and Blue BitShares have equal market value and difficulty then merged mining is equally as profitable single mining. Both Red and Blue chains benefit from the added hash power and yet the miner does not gain any added value unless he expects a new alt-chain to rise in value over time.

If Red and Blue chains have different values and difficulties then miners will have to carefully choose which chains they mine based upon the expected growth of both chains relative to the division of their hashing power. This would enable good and useful merged mining without the costs of unprofitable merged mining being foisted on the larger networks or creating a 'master / slave' chain setup.

## Atomic Cross-Chain Trading

The problem of *atomic cross-chain trading* is one where (at least) two parties, Alice and Bob, own coins in separate crypto-currencies (e.g. Bitcoin and Litecoin), and want to exchange them without having to trust a third party (centralized exchange).

A non-atomic trivial solution would have Alice send her Bitcoins to Bob, and then have Bob send Litecoins to Alice - but Bob has the option of going back on his end of the bargain and simply not following through with the protocol, ending up with both Bitcoins and Litecoins

The algorithm for performing atomic-cross-chain trading is described on the Bitcoin wiki and will be supported by BitShares. This will enable users to trade BitBTC for actual BTC without the need for an escrow agent or trust and the entire process can be automated by software.

This feature can also be used to trade between parallel BitShare chains which adds to the scalability of the network.

## Rotating Block-Chain

Another aspect of the BitShare block-chain is that all unspent outputs must be less than one year old. Outputs that go unspent for more than 1 year forfeit their dividends and are charged a 5% transaction fee to move their output forward in the chain. Balances below the average transaction fee are forfeited entirely. This will allow the network to recover value from lost keys and eliminate the need to store transactions and outputs forever at ever increasing costs (and no benefit if the keys were lost). Because the block-chain is rotating it is possible to define the maximum total disk size required to process the chain. This maximum size can be adjusted upward in the future, but it is recommended that the network set the limit based upon the average amount of RAM shipped in new computers. This will insure that the dataset could easily fit in RAM and thus all nodes can efficiently process all transactions which will be important given the extra work required to perform the market-making function.

## Generalized Escrow for Physical Delivery

Escrow is important when dealing with untrusted 'anonymous' individuals who have the opportunity to fail to uphold their end of the bargain. The traditional approach is to use an escrow agent (such as PayPal) which is able to reverse transactions and mediate disputes. Unfortunately, traditional escrow agents represent a 3rd party that must be trusted in every transaction. If this escrow agent is not anonymous they could be held liable for facilitating certain transactions, yet if they are anonymous then how can they be trusted?

For legal reasons it is critical that no party, even escrow agents, be obligated by any legally binding contract. Such a contract would imply counterparty risk and trigger many laws and regulations associated with escrow and arbitration services. Instead, the BitShares escrow system works on the assumption that at no time is any party legally obligated to take any particular action and yet all parties are motivated by market forces to take honest and moral actions.

BitShares solves this problem by building escrow functions into the block-chain. Any user can register with the chain as an anonymous escrow agent and define the parameters of the escrow exchanges they will perform including: timetables, fees, good-faith deposits, required evidence, BitMessage address used for anonymous communication in the event of a dispute, and relevant procedures the escrow agent recommends. Certain parameters are enforced by the block chain (such as fees, good-faith deposits, and time tables) and everything else is 'unenforceable' and dependent upon voluntary actions of all parties. Fortunately, profit motives prove more effective than laws and court cases in ensuring honest outcomes.

If all goes well the escrow agent is never involved. However, if there is ever a dispute regarding the transaction, either party may post a new transaction to the blockchain that will 'freeze the funds' until the escrow agent makes a decision. The escrow agent only has the power to divide the funds among the parties to the transaction. The escrow agent is also bonded by other agents. Therefore, any party to the transaction may dispute the decision of the escrow agent as many times as they are willing to pay for until the decision is upheld 3 times in a row.

While an escrow agent has unresolved disputes no new transactions may be entered into the network that reference that agent. This creates financial incentive for the agent to resolve all disputes in an honest and timely manner.

All parties profit by being honest and face losses if they are dishonest and even attempts at collusion are not profitable due to the appeal process and the fact that agents can be selected by both parties to the transaction. The escrow agent collects a fee from every transaction that references their services and therefore does not want to risk their reputation or surety bond to help one individual to cheat another.

Despite the potential of this escrow system to offer relatively fast and secure direct wire transfers or intra-bank transfers between individuals, it is limited in its ability to prevent chargebacks / reversals. For this reason, it is recommended that all payments received do so via wire-transfer or ACH and that those payments are allowed to age before releasing escrow.

## Decentralization

### Decentralizing Hashing Function

The proof-of-work used by Bitcoin is double SHA256 and has resulted in the production of specialized ASIC chips designed to perform this function. This level of specialization has caused mining to become a high-risk specialty business that is controlled by a small minority of the Bitcoin community. This centralization becomes a liability on the network because these miners can be manipulated or shut down just like the exchanges. Mining pools are another form of centralization that also serves to centralize power. Taking out a single mining pool could disrupt the hashing power of the network to such an extent that it could delay transactions for days until the difficulty could adjust.

The first step toward keeping the proof-of-work more decentralized is to design a hash function that will perform best on a CPU which is a ‘general purpose device’ and will not benefit at all from a specialized GPU or even more specialized ASIC. There are several keys to creating such an algorithm.

First, it must be based upon utilizing the most transistors in the most efficient means available that is also widely available to all consumers. RAM and cache are very dense, highly-optimized ASIC chips that are already distributed far and wide. Historically RAM and CPU power availability have tended to grow at about the same rate; therefore, RAM usage is a requirement that specialized ASIC chips or even GPUs will not be able to optimize away via ‘parallel’ operation. This leaves all performance gains to be serial in nature. Another characteristic of using RAM is that system bus speed will be far more important than CPU power as the CPU will be starved for data most of the time. By keeping the CPU starved for data optimizations to the CPU processing will not affect the bottleneck and therefore even a 10 fold increase in performance will not result in an increase in throughput.

Second, it must be based upon sequential data processing with no ability to perform branch prediction. This alone would prevent most data-parallel or prefetching optimizations from working which will make the GPU architecture perform far worse than a CPU. GPUs also suffer from memory bus limitations and their performance drops significantly if the working set cannot be kept in the much smaller local caches associated with each core of the GPU. These characteristics alone would keep the CPU power distributed and prevent any attacks with specialized hardware from having much advantage.

The proposed proof-of-work uses sha256 to seed 8 fast random number generators which will populate 128MB of RAM. In the process of populating the RAM pseudo-random branching will prevent pipelining and result in some extra CityHashCRC128 operations being mixed into the pseudo-random population of the entire 128MB address space. After all 128MB has been populated, it is hashed via CityHashCRC128 and finally ends with a sha1 of the CityHashCRC32 result.

This proposed implementation takes advantage of the following characteristics of CPUs and GPUs to ensure that the CPU is the ideal specialized ASIC.

1. GPUs can only perform 1 instruction every 4 clock cycles in a single-threaded context.
2. CPUs operate at 3 to 4 times the frequency of GPUs
3. CityHash leverages superscalar CPUs like the Intel Core i7 to perform multiple instructions per clock cycle.
4. CityHashCRC128 leverages the hardware accelerated CRC32 instruction only available with SSE 4.2 and not present on GPUs nor likely to be added in the future.
5. GPUs have very poor behavior in the presence of branch misprediction.

Based upon factors 1, 2, and 3 a CPU should be about 32 to 64 times faster than a GPU in single threaded operation. Factoring in CRC32 should result in another 4x improvement over software implementations for a total of 128 to 256 times faster on the CPU vs a GPU in a single-threaded operation. Lastly, branch misprediction should impact the GPU far more severely than the CPU. In total, we estimate that a GPU would need to have 2048 full multiprocessors (not stream processors) and about 256 GB of RAM just to match the throughput of a single 4Ghz Intel Core i7 for this particular problem. Our numbers would have to be off by a factor of 64 just to get the memory requirements low enough to operate on the highest end GPUs.

Because the proof-of-work is more CPU intensive than a signature validation, a secondary proof-of-work must be performed that takes about 1 second and can be verified with a single sha256 operation before a block header's proof-of-work will be validated and broadcast by nodes. This will prevent denial of service attacks against the network.

One last decentralizing 'safety net' is the ability of the network to upgrade the hashing algorithm to keep it optimized for the CPU. If it becomes apparent that non commodity hardware is about to gain a meaningful mining advantage then long before that advantage is exercised the network can upgrade its hashing algorithm. The mere threat of this recourse and the stated intent to exercise this option in the launch of the chain should prevent any players from investing significant money in special purpose hardware and invalidate any claims of foul play when their investment in specialized hardware is devalued.

### Built-in Decentralized Mining Pool (P2Pool)

The techniques used by P2Pool to enable a distributed mining pool with no central server could be integrated to make it quick and easy for most users to do some mining even as the difficulty increases. This would not be a requirement of the BitShare protocol, but would be supported by the network.

## Security

### 51% Denial of Service Resistance

Because all nodes have financial incentive to receive dividends they will proactively reject any new blocks that do not include 80% of the known valid transaction fees. All nodes have a financial incentive to validate chains and refuse to do business with anyone who builds off of blocks that would deny them dividends. All miners have incentive to reject blocks that include a large number of ‘never-before-seen’ transactions and fees because it means someone is ‘holding out’ in an effort to collect fees or manipulate the network. Because most users can ‘profitably’ mine all users will actively cooperate in preventing these kinds of manipulation attempts. As a result, the cost of a 51% DOS attack requires the attacker to subsidize the entire network and their competition which will increase the profitability of mining and thus make it more expensive to maintain the 51% Double Spend attack.

### Encrypted Communications

All communication between nodes will be encrypted for two reasons: it will frustrate packet filtering, and it will make it harder to determine the origin of new transactions.

## Economics of BitShares

BitShares attempts to arrange for all actors to act proactively to ensure that collateral requirements are met even during the most extreme market fluctuations. To illustrate how these market forces will interact with the BitShare block-chain rules lets consider some example market situations.

### Rapid Fall in BitShare Value

If the value of a BitShare starts to fall rapidly against BitGold, then all shorts in the system will be faced with a ‘squeeze’ which will force them to buy proactively before their margin is called. If their margin is hit, then they will suffer a 5% fee or worse, complete loss of their collateral. The result of this short-squeeze is that the value of BitGold would rise dramatically above market value of Gold causing even more shorts to face margin calls. This would create an opportunity for new shorts to enter market with full collateral backing their new position. These new shorts would profit when the price settles down after the short-squeeze is over. As a result all market participants will be pro-active about monitoring the price and their collateral which should result in the minimal amount of volatility.

### Rapid Rise in BitShare Value

If the value of BitShares rises rapidly against Gold, then holders of BitGold will see that it is overvalued relative to BitShares. Knowing that other market participants are attempting to buy or sell BitGold based upon its value relative to Gold there will be a rush to sell BitGold at a profit until the price of BitGold in BitShares reaches the price of Gold in BitShares.

This fall in the price of BitGold would mean that the shorts would be over-collateralized and incurring unnecessary opportunity costs. These costs would cause them to cover their position and take their profit.

### Connecting Gold to BitGold Price

All market participants have something to gain if a common understanding can be reached that BitGold is an derivative of a 1oz gold coin bond at the current dividend rate. However, initially there will be no ‘trust’ in what BitGold actually means. As a result market participants will start out placing orders with a wide spread. As the market depth increases the spread will also decrease until a price is reached that has market consensus and is near parity with a 1oz gold bond paying the current dividend rate.

All parties will be going long or short BitGold based upon which direction they think BitGold will move. The only rational way to invest is to assume that it will follow the price of physical gold because on what grounds would you assume that it would diverge from physical gold in any particular direction? The only grounds for a price divergence from gold is a changing demand for BitGold based upon its yield which would give BitGold a premium or discount relative to gold. This premium or discount would be a largely fixed offset and mostly independent of the BitShare to Gold price exchange risk.

There is clearly a difference between ETF gold and physical gold price. Because most individuals have no ability to directly transact in ETF gold, but could trade a gold coin. BitGold could be defined as the price to receive immediate delivery of a 1 oz Gold Eagle and thus slightly decoupling it from the manipulations in the ETF price and also factoring in premiums on Gold Eagles.

### What happens if a BitAsset goes ‘no-bid’?

The first thing that must be understood is that a BitAsset always has value proportional to the dividends backing it. Therefore, the short-position incurs a constant opportunity-cost by not covering. Likewise, the long is still receiving a revenue stream that has value independent of the value of a BitShare and therefore ‘above-market’ dividend rates will attract new buyers to that BitAsset which means that all BitAssets are always liquid based solely on relative dividend rates. As a result no BitAsset will ever go ‘no-bid’ unless BitShares also go no-bid.

For this reason the early adopters face limited (if any) risk in being the first to purchase BitGold. They would be trading BitShares, at say 10% APR, for BitGold that paid twice the BitShares-per-block and therefore profit even if they are the only buyer. When it comes time to 'unwind' this one trade, the price will be determined by whomever wants the liquidity more. If the short wants to stop the bleeding opportunity cost, they will be forced to buy back at a higher price. If the long wants to convert to another asset then they may sell at a lower price. Either way, it is unlikely that there would ever be only two players in any given BitAsset market based only on the opportunity to 'profit' from higher interest rates.

### Market Effects of Dividends

Both BitUSD and BitShares pay dividends at some rate with a dividend ratio normally between 1.5 and 2.5. To price them today you would have to calculate the net-present-value of both revenue streams which should be proportional to both BitUSD and BitShares and therefore the price of BitUSD to BitShares is almost 100% correlated to the exchange rate between USD and non-dividend paying BitShares. Ultimately the premium or discount on BitUSD relative to actual USD will approach the 'borrowing opportunity costs' on the shorts paired against the 'risk premium' demanded by the longs. All other returns made by the holders of BitUSD are derived from the increasing value of the BitShare network itself of which they are a part.

### What happens if there is a market crash that causes margins to be insufficient?

In this event the shorts would be liquidated at market price and the short-term value of the long position may be below slightly below par. Only the most severe crash in the value of BitShares could trigger such an event as it is unlikely that any other asset class could rise in value relative to a stable BitShare value in less than 60 minutes. With the price below parity, market participants are faced with two options, hold until the market stabilizes or 'sell' in the middle of the correction and take a loss. Because all market participants know that the price of BitUSD must recover due to market forces many buyers will enter the market for BitUSD any time it is on sale and thus provide a floor.

If BitShares lose all value it would be a complete collapse of the entire system and everyone would lose. This would be a very unlikely event barring a breach in the block-chain algorithm or encryption. Early adopters would receive higher dividend rates due to the smaller monetary base and therefore be compensated for taking a greater risk. Those who come later will have much more confidence in the algorithm and therefore receive a lower dividend rate.

### How to price BitUSD?

So far we have shown how the price of BitUSD is highly correlated to actual USD; however, we have not provided any rational means for actually establishing the price. So lets look at the value proposition of owning BitUSD. *You get a pseudo-anonymous, secure, dividend paying asset that has all of the properties of Bitcoin and almost none of BitShare/USD exchange rate risk*. With an effective yield on BitUSD of 20% per year you must compare it against other USD investments, such as lending it to the bank at 3% per year. By performing a net-present-value calculation you can determine that 1 BitUSD should sell at about $1.14 based upon yield alone.

This value must be adjusted based upon any premium paid for the crypto-currency features and any discount paid for crypto-currency risks. These premium / discount rates will cause the price to fluctuate between $1.10 and $1.20 and over time that range will narrow as the perceived risks decrease and benefits become clearer.

So far I have only looked at one side of the price equation, that of someone looking to buy BitUSD from someone who already owns BitUSD. But before anyone can own BitUSD someone must create it and that means taking a short position in BitUSD and forgoing a 10% / year dividend. This individual needs dollars to fall against BitShares by 10% just to break even. Therefore, assuming an expectation of price stability he will only short BitUSD when 1 BitUSD is selling for more than $1.14 so he can collect the premium required to offset his costs (10%). This will cause the supply of BitUSD to grow until the price stabilizes around $1.14. If he expects BitShares to go up by more than 10% then he can effectively leverage his position by shorting 1 BitUSD at a price below $1.14 to attract more buyers.

The effect of being able to purchase BitUSD at below $1.14 is to increase the effective rate of return to more than 20%. The effect of having to pay a premium for BitUSD above $1.14 is to decrease the effective rate of return to something less than 20%. Ultimately, the market will establish the proper premium based upon the desired interest rate required to balance the risk/return ratio for lending USD to the network for BitUSD backed by BitShares.

Note: all prices in the above example were based upon an assumed 3% discount rate in the net present value and represent only one means of estimating a fair market price. Ultimately all prices must be determined on the market and will factor in far more factors. The critical thing to understand is that *BitUSD is an asset used to hedge a position in BitShares against changes in the price of USD and is not supposed to have an exact 1:1 exchange rate with USD.*

## Implication of BitUSD for enabling Local Exchanges

The challenge facing LocalBitcoins' users is that the buy-sell spread in any given town is much greater than the buy-sell spread globally. The result is that it is much more expensive to trade in the thinner local market and without a centralized global exchange with accurate trades, reporting price discovery would be difficult further contributing to wider buy / sell spreads.

Because BitUSD is traded globally and in a decentralized manner and yet maintains near parity with a *paper-USD interest bearing bond*, the buy sell spread between BitUSD and paper-USD will be much smaller than what would exist for LocalBitcoins. The effect of this reduced spread is that it will probably compete with escrow fees and time delays associated with remote exchanges and therefore there will be a much larger local market.

It also means that friends and family would probably be willing to lend you paper-USD for BitUSD because they wouldn't have to worry about exchange rate risks and could benefit from a real rate of return. Once they get ‘hooked’ on the interest they receive they may never look back.

## Use Cases

### Local ‘Deposit’

Grandma wants to earn a 10% return on her dollars, but is unable to use a computer. Her grandson decides to help her out, so he receives the dollars from his grandmother and then uses them to buy BitUSD. He buys his BitUSD by posting an ad on craigslist saying that he is looking to buy some. Someone responds to the ad and they meet up to exchange BitUSD for paper dollars. The grandson then prints out the private-key and gives it to his grandmother to keep under her mattress.

### Local ‘Withdraw’

A year later Grandma wants to get her dollars back, so she contacts her grandson and gives him her private key. The grandson then gets on Craigslist and sees an ad for someone nearby who wants to buy some BitUSD. They meet up and trade and the grandson then gives the money to his grandmother.

### Escrow Free Remote ‘Deposit’

George lives in the middle of nowhere and the nearest person with BitUSD is over 2 hours away. Fortunately, he has family who live in a major city, so he calls up his brother and offers him $10 to buy $1000 worth of BitUSD from another local. His brother agrees, so George sends him $1010 and his brother then buys 1000 BitUSD and then transfers (via the BitShare blockchain) those BitUSD to George in the middle of nowhere.

### Short Selling

Sam is a trader who specializes in crypto-currencies. He has been watching the market and sees that BitUSD is ‘overvalued’ relative to BitShares. Therefore he decides to 'short' BitUSD by selling it into the market. To do this he is giving up his dividends. If he was right, the value of BitUSD will fall (relative to BitShares) and he will be able to buy back the BitUSD for less and make a profit greater than his dividends. If he was wrong, then the value of BitUSD could rise and the network could cover his position causing Sam to lose money. As a result, it is only profitable to short if you expect the price to fall at a rate faster than the dividends you give up or if you can sell the resulting BitUSD at a premium.

### Speculator with Leverage

Alex is an early adopter of BitShares (BTS), he has mined 100 BTS and believes that they will triple in value in the months ahead. He could simply hold his position, but instead he wants to leverage up. As a result, Alex shorts BitUSD. If he is right, then he will gain more from this short position than the dividends he might have earned by simply holding BTS. In this way Alex is creating BitUSD for the 'risk-averse' in the early days when BitShares are already appreciating rapidly and paying a very high dividend.

### Currency Hedger

Alice is a currency trader who wants to play the EUR/USD market. Alice mines some BitShares and then uses them to buy BitEUR and short BitUSD because she expects EUR to go up relative to USD. While she maintains this position she has no net exposure to BitShare price changes as any losses in her short position are made up in her long position.

### BitShare Bubble Speculator

David thinks that BitShares are overpriced in a new bubble, so he buys BitUSD which he expects to rise in value against BitShares and also earns a higher dividend rate in the process.

### Merchant Services

Fernando runs an online store and wants to accept payments via a crypto-currency. Unfortunately, all of his suppliers price things in USD. Fernando instead opts to price things in BitUSD. As a result his customers get price stability, Fernando avoids all exchange fees that would be incurred if using something like Mt.Gox merchant services, and Fernando gets to earn interest while he waits to cash out.

### Bitcoin Speculator

Luke has some Bitcoins and wants to buy crypto-bitcoins (BitBTC), using the BitShare exchange. First, Luke must acquire some BitBTC so he finds Charles who has BitBTC and is looking to get real BTC. So, Luke and Charles use atomic cross-chain trading to exchange BitBTC for BTC without having to worry too much about the 'exchange rate' as it should be about 1:1. This 'feature' for cross-chain-trading would be 'built-in' the BitShare client where Luke and Charles would only need to specify the 'addresses' in each chain and the exact exchange ratio. The clients would support 'broadcasting' bids/asks to negotiate 'real-time' counter-parties and all transactions would 'expire' within 20 minutes. Because the trading range on BTC to BitBTC is very small the market should be very liquid and very quick and can easily require all nodes to be alive and interactive without having to worry about a 'thin' market. It would likely work even if only 2 people were online at the same time.

### 100% Reserve Gold ‘Bank’

An interesting side effect of the creation of dividend-paying BitGold that tracks parity with gold is that it enables the creation of a decentralized, peer-to-peer, “100% reserve gold bank”. To make a deposit into this bank, someone could post an ad looking to exchange 1 gold coin for 1 BitGold. Someone looking to withdraw gold from the bank would respond to this ad. Assuming a 1:1 ratio of depositors to those who want to withdraw funds there should be little to no premium or fee associated with such a trade.

If there are more depositors than those looking to withdraw funds then depositors would have to pay a small “ATM” fee to make a deposit. If the situation were reverse then those making a withdrawal would end up having to pay the “ATM” fee. The “ATM” fee will serve to regulate the supply and demand for those seeking to make deposits or withdraws. When the deposit fee is high, then people will hold off until it falls. This high deposit fee will create a profit incentive for ‘shorts’ to borrow more BitGold to sell in exchange for real Gold and profit from the fee. When the withdrawal fee is high, then it will attract depositors who will interpret this as being paid to make a deposit.

Note: calling this system a 'bank' is merely an analogy used to develop a mental model. BitShares is not a bank, doesn't take deposits, nor promises to pay anything. Clearly, a 100% reserve gold bank would have to charge you storage and transaction fees and require certificates of deposit for certain time periods to provide any return.

## Legal Classification of BitShares and BitShare-derived BitAssets

Before offering our opinion on the legal classification of BitAssets we want to remind the reader that we are not lawyers and the following does not constitute legal advice. Please consult a legal professional in your jurisdiction before taking any actions based upon our opinions expressed below.

Throughout this paper we make reference to short, long, margin, call and put options and other traditional financial terms and instruments, however these are only analogies used to explain the behavior of these new BitAssets. In our opinion these instruments do not meet the legal definition of a *financial asset*, *instrument*, *bond*, or anything else on the books aside from the most generic term *'asset'*. Before attempting to classify these new BitAssets lets review the current definitions.

A ***financial asset*** is an ***intangible asset*** that derives value because of a ***contractual claim***.

A ***financial instrument*** is defined as "any ***contract*** that gives rise to a ***financial asset*** of one entity and a ***financial liability*** **or** ***equity*** *instrument of another entity*" according to IAS 32 and 39 (International Accounting Standards Board)

A ***contract*** is a voluntary agreement by ***two or more parties***, each of whom intends to create one or more ***legal obligations*** between them. A contract is a ***legally enforceable promise*** or undertaking that something will or will not occur.

Elements of a contract include:

1. Offer and acceptance and Meeting of the Minds
2. Intention to be Legally Bound
3. Consideration

Additionally the parties to a contract must have capacity to contract, its purpose must be lawful, the form must be legal, the intent must be to create a legal relationship, and the parties must consent.

Under European Union Law you must consider the MIFID (Markets in Financial Instruments Directive). This directive defines a **regulated market** as a multilateral system operated and/or managed by a ***market operator*** which brings together or facilitates the bringing together of multiple ***third-party*** buying and selling interests in ***financial instruments*** - in the system and in accordance with its non-discretionary rules - in a way that results in a ***contract*** in respect of the ***financial instruments*** admitted to trading under its rules and/or systems, and which is authorised and functions regularly in accordance with the provisions of Title III.

The common denominator behind all existing financial assets and liabilities (including cash) is a ***contractual obligation***. If there are no contractual obligations made by any party to any other party then by definition BitShare derived BitAssets are not financial instruments. So lets see if we can find anything within BitShares that satisfies all or even most of the requirements of a contract.

### 1) Bid / Ask Transaction Published to the Block Chain.

A bid or ask is a cryptographically signed transaction by a single, anonymous party. There is no signature by any other party and no obligation to perform. The bid or ask transaction has no legal standing and creates no legal relationships. This bid or ask is processed by a network of anonymous individuals who have no capacity to contract with the anonymous party submitting the bid or ask. In theory, the bid includes payment to anyone who includes the bid in a block and could be considered signed and accepted by the miner. However, once the transaction has been included in a block there is still no outstanding obligation or legal relationship between the two anonymous parties. Furthermore, simply including the transaction in a single block by a single miner does not actually cause the transaction to be executed. It must also be accepted by all other nodes in the network and even if it is accepted there exists no legal relationship or obligation between any two parties.  Furthermore, the result of the accepted transaction is merely an anonymous update to a global shared database and could constitute free speech.

### 2) Short Sell Transaction Published to the Block Chain

These transactions have all of the properties of a Bid / Ask transaction with the only difference being the type of BitAsset used as the input to the transaction and the nature of the resulting outputs. It is still signed by a single anonymous party and is never signed by any other party. There is no legal obligation created nor legal relationship between two or more parties.

### 3) Margin Calls and Covering executed by Miners

No party has a contractual obligation to provide additional margin nor to force covering; however, no party has the ability to prevent their position from being covered when the majority of the network agrees. As a result there is no obligation of any party to enforce the margin nor legally enforceable consequences if they do not.  In fact, no entity is able to enforce the margin and therefore no one to hold liable for failure to act.

### 4) Contract between Developers and Users

BitShares is a protocol for exchanging information that could be implemented by any number of individuals. The developers release the software open source without warranty or promise of any specific behavior. Users of the software get to choose which version to use and which network to join and therefore are in complete control over how they react to the information they receive from the network. Users are even free to modify their software at will and therefore any actions or decisions made by the software are entirely an extension of the user's will and not that of the developers.

Lastly, the developers of BitShares have only created an accounting system that manages a decentralized database. The value of any particular entry within this database is not under control of the developers.

### 5) Exchange Regulations

A centralized Bitcoin / Litecoin exchange run by a ***market operator*** can be regulated because upon accepting deposits of the BitAssets known as Bitcoin or Litecoin, the exchange *converts* them into a *promise to pay* **financial instrument** in the form of an account balance with a particular server.

With BitShares there is no *market operator* and at no point does any actor in the exchange convert a *BitAsset* into a *financial instrument* for the purposes of bringing together multiple *third-parties*. The reason for this is that there is no *first* or *second* party and no *contract* between any parties.

### 6) Distributed Escrow and Arbitration System

To facilitate exchanges with traditional assets and financial instruments, BitShares provides a distributed informal, non-binding, escrow and arbitration system. There are two parties to every non-disputed escrow transaction and three parties in the event of a dispute. There exists an non-binding agreement between the two parties that includes an arbitration clause allowing the defined, but anonymous, 3rd party to decide any disputes at their whim in an entirely non-binding (in a legal sense) way. There does exist a private informal agreement between two parties that is not known to the wider network. The escrow agent never receives funds nor has the ability to send the funds any place but one or both of the parties.

Escrow agents would be subject to any laws, regulations, and licensing requirements applicable to arbitration ***if** the users expect their decision to be legally enforceable*. Fortunately, escrow agents and users specifically acknowledge that no party is under any legal obligation to take any particular action at all and that there is ***no intent to create a legal relationship****.* By specifically stating that at all times no party is held to be legally liable to follow any specific agreement and that there is no *intent to create a legal relationship* between any two parties, the result is that all parties are acting in an informal, purely voluntary, manner outside the jurisdiction of any court. It would be like agreeing to meet someone at the pub and then failing to show up.

> ***Social and market pressures would conspire to motivate all parties to make honest and ethical decisions despite the complete lack of legal obligation to do so.***

The only legal question that remains is whether or not an individual trading a BitAsset for a tangible good or traditional financial-asset (such as cash) in a noncommercial manner could be classified as a money transmitter by any sane regulatory system or court. FinCIN has already published guidance that indicates that buying and selling non-financial assets with a BitAsset is not engaging in money transmission nor a money services business. It could be argued that as long as there are only two parties, no contracts and no party is operating on behalf of anyone else, there is no money transmission. This would be like claiming someone who exchanged gold for cash on craigslist in a noncommercial manner is a money transmitter.

All opinions presented above do not constitute legal advice as we are not lawyers. Please seek a professional opinion before taking any actions that may have legal consequences.

## Alternative Systems

BitShares is being introduced as a new alternative to many prior attempts at creating a decentralized exchange and means of transacting in digital currencies tied to other asset classes such as dollars, gold or silver. Many of the most developed of these systems will be addressed below and we will discuss how they are differ from BitShares in respect to the criteria laid out at the start of the paper.

### Ripple

Ripple is a peer-to-peer network with its own currency (XRP) that facilitates transferring and trading or exchanging currency in any unit. **Ripple is not a trustless** network, but instead a means of shifting credit through a network of friends and family. Each individual must publish a line of credit extended to everyone they know and is at risk of default. In our opinion, this is not a socially viable arrangement which means that most people will end up using Ripple Gateways. A Ripple Gateway acts like a bank by accepting deposits in exchange for credit on the Ripple network. Gateways are likely subject to all of the laws and regulations that apply to money transmitters or any company that accepts deposits. The end result is that **Ripple is not Decentralized and does not provided Limited Liability** for all parties.

Furthermore, Ripple does not support shorts, call, or put options and is therefore **not Diverse.** Without relying on a centralized Gateway such as Mt. Gox or Bitstamp, currency trades are **not aggregated, atomic, nor passive.**

Lastly, **Ripple is not private** because everyone must link their Ripple identity with their real world identity in order to establish lines of credit with friends, family, or Gateways. Ripple is currently not Open Source despite promises to change that in the future.

Lastly, Ripple is not viral in that it offers little value that would appeal to anyone outside of the crypto-currency movement or perhaps businesses that wish to start a Gateway.

### Local Bitcoins

Local Bitcoins is a form of over-the-counter exchange with built in escrow service. While the trades occur in person, the website is not decentralized and the escrow service is dependent upon trust. Furthermore, the exchanges are not fast, atomic, private, aggregated, nor secure. The Price is *not* Right because there is no bid/ask system and all trades ultimately reference a centralized exchange. It is not diverse because there are no call, put, or short positions. The website is also exposed to significant liability due to their escrow service.

### Colored Coins

Colored coins are a means marking coins in the Bitcoin block chain and turning them into cryptographic bearer bonds. This system is inherently based upon trust in the issuer, has significant legal liabilities, and the resulting bearer bonds are not fungible between issuers. This system also lacks diversity without shorts, call, or put options and doesn't solve the problem of a decentralized order book nor passive order execution. Lastly, there is no value proposition that would cause their adoption to be viral nor increase the liquidity in the market. Trades of colored coins cannot be passive, nor aggregated without a centralized exchange.

### Open Transactions

Open Transactions is a system of federated transaction servers that allow users to transact, trade, and exchange in cryptographic bearer bonds published by 3rd parties. This system is inherently based upon trust in the issuers, requires auditing of the transaction servers, and would result in thin markets with wide spreads as different issuers of dollar bonds are not fungible. The creation of a basket of issuer's would serve to distribute but not eliminate risk of default and subsidize the less creditworthy issuers with trust given to the more creditworthy issuers. The system also provides no compelling features to cause viral adoption and the proposed systems for coordinating prices across multiple servers violates the Price is Right principle.

# BitShares

## A Peer-to-Peer Polymorphic Digital Asset Exchange (P2P-PDAE)

Ripple
Local Bitcoins
Colored Coins
Open Transactions