BitShares Documentation

BitShares-Core
contributors

Aug 17, 2023

Technology

Welcome to the BitShares Documentation

Welcome to the documentation portal for the BitShares Blockchain. The content on this page is managed by the BitShares community and is constantly improved.

The purpose of this site is to provide in-depth documentation about the BitShares Blockchain and make it easier for users and developers to leverage the full power of the BitShares Blockchain.

- BitShares Whitepaper
- **Development**
  - BitShares Developers Documentation Portal
  - BitShares-Core Release
  - BitShares-UI Release
- **New: SimpleGUIWallet**
  - *Securing BitShares with Ledger Nano*

CHAPTER 1

Graphene

1.1 Welcome to the Graphene Documentation

The developers of BitShares formed Cryptonomex to monetize the technology, experience, reputation and good will they accumulated during their first two years of development and operations. Much of that technology is embodied in Graphene™, an industrial strength software platform for deploying third generation cryptographically secure decentralized ledgers known as block chains.

Graphene based systems have orders of magnitude better performance than first-generation Bitcoin-derived systems or even the second generation “Bitcoin 2.0” systems that constitute our current closest competitors. Graphene based systems go beyond mere “checkbook” style payments to offer a broad range of financial services distinguished by their transparency and inherent incorruptibility.

This page documents the Graphene technology built by Cryptonomex. You can see Graphene as a toolkit for real-time blockchains. We separated the documentation into smaller parts for convenience and for the sake of easy location of relevant information.

1.1.1 Recent Updates

- `17/04/04` Stress Test results available in bitshares/papers/index
- `16/06/29` bitshares/tutorials/distributed-access-hosting
- `16/04/07` Getting Started
- `16/03/17` integration/traders/index, integration/libraries/index
- `16/03/15` bitshares/investor/index, bitshares/investor/claim, bitshares/migration/legacy-blockchain
- `16/03/02` bitshares/user/referral-program
- `16/03/01` bitshares/tutorials/cli-wallet-usage, bitshares/tutorials/transfer-funds-cli, bitshares/user/voting, bitshares/tutorials/voting
- `16/02/13` Huge improvements in the Public API

- `16/02/08` bitshares/user/committee, bitshares/tutorials/committee-approve-proposal, bitshares/user/vesting
- `16/02/01` integration/merchants/merchant-protocol, Added search to the navigation
- `16/01/19` testnet/index, bitshares/tutorials/pm-create-manual, bitshares/user/eba
- `16/01/13` bitshares/tutorials/uia-update-manual, bitshares/tutorials/uia-create-manual, bitshares/tutorials/uia-create-gui, integration/network-setup, integration/tutorials/index
- `16/01/12` bitshares/user/assets, bitshares/tutorials/uia-create-manual bitshares/tutorials/mpa-create-manual, bitshares/user/assets-faq, bitshares/user/privbta, bitshares/tutorials/publish-feed, bitshares/user/pm, bitshares/tutorials/pm-create-manual, bitshares/tutorials/pm-close-manual

1.1.2 Blockchain Specific Guides

The Graphene Technology has been applied to several blockchain already. BitShares 2.0 has been the first application of Graphene technology and you will be able to find almost everything feature implemented in BitShares 2.0. Further blockchains will be added independently.

BitShares 2.0 is a Financial Smart Contracts platform that enables trading of digital assets and has market-pegged assets that track the value of their underlying asset (e.g. bitUSD tracking the U.S. dollar).

CHAPTER 2

What is BitShares?

Table of Contents

2.1 BitShares 2.0

BitShares is a technology supported by next generation entrepreneurs, investors, and developers with a common interest in finding free market solutions by leveraging the power of globally decentralized consensus and decision making. Consensus technology has the power to do for economics what the internet did for information. It can harness the combined power of all humanity to coordinate the discovery and aggregation of real-time knowledge, previously unobtainable. This knowledge can be used to more effectively coordinate the allocation of resources toward their most productive and valuable use.

Bitcoin is the first fully autonomous system to utilize distributed consensus technology to create a more efficient and reliable global payment network. The core innovation of Bitcoin is the Blockchain, a cryptographically secured public ledger of all accounts on the Bitcoin network that facilitates the transfer of value from one individual directly to another. For the first time in history, financial transactions over the internet no longer require a middle man to act as a trustworthy, confidential fiduciary.

BitShares looks to extend the innovation of the blockchain to all industries that rely upon the internet to provide their services. Whether its banking, stock exchanges, lotteries, voting, music, auctions or many others, a digital public ledger allows for the creation of distributed autonomous companies (or DACs) that provide better quality services at a fraction of the cost incurred by their more traditional, centralized counterparts. The advent of DACs ushers in a new paradigm in organizational structure in which companies can run without any human management and under the control of an incorruptible set of business rules. These rules are encoded in publicly auditable open source software distributed across the computers of the companies' shareholders, who effortlessly secure the company from arbitrary control.

BitShares does for business what bitcoin did for money by utilizing distributed consensus technology to create companies that are inherently global, transparent, trustworthy, efficient and most importantly profitable.

BitShares has went through many changes and has done its best to stay on top of blockchain technology. Towards the end of 2014 some of the DACs were merged and the X was dropped from "BitShares X" to become simply BitShares (BTS).

2.2 Background

BitShares X was first introduced in a White Paper titled "A Peer-to-Peer Polymorphic Digital Asset Exchange" by Daniel Larimer, Charles Hoskinson, and Stan Larimer. Shortly after authoring the White Paper, the project was founded by Daniel Larimer of Invictus Innovations after receiving funding from Chinese venture capital firm BitFund.PE. Charles Hoskinson, founder of the Bitcoin Education Project, was a co-founder of the original project but has since left the team. The BitShares X project received a lot of attention in August 2013 when it was covered by CoinDesk and subsequently announced to the the BitcoinTalk forums on August 22nd 2013 as a project announcement. The project generated a good amount of buzz around the proposal, though the original scope and timelines have since modified.

2.3 Consensus Technology

Consensus is the mechanism by which organizations of people decide upon unitary rational action. While not considered technology in the traditional since, consensus "technology" is the basis of democratic governance and the coordination of free market activity first coined by Adam Smith as the "Invisible Hand." The process of consensus decision-making allows for all participants to consent upon a resolution of action even if not the favored course of action for each individual participant. Bitcoin was the first system to integrate a fully decentralized consensus method with the modern technology of the internet and peer-to-peer networks in order to more efficiently facilitate the transfer of value through electronic communication. The proof-of-work structure that secures and maintains the Bitcoin network is one manner of organizing individuals who do not necessarily trust one another to act in the best interest of all participants of the network. The BitShares ecosystem employs Delegated Proof of Stake in order to find efficient solutions to distributed consensus decision making.

2.4 Distributed Autonomous Companies

Distributed Autonomous Companies (DAC) run without any human involvement under the control of an incorruptible set of business rules. (That's why they must be distributed and autonomous.) These rules are implemented as publicly auditable open source software distributed across the computers of their stakeholders. You become a stakeholder by buying "stock" in the company or being paid in that stock to provide services for the company. This stock may entitle you to a share of its "profits", participation in its growth, and/or a say in how it is run.

2.5 Community

The BitShares community is a global network of people who all share the same goal of creating and participating in various Distributed Autonomous Companies. The community mainly revolves around the BitShares Team and third parties who use Graphene (the toolkit that makes BitShares possible) to create their own Distributed Autonomous Companies. The main discussions in the BitShares community takes place openly at BitSharestalk.org.

CHAPTER 3

The History of BitShares

Table of Contents

3.1 The History of BitShares as laid out by Stan Larimer

"Here are the first parts of a planned series of blog articles that will appear on the bitshares.org website as soon as I am sufficiently pleased with them. This series is intended to be a resource for newbies and a summary of all that has been accomplished in the past year. Think of this as the Official Year One Newsletter."

- Part One Source
- Part Two Source
- Part Three Source

3.2 Part One

On the second day of June 2013 is the anniversary of the invention of BitShares. That day, a rogue entrepreneur named Dan "Bytemaster" Larimer was struck on the head by a proverbial migrating coconut. When he regained consciousness, he realized that he had invented bit-USD, the key insight that makes BitShares possible. Before sundown he had reworked his original BitShares whitepaper and published the whole new concept at bitcointalk.org:

- Creating a Fiat/Bitcoin Exchange without Fiat Deposits

Over the next five weeks, Bytemaster engaged in a series of vigorous forum discussions defending and refining the concept. There he met Charles Hoskinson who helped to vet the idea and develop a business plan. Charles presented the plan to Li Xiaolai in China who agreed to fund the development. On American Independence Day, the Fourth of July 2013, Invictus Innovations was incorporated in the state of Virginia.

The next several months were spent bootstrapping the company and publishing articles, many of which may be found on the bitsharestalk.org thread at Advice, Tutorials, and General References for Newbies.

In September, the concept of a Distributed Autonomous Company (DAC) was invented and introduced to the world in two groundbreaking LetsTalkBitcoin.com articles:

- Overpaying for Security
- Bitcoin and the Three Laws of Robotics

Invictus introduced the BitShares Vision to the world via presentations by Hoskinson and Larimer at the Atlanta Bitcoin Conference in October 2013. It is here that the plans for Keyhotee were first introduced – an integrated multi-wallet, communication, and DAC interface application intended to defend privacy and help spread knowledge of BitShares technologies outside the crypto-currency community.

Hoskinson and Larimer parted company at this point. They each agreed to keep their reasons confidential and there is no bad blood from our point of view. The only official statement on the subject was made by CEO Bo Shen to end a minor forum firestorm here:

BitSharestalk

It is our opinion that Charles Hoskinson is the best dealmaker we have ever seen, and we miss his vision and talent for recruiting allies. No doubt he will help make his new Ethereum team very successful.

Despite this loss, all of this activity was beginning to create a buzz that would soon explode on the scene with a sequence of revolutionary innovations at roughly monthly intervals that continue to this very day.

The first was ProtoShares…

3.3 Part Two

November's Innovation – BitShares PTS

BitShares PTS (formerly called ProtoShares) was developed for an entirely different reason than what its paradigm-shattering role became shortly after launch. In fact, every one of the subsequent breathtaking innovations came about from reacting to opportunities and lessons learned from the previous month's breakthroughs and, um, screw-ups. Necessity is the mother of invention. I wish we could say we had it all planned out in advance, but no business plan survives first contact with the market. We are merely blessed opportunists.

Initially, we were just looking for a way serve people interested in our first objective, BitShares X. A way for them to start mining and trading it early. BitShares X was first viewed as a coin backed by a built-in business that gives it more worth than the speculative value of a meme or some alternative technical implementation. In this first case, that integral unmanned business was a decentralized bank and exchange.

Yep. Your coins would now contain a bank, not the other way around.

Needless to say, this kind of second-generation crypto-company takes a lot longer to build and early adopters were growing impatient. So our plan was to just offer a plain old Bitcoin clone whose coins would be a BitShares X prototype - upgradable into BitShares X "bitshares" when it was ready to launch. We would simply initialize the first 10% of the bitshares to match all the public keys of PTS holders, giving them instant matching control of the same number of bitshares in BitShares X. This is how the concept of a protocoin was born.

We envisioned many exciting uses for protocoins. For example, they could be used as A way to separate investing in an idea from investing in one or more implementations of the idea. An incentive for competitors to cooperate on building an implementation because they could all be common stakeholders in the idea. A way to vet an idea and attract venture capitalists based upon prediction market evidence that the idea has value. A way for developers to invest in an idea and raise funding by generating growth from showing more and more evidence that they will successfully implement the idea in a way that benefits investors in the idea. A way for someone with a good idea but lacking the ability to implement it to share it and benefit from its ultimate implementation by somebody else. A way for an entire community to participate in "pre-mining" in a way that might be deemed fair (e.g. for unmanned businesses that must start out with enough currency to operate and enough credibility to get market depth on exchanges from Day One.) A more graceful "soft fork" way to upgrade to version two of a DAC by instantiating the new in parallel with the old and let the owners (shareholders) not just the employees (miners) decide when and if value transitions from the old to the new. A way to build a community and get them to cooperate on the implementation because they all have a stake in the idea. So you see, right off the bat we are talking about two assets: PTS and BTS. Before long, we would be talking about entire families of such assets. Second-generation crypto-currencies that we began to call crypto-equities because the coins also seemed like "shares" in the underlying unmanned business that gave the currency value - BitShares.

Since then, we have come to prefer the inverse of this dual metaphor:

Bitcoin is a type of crypto-company that implements a coin not BitShares as a type of crypto-coin that implements a company.

Of course, BitShares are something very different than shares in a government-created and therefore government-regulated organization. We are speaking metaphorically to help people understand how they work and what gives them value. They can still be viewed as ordinary altcoins (ok, incredibly powerful ordinary altcoins) as far as their underlying technology is concerned.

Charles Evans explored this dual metaphor in this delightful blog article:

A BitRose by Any Other Name. http://bitshares.org/a-bitrose-by-any-other-name/

We offered a bounty for an experienced coin designer to build the PTS protocoin for us. A developer known as FreeTrade answered the call. It took him about a month to clone it from the Bitcoin library. Then, while we were still evaluating his code, another independent entrepreneur known as Super3 downloaded the open-source from FreeTrade's library and started it running. On November 5, 2013 Super3 went down in history as the miner of the first protocoin block in crypto-equity history!

POW! The rest of the world (who had been eagerly awaiting the launch based on the several months we had been writing about it) jumped on it with everything they had. It took just a few days before the competition became so intense that people had a hard time mining solo with their individual computers. They started joining pools that several enterprising businessmen quickly set up and then everyone started renting cloud computers to remain competitive. By the end of the third week, there were hundreds of thousands of mining nodes competing. Several independent coin exchanges jumped in and listed PTS, driving it immediately into the top ten of the over 100 coins listed on coinmarketcap.com at the time.

So you see, we really don't own PTS. It was launched by the industry for the industry. We just described what ought to exist, and a decentralized industry of entrepreneurs produced it practically overnight.

Of course, that moon shot may have had something to do with one small suggestion we made literally at the last minute: we decided to recommend PTS be the basis for more than just BitShares X. PTS should also be used to initialize all of the other second-generation assets we had been writing about. Mine once for a whole family of assets. Why should you have to keep mining over and over again to get a "fair" distribution?

In fact, we recommended that other developers do the same thing. Suddenly BitShares PTS was backed by more than thin air. More than just one unmanned business. More than just one company’s product line of unmanned businesses. It could well become backed by a good portion of the unmanned business industry!

BitShares PTS was valuable because as a universal prototype it was upgradable to multiple future releases like BitShares X.

Just like a good deal on Microsoft Office 1.0 might get you free upgrades on Word, Excel, PowerPoint and all the rest . . . for as long as you both shall live!

To a community willing to speculate on any altcoin with a cute name, that was all it took. Now there was something tangible to speculate on. Soon crypto-currency speculators would be demanding to know every new asset’s business case.

Imagine that! We had almost accidentally changed the crypto-currency industry forever.

It was just our opening shot.

3.4 Part Three

3.4.1 December’s Innovation – TAPOS and the End of Mining

In the weeks that followed it became increasingly obvious that the whole paradigm of mining on which the crypto-currency industry is founded was horribly flawed. While generally billed as a “fair” lottery for wide distribution of a new currency, it was clear that the ordinary guy was still at a disadvantage. Technically savvy people could use and optimize the tools - others could not install their wallet. Wealthy individuals could rent computers by the thousands - others had no computer at all. Only a very small percentage of the general population was benefiting - sucking up the lion’s share of the coins and then reselling them on the market at a profit.

Now, there’s nothing wrong with using your brains or wealth to earn a profit while contributing to society (like, say, developing a new technology), but as far as the general public was concerned, this small elite group of individuals were effectively just selling the currency into existence. Most of the general population had to buy them from the market anyway!

And even those elite few only got to keep a small percentage of what the market was willing to pay for the currency. They were required to destroy most of what they received from the market doing the electronic equivalent of digging holes and filling them back in. The whole industry was ein bisschen poco loco.

“No, wait!”, the Bitcoin-trained community protested, “burning the seed capital is the price we must pay for securing the network!”

Except the network was not really being secured. Economies of scale dictate that hashing power will always migrate toward specialized capital-intensive organizations ultimately killing the very decentralization that mining was supposed to ensure. Today, most Bitcoin mining power is concentrated in the hands of a half-dozen individuals with just two of them controlling over 51%. And they proudly collaborate “for the good of the network.”

Bytemaster recognized that Bitcoin could be viewed as an unprofitable company and its coins as stock in that company. Stock value was generally rising because demand for its services (efficient private money transmission) exceeded supply. But, meanwhile it was bleeding red ink. 100% of its transaction fees were going to pay its employees (the miners). But that still wasn’t enough. It had to print more money (up to 12% annual inflation) also to pay its employees. So Bitcoin is a company with annual losses near 12%. (And the employees were only getting to keep a few percent of the money being wasted on them.)

He decided that eliminating those employees was a key objective that would inevitably lead to a whole new generation of profitable crypto-businesses. Assets based on destructive mining would go the way of the dinosaur, unable to compete with profitable business models of second generation assets that could afford to pay dividends and interest to their holders. It was just a matter of time.

So a month after the ProtoShares revolution, around December 1, Bytemaster fired his second shot heard round the world: all his future designs would replace Proof of Work mining with a Proof of Stake derivative.

Transactions as Proof of Stake (TAPOS) and the End of Mining . An algorithm that was lightweight enough to run invisibly on anyone's computer, for free! Mining was dead. Next generation crypto-assets would be profitable. They would be valuable because they returned a yield, rather than for superficial speculative reasons.

There were merely a few technical wrinkles to iron out…

3.5 History of Funding

Also see, Summary of Key Facts for Invictus Stakeholders

When Invictus of VA was formed under Charles Hoskinson's term as CEO, our purpose was to create a company that would achieve all the objectives of Mr. Li as our primary investor.

(Since shortly after our founding, Mr. Li Xiaolai has held a subscription agreement that entitles him to buy 25% of our shares for a fixed price payable in increments spread out over the first year. Mr. Li also acquired an additional 1% from Charles Hoskinson in a separate purchase. This means that his total stake in Invictus is 26% of which he has completed payments on 21% as scheduled. His final payment for the last 5% is on hold pending completion of a restructuring forced by discovery of certain applicable U.S. regulations. All these shares will be equally treated.)

We had three nested tasks:

Build and launch BitShares X Build a company to Build and launch BitShares X. Build a decentralized industry in which this company could build and launch BitShares X (and many more).

Part of our task was to research the legal requirements to accomplish all of these goals.

In the process of studying the requirements in the United States we ran into a number of issues and uncertainties. In particular, there are strict rules about who can own shares of a U.S. corporation.

We recommended to Mr. Li that he ask an attorney he trusts to start over and create a company that would be able to meet all of the goals and honor all of his commitments. It has taken six months to work out all the details, after consulting with Li's attorney and multiple U.S law firms.

We will soon be ready to release a public statement about the details, but the bottom line is that Invictus Innovations Incorporated, LTD in Hong Kong is the company we intended to create in Virginia, except with the ability to meet the needs of Asian investors better than we can here.

So, you can think of it as relocating the Virginia company, but legally they are two independent companies with independent management aiming to meet Mr. Li's goals and obligations 100%.

The Virginia company now only handles small tasks associated with American payroll and payment processing. Further details on this decomposition into independent businesses optimized to comply with all regulations in their domains will be forthcoming.

3.6 The Great Consolidation

In the late part of 2014 it became obvious that Bytemaster had to lend his energies to other projects. People had donated AGS funds with the expectation of future DACs. With the decreasing funding due to dropping BTC prices and the requirements of Dan Larimer, the Great Consolidation occurred. Follow My Vote and DNS were merged into BTS so that all developers could be brought to work directly on one product instead of DACs all competing for users.

One outcome of this was also the addition of paying on the blockchain. Previously BitShares was a purely deflationary blockchain with dividends paid out by the burning of transaction fees. (Less currency in existence gives more value to those remaining.) With a pressing need to be the most innovative crypto-currency out there, it was determined that the

Delegates needed to start paying. So the cap on Bitshares was raised to be slowly paid out similar to the inflation in Bitcoin. The rate was made to be kept under the current level of Bitcoin inflation, but delivering direct and meaningful value. Timeline of BitShares by forum announcements

- Momentum Proof of Work Introduced on BTT - October 18 2013
  - https://bitcointalk.org/index.php?topic=313479.0
  - http://static.squarespace.com/static/51fb043ee4b0608e46483caf/t/52654716e4b01acd1ac8a085/1382369046208/MomentumProofOfWork.pdf (White Paper)
  - https://bitsharestalk.org/index.php?topic=962.msg9752#msg9752
- Keyhotee ID Preorder - November 3, 2013
  - https://bitsharestalk.org/index.php?topic=2.msg2#msg2
- Mining of Bitshares PTS (Protoshares) - November 5, 2013
  - https://bitsharestalk.org/index.php?topic=4.msg4#msg4
- Transactions as Proof of Stake - November 30, 2013
  - https://bitsharestalk.org/index.php?topic=1138.msg12010#msg12010
  - http://the-iland.net/static/downloads/TransactionsAsProofOfStake.pdf
  - https://bitsharestalk.org/index.php?topic=1138.msg11968#msg11968
  - https://bitsharestalk.org/index.php?topic=1138.msg12967#msg12967
- Consensus + TaPoS
  - https://bitsharestalk.org/index.php?topic=1138.msg29905#msg29905
  - https://bitsharestalk.org/index.php?topic=3588.msg45119#msg45119
- The Inception of DPOS - December 8, 2013
  - https://bitsharestalk.org/index.php?topic=1138.msg13602#msg13602
  - https://bitsharestalk.org/index.php?topic=1138.msg14784#msg14784
- The Inception of AGS - December 14, 2013
  - https://bitsharestalk.org/index.php?topic=1397.msg14794#msg14794
- Official AGS Announcement - December 25, 2013
  - https://bitsharestalk.org/index.php?topic=2644.msg32817#msg32817
- February 28 Snapshot Announced - January 26, 2014
  - https://bitsharestalk.org/index.php?topic=2591.45
- Bitshares X Whitepaper - February 14th, 2014
  - https://docs.google.com/document/d/1RLcjSXWuU9vBJzzqLEXVACSCdn8zXKTTJRN_LfoCjNY/edit?pli=1#
- TaPos with a Trustee - March 28, 2014
  - https://bitsharestalk.org/index.php?topic=3865.msg48605#msg48605
- BitShares X released by DACsunlimited, July 19th, 2014
  - https://bitsharestalk.org/index.php?topic=5750.0

In addition there are numerous threads discussing The Great Consolidation.

CHAPTER 4

Delegated Proof of Stake (DPOS)

Delegated Proof of Stake (DPOS) is a new method of securing a crypto-currency's network. DPOS attempts to solve the problems of both Bitcoin's traditional Proof of Work system, and the Proof of Stake system of Peercoin and NXT. DPOS implements a layer of technological democracy to offset the negative effects of centralization.

Table of Contents

4.1 Background

Delegated proof of stake mitigates the potential negative impacts of centralization through the use of witnesses (formally called *delegates*). A total of *N* witnesses sign the blocks and are voted on by those using the network with every transaction that gets made. By using a decentralized voting process, DPOS is by design more democratic than comparable systems. Rather than eliminating the need for trust all together, DPOS has safeguards in place the ensure that those trusted with signing blocks on behalf of the network are doing so correctly and without bias. Additionally, each block signed must have a verification that the block before it was signed by a trusted node. DPOS eliminates the need to wait until a certain number of untrusted nodes have verified a transaction before it can be confirmed.

This reduced need for confirmation produces an increase in speed of transaction times. By intentionally placing trust with the most trustworthy of potential block signers, as decided by the network, no artificial encumbrance need be imposed to slow down the block signing process. DPOS allows for many more transactions to be included in a block than either proof of work or proof of stake systems. DPOS technology allows cryptocurrency technology to transact at a level where it can compete with the centralized clearinghouses like Visa and Mastercard. Such clearinghouses administer the most popular forms of electronic payment systems in the world.

In a delegated proof of stake system centralization still occurs, but it is controlled. Unlike other methods of securing cryptocurrency networks, every client in a DPOS system has the ability to decide who is trusted rather than trust concentrating in the hands of those with the most resources. DPOS allows the network to reap some of the major advantages of centralization, while still maintaining some calculated measure of decentralization. This system is enforced by a fair election process where anyone could potentially become a delegated representative of the majority of users.

4.2 Rationale Behind DPOS

- Give shareholders a way to delegate their vote to a key (one that doesn't control coins 'so they can mine')
- Maximize the dividends shareholders earn
- Minimize the amount paid to secure the network
- Maximize the performance of the network
- Minimize the cost of running the network (bandwidth, CPU, etc)

4.2.1 Shareholders are in Control

The fundamental feature of DPOS is that shareholders remain in control. If they remain in control then it is decentralized. As flawed as voting can be, when it comes to shared ownership of a company it is the only viable way. Fortunately if you do not like who is running the company you can sell and this market feedback causes shareholders to vote more rationally than citizens.

Every shareholder gets to vote for someone to sign blocks in their stead (a representative if you will). Anyone who can gain 1% or more of the votes can join the board. The representatives become a "board of directors" which take turns in a round-robin manner, signing blocks. If one of the directors misses their turn, clients will automatically switch their vote away from them. Eventually these directors will be voted off the board and someone else will join. Board members are paid a small token to make it worth their time ensuring uptime and an incentive to campaign. They also post a small bond equal to 100x the average pay they receive for producing a single block. To make a profit a director must have greater than 99% uptime.

4.2.2 Pooled Mining as Delegated Proof of Work

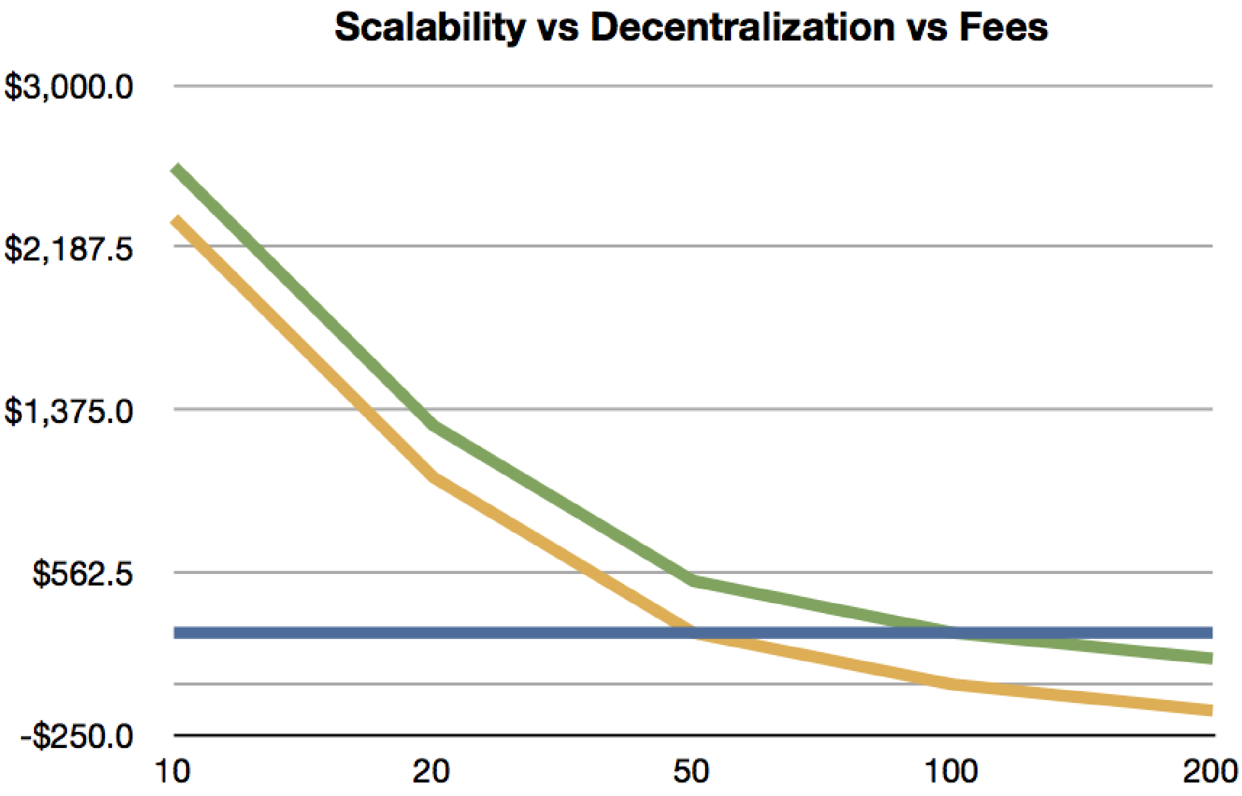
So how is this different than Bitcoin? With Bitcoin, users must pick a mining pool and each pool generally has 10% or more of the hash power. The operator of these pools is like a representative of the clients pointed at the pool. Bitcoin expects the users to switch pools to keep power from becoming too centralized, but collectively five major pools control the network and manual user intervention is expected if one of the pools is compromised. If a pool goes down then the block production rate slows proportionally until it comes back up. Which pool one mines with becomes a matter of politics.

4.2.3 Reasons to not randomly select representatives from all users

- High probability they are not online.
- Attackers would gain control proportional to their stake, without any peer review.
- Without any mining at all, the generation of a random number in a decentralized manner is impossible and thus an attacker could control the random number generation.

4.3 Scalability

Assuming a fixed validation cost per transaction and a fixed fee per transaction, there is a limit to the amount of decentralization that can take place. Assuming the validation cost exactly equals the fee, a network is completely centralized and can only afford one validator. Assuming the fee is 100x the cost of validation, the network can support 100 validators.



Systems like Nxt and Peercoin will have excessive fees if they intend to allow everyone to be a validator and earn fees at scale. What this means for Nxt and Peercoin is that anyone with less than 1% stake cannot validate profitably unless their fees are higher than our DPOS chain. If these chains assume 100 delegates is too centralized and start promoting they have 1000 validators, then their fees must be 10x those of DPOS. If such a chain grew to be the size of Bitcoin ($10 B) then only those with $1M worth of coin could validate profitably and most would consider that an elite club. If they reduce the minimum stake to be a validator to $1000, then their fees would be 10,000 times higher than DPOS.

Developers of DPOS assume that everyone with less than the amount required to validate won't participate. Also assumed is a "reasonable" distribution of wealth. It's clear that unless alternate chains have unusually high fees, there will only be a handful of people with enough stake to validate profitably.

In conclusion, the only way for POS to work efficiently is to delegate. In the case of Nxt, they can pool their stake by some means and ultimately this will end up like DPOS prior to approval voting with a variable number of delegates. Delegates wouldn't actually receive any income as with mining pools because the validation expenses will consume the vast majority of the transaction fees.

The end result is that decentralization has a cost proportional to the number of validators and that costs do not disappear. At scale, these costs will centralize any system that does not support delegation. This kind of centralization should be designed as part of the system from the beginning so that it can be properly managed and controlled by the users, instead of evolving in some ad hoc manner as an unintended consequence.

4.4 Role of Delegates

- A witness is an authority that is allowed to produce and broadcast blocks.
- Producing a block consists of collecting transactions of the P2P network and signing it with the witness' signing private key.
- A witness' spot in the round is assigned randomly at the end of the previous block

4.5 Voting Algorithm

4.5.1 How do I get "votes?"

- Persuade others to give upvotes to your witness
- When another user gives an upvote to your (and possibly other) delegates
- A user can give an upvote for more than one witness. As a result all upvoted witnesses get a vote
- Convince proxies (that vote on behalf of their followers) to vote for you

4.5.2 Why use only upvotes?

- Giving only upvotes, and allowing multiple votes per share, is called **Approval Voting**, and comes with several advantages over the old *delegation* voting.
- No downvotes are needed, which not only simplifies usability but also reduces code and complexity.

4.5.3 How are 'votes' counted?

Once every *maintenance interval*, all votes are recounted and the corresponding result takes effect.

4.5.4 Is there an anti-vote?

Not any more. After discovering emski's attack the developers decided to use **Approval Voting**.

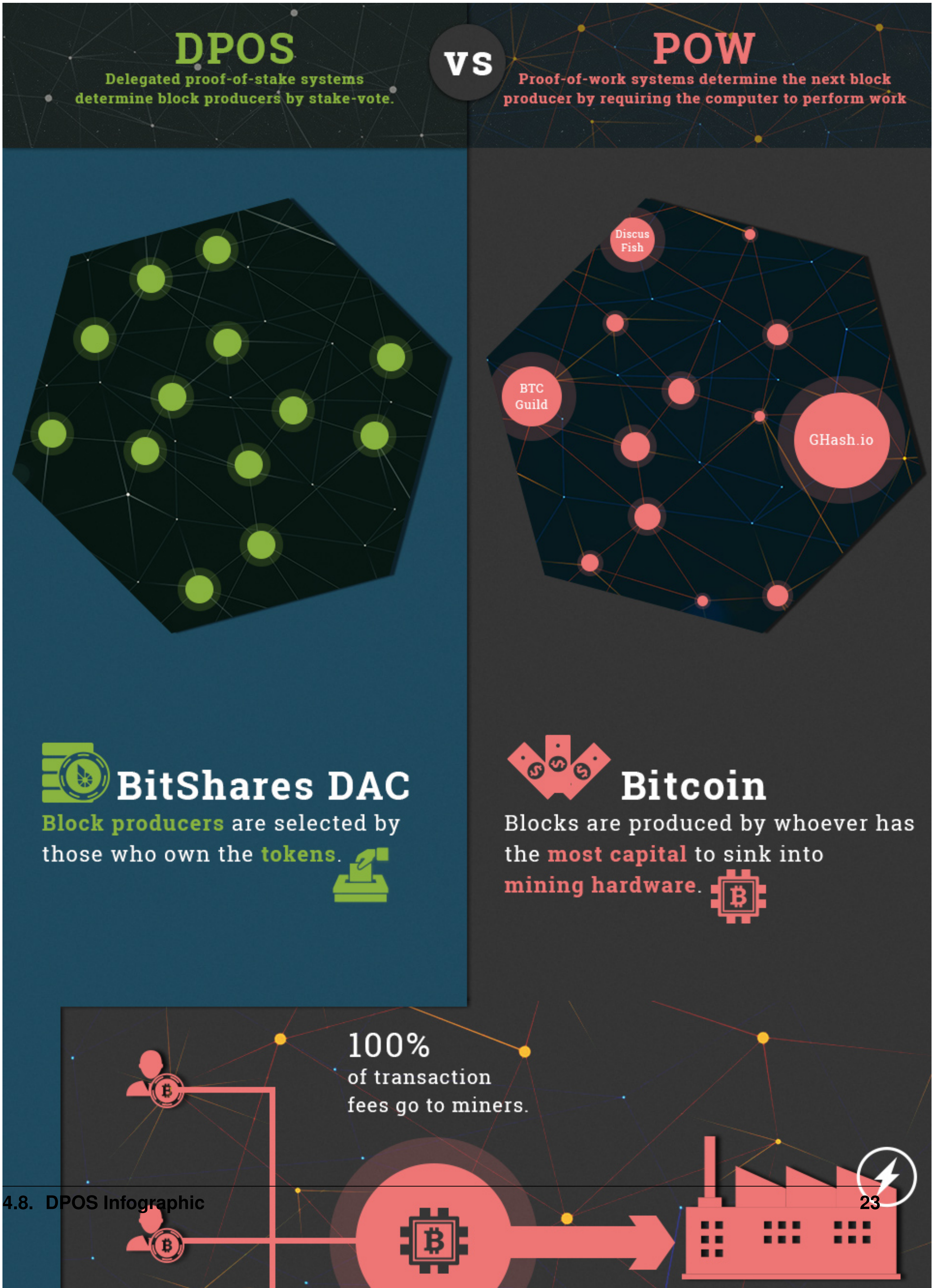
4.6 Disincentives for Attacks

- By choosing not to produce a block, a witness risks getting fired and they lose guaranteed profits in the future.
- A dishonest delegate would only fail to produce a block if they were sure to win something from it
- If a lottery only payed out 50% to a jackpot (giving the other 50% to charity) then the most this dishonest delegate could do is break even.
- Witnesses can't sign invalid blocks as the block needs confirmation by the other witnesses as well

4.7 How many witnesses are securing the network

This is totally in the hands of the shareholders. If the majority votes for 50 witnesses, then 50 witnesses will be used. If the shareholders only vote for 20, so be it. The minimum possible witness count is 11.

4.8 DPOS Infographic


DPOS
Delegated proof-of-stake systems determine block producers by stake-vote.
vs
POW
Proof-of-work systems determine the next block producer by requiring the computer to perform work
Discus Fish
BTC Guild
GHash.io
BitShares DAC
Block producers are selected by those who own the tokens.
Bitcoin
Blocks are produced by whoever has the most capital to sink into mining hardware.
100%
of transaction fees go to miners.

4.9 Sources and Discussions

- https://bitsharestalk.org/index.php?topic=5164.msg67657#msg67657
- https://bitsharestalk.org/index.php?topic=5205.0
- https://github.com/BitShares/bitshares_toolkit/wiki/Delegated-Proof-of-Stake
- https://bitsharestalk.org/index.php?topic=4984.0
- https://bitsharestalk.org/index.php?topic=4927.0
- https://bitsharestalk.org/index.php?topic=4869.0
- https://bitsharestalk.org/index.php?topic=4853.0
- https://bitsharestalk.org/index.php?topic=4836.0
- https://bitsharestalk.org/index.php?topic=4714.0

CHAPTER 5

What is different BitShares

Here we give a brief overview of what is different in BitShares 2.0 when compared to satoshi-based blockchains such as Bitcoin, Litecoin, etc.. from the perspective of an exchange.

Table of Contents

5.1 Several Tokens

In contrast to all satoshi-based clients, BitShares 2.0 offers a variety of blockchain tokens. There is not just the BTS (core token) but many others. Hence, as an exchange you need to distinguish different assets, either by their id (1.3.0 (BTS), 1.3.1 (USD), . . .) or by there symbol.

5.2 Registered Identities

All participants in BitShares 2.0 are required to have a registered unique name. This is similar to mail addresses and are used to address recipients for transfers. As an exchange you will only ever need to tell your customers your BitShares account name and they will be able to send you funds.

5.3 No More Addresses

In BitShares 2.0, we have separated the permissions from the identity. Hence, as an exchange you don't need to ever deal with addresses again. In fact, you actually cannot possibly use an address because they only define so called *authorities* that can control the funds (or the account name). This should greatly simplify integration as you don't need to store thousands of addresses and their corresponding private keys.

5.4 Memos

In order to distinguish customers, we make use of so called *memos* similar to BitShares 1, which are encrypted. In contrast to BitShares 1.0, we now have a separated memo key that is only capable of decoding your memo and cannot spend funds. Hence, in order to monitor deposits to the exchange you no longer need to expose the private key to an internet connected machine. Instead you only decode the memo and leave the funds where they are.

5.5 Securing Funds

Funds can be secured by *hierarchical cooperate accounts*. In practice, they are (Threshold) Multi-Signature accounts from which funds can only be spend if several signatures are valid. In contrast to mostly every other crypto currency, you can propose a transaction on the blockchain and don't need other means of communications to add your approval to a certain transactions. You can find more details about these account types in

- account-membership
- securing-funds

5.6 Full Nodes and Clients

We have rewritten the core components from scratch and separated the core P2P and blockchain components from the wallet. Hence, you can run a full node without a wallet and connect your wallet to any public (or non-public) full-node (executable *witness_node*). The communication can be established securely but the private keys never leave the wallet.

5.7 Object IDs

Since BitShares 2.0 offers a variety of features to its users that are different in many ways, we have decided to address them using *object ids*.

For instance:

<table>
<tr><th colspan="2">Object ID | translates to</th></tr>
<tr><td>`1.3.1`</td><td>asset USD</td></tr>
<tr><td>`1.3.0`</td><td>asset BTS</td></tr>
<tr><td>`1.2.<id>`</td><td>user with id `<id>`</td></tr>
<tr><td>`1.6.<id>`</td><td>block signer `<id>`</td></tr>
<tr><td>`1.11.<id>`</td><td>operation with id `<id>`</td></tr>
</table>

CHAPTER 6

Technology - BitShares.org

- https://bitshares.org/

The BitShares platform itself is run and maintained by the BitShares community an open consortium of individuals and organizations committed to providing universal access to the power of smart contracts.

Working together, this community has designed and developed the BitShares platform to include numerous innovative features which are not found elsewhere within the smart contract industry:

Table of Contents

6.1 Price-Stable Cryptocurrencies

- SmartCoins provide the freedom of cryptocurrency with the stability of the dollar

A SmartCoin is a cryptocurrency whose value is pegged to that of another asset, such as the US Dollar or gold. SmartCoins always have 100% or more of their value backed by the BitShares core currency, BTS, to which they can be converted at any time at an exchange rate set by a trustworthy price feed. In all but the most extreme market conditions, SmartCoins are guaranteed to be worth at least their face value (and perhaps more, in some circumstances). Like any other cryptocurrency, SmartCoins are fungible, divisible, and free from any restrictions. (Read more..)

6.2 Decentralized Asset Exchange

- BitShares provides a built in high-performance decentralized exchange - "DEX"

BitShares provides a high-performance decentralized exchange, with all the features you would expect in a trading platform. It can handle the trading volume of the NASDAQ, while settling orders the second you submit them. With this kind of performance on a decentralized exchange, who needs risky centralized exchanges? (Read more..)

6.3 Industrial Performance and Scalability

- BitShares is capable of 100,000 TPS with proper industrial-grade setup

High performance blockchain technology is necessary for cryptocurrencies and smart contract platforms to provide a viable alternative to existing financial platforms. BitShares is designed from the ground up to process more transactions every second than VISA and MasterCard combined. With Delegated Proof of Stake, the BitShares network can confirm transactions in an average of just 1 second, limited only by the speed of light. (Read more..)

6.4 Dynamic Account Permissions

- On-the-fly management, risk prevention, authority assignments and much more for corporate environments

BitShares designs permissions around people, rather than around cryptography, making it easy to use. Every account can be controlled by any weighted combination of other accounts and private keys. This creates a hierarchical structure that reflects how permissions are organized in real life, and makes multi-user control over funds easier than ever. Multi-user control is the single biggest contributor to security, and, when used properly, it can virtually eliminate the risk of theft due to hacking. (Read more..)

6.5 Recurring & Scheduled Payments

- Flexible withdrawal permissions, subscriptions and bills

BitShares is the first smart contract platform with built-in support for recurring payments and subscription payments. This feature allows users to authorize third parties to make withdrawals from their accounts within certain limits. This is a convenient way to "set it and forget it" for monthly bills and subscriptions. (Read more..)

6.6 Referral Rewards Program

- Network growth through adoption rewards and single-level referrals

BitShares has an advanced referral program built directly into its software. Financial networks derive their value primarily from their network effect: more people on the same network increases the value of that network for everyone. BitShares capitalizes on this by rewarding those who sign up new users, and does so in a fully transparent and automated way. (Read more..)

6.7 User-Issued Assets

- Regulation-compatible crypto-assets from the Token Factory.

The BitShares platform provides a feature known as "user-issued assets" to help facilitate profitable business models for certain types of services. The term refers to a type of custom token registered on the platform, which users can hold and trade within certain restrictions. The creator of such an asset publically names, describes, and distributes its tokens, and can specify customized requirements, such as an approved whitelist of accounts permitted to hold the tokens, or the associated trading and transfer fees. (Read more..)

6.8 Stakeholder-Approved Project Funding

- Built in dApps powered by a core utility token

BitShares is designed to be self funding and self-sustaining by giving the stakeholders the power to direct where blockchain reserves are spent. BitShares has a reserve pool of 1.2 billion BTS (about $8 million dollars) that automatically grows as transaction fees are collected and the share price rises. Each day, the blockchain is authorized to spend up to 432,000 BTS (about $77,000 per month), which is enough to hire a small team to maintain the network for years, even with no price appreciation. (Read more..)

6.9 Transferable Named Accounts

- Human-readable account names registered in the blockchain

Named accounts enable users to easily remember and communicate their account information. We don't use IP addresses to browse the internet or numbers to identify our email, so why shouldn't we have human-friendly account names for our financial transactions? (Read more..)

6.10 Delegated Proof-of-Stake Consensus

- A robust and flexible consensus protocol

Delegated Proof of Stake (DPOS) is the fastest, most efficient, most decentralized, and most flexible consensus model available. DPOS leverages the power of stakeholder approval voting to resolve consensus issues in a fair and democratic way. All network parameters, from fee schedules to block intervals and transaction sizes, can be tuned via elected delegates. Deterministic selection of block producers allows transactions to be confirmed in an average of just 1 second. Perhaps most importantly, the consensus protocol is designed to protect all participants against unwanted regulatory interference. (Read more..)

CHAPTER 7

Things you should know

7.1 For the Starter

- **Security and Control over accounts and funds**: No one can access your funds unless you let them, intentionally, or unintentionally. With the power to be independent from 3rd parties, comes the responsibility to protect what belongs to you.
- **Can interact with people directly**: With BitShares it becomes possible to interact with people directly without needing to go through a middleman. Hence, BitShares is a platform of free speech that implements a payment platform and exchange for digital goods.
- **Fast**: Transactions in BitShares are verified and irrevocable in only a few seconds time.
- **Decentralized Committee**: Decisions that can effect the BitShares ecosystem are made using a on-chain committee voted upon by shareholders. Hence, no single entity can change the deal retroactively.
- **Flexible**: Protocol upgrades (formerly known as *hard forks*) can be implemented and executed to improve the BitShares business over time and allow to react on.

7.2 For the Investor

- **Become BTS Holder**: If you buy `BTS` either from a partner exchange or from the DEX, you become a BTS Holder of the BitShares decentralized business and as such can take a cut of its profits and participate in votes for future directions.
- **Expenses**: Vote for expenses of the business and hire workers to do important tasks for BitShares.
- **Leaders**: Participate in political decisions by voting for committee members that represent your views!
- **Protocol upgrades**: Improve the technology, integrate new features and adept legal and regulative changes by voting for upgrades.
- **Decision making for a profit**: Take part in decision finding about fair pricing models for transaction fees to a) increase growth and b) make BitShares profitable for its shareholders

CHAPTER 8

Assets Tokens

User Issued Assets (UIAs)

Freely traded tokens created by individuals used for a variety of use-cases, such as stock, miles, event tickets or reputation points.

8.1 User Issued Assets (UIAs)

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. On the one hand, UIAs can be used as simple event tickets deposited on the customers 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.

All you need to do is click in order to create a new UIA is a few mouse clicks, define your preferred parameters for your coin, such as supply, precision, symbol, description and see your coin's birth after only a few seconds. From that point on, you can issue some of your coins to whomever you want, sell them and see them instantly **traded against any other existing coin** on BitShares.

Unless you want some restriction. As the issuer, you have certain privileges over your coin, for instance, you can allow trading only in certain market pairs and define who actually is allowed to hold your coin by using white- and blacklists. Of course, an issuer can opt-out of his privileges indefinitely for the sake of trust and reputation.

As the owner of that coin, you don't need to take care of all the technical details of blockchain technology, such as distributed consensus algorithms, blockchain development or integration. You don't even need to run any mining equipment or servers, at all.

So what's the drawback?

There is a drawback in this scenario, namely, a centralized issuance of new tokens. To some extend, this could be managed by a hierarchical multi-signature issuer account that prevents any single entity from issuing new coins but instead requires a consensus among an arbitrary set of people to agree on any changes to the coin.

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.

8.1.1 Use Cases

- Reward Points
- Fan Credits
- Flight Miles
- Event Tickets
- Digital Property
- Crowd-Funding
- Company Shares

8.1.2 How to create a new UIA by using GUI

- How can I create a new UIA by using GUI?

Market-Pegged Assets (MPA)

These SmartCoins track the value of an underlaying asset, such as Gold, or U.S. Dollar. Smartcoins can be created by anyone contracting with the BitShares ecosystem and putting sufficient BTS (at least 175%) into the so called contract for difference as collateral.

8.2 Market Pegged Assets (MPAs)

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

Instead of creating a UIA where the full control over supply is in the hands of the issuer, we can also create a **Market Pegged Asset** (MPA) and let the market deal with demand and supply. All we need is a *fair price* and another asset that can be used as collateral.

Why would we need *collateral* for? Since the issuer of a MPA has no control over the supply, the blockchain protocol deals with increasing and decreasing supply. In order for a user to get some of the new coins, he will need to put collateral into a **smart contract** (technically, this contract is a *contract for difference*).

> A simple example would be a MPA that is backed by USD (a stable crypto token within BitShares) that requires a collateral ratio of 200%. Then, in order to get new coin, we can borrow 100 USD worth of new coins by paying 200 USD.

By this, the supply of your coin is increased by 100. But how would it be decreased? The USD are locked in the smart contract and can only be reclaimed if the debt (here, 100 coins) are returned. Returning them will result in the coins being removed from the supply because the are no longer backed by any collateral.

So what for do we need a *fair price*? Remember that we chose a collateral ratio of 200%? That number tells us how well *backed* your coins are by the collateral. But what would happen if the value of your coin goes to the moon? Then your collateral ratio will reduce to say 150%. At a certain percentage, the blockchain will automatically trigger so called *Margin Calls* which will

1. Take your collateral (here, USD)
2. Sell it in the market to buy back the coin you owe
3. Close the contract
4. Pay your the residual USD

A *fair price* thus tells the market what your coin is worth (e.g. traded for on external exchanges) and triggers margin calls if necessary.

But there is more! Everyone that holds your (MPA) coin in BitShares can convert the coin into the backing asset at a fair price. This procedure is called "settlement" and ensures that your MPA is always worth **at least** the *fair price*.

In the User Interface, MPAs are easily distinguishable from UIAs in the asset explorer.

8.2.1 SmartCoins

BitAssets can be created and owned by anyone on the network. However, those that are owned by the BitShares Committee, are called

SmartCoins. Among these are:

- (Bit)USD
- (Bit)CNY
- (Bit)EUR
- (Bit)GOLD
- (Bit)Silver

Balances in these assets are labeled with *USD*, *CNY*, etc., because represent the same value as their underly.

8.2.2 Collateralized Tokens

A *SmartCoin* (synonym for MPA) is a crypto-currency 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 CFD.

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

8.2.3 Market Mechanics

Each BitAsset has a feed that is provided by the witnesses that indicate a fair price for that asset. This so called *Settlement Price* or *Feed Price* is used to margin call positions that borrowed BitAssets and can no longer maintain the minimum collateral ratio (i.e. maintenance collateral ratio). The collateral of these positions is used to buy back the debt from the market automatically and the position will be closed. By these rules, the network enforces the exchange participants to always maintain a collateral that is higher than the minimum requirement. Currently, the minimum required collateral ratio is **175%** and can be changed by the witnesses.

Read more about the *margin call mechanics* before trading.

Exchange Backed Assets (EBA)

This kind of asset is commonly known as I owe you (IOU). It represents the right to withdraw the same amount (minus fees) of a backing asset from a central entity. Often they are issued by a bank, an exchange or an other financial institute to represent deposit receipts.

8.3 Exchange Backed Assets (EBA)

Exchange Backed Assets represent deposit receipts that are issued by a centralized entity, such as exchanges, banks or other institutes. These can either be interpreted as *I owe you* (IOUs) or certificates for a deposit at that institute.

From the blockchain perspective, EBA are equivalent to a *User Issued Assets (UIAs)* that is created and issued by an exchange, bank or financial institute. Hence, it is their responsibility to credit you with the corresponding blockchain token (the EBA) on deposits.

8.3.1 Use Case

The most common use case would be a centralized exchange that allows their users to deposit crypto currencies in their wallets. These deposits are usually stored in their own database and the customers internal account balance is matched accordingly. These database balances serve as **deposit receipts** but obviously require some trust that the database is properly secured against any kind of attacks.

Instead of increasing an internal account balance of a user, new shares of an EBA can be issued to the user on deposits. Since EBAs are blockchain tokens, they can be traded on the decentralized exchange similar to any other exchange.

In order to reclaim his crypto tokens on their native blockchain, the users sends back the EBAs to the institute who then destroy the EBAs and transfer the corresponding asset back to its rightful owner.

Since EBAs are implemented as UIA, you can read more about the underlying technology on the *corresponding page - UIA*.

Privatized Bit-Assets

A flexible mixture between UIA and MPA that allows 3rd parties to create their own customized MPAs.

8.4 Privatized BitAssets

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. 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.

Fee Backed Assets

An FBA is a token that pays you a fraction of the transaction fees generated by a particular feature that has been funded independent of BitShares.

8.5 Fee Backed Asset

Existing core features of the BitShares protocol are Market Pegged Assets (MPA) and issuer backed User Issued Assets (UIA). In this proposal, we introduce another type of asset: *Fee Backed Assets (FBA)*.

Feed backed assets allow to propose and fund *market based* innovation by sharing a cut of future profits generated by this particular innovation with the people that helped fund it. Think of it as a *Kickstarter* for features. Hence, if people can profit from successful features in the form of fees then it can help the BitShares ecosystem to become more adaptable over time as it promotes innovation and can pay for its development.

If you have any features in mind that require new kind of transaction on the blockchain, you can code that feature and fund it with an FBA.

Feed Backed Assets have been proposed in BSIP-0007.

Prediction Market Asset

A prediction market is similar to a MPA, that trades between 0 and 1, only. After an event, a price feed can be used to determine which option to take and participants can settle at this price.

8.6 Prediction Markets

A prediction market is a specialized BitAsset such that total debt and total collateral are always equal amounts (although asset IDs differ). No margin calls or force settlements may be performed on a prediction market asset. A prediction market is globally settled by the issuer after the event being predicted resolves, thus a prediction market must always have the *global_settle* permission enabled. The maximum price for global settlement or short sale of a prediction market asset is 1-to-1.

Table of Contents

Note: In the following, we denote a *positive outcome* as a predication market that resolves to *true* (i.e. a price feed of *1*) and a *negative outcome* to resolve to *false* (i.e., a price feed of *0*)

If the bet resolves to *true* (i.e. a price feed of *1*), then the PM-asset can be settled release the collateral to the holder of the asset.

If, instead, the bet resolves to *false* (i.e. a price feed of *0*), then those that sold the PM-asset on the market and went short, made a profit since it PM-asset became worthless.

8.6.1 Creation

Prediction markets are assets that trade freely and can be borrowed from the market at a 1:1 ratio with the backing asset (which could be any other asset, including BTS, USD, GOLD).

8.6.2 Betting

A user can take either bet on a positive outcome, or a negative outcome. We here show how this works, technically.

Betting for a Positive Outcome

If you are confident that the bet will resolve positive, you want to **hold** that particular PM-asset since it allows you to settle it for it's collateral on a 1:1 basis.

In order to get hold of those tokens, you can put a buy order for them at any price (between 0 and 1) and wait for it to be filled, or buy at market rates. By this technique, a user can pre define at which odds to buy shares.

For instance, if you think that the bet resolves positively at a probability of *80%*, you can put your buy order at a price of *0.8*. If the bet resolves positively (price feed of *1*), then you can settle your shares at *1* and make a 20% profit.

If you can buy tokens at a price of *0.2* (i.e. market participants think it is unlikely to resolve positively), then you could make *80%* profits at a risk of loosing with *80%* probability.

After closing of the bet, a user can claim his profits by **settling** his borrow position and taking out the collateral:

- **Settlement in the CLI wallet**:

```
>>> settle_asset <account> <amount> <symbol> True
```

- **Borrowing in the GUI wallet**: A settlement button is available when hovering the asset in your account's overview.

Betting for a Negative Outcome

In order to bet for a negative outcome (bet resolves to *false* with a price feed of *0*), you need to **sell** the tokens. In order to get them, you should **not** buy them at the market, but instead **borrow** them from the network by paying collateral at a 1:1 ratio.

For example, in the *PM.PRESIDENT2016* if you want to bet on a negative outcome with *100k BTS*, you can borrow *100k PM.PRESIDENT2016* by paying *100k BTS* to the network.

Note: Since PM-Assets can technically be pegged by any other asset, you may need to pay USD (or anything else) instead of BTS.

Once you borrowed the token, you can sell them at any price between *0* and *1*. If you thing the probability of a negative outcome is *20%*, you should consider selling your tokens at *0.2*.

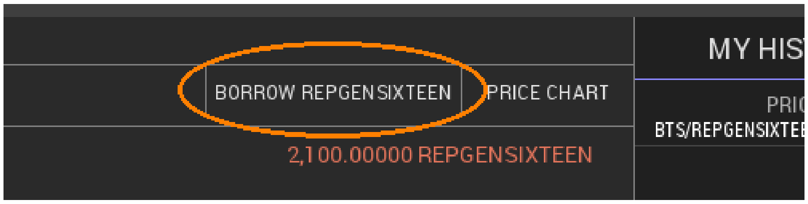
If the bet resolves negatively (price feed of *0*), your debts is worth *debt = amount * price = 0 BTS*, you can reclaim your collateral at zero cost, and get to keep *20%* profits from selling the token at *0.2*. If instead the bet resolves positively and you sold all tokens, you cannot close your borrow position to redeem your collateral. However, your total loss is reduced by *20%* for selling the tokens at the market.

If, by the end of the bet, you still have some of the tokens left, you can of course close your borrow position partly and redeem the corresponding percentage of the collateral.

- **Borrowing in the CLI wallet**:

```
>>> borrow_asset <account> <amount> <PMsymbol> <1:1-amount> true
```

- **Borrowing in the GUI wallet**: Of course, the asset can also be borrowed in the **GUI/web wallet** by using the *Borrow x* button in the market.



8.6.3 Resolving

A price feed needs to be published for the prediction market by the issuer or feed producer. It is essentially a global settlement which will set the parameters of the asset such that the holders of the asset can settle at the outcome of the bet (0, or 1). The details are shown in the guide pm-close-manual (ref: *dev.bitshares.works* material)

CHAPTER 9

Blockchain Governance

The blockchain can and needs to be governed by **elected** individuals and businesses. The so called *committee* (a set of many individuals), can change blockchain parameters such as block size, block confirmation time and others. Most importantly, though, they deal with the business plan of the blockchain and tweak costs and revenue streams (mainly transaction fees). In contrast to most existing crypto currencies, we re not hoping for a fee market to grow but instead have the committee members deal with fine-tuning of the business plan. Fortunately, the BTS Holders have the final say to approve the executive committee.

Hence, we see businesses competing for seats in the committee to define blockchain parameters.

If business ideas requires certain blockchain parameters or a particular set of fees to be profitable, there are several options:

- Argue with shareholders to approve committee members that vote in their favor
- Get elected as committee member by showing that the business is worth being available in that particular chain
- Deploy the innovative business idea as a smart contract on the blockchain and have the shareholders approve the upgrade in combination with *Fee Backed Asset* that pays future fees of the smart contract to holders of that asset (*Fee Backed Asset*)

CHAPTER 10

Community Memberships

Table of Contents

10.1 About BitShares Members

BitShares 2.0 separates responsibilities and incentives activities that are beneficial to the network, thus acknowledging different skill sets and interested community members to have incentives to contribute in the most appropriate way.

- Witnesses are paid for maintaining the back-bone of the network.
- Committee members are unpaid volunteers that organize the community and propose changes to the network.
- Marketers are paid in referral fees.
- Workers are paid for whatever they propose and do.

- BTS Holders are people holding BTS. They can cast a vote and influence the DAC's businesses

Each of the above (except Marketers) requires users to vote for the people, proposals, and/or changes. Those with sufficient approval will be compensated.

Workers are the "catch all" group where if you have an idea for something that could improve the network, you can get "paid" by the network to do it. Organizing meet-ups, developing a new tool or feature for the community, and maintaining websites and infrastructure (e.g. the mumble server team or linux distribution) are all examples of things workers may do.

10.2 BTS Holders

In contrast to most crypto-currencies, BitShares does not claim to be a currency but rather an *equity* in a decentral autonomous company (DAC). As a result, the market valuation of BitShares is free floating and may be as volatile as any other equity (e.g. of traditional companies).

Every entity hold the core token (BTS) is considered a BTS Holder of the BitShares decentralized company.

Nonetheless, BTS tokens can be used as *collateral* in financial smart contracts such as market pegged assets and thus back every existing smartcoin such as the bitUSD.

10.3 Committees

Since Bitcoin struggled to reach a consensus about the size of their blocks, the people in the cryptocurrency space realized that the governance of a DAC should not be ignored. Hence, BitShares offers a tools to reach on-chain consensus about business management decisions.

The BitShares blockchain has a set of parameters available that are subject of BTS Holder approval. BTS Holders can define their preferred set of parameters and thereby create a so called *committee member* or alternatively vote for an existing committee member. The BitShares committee consists of several *active* committee members.

The BitShares ecosystem has a set of parameters available that are subject of BTS Holder approval. Initially, BitShares has the following blockchain parameters:

- **fee structure**: *fess that have to be paid by customers for individual transactions*
- **block interval**: *i.e. block interval, max size of block/transaction*
- **expiration parameters**: *i.e. maximum expiration interval*
- **witness parameters**: *i.e. maximum amount of witnesses (block producers)*
- **committee parameters**: *i.e. maximum amount of committee members*
- **witness pay**: *payment for each witnesses per signed block*
- **worker budget**: *available budget available for budget items (e.g. development)*

Please note that the given set of parameters serves as an example and that the network's parameters are subject to change over time.

Additionally to defining the parameters any active witness can propose a protocol or business upgrade (i.e. hard fork) which can be voted on (or against) by BTS Holders. When the total votes for the hard fork are greater than the median witness weight *w* then the hard fork takes effect.

10.4 Witnesses

In BitShares, the witnesses' job is to collect transactions, bundle them into a block, sign the block and broadcast it to the network. They essentially are the block producers for the underlying consensus mechanism.

For each successfully constructed block, a witness is payed in shares that are taken from the limited reserves pool at a rate that is defined by the BTS Holders by means of approval voting.

10.5 Workers / Budget Items

Thanks to the funds stored in the reserve pool, BitShares can offer to not only pay for its own development and protocol improvement but also support and encourage growth of an ecosystem.

10.5.1 Payouts

A blockchain parameter (defined by BTS Holders through the committee) defines the daily available budget. No more than that can be paid at any time to all workers combined.

The daily budget is distributed as follows:

- The available budget is taken out of reserves pool.
- The budget items are sorted according to their approval rate (`Pro - Con`) in a descending order.
- Starting at the worker with the highest approval rate, the requested daily pay is payed until the daily budget is depleted.
- The worker with the least approval rate that was paid may receive less than the requested pay

Hence, in order to be successfully funded by the BitShares ecosystem, the BTS Holders approval for your budget item needs to be highly ranked.

Since the payments for workers from the non-liquid reserve pool result in an increased supply of BTS, these payments are vesting over a period of time defined by BTS Holders.

10.5.2 Working for BitShares

In order to be get paid by BitShares, a proposal containing

- the date of work begin,
- the date of work end,
- a daily pay (denoted in BTS),
- the worker's name, and
- an internet address.

has to be publish on the blockchain and approved by BTS Holders.

A worker can also choose on of the following properties:

- **vesting**: *pay to the worker's account*
- **refund**: *return the pay back to the reserve pool to be used for future projects*
- **burn**: *destroys the pay thus reducing share supply, equivalent to share buy-back of a company stock.*

10.5.3 Pseudo Workers

Three types of pseudo workers exist that are not primarily used to for salary.

Polling Workers

A worker proposal can be used to poll the BTS Holders for an opinion. Those workers usually have no or very small pay. Additionally, they come with a *proposal*, *recommendation* or other topic on which BTS Holders can publish a binary opinion (pro, or contra).

Refund Worker

This worker is used to set an approval limit for worker proposals and their payment by simply refunding his payment/salary to the reserve pool. If its amount of daily pay is as large as the daily available funds, and the worker has highest approval among all worker proposals, all funds will be returned to the reserves and no one will be payed. If, however, an other worker proposal has more votes than the refund worker, the proposal gets paid its salary, and the rest is return.

Burn Worker

This type of worker is similar to the *Refund Worker* above but **burns** his pay.

CHAPTER 11

Decentralized Exchange (DEX)

The decentralized exchange (further denoted simply as *the DEX*) allows for direct exchange of digital goods traded in the BitShares ecosystem.

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 in full or only partially.

- **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 BitShares, order matching is performed by the protocol, which is unaware of implications concerning the involved assets.
- **Global Unified Order Book**: Since BitShares is global, anybody with an internet access can use the DEX for trading. This brings the world's liquidity to a single order book for decentralized trading.
- **Trade Almost Anything**: The BitShares DEX is asset agnostic. Hence you can trade at **any** pair. While some pairs may end up with low liquidity, such as SILVER:GOLD, other pairs such as USD:EUR for FOREX trading will see huge volume.
- **No Limits**: The BitShares protocol is unable to limit your trading experience.
- **Decentralized**: The DEX is decentralized across the globe. This not only means that there is no single point of failure, but it also implies that the BitShares exchange is open for trading 24/7 because it's always daytime somewhere.
- **Secure**: Your funds and trades are secured with industry-grade elliptic curve cryptography. No one will be able to access your funds unless you let them. To further strengthen the security, we allow our customers to setup escrow and multi-signature schemes.
- **Fast**: In contrast to other decentralized networks, the BitShares DEX allows for real-time trading and is only limited by the speed of light and the size of the planet.
- **Provable Order Matching Algorithm**: What makes the BitShares DEX unique is the provable order matching algorithm. Given a set of orders, you will always be able to provably verify that these orders have been matched properly.
- **Collateralized Smartcoins**: One of the biggest features of BitShares are its *smartcoins* such as bitUSD, bitEUR, bitCNY, and others. For the sake of convenience, these assets are denotes simply as USD, EUR, CNY, etc. in

the wallet. These digital tokens represent the same value as their underlaying physical asset. Hence 1 USD in this wallet is worth $1 and can be redeemed as such. Any of these tokens is backed by BitShares' company shares (BTS) being locked up as collateral and being available for settlement at its current price.

11.1 Trading

This page will give a very quick introduction on how to interpret the terms used by the DEX and how trading pairs are presented.

Table of Contents

11.1.1 Pairs

In BitShares, almost any asset can be traded with all other assets. Once we have picked two assets, we usually refer to a *market pair*. For instance, we can trade USD against EUR in the USD:EUR pair.

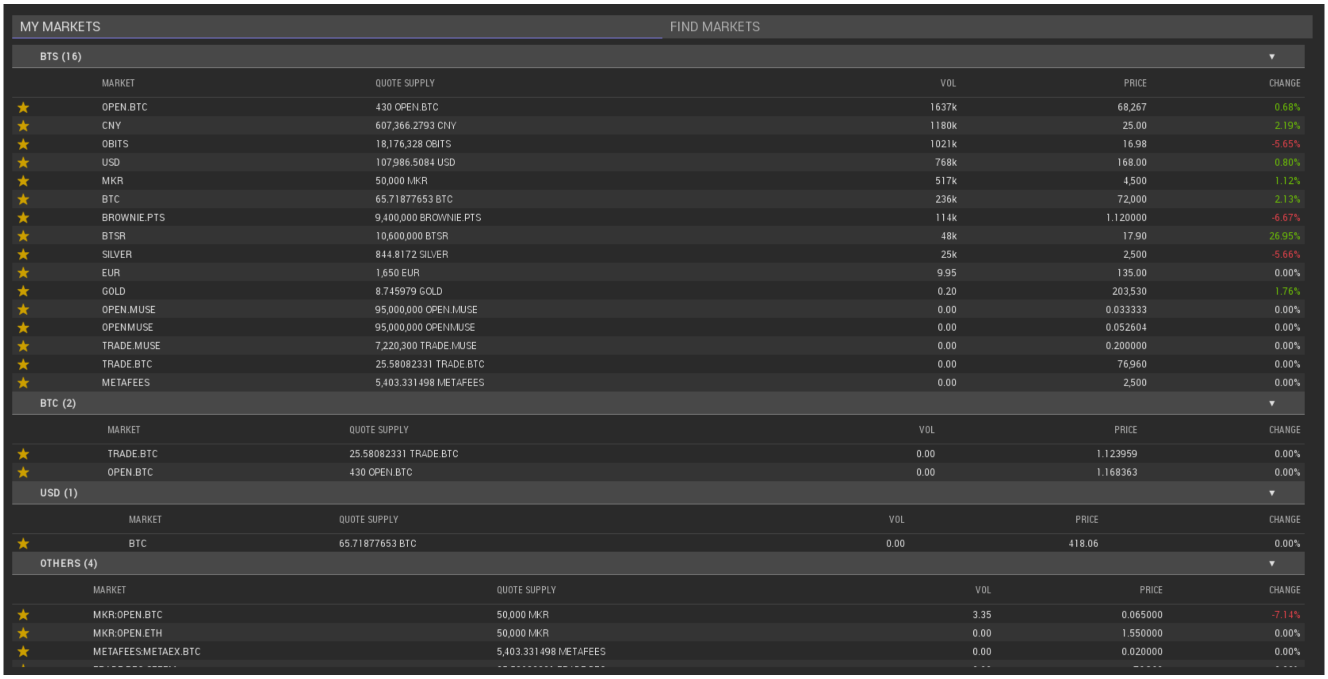
For sake of consistency, we will use the generalized terms *base* and *quote* such that pairs are represented as:

```
quote : base
```

and for instance with *base* being USD and *quote* being EUR, denote the EUR:USD pair.

11.1.2 Market Overview

The market overview that can be access via the explorer, shows a set of predefined default markets. Note that the list of default markets may vary depending on the wallet provider. Further markets can be added using the *Find Markets* tab. Adding a *Star* to your favorite markets will make it appear in your list of default markets.



BTS (16)

	MARKET	QUOTE SUPPLY	VOL	PRICE	CHANGE
★	OPEN.BTC	430 OPEN.BTC	1637k	68,267	0.68%
★	CNY	607,366.2793 CNY	1180k	25.00	2.19%
★	OBITS	18,176,328 OBITS	1021k	16.98	-5.65%
★	USD	107,986.5084 USD	768k	168.00	0.80%
★	MKR	50,000 MKR	517k	4,500	1.12%
★	BTC	65.71877653 BTC	236k	72,000	2.13%
★	BROWNIE.PTS	9,400,000 BROWNIE.PTS	114k	1.120000	-6.67%
★	BTSR	10,600,000 BTSR	48k	17.90	26.95%
★	SILVER	844.8172 SILVER	25k	2,500	-5.66%
★	EUR	1,650 EUR	9.95	135.00	0.00%
★	GOLD	8.745979 GOLD	0.20	203,530	1.76%
★	OPEN.MUSE	95,000,000 OPEN.MUSE	0.00	0.033333	0.00%
★	OPENMUSE	95,000,000 OPENMUSE	0.00	0.052604	0.00%
★	TRADE.MUSE	7,220,300 TRADE.MUSE	0.00	0.200000	0.00%
★	TRADE.BTC	25.58082331 TRADE.BTC	0.00	76,960	0.00%
★	METAFEES	5,403.331498 METAFEES	0.00	2,500	0.00%

BTC (2)

	MARKET	QUOTE SUPPLY	VOL	PRICE	CHANGE
★	TRADE.BTC	25.58082331 TRADE.BTC	0.00	1.123959	0.00%
★	OPEN.BTC	430 OPEN.BTC	0.00	1.168363	0.00%

USD (1)

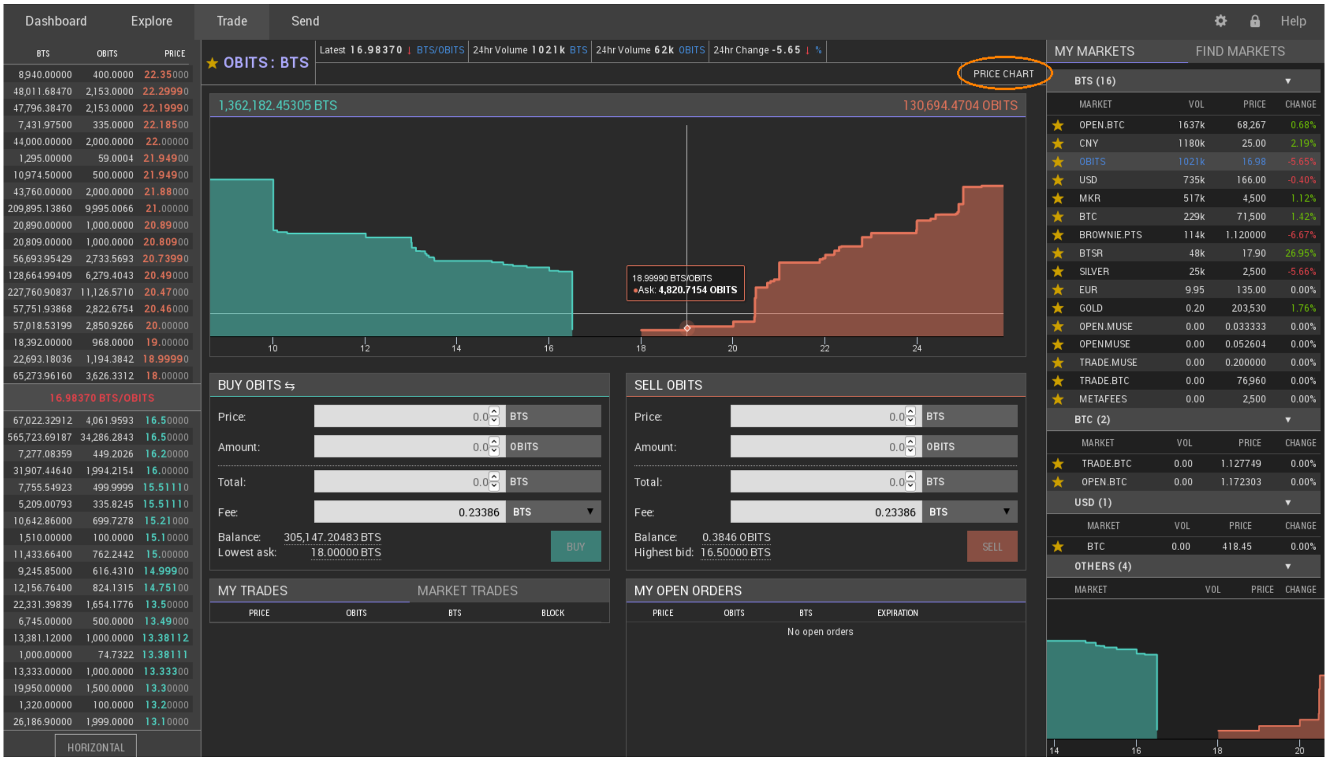
	MARKET	QUOTE SUPPLY	VOL	PRICE	CHANGE
★	BTC	65.71877653 BTC	0.00	418.06	0.00%

OTHERS (4)

	MARKET	QUOTE SUPPLY	VOL	PRICE	CHANGE
★	MKR:OPEN.BTC	50,000 MKR	3.35	0.065000	-7.14%
★	MKR:OPEN.ETH	50,000 MKR	0.00	1.550000	0.00%
★	METAFEES:METAEX.BTC	5,403.331498 METAFEES	0.00	0.020000	0.00%

11.1.3 Market

When entering a market, you will presented with either the market depth



Latest 16.98370 ↓ BTS/OBITS | 24hr Volume 1021k BTS | 24hr Volume 62k OBITS | 24hr Change -5.65 ↓ %

BTS	OBITS	PRICE
8,940.00000	400.0000	22.35000
48,011.68470	2,153.0000	22.29990
47,796.38470	2,153.0000	22.19990
7,431.97500	335.0000	22.18500
44,000.00000	2,000.0000	22.00000
1,295.00000	59.0004	21.94900
10,974.50000	500.0000	21.94900
43,760.00000	2,000.0000	21.88000
209,895.13860	9,995.0066	21.00000
20,890.00000	1,000.0000	20.89000
20,809.00000	1,000.0000	20.80900
56,693.95429	2,733.5693	20.73990
128,664.99409	6,279.4043	20.49000
227,760.90837	11,126.5710	20.47000
57,751.93868	2,822.6754	20.46000
57,018.53199	2,850.9266	20.00000
18,392.00000	968.0000	19.00000
22,693.18036	1,194.3842	18.99990
65,273.96160	3,626.3312	18.00000
16.98370 BTS/OBITS		
67,022.32912	4,061.9593	16.50000
565,723.69187	34,286.2843	16.50000
7,277.08359	449.2026	16.20000
31,907.44640	1,994.2154	16.00000
7,755.54923	499.9999	15.51110
5,209.00793	335.8245	15.51110
10,642.86000	699.7278	15.21000
1,510.00000	100.0000	15.10000
11,433.66400	762.2442	15.00000
9,245.85000	616.4310	14.99900
12,156.76400	824.1315	14.75100
22,331.39839	1,654.1776	13.50000
6,745.00000	500.0000	13.49000
13,381.12000	1,000.0000	13.38112
1,000.00000	74.7322	13.38111
13,333.00000	1,000.0000	13.33300
19,950.00000	1,500.0000	13.30000
1,320.00000	100.0000	13.20000
26,186.90000	1,999.0000	13.10000

1,362,182.45305 BTS

130,694.4704 OBITS

18.99990 BTS/OBITS
●Ask: **4,820.7154 OBITS**

BUY OBITS ⇆

Price: 0.0 BTS
Amount: 0.0 OBITS
Total: 0.0 BTS
Fee: 0.23386 BTS ▼
Balance: 305,147.20483 BTS
Lowest ask: 18.00000 BTS

SELL OBITS

Price: 0.0 BTS
Amount: 0.0 OBITS
Total: 0.0 BTS
Fee: 0.23386 BTS ▼
Balance: 0.3846 OBITS
Highest bid: 16.50000 BTS

MY TRADES | MARKET TRADES

PRICE	OBITS	BTS	BLOCK

MY OPEN ORDERS

PRICE	OBITS	BTS	EXPIRATION

No open orders

BTS (16)

	MARKET	VOL	PRICE	CHANGE
★	OPEN.BTC	1637k	68,267	0.68%
★	CNY	1180k	25.00	2.19%
★	OBITS	1021k	16.98	-5.65%
★	USD	735k	166.00	-0.40%
★	MKR	517k	4,500	1.12%
★	BTC	229k	71,500	1.42%
★	BROWNIE.PTS	114k	1.120000	-6.67%
★	BTSR	48k	17.90	26.95%
★	SILVER	25k	2,500	-5.66%
★	EUR	9.95	135.00	0.00%
★	GOLD	0.20	203,530	1.76%
★	OPEN.MUSE	0.00	0.033333	0.00%
★	OPENMUSE	0.00	0.052604	0.00%
★	TRADE.MUSE	0.00	0.200000	0.00%
★	TRADE.BTC	0.00	76,960	0.00%
★	METAFEES	0.00	2,500	0.00%

BTC (2)

	MARKET	VOL	PRICE	CHANGE
★	TRADE.BTC	0.00	1.127749	0.00%
★	OPEN.BTC	0.00	1.172303	0.00%

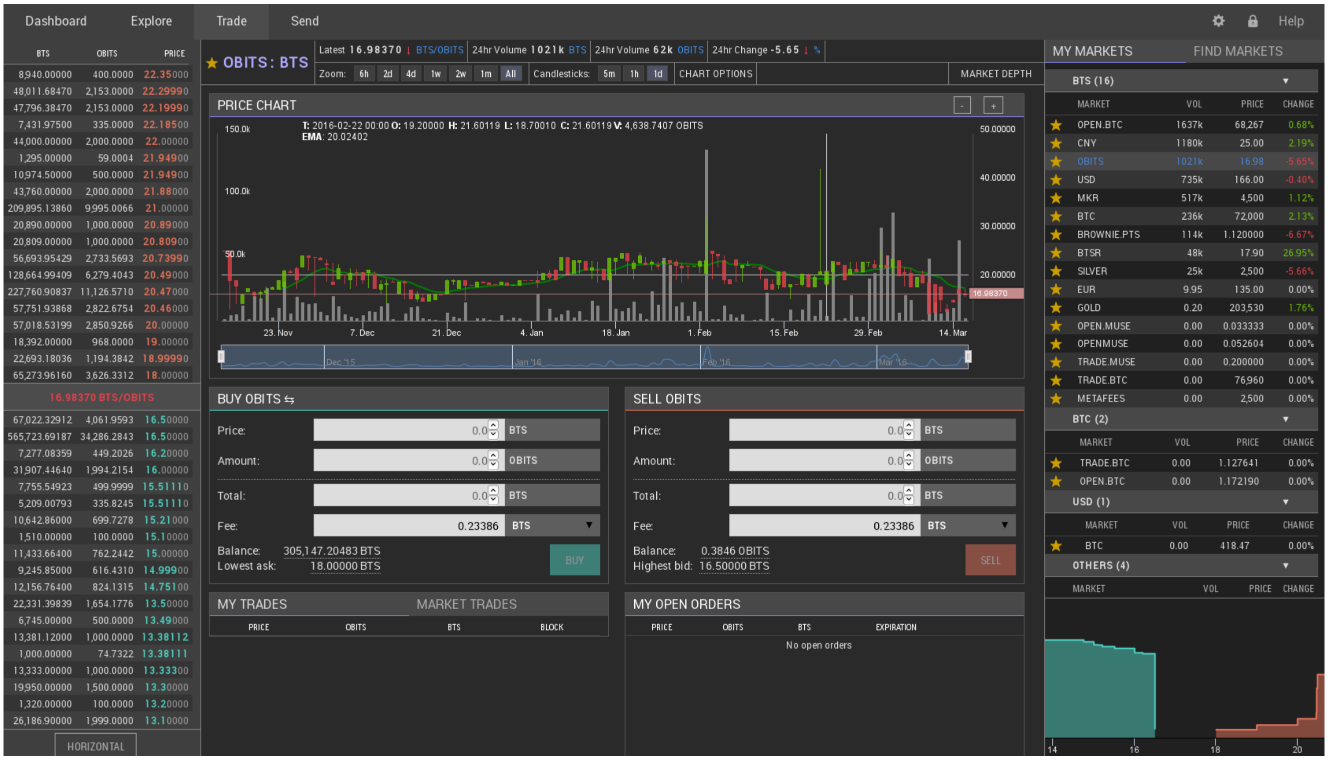
USD (1)

	MARKET	VOL	PRICE	CHANGE
★	BTC	0.00	418.45	0.00%

OTHERS (4)

MARKET	VOL	PRICE	CHANGE

. . . or the price chart depending on your settings.



Latest 16.98370 ↓ BTS/OBITS | 24hr Volume 1021k BTS | 24hr Volume 62k OBITS | 24hr Change -5.65 ↓ %

T: 2016-02-22 00:00 O: 19.20000 H: 21.60119 L: 18.70010 C: 21.60119 V: 4,638.7407 OBITS
EMA: 20.02402

BTS	OBITS	PRICE
8,940.00000	400.0000	22.35000
48,011.68470	2,153.0000	22.29990
47,796.38470	2,153.0000	22.19990
7,431.97500	335.0000	22.18500
44,000.00000	2,000.0000	22.00000
1,295.00000	59.0004	21.94900
10,974.50000	500.0000	21.94900
43,760.00000	2,000.0000	21.88000
209,895.13860	9,995.0066	21.00000
20,890.00000	1,000.0000	20.89000
20,809.00000	1,000.0000	20.80900
56,693.95429	2,733.5693	20.73990
128,664.99409	6,279.4043	20.49000
227,760.90837	11,126.5710	20.47000
57,751.93868	2,822.6754	20.46000
57,018.53199	2,850.9266	20.00000
18,392.00000	968.0000	19.00000
22,693.18036	1,194.3842	18.99990
65,273.96160	3,626.3312	18.00000
16.98370 BTS/OBITS		
67,022.32912	4,061.9593	16.50000
565,723.69187	34,286.2843	16.50000
7,277.08359	449.2026	16.20000
31,907.44640	1,994.2154	16.00000
7,755.54923	499.9999	15.51110
5,209.00793	335.8245	15.51110
10,642.86000	699.7278	15.21000
1,510.00000	100.0000	15.10000
11,433.66400	762.2442	15.00000
9,245.85000	616.4310	14.99900
12,156.76400	824.1315	14.75100
22,331.39839	1,654.1776	13.50000
6,745.00000	500.0000	13.49000
13,381.12000	1,000.0000	13.38112
1,000.00000	74.7322	13.38111
13,333.00000	1,000.0000	13.33300
19,950.00000	1,500.0000	13.30000
1,320.00000	100.0000	13.20000
26,186.90000	1,999.0000	13.10000

BUY OBITS ⇆

Price: 0.0 BTS
Amount: 0.0 OBITS
Total: 0.0 BTS
Fee: 0.23386 BTS ▼
Balance: 305,147.20483 BTS
Lowest ask: 18.00000 BTS

SELL OBITS

Price: 0.0 BTS
Amount: 0.0 OBITS
Total: 0.0 BTS
Fee: 0.23386 BTS ▼
Balance: 0.3846 OBITS
Highest bid: 16.50000 BTS

PRICE	OBITS	BTS	BLOCK

PRICE	OBITS	BTS	EXPIRATION
No open orders			

BTS (16) ▼

	MARKET	VOL	PRICE	CHANGE
★	OPEN.BTC	1637k	68,267	0.68%
★	CNY	1180k	25.00	2.19%
★	OBITS	1021k	16.98	-5.65%
★	USD	735k	166.00	-0.40%
★	MKR	517k	4,500	1.12%
★	BTC	236k	72,000	2.13%
★	BROWNIE.PTS	114k	1.120000	-6.67%
★	BTSR	48k	17.90	26.95%
★	SILVER	25k	2,500	-5.66%
★	EUR	9.95	135.00	0.00%
★	GOLD	0.20	203,530	1.76%
★	OPEN.MUSE	0.00	0.033333	0.00%
★	OPENMUSE	0.00	0.052604	0.00%
★	TRADE.MUSE	0.00	0.200000	0.00%
★	TRADE.BTC	0.00	76,960	0.00%
★	METAFEES	0.00	2,500	0.00%

BTC (2) ▼

	MARKET	VOL	PRICE	CHANGE
★	TRADE.BTC	0.00	1.127641	0.00%
★	OPEN.BTC	0.00	1.172190	0.00%

USD (1) ▼

	MARKET	VOL	PRICE	CHANGE
★	BTC	0.00	418.47	0.00%

OTHERS (4) ▼

MARKET	VOL	PRICE	CHANGE

You can switch between your views by pressing the corresponding button as highlighted below.

11.1.4 Order Books

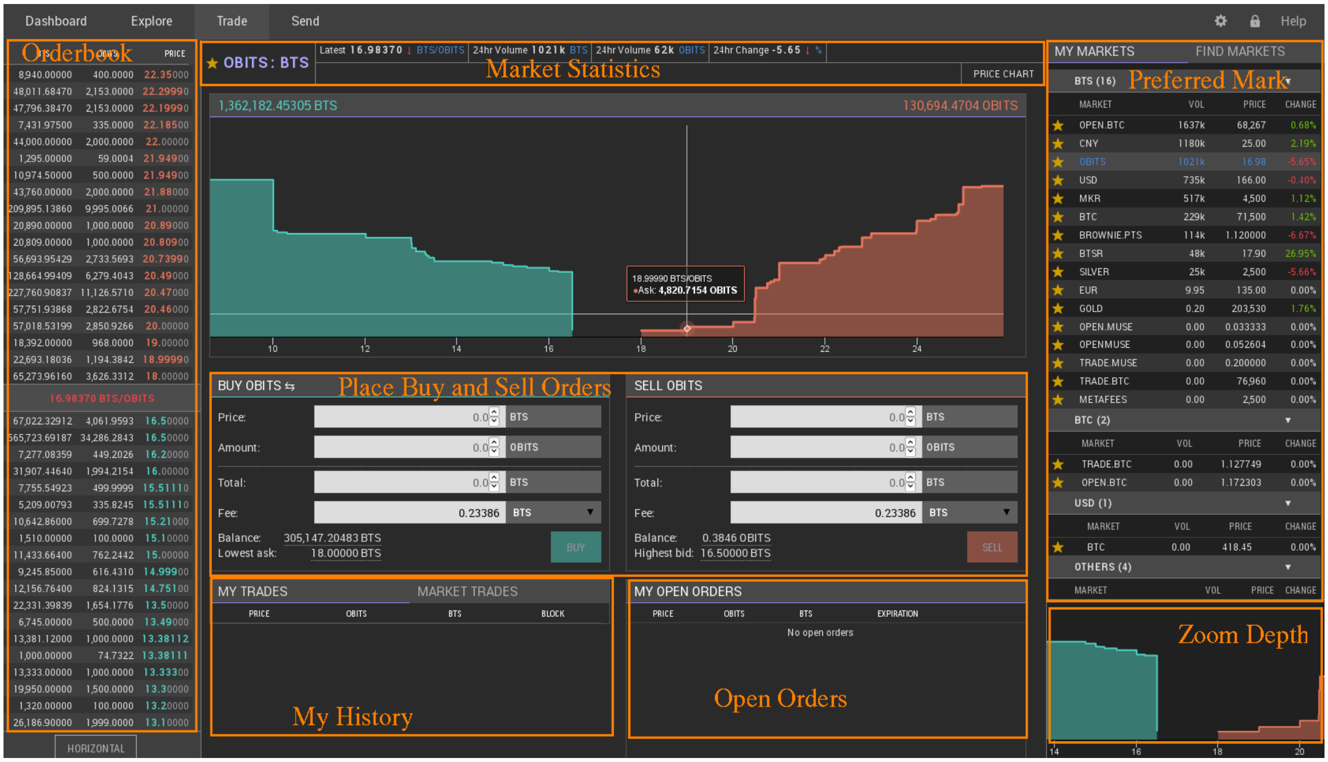
The order book consists of an *ask* and a *bid* side. Since trading pairs do not have a preferred orientation, and can be flipped, the following table shall give an overview of ask/bid and the corresponding buy/sell operations for each side:

Side	Sell	Buy
Ask	*quote*	*base*
Bid	*base*	*quote*

Obviously, what is on the bid side of the USD:EUR pair will be on the ask side on the EUR:USD pair. Of course prices are internally represented as fractions, and thus results in both pairs being identical.

11.1.5 Trading

To place a trading order, it is required to fill the form on either the *ask* or the *bid* side (respectively, *buy* or *sell* side). You will need to define a *price* and an *amount* to sell/buy. The cost for this order will be calculated automatically. Note that there will be an additional fee required to actually place the order.



BTS	OBITS	PRICE
8,940.00000	400.0000	22.35000
48,011.68470	2,153.0000	22.29990
47,796.38470	2,153.0000	22.19990
7,431.97500	335.0000	22.18500
44,000.00000	2,000.0000	22.00000
1,295.00000	59.0004	21.94900
10,974.50000	500.0000	21.94900
43,760.00000	2,000.0000	21.88000
209,895.13860	9,995.0066	21.00000
20,890.00000	1,000.0000	20.89000
20,809.00000	1,000.0000	20.80900
56,693.95429	2,733.5693	20.73990
128,664.99409	6,279.4043	20.49000
227,760.90837	11,126.5710	20.47000
57,751.93868	2,822.6754	20.46000
57,018.53199	2,850.9266	20.00000
18,392.00000	968.0000	19.00000
22,693.18036	1,194.3842	18.99990
65,273.96160	3,626.3312	18.00000
16.98370 BTS/OBITS		
67,022.32912	4,061.9593	16.50000
565,723.69187	34,286.2843	16.50000
7,277.08359	449.2026	16.20000
31,907.44640	1,994.2154	16.00000
7,755.54923	499.9999	15.51110
5,209.00793	335.8245	15.51110
10,642.86000	699.7278	15.21000
1,510.00000	100.0000	15.10000
11,433.66400	762.2442	15.00000
9,245.85000	616.4310	14.99900
12,156.76400	824.1315	14.75100
22,331.39839	1,654.1776	13.50000
6,745.00000	500.0000	13.49000
13,381.12000	1,000.0000	13.38112
1,000.00000	74.7322	13.38111
13,333.00000	1,000.0000	13.33300
19,950.00000	1,500.0000	13.30000
1,320.00000	100.0000	13.20000
26,186.90000	1,999.0000	13.10000

★ OBITS : BTS

Latest 16.98370 ↓ BTS/OBITS | 24hr Volume 1021k BTS | 24hr Volume 62k OBITS | 24hr Change -5.65 ↓ %

1,362,182.45305 BTS

130,694.4704 OBITS

18.99990 BTS/OBITS
●Ask: 4,820.7154 OBITS

BUY OBITS ⇆

Price: 0.0 BTS
Amount: 0.0 OBITS
Total: 0.0 BTS
Fee: 0.23386 BTS ▼
Balance: 305,147.20483 BTS
Lowest ask: 18.00000 BTS

SELL OBITS

Price: 0.0 BTS
Amount: 0.0 OBITS
Total: 0.0 BTS
Fee: 0.23386 BTS ▼
Balance: 0.3846 OBITS
Highest bid: 16.50000 BTS

MY TRADES | MARKET TRADES

PRICE	OBITS	BTS	BLOCK

MY OPEN ORDERS

PRICE	OBITS	BTS	EXPIRATION
No open orders			

BTS (16) ▼

	MARKET	VOL	PRICE	CHANGE
★	OPEN.BTC	1637k	68,267	0.68%
★	CNY	1180k	25.00	2.19%
★	OBITS	1021k	16.98	-5.65%
★	USD	735k	166.00	-0.40%
★	MKR	517k	4,500	1.12%
★	BTC	229k	71,500	1.42%
★	BROWNIE.PTS	114k	1.120000	-6.67%
★	BTSR	48k	17.90	26.95%
★	SILVER	25k	2,500	-5.66%
★	EUR	9.95	135.00	0.00%
★	GOLD	0.20	203,530	1.76%
★	OPEN.MUSE	0.00	0.033333	0.00%
★	OPENMUSE	0.00	0.052604	0.00%
★	TRADE.MUSE	0.00	0.200000	0.00%
★	TRADE.BTC	0.00	76,960	0.00%
★	METAFEES	0.00	2,500	0.00%

BTC (2) ▼

	MARKET	VOL	PRICE	CHANGE
★	TRADE.BTC	0.00	1.127749	0.00%
★	OPEN.BTC	0.00	1.172303	0.00%

USD (1) ▼

	MARKET	VOL	PRICE	CHANGE
★	BTC	0.00	418.45	0.00%

OTHERS (4) ▼

MARKET	VOL	PRICE	CHANGE

Once the order is filled (i.e. someone sold/bought your offer), your account will be credited by the corresponding asset.

Unfilled orders can be canceled at any time.

11.1.6 Order Matching

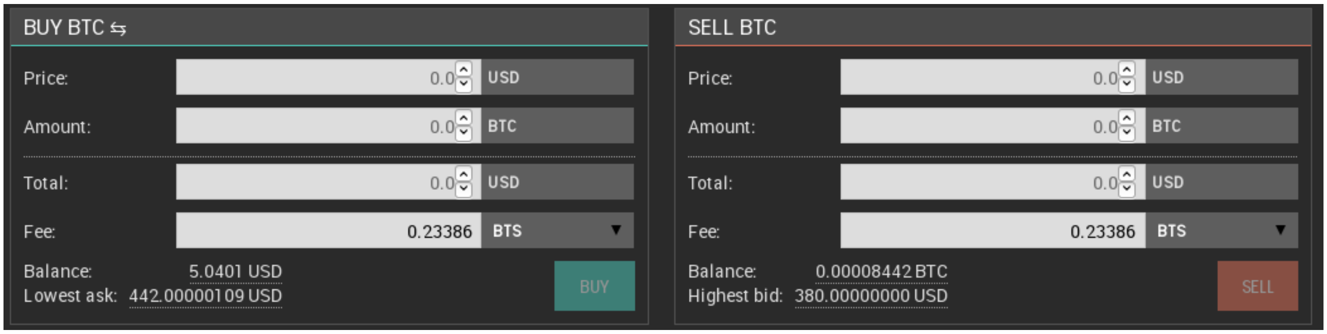
BitShares 2.0 matches orders on a first-come, first-serve basis and gives the buyer the best price possible up to the limit (also known as “walking the book”). Rather than charging *unpredictable fees* from market overlap (as has been in the previous network), the network charges a defined fee based upon the size of the order matched and the assets involved. Each asset issuer gets an opportunity to configure their fees.

The decentralized exchange (DEX) of BitShares has a similar look&feel as traditional centralized exchanges. However, trading in the DEX can have many different appearances, depending on what user-interface is used. We here describe the user interface of the official wallet.

11.1.7 Playing Orders

Orders can be placed in the same way as everywhere else, by providing

- the amount to buy/sell
- the price at which to buy/sell



Price: 0.0 USD
Amount: 0.0 BTC
Total: 0.0 USD
Fee: 0.23386 BTS
Balance: 5.0401 USD
Lowest ask: 442.00000109 USD

Price: 0.0 USD
Amount: 0.0 BTC
Total: 0.0 USD
Fee: 0.23386 BTS
Balance: 0.00008442 BTC
Highest bid: 380.00000000 USD

11.1.8 Fees

In contrast to other exchanges, BitShares asks for a tiny **flat fee** for placing an order. This fee can be payed in USD, BTC, or GOLD and is independent of the actual assets that are traded.

If you cancel an order that has not been fully or partially filled, 90% of the fee will be payed back to your account. However, this chargeback will be in `BTS` and not in the asset you have originally paid the fee in.

11.2 Short Selling BitAssets

In order to increase your exposure to BTS and offer liquidity to BitAssets, such as USD, EUR, GOLD, etc., you can go *borrow* this bitAsset from the network and *sell it short*. We will here briefly describe the procedure.

Table of Contents

11.2.1 Borrowing

The BitShares network is capable of issuing any amount of any BitAsset and lend it out to participants given enough collateral.

- **settlement price**: The price for 1 BTS as it is traded on external exchanges.
- **maintenance collateral ratio** (MCR): A ratio defined by the witnesses as minimum required collateral ratio
- **maximum short squeeze ratio** (MSQR): A ratio defined by the witnesses as to how far shorts are protected against short squeezes
- **short squeeze protection** (SQP): Defines the most that a margin position will ever be forced to pay to cover
- **call price** (CP): The price at which short/borrow positions are margin called

11.2.2 Margin Call

The BitShares network is capable of margin calling those positions that do not have enough collateral to back their borrowed bitAssets. A margin call will occur any time the highest bid is less than the *call price* and greater than *SQP*. The margin position will be forced to sell its collateral anytime the highest offer to buy the collateral is less than the call price (x/BTS).:

```
SQP        = settlement price / MSQR
call price = DEBT / COLLATERAL * MCR
```

The margin call will take the collateral, buy shares of borrowed bitAsset at market rates up to the SQP and close the position. The remaining BTS of the collateral are returned to the customer.

Read more about the margin call mechanics before trading.

11.2.3 Settlement

Holders of any bitAsset can request a settlement at a *fair price* at any time. The settlement closes the borrow/short positions with lowest collateral ratio and sells the collateral for the settlement.

Note, that there is a maximum daily settlement volume (currently 2%) defined by the committee to prevent exploitation via external price movements.

11.2.4 Selling

After burrowing bitAssets, they can be sold free at any of the corresponding markets at any price a buyer is willing to pay. With this step, the short-selling is now complete and you are short that particular bitAsset.

11.2.5 Updating Collateral Ratio

At any time, the holder of a borrow/short position can modify the collateral ratio in order to flexibly adjust to market behavior. If the collateral ratio is increase, an additional amount of BTS is locked as collateral, while reducing the collateral ratio will require an amount of the corresponding BitAsset to be payed back to the network.

11.2.6 Covering

To close a borrow/short position, one must hold the borrowed amount of that particular bitAsset to hand it over to the BitShares network. After that, the BitAssets are reduced from the corresponding supply and the collateral is released and given back to its owner.

11.2.7 Discussion

Shorts can pick their place in line for settlement. Think of it this way, if you fall in the bottom 2% of shorters by collateral you have been given notice of potential margin call since only 2% can be settled, daily. This is like any other market where they give you 24 hours to add collateral. If someone is short and doesn't want to meet the new higher collateral limits then they can either cover on their own terms or add collateral.

By giving 24 hours shorts have an opportunity to cover prior to any price manipulation by big players.

If there is a 10% premium on BitUSD relative to the feed, then the attacker would have to increase reported price feed (value of BTS) by 10% just to get the force-settlement price to equal the previously fair value for BitUSD. They would have to push beyond 10% before the short starts taking a loss relative to a voluntary cover. All savvy market participants would be aware of a large force-settle order and would therefore reset the manipulator making it much harder to manipulate the price. In effect, price manipulation represents "free money" to those who know it is going on.

Look at it another way, someone enters a large force-settlement order it becomes an opportunity for the shorter to do reverse manipulation. It is a tug of war where both sides (short and long) have equal opportunity to manipulate the market in their favor. They go to battle and the result is just the fair market price at that point in time. It is not a guaranteed win for the potential manipulator.

11.3 Margin call mechanics

The mechanics of a margin call in Bitshares are currently poorly understood, so I'd like to try to clarify a little by using examples from the `USD:BTS` market. I think part of the current confusion lies in people talking about the same market but using different market directions, ie. `USD:BTS` or `BTS:USD`, so terms like above/below don't mean the same thing to different people. I will only use USD in these examples, but USD can be replaced by any bit asset in this context. I prefer to use the `USD:BTS` market direction, so these examples will have prices in BTS/USD.

Table of Contents

11.3.1 What is a margin call?

A margin call is the market forcing you to sell your collateral in order to buy enough USD to close your position. In the USD:BTS market a margin call is equivalent to a bid: it is an order to buy USD for BTS.

A margin call will happen because the price has increased to the point where your collateral is insufficient with respect to the current collateral requirements of the Bitshares market rules. The required collateral is a tuneable parameter in Bitshares, set by the maintenance collateral ratio (MCR) which is maintained by the feed producers (i.e., the witnesses).

11.3.2 How is the call price calculated?

As mentioned above the call price of a margin position depends on the MCR and the amount of debt and collateral in your position. It is independent of the price feed (settlement price). As an example, say you have opened the following position:

- Debt: `10 USD`
- Collateral: `10000 BTS`
- MCR is `1.75`

The call price of your position is `10000 BTS / (10 * 1.75 USD) = 571.429 BTS/USD`.

11.3.3 How is the collateral ratio (CR) calculated?

The collateral ratio depends on the feed price (settlement price). Taking a feed price of `300 BTS/USD` and building on the above example with `10 USD` debt and `10000 BTS` collateral:

- CR: `(10000 BTS / 300 BTS/USD) / 10 USD = 3.33`

11.3.4 Execution Conditions

When will a margin call happen?

This is where it gets complicated. Margin Call are only possible if the feed price is below your call price. A margin call will happen whenever the squeeze protection price goes above the call price of your position. To better understand how this works, let's go back to our margin position and look at collateral ratios:

Say we have the following:

- Debt: `10 USD`
- Settlement price: `300 BTS/USD`
- CR: `1`

- Collateral is therefore `3000 BTS`

This is also known as the Black Swan level, and we want to perform a margin call before the collateral ratio goes this low. This is why we have the Maintenance Collateral Ratio (MCR), to enforce a buffer zone before a position goes into Black Swan territory. So if we apply the MCR of `1.75` to this position:

- Debt: `10 USD`
- Settlement Price: `300 BTS/USD`
- CR: `1.75`
- Collateral is therefore `3000 BTS * 1.75 = 5250 BTS`

This is much safer, there is a bit of margin for the position to be closed before going into Black Swan levels. Since in our example, the USD **requires** `1.75` ratio, the call price of this position is now exactly equal to the feed price of `300 BTS/USD`.

- Call price: `5250 / (10 * 1.75) = 300 BTS/USD`

The remaining question then is, at what point should we force the position to attempt to close itself? This is where the SQPR comes in. Let's look at two scenarios, SQPR of `1.1` and SQPR of `1.5`:

** SQPR of `1.1` **

- Settlement price: `300 BTS/USD`
- SQPR: `1.1`
- Squeeze Protection Price (SQPP): `330 BTS/USD`

In this case, any margin position that has a call price below `330 BTS/USD` will be forced to settle, and therefore be added to the orderbook as an order to buy USD for BTS.

** SQPR of `1.5` **

- Settlement price: `300 BTS/USD`
- SQPR: `1.5`
- Squeeze Protection Price (SQPP): `450 BTS/USD`

In this case, any margin position that has a call price below `450 BTS/USD` will be forced to settle, and therefore be added to the orderbook as an order to buy USD for BTS.

Discussion

Another way of looking at this is by looking at the Collateral Ratio of the position. If we want to stay at or above the squeeze protection price, what is the required collateral ratio? Let's do the math:

- Settlement Price: `300 BTS/USD`
- MCR: `1.75`
- SQPR: `1.1`
- Debt: `10 USD`
- Call price: `CP = SQPP = 300 * 1.1 = 330 BTS/USD`
- Collateral = `(10 USD * 1.75) * 330 BTS/USD = 5775 BTS`

The collateral ratio of this position is `(5775 BTS / 300 BTS/USD) / 10 USD = 1.925`.

This is equivalent to the MCR

- SQPR: `1.75 * 1.1 = 1.925`.

In other words, in order to stay **safe** and not be margin called, the margin position must maintain a collateral ratio higher than `MCR * SQPR`.

- **Safe position**: `CR > MCR * SQPR`

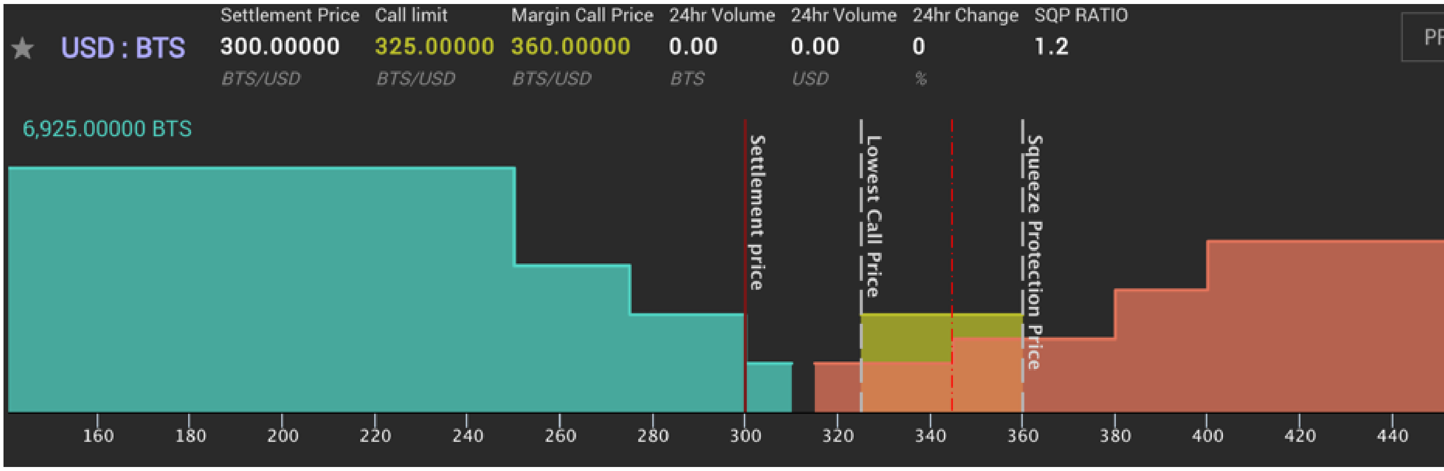
At what price will the margin call execute?

This is the part I believe is most misunderstood, so I will use some screenshots of a fictional `USD:BTS` market to explain. We will use the following parameters:

- SQPR: `1.2`
- MCR: `1.75`
- SQPR * MCR: `2.1`
- Settlement price: `300 BTS/USD`
- Squeeze protection price: `300 * 1.2 = 360 BTS/USD`
- Debt: `10 USD`
- Collateral: `5687.5`
- CR: `1.896`
- Call price: `325 BTS/USD`

From what we've seen above, it's clear that this position should be margin called: it has a CR of `1.896` which is well below the safe ratio of 2.1.

It will therefore get added to the order book as a bid to buy USD like this:



	Settlement Price	Call limit	Margin Call Price	24hr Volume	24hr Volume	24hr Change	SQP RATIO
★ USD : BTS	300.00000	325.00000	360.00000	0.00	0.00	0	1.2
	BTS/USD	BTS/USD	BTS/USD	BTS	USD	%	

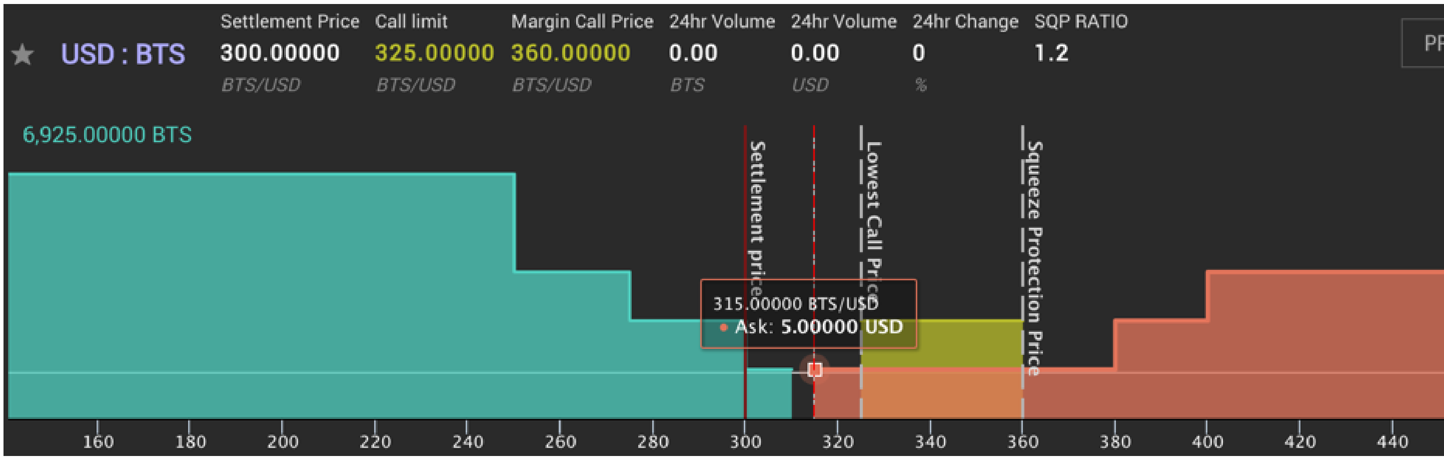
The margin called order will buy any USD priced in the range `325-360 BTS/USD`. The squeeze protection price acts as a price ceiling, meaning the forced margin order will not execute at a very high price in an illiquid market: it is protected from high prices by the SQPR.

11.3.5 Margin calls only execute in the range [Call Price - SQPP]

A margin call will occur any time the lowest ask is higher than the call price and lower than the SQPP. This has several consequences, as we will see below. It can create some very strange situations, and also force the margin called orders to "buy high".

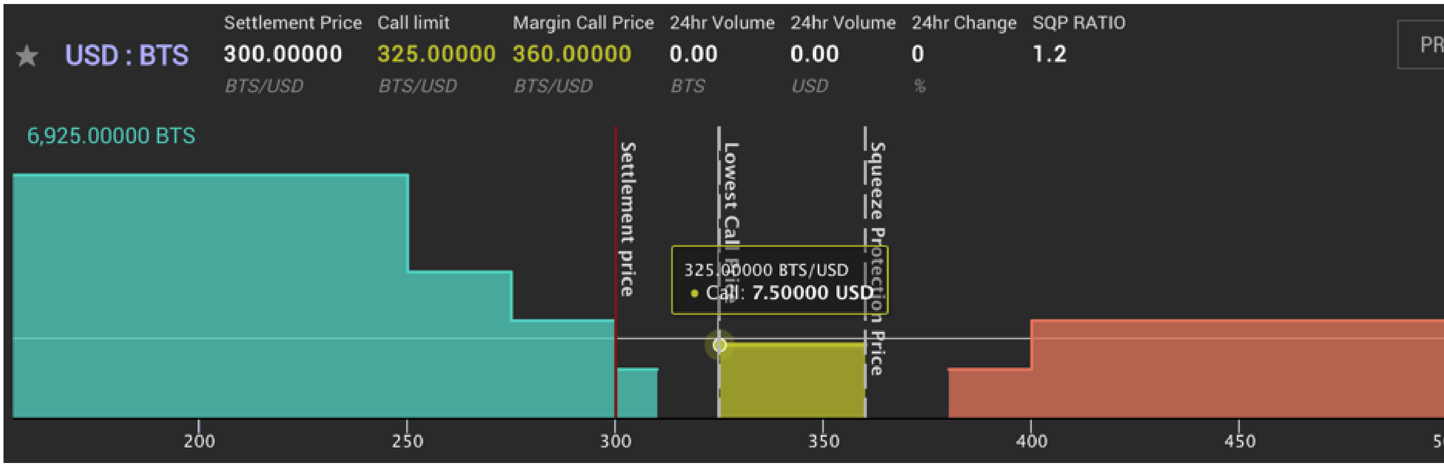
Consequence #1: Asks below the call price prevent margin calls from executing

Because margin calls only execute in the range Call Price - SQPP, if there is a sell order for `5 USD` at `315 BTS/USD` in this market, the call order will not use it, which makes the market look like this:



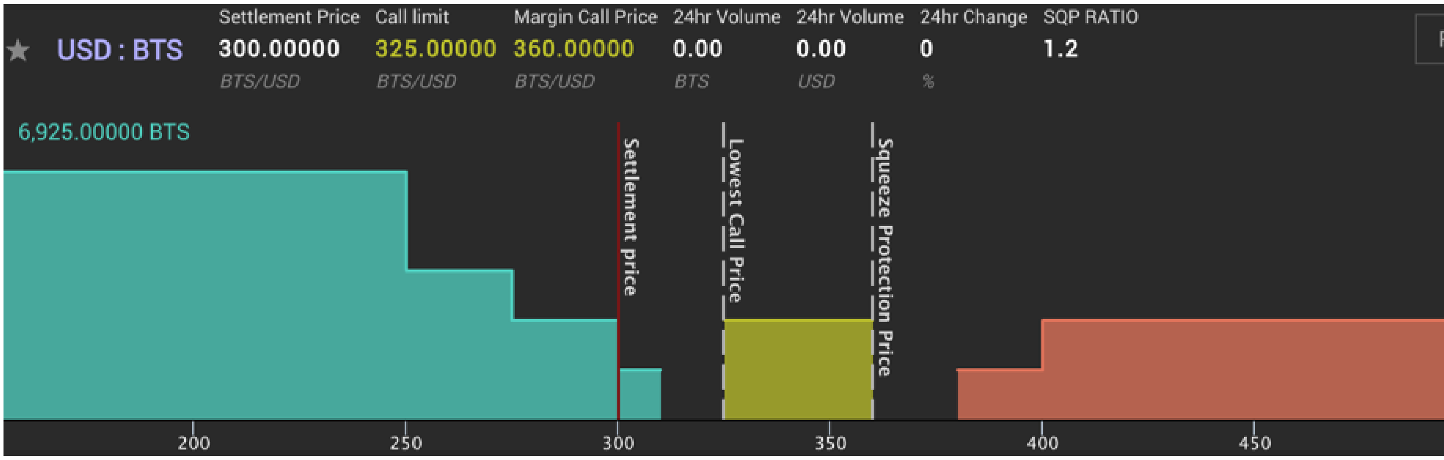
	Settlement Price	Call limit	Margin Call Price	24hr Volume	24hr Volume	24hr Change	SQP RATIO
★ USD : BTS	300.00000	325.00000	360.00000	0.00	0.00	0	1.2
	BTS/USD	BTS/USD	BTS/USD	BTS	USD	%	

If a second sell order of `2.5 USD` were added at `345 BTS/USD`, the margin called order would still not buy any USD because of the "blocking" sell order at `315 BTS/USD`:



	Settlement Price	Call limit	Margin Call Price	24hr Volume	24hr Volume	24hr Change	SQP RATIO
★ USD : BTS	300.00000	325.00000	360.00000	0.00	0.00	0	1.2
	BTS/USD	BTS/USD	BTS/USD	BTS	USD	%	

If the order at `315 BTS/USD` were to be removed, either from being canceled or from being filled, the order at `345 BTS/USD` would instantly get filled by the margin called order, and the margin called position would have a reduced debt of `10 - 2.5 = 7.5 USD`:



Consequence #2: Margin calls cannot "buy cheap" As we've seen above, unless the settlement price goes above the call price of the position, forced margin calls always buy at a premium relative to the settlement price. Even if there are sell orders available at or near the feed price, the margin called orders will not be matched with those sell orders if their call price is higher than the price of those sell orders.

CHAPTER 12

Investor Guide

Note: This guide is still under construction. Please excuse if what you are searching for is not yet available.

The investor guide serves as an entry point for existing and potential investors in the BitShares ecosystem. We here merely discuss the BTS token as well as investment opportunities available within BitShares itself and deliberately do not advertise 3rd party businesses. Please be reminded that this is an information platform and thus we do not give investment advice.

12.1 Claim your Investment

You are considered as a AngelShare holder if you have donated BTC or BTS to one of these addresses:

- **BTC**: `1ANGELwQwWxMmbdaSWhWLqBEtPTkWb8uDc`
- **PTS**: `PaNGELmZgzRQCKeEKM6ifgTqNkC4ceiAWw`

There is also an AngelShare Explorer specifically for these donations

AngelShares have been gifted 50% of the initial BTS shares. The other 50% went to AngelShares, the other went to holders of PTS.

12.1.1 Claiming your Stake

In order to claim your BTS, you need to look in your bitcoin wallet and search for transactions the the above mentioned address. The keys that correspond to the inputs of that transaction are what you need to obtain your BTS (FAQ).

If you have located the private keys (in wallet import format - WIF), you can safely import them into your BitShares account using the *Import Keys* tools in the Wallet Management Console of your BitShares wallet.

CHAPTER 13

Migrating from BitShares 1.0 to BitShares 2.0

This migration tutorial is relevant only to those customers and investors that have participated in BitShares 1.0. We show improvements, new features and give assistance for claiming your funds in BitShares 2.0.

Table of Contents

13.1 What is new in BitShares 2.0

Links take to (https://bitshares.org/) information pages.

- **Votable Network Parameters**: BitShares 2.0 will allow its BTS Holders to fine-tune any parameter available to the protocol. This includes, block size, block interval, but also the payment for block producers and transaction fees.
- **Flexible and Dynamic Access Control**: BitShares 2.0 allows customers and participants a flexible and dynamic access to its funds or account handle. A so called *Authority* can consist of a flat hierarchy similar to *multi-signature* in Bitcoin, but could also support tree hierarchies never to be seen before. Read more about this about dynamic account permissions.
- **Transferable Account Names**: Since Control over Funds is separated from the control over an account, we can have transferable account names that are registered on the blockchain. Named accounts allows for much easier transfers because no cryptic strings needs to be handed out. Read more about transferable named accounts.
- **On-Chain Proposed Transactions**: In traditional crypto currencies, a multi-signature transaction has to be transfered to its corresponding signers on separated communication channels (off-chain). BitShares 2.0 allows

to propose transactions on the chain and have the signers be notified for their required signature automatically. No more manual communications are required.

- **New Full-Node/Client Concept**: We recognize the hassles some people had when synchronizing the BitShares 1.0 blockchain with the heavy-weighted BitShares full client. In order to offer more comfort and a faster trading experience, we decided to separated the user-interface from the block syncing core component that connects to the peer-to-peer network. Of course, both are open source and a full node can run easily, we understand that some users mainly prefer to use the frontend not bothering about the blockchain.
- **Referral Program**: PayPal and Dwolla showed the success of referral programs, a program that could easily and cheaper be implemented in a decentralized software protocol. Hence we took our chance and implemented a blockchain based referral program. From every transaction fee, paid by a customer you referred, you will get a fraction. Of course, this fraction can be tuned by BTS Holders! Read more about the referral program.
- **Recurring & Scheduled Payments**: We wanted to offer a way to have our rent payed automatically. So we implemented it in the blockchain. In BitShares 2.0, participants are capable of allowing others to withdraw funds from your account. Of course, you can define a daily/weekly or monthly limit. Read more about recurring and scheduled payments.
- **Additional Privatized BitAssets**: In contrast to Market Pegged Assets (also known as BitAssets) that have a price feed published by witnesses that have approval of BTS Holders, a *privatized* bitasset allows to create market pegged assets that have an individual set of price feed publishers that do not need BTS Holders' approval. Hence, everyone can create a privatized bitAsset to track an individual value, such as indices, or binary predictions.

13.2 What has changed since BitShares 0.9

- **BitAssets are Contracts-For-Difference**: Our research has identified an improved mechanism to achieve a solid *peg* of bitAssets to its underlay. BitAssets like the bitUSD in BitShares 2.0 will always trade for *at least* the value of its underlying asset, i.e. $1. We have summarized the economical analysis and incentives for market participants here: bitAssets 2.0
- **Faster Blocks**: Initially, the BitShares 2.0 blockchain will come with 3 seconds block interval with the option to reduce down to 1 second if BTS Holders agree.
- **Industrial Performance**: BitShares 2.0 can support massive load and works well beyond 100k transactions per second. Find out how we achieve industrial performance and scalability.
- **New Reactive UI**: The BitShares 1.0 user interface was powerful but lacking in responsiveness and performance. For Bitshares 2.0 we've reimplemented the whole wallet using the React.js framework developed by Facebook, which is well-known for having excellent performance. The new BitShares UI is an entirely browser-based wallet, with private keys maintained in the browser. We expect a flourishing ecosystem of forked and tweaked wallets based off of our UI.
- **Accounts must be registered**: In BitShares 2.0 we have separated *authorities* from transaction partners. Hence, if Alice wants to send funds to Bob, it may be required that only Celine signs for that transaction. Also, BitShares 2.0 has a referral program. Both features combined make it necessary that participants *register* an account on the blockchain.

- **No more Hierarchies in Account Names**: In BitShares 1, there have been hierarchies in account names. Namely, you could only create a sub-account `home.wallet` if you also owned `wallet`. In BitShares 2.0, these hierarchies no longer exist and to register `home.wallet` you don't need to own `wallet`.
- **Explicit Privacy**: The *TITAN* technology in BitShares 2.0 slowed down blockchain processing significantly. Because of this and because TITAN did not really offer good privacy, we eliminated TITAN as a default transaction feature. Hence: **Account transactions are public now as well.** However, since we recognize the value of financial privacy, we offer *blinded* transactions that hide the transferred *amount*, and *stealth* transactions that hide the sender and receiver. A combination of both is also possible.
- **Prices are Fractions**: To circumvent rounding errors, all prices in BitShares 2.0 are represented as fractions.
- **Delegates are now Witnesses and Payed Positions are now Budget Items**: Since we have separated the business part from the block producing part, we now call block producers (formerly known as *delegates*) witnesses, while the additional payed position for workers are called budget items.

13.3 Blockchain Upgrade

BitShares 2.0 will be initialized with what is called a *Genesis Block*. That genesis block will be constructed from the balances of BitShares 1.0. BitShares 1.0 offers many features that need to be migrated into BitShares 2.0. To simplify the process and reduce the risk of errors, the following conditions will be met:

- **Funds**:
  - **BTS Tokens**: All BTS balances will be migrated 1:1. The supply not change!
  - **User-Issued-Assets**: All UAI tokens will be migrated 1:1
  - **BitAssets**: Because the new chain is a simple migration and should retain all the same "perceived value", all BitAssets and short positions are migrated 1:1.
- **Account Names**: Under BitShares 2.0, accounts are transferable and have different prices based upon the "quality" of the account name. Any "premium" names registered on or after 2015-06-08 (US Eastern time) will be given the prefix "bts-" or similar after the migration. All account names registered on or after 2015-06-18 (US Eastern time) will be prefixed with "bts-" unless they were registered using the BitShares Faucet.
  - **Premium Name**: No numbers and has vowels
  - **Cheap Name**: Has numbers or no vowels

  All other account names will be migrated with their corresponding owner/active keys.
- **Open Orders**: Open orders (except open short positions) will **not** migrate and the funds will be credited to the corresponding owners.
- **Open Shorts**: Short orders will be migrated to BitShares 2.0 on a 1:1 ratio. You collateral will be imported as a separated account (e.g. `usd-collateral-holder-124`) under your control.
- **Transaction History**: Transaction histories of BitShares 1.0 will be inaccessible in BitShares 2.0.
- **Vesting Balances**: Vesting balances will migrate under the existing terms, if two or more vesting balances were partially claimed as part of the same transaction prior to the snapshot the vesting balances may be merged into a single balance.

- **Unclaimed Delegate Pay**: Delegates that did not claim their pay prior to the snapshot will be able to claim their pay by importing their corresponding keys similar to any other balance.
- **Assets**: User issued assets and market pegged assets will migrated with their corresponding issuer and holders.
- **Deprecated Features**: Some features have turned out to be unreliable or impractical and will thus deprecate:
  - **Wall Messages** will not be migrated as the feature is now deprecated
  - Asset **description information** is no longer part of the blockchain state and will not be migrated
  - Account **public data** is deprecated and is no longer part of the blockchain state
  - BitShares URL scheme: `bts://` will be deprecated due to migration to hosted web wallets

CHAPTER 14

BitShares Accounts

In BitShares, you can create an account relatively easily by using the BitShares UI wallet. The account comes with the Private/public keys. You should keep the information safe. Also, BitShares account gives you some benefits (i.e., Lifetime Membership (LTM) and Referral Program) and important roles (i.e., voting). We recommend you to read through BitShares Accounts information to learn more.

14.1 Account

In BitShares, you can create readable and memorable own unique account name for your BitShares account. You do not need to write down a long random number as your account name. The BitShares account name would be helpful to identify other BitShares accounts.

Table of Contents

When you first time connect to one of BitShares UI wallets, you will find **Welcome to BitShares** page. As a default, you will create a Cloud Wallet. You can imagine the Cloud Wallet smiler to your normal bank account. You remember your account name and a password and the bank manage and save your funds for you.

A Local Wallet, as opposed to a Cloud Wallet, is another type of Wallet. You create your account name and a password and also you have to manage your funds. That means you have to create your account backup files and keep them in a safe place. The Local Wallet creation form is the advanced form. You can find the link on the same "Welcome to BitShares" page.

It's important to understand that **only** you know your password, and no one can recover it. The account information is registered to the blockchain with private/public keys of the account. Only the account creator knows the password and finds out the private keys. We will look into three types of keys (i.e., active, owner, and memo key) in anther section.

14.1.1 BitShares UI Wallet

If you create an account at one of BitShares partners, the account name will be available among BitShares partners. So, you will be able to use the BitShares account name to communicate (e.g., sending fund) with **other BitShares account holders** like sending an email. The advantage of using account name is you, and other people can identify the account holder.

- If you want to see the BitShares wallet, go to this link. It opens BitShare UI wallet

14.1.2 Identifier

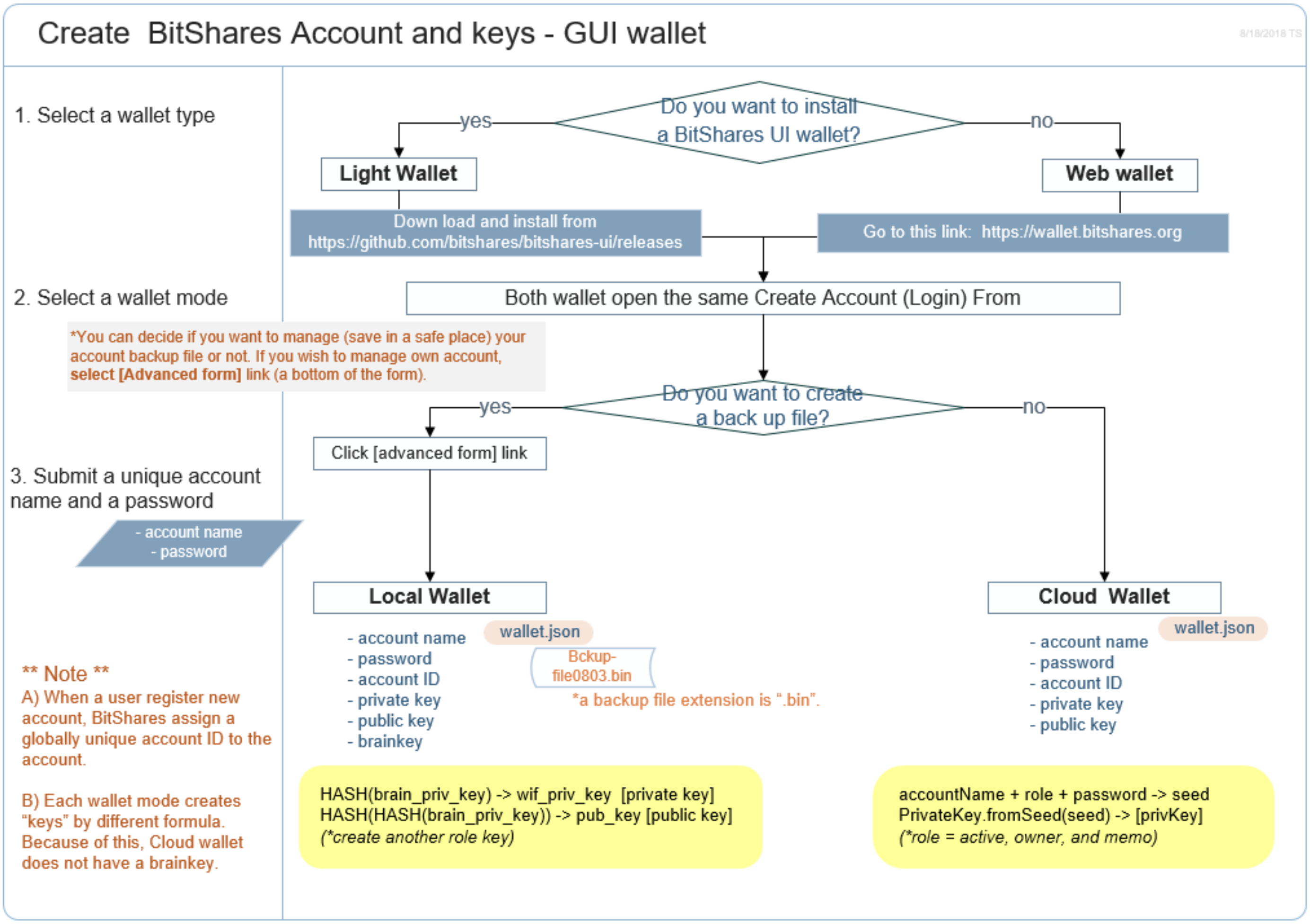
When you create a BitShares account, BitShares 2.0 registers the account name to the blockchain and also assigns an incrementing identifier (account id) during the registration. You will not need to remember the account_id while you use the BitShares wallet operations (i.e., send fund, place order, etc).

If you want to know your acount_id. go to a cryptofresh and search your account name. You will find your account id under your account name.

The identifier (account_id) comes with many advantages: Besides improved scalability, we have separated the identity from the transaction authorizing signature. In practice, owning an account name is autonomous from being able to spend its funds. Furthermore, both rights (we call them permissions) can split among an arbitrary complex relation of people (we call them authorities) using weights and required thresholds.

To separating authorities from identities, BitShares 2.0 can be much faster in processing delay while having much smaller transaction sizes. All participants are forced to have a named account on the blockchain. Also, most transactions are tied to the account name and can be linked to individuals (this includes transfers, trades, shorts, etc. but not stealthed transactions).

14.1.3 Accounts and keys


Create BitShares Account and keys - GUI wallet
8/18/2018 TS
1. Select a wallet type
Do you want to install a BitShares UI wallet?
yes
no
Light Wallet
Web wallet
Down load and install from https://github.com/bitshares/bitshares-ui/releases
Go to this link: https://wallet.bitshares.org
2. Select a wallet mode
Both wallet open the same Create Account (Login) From
Do you want to create a back up file?
yes
no
Click [advanced form] link
3. Submit a unique account name and a password
- account name
- password
Local Wallet
Cloud Wallet
- account name
- password
- account ID
- private key
- public key
- brainkey
wallet.json
Bckup-file0803.bin
- account name
- password
- account ID
- private key
- public key
wallet.json

*You can decide if you want to manage (save in a safe place) your account backup file or not. If you wish to manage own account, **select [Advanced form]** link (a bottom of the form).

*a backup file extension is ".bin".

** Note **

A) When a user register new account, BitShares assign a globally unique account ID to the account.

B) Each wallet mode creates "keys" by different formula. Because of this, Cloud wallet does not have a brainkey.

```
HASH(brain_priv_key) -> wif_priv_key  [private key]
HASH(HASH(brain_priv_key)) -> pub_key [public key]
(*create another role key)
```

```
accountName + role + password -> seed
PrivateKey.fromSeed(seed) -> [privKey]
(*role = active, owner, and memo)
```

14.2 Memberships

In the BitShares, there are two types of Membership Groups. Everyone becomes a Basic account member when created new BitShares account. Then, you can upgrade to a Lifetime membership (LTM) account. The **Lifetime member** (LTM) account gives the options and benefits to all BitShares holders.

14.2.1 Membership Group Types

Basic Account Members A regular default account. It's free, but not qualify for any cashback on transaction fees.

Lifetime Members One time upgrade fee is required. Lifetime Members get a percentage cashback on every transaction fee they pay and income from referrals (Referral Program).

(Annual Members) This membership has been removed. (*see the below notes)

To find out your Membership stats on the BitShares UI wallet, go to your account menu and select **Membership stats**. You can find your current membership status and the *upgrade fee* to become a LTM.

Note: In Q1/2016, the *annual membership* has been removed from the code base and no longer exists. References to this kind of memberships can be safely ignored.

Note: Due to some discrepancies, the annual membership has been disabled in most web wallets and will be re-enabled after a proper update eventually.

14.3 Fees

In the BitShares Blockchain Network, every operation is assigned an individual fee. Each operation has different transaction fee. You can check each operation fee schedule if you are interested.

Table of Contents

14.3.1 Fee Types

There are different Transaction Fee Types. And each operation has own transaction fee amount. Some operations ask Regular Transaction Fee and Price of per KByte Transaction Size.

For instance, *Transfer operation* asks both (Regular Transaction Fee and Price of per KByte Transaction Size) fees. The *Price per KByte Transaction Size* comes from a size of memo you send. The memo is encrypted by default and can only be decrypted by the participants of the transfer. It's safe to use to sens a message. However, the transfer fee depends on the length of the memo.

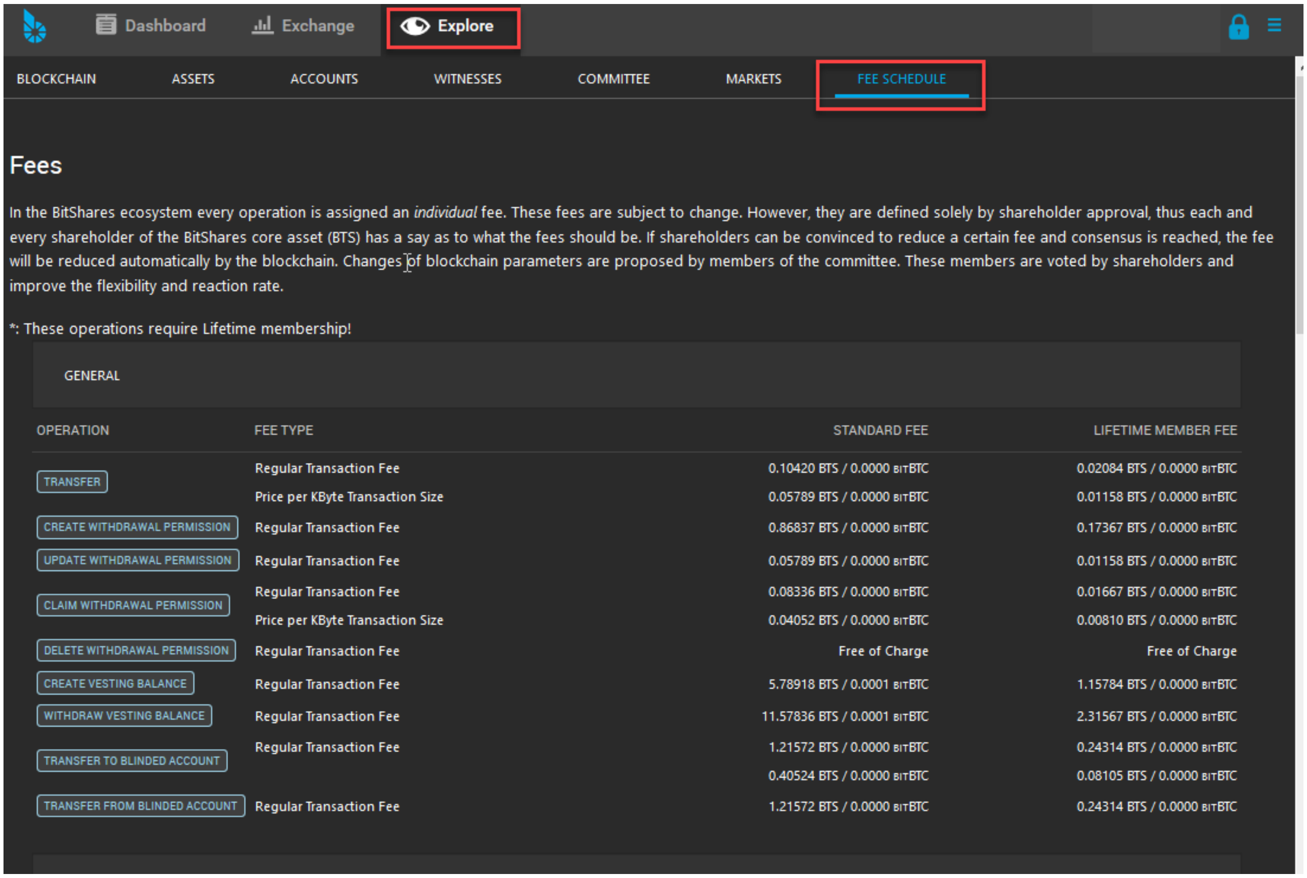
You can use the memo section to send a message. Also, some transactions require you to input a necessary information in the memo section. Be sure if you put each information in a correct place before you confirm your transaction!

- **Fee Types**

- Regular Transaction Fee
- Price per KByte Transaction Size
- Symbols with 3 Characters (Create Asset Operation)
- Symbols with 4 Characters (Create Asset Operation)
- Longer Symbols (Create Asset Operation)
- Basic Fee (Create Account)
- Fee for Premium Names (Create Account)
- (Lifetime Membership Fee)

- **Fee Schedules**
  - You can find each Operation Fee List here.

Example: Fee Schedule View



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

*: These operations require Lifetime membership!

GENERAL

OPERATION	FEE TYPE	STANDARD FEE	LIFETIME MEMBER FEE
TRANSFER	Regular Transaction Fee	0.10420 BTS / 0.0000 bitBTC	0.02084 BTS / 0.0000 bitBTC
	Price per KByte Transaction Size	0.05789 BTS / 0.0000 bitBTC	0.01158 BTS / 0.0000 bitBTC
CREATE WITHDRAWAL PERMISSION	Regular Transaction Fee	0.86837 BTS / 0.0000 bitBTC	0.17367 BTS / 0.0000 bitBTC
UPDATE WITHDRAWAL PERMISSION	Regular Transaction Fee	0.05789 BTS / 0.0000 bitBTC	0.01158 BTS / 0.0000 bitBTC
CLAIM WITHDRAWAL PERMISSION	Regular Transaction Fee	0.08336 BTS / 0.0000 bitBTC	0.01667 BTS / 0.0000 bitBTC
	Price per KByte Transaction Size	0.04052 BTS / 0.0000 bitBTC	0.00810 BTS / 0.0000 bitBTC
DELETE WITHDRAWAL PERMISSION	Regular Transaction Fee	Free of Charge	Free of Charge
CREATE VESTING BALANCE	Regular Transaction Fee	5.78918 BTS / 0.0001 bitBTC	1.15784 BTS / 0.0000 bitBTC
WITHDRAW VESTING BALANCE	Regular Transaction Fee	11.57836 BTS / 0.0001 bitBTC	2.31567 BTS / 0.0000 bitBTC
TRANSFER TO BLINDED ACCOUNT	Regular Transaction Fee	1.21572 BTS / 0.0000 bitBTC	0.24314 BTS / 0.0000 bitBTC
		0.40524 BTS / 0.0000 bitBTC	0.08105 BTS / 0.0000 bitBTC
TRANSFER FROM BLINDED ACCOUNT	Regular Transaction Fee	1.21572 BTS / 0.0000 bitBTC	0.24314 BTS / 0.0000 bitBTC

Paying Fees

Each time you perform an activity (i.e., send fund, place an order, etc), you pay a small amount of fee. Any transaction fee can be paid by paying any asset that has a Core exchange rate (i.e., price) at which the asset can be exchange implicitly into BTS to cover the network fee. When you confirm your activity (transaction), you can see a fee amount for the transaction.

Order Cancellation

If you cancel an order that has not been fully or partially filled, 90% of the fee will be payed back to your account. However, this cashback will be in BTS (CORE token) and not in the asset you have originally paid the fee in.

14.3.2 Standard Fee and Lifetime Membership Fee

Your transaction fees depend on your membership status. If you are a Basic Member, you pay "Standard Fee". And if you are a Lifetime Member, you pay "Lifetime Member Fee".

20% of each transaction fee goes to the network. And if you are a **Lifetime Members, you get cashback of 80% of the fee** you payed.

For many cases it may make sense to upgrade the account even though you don't want to participate in marketing at all simply for the reasons to get a cashback of 80% of the fees you pay for your own transactions!

Note: Technically, the fees that you pay stay the same, but a part of the fees is refunded in the form of a **vesting balance**. Once the fees have vested you can withdraw them.

14.3.3 Asset Creation Fee

We talked about "Transfer Operation" Fees. Some of the transfer fees depend on the length of the memo. Similarly, an **Asset Creation Fee** depends on the length of your asset symbol. **Three (3) Character Symbols** are the shortest and are rather expensive while symbols with **five (5) or more characters** are significantly cheaper.

50% of the asset creation fee is used to pre-fill the assets fee pool. From the other **50%**, **20% go to the network and 80% go to the referral program**. This means that if you are a lifetime member, you get back 40% of the asset creation fee after the vesting period (currently 90 days).

How to Profit by Issuing an Asset

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

Fee Pools

Issuers may optionally maintain a Fee Pool. The **Fee Pool is a pool of BTS** and an exchange rate at which the issued asset may be converted into 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.

Note: 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.

If the assets fee pool is funded, the fees can be payed in the native UIA instead of BTS.

14.4 Referral Program

The purpose of the referral program is to incentivize people to bring in more people. It compares to a Multi-Level-Marketing (MLM) scheme with the difference of having only **1 level** where referred individuals can opt-out by upgrading their account to a Life-Time Member (LTM). Every lifetime member can get a cut of the fees based on child accounts linked to ours via referral.

Table of Contents

14.4.1 Participation

Every BitShares Holder can become a Lifetime Member and participate in the Referral Program. In this program:

Basic Accounts are free, but do not qualify for the referral program, nor any cash back on transaction fees.

Lifetime Members pay an upgrade fee and earn **80% cash back on every fee they pay**. They also qualify for **80% cashback of the fees paid by Basic Accounts they refer** to the network. These 80% can be split among the registrar, that actually registers the accounts, and an affiliate referrer, that brought in the new user.

The referral fees are controlled by the blockchain and are distributed like this:

- 20% go to the network
- 80% go to the referral program
  - of this 80%, x% go to the registrar
  - of this 80%, 100%-x% go to the affiliate referrer

14.4.2 How can I do?

If you want to participate in the referral program, you need to have a life-time member account, first! Then you can bring in new users by

- (1)- running your own faucet and actually register new accounts (will give you 80% of all the fees of those minus a fraction that you decide to give to affiliates (the referrers)
- (2)- referring people to a hosted wallet that offers you a cut of the fees as an affiliate.

The case below, most hosted wallets add your account as affiliate if you provide the following link structure to people

```
https://<url>/?r=<your-account>
```

with `<your-account>` being the name of your BitShares Lite-Time Member account.

Note: If you want link to pages with in the wallet(e.g., a particular decentralized market), you need to have the `?r=` parameter **before** the `#`. Example : `https://<url>/?r=<your-account>#/market/USD_BTC`

- (3)- or sending your referral link to people you want to refer to BitShares, your referral link would be:

```
https://wallet.bitshares.org/?r=<your-account-name>

(*You might want to use yow wallet address instead of "wallet.bitshares.
↪org"*)
```

Example:

When an Basic Account pays $100 to become a Lifetime Member, $50 is paid to their Referrer, $30 is paid to the nearest Lifetime Member, and $20 is paid to the Network. After this point the Lifetime Member becomes its own referrer and nearest Lifetime Member and its prior Referrers no longer get any revenue from this user.

14.4.3 Fee Division

Every time an account you referred pays a transaction fee, that fee is divided among several different accounts. The network takes a cut, and the Lifetime Member who referred the account gets a cut.

The **registrar** is the account that paid the transaction fee to register the account with the network. The registrar gets to decide how to divide the remaining fee between themselves and their affiliate.

Fee status

Pending Fees Fees paid are only divided among the network, referrers, and registrars once every maintenance interval.

Vesting Fees Most fees are made available immediately, but fees over the vesting threshold (such as those paid to upgrade your membership or register a premium account name) must vest for some period as defined by the committee.

To see your vesting balances, open the side menu and select **Vesting balance**. Vesting balances are recalculated hourly, so you might not yet see them right away.

14.4.4 Claiming Referral Bonus and Cashback

If you have a lifetime memb1er account and

- already paid some fees, or
- have referred people that paid some fees,

you can claim them in the "Vesting balances" of your account.

14.5 Vesting Balances

In BitShares 2.0, some balances are vesting over time. This feature has been introduced initially in BitShares 1 when merging several blockchain businesses into one blockchain.

Table of Contents

14.5.1 What is it?

Vesting balances contain any fees earned through the referral program or from worker pay, for example. They have a certain vesting period and are continually unlocked during that vesting period until all of the balances are available.

Account income

We make even more use of this functionality in such that an account's income in form of

- worker pay,
- witness pay,
- the referral program, or
- cashback

is vesting over several days with different strategies.

For instance, a worker can define for how long he would like his pay to vest to encourage BTS Holders to vote for him due to no imminent additional sell pressure from the worker.

Strategies

1. **CCD / Coin Days Destroyed**

The economic effect of this vesting policy is to require a certain amount of "interest" to accrue before the full balance may be withdrawn. Interest accrues as coindays (balance * length held). If some of the balance is withdrawn, the remaining balance must be held longer.

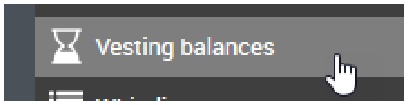
2. **Linear Vesting with Cliff**

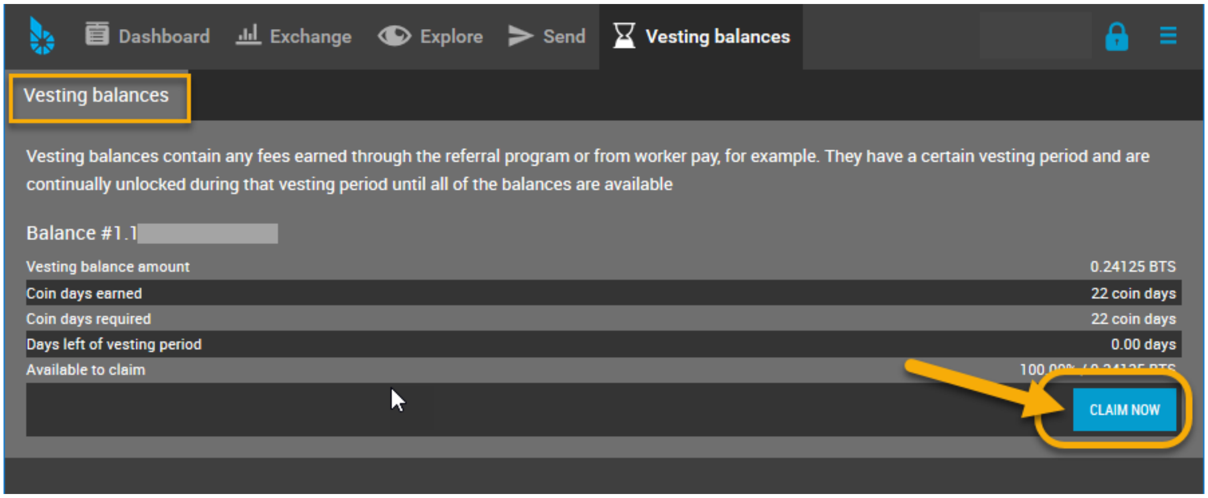
This vesting balance type is used to mimic traditional stock vesting contracts where each day a certain amount vests until it is fully matured.

14.5.2 Claiming A Vesting Balance

You can claim vesting balances by using BitShares User interface. (You might need to wait certain days to claim.)

Open the side dropdown menu and select **[Vesting Balances]**





Vesting balances

Vesting balances contain any fees earned through the referral program or from worker pay, for example. They have a certain vesting period and are continually unlocked during that vesting period until all of the balances are available

Balance #1.1[redacted]

Vesting balance amount	0.24125 BTS
Coin days earned	22 coin days
Coin days required	22 coin days
Days left of vesting period	0.00 days
Available to claim	100.00% / 0.24125 BTS

14.6 Permissions

Table of Contents

14.6.1 Permission Models

In BitShares, each account is separated into the permission types below;

Owner Permission This permission has administrative powers over the whole account and should be considered for 'backup' strategies.

Active Permission Allows to access funds and some account settings, but cannot change the owner permission and is thus considered the "online" permissions.

Both can be defined in the Permissions tab of your account using so called *authorities* together with a so called *threshold* that has to be exceeded in order for a transaction to be valid.

- **Authorities** :In BitShares an authority consists of one or many entities that authorize an action, such as transfers or trades.
  - An authority consists of one or several pairs of an account name with a weight.
  - In order to obtain a valid transaction, the sum of the weights from signing the parties has to exceed the threshold as defined in the permissions.
- **Hierarchical Corporate Accounts**

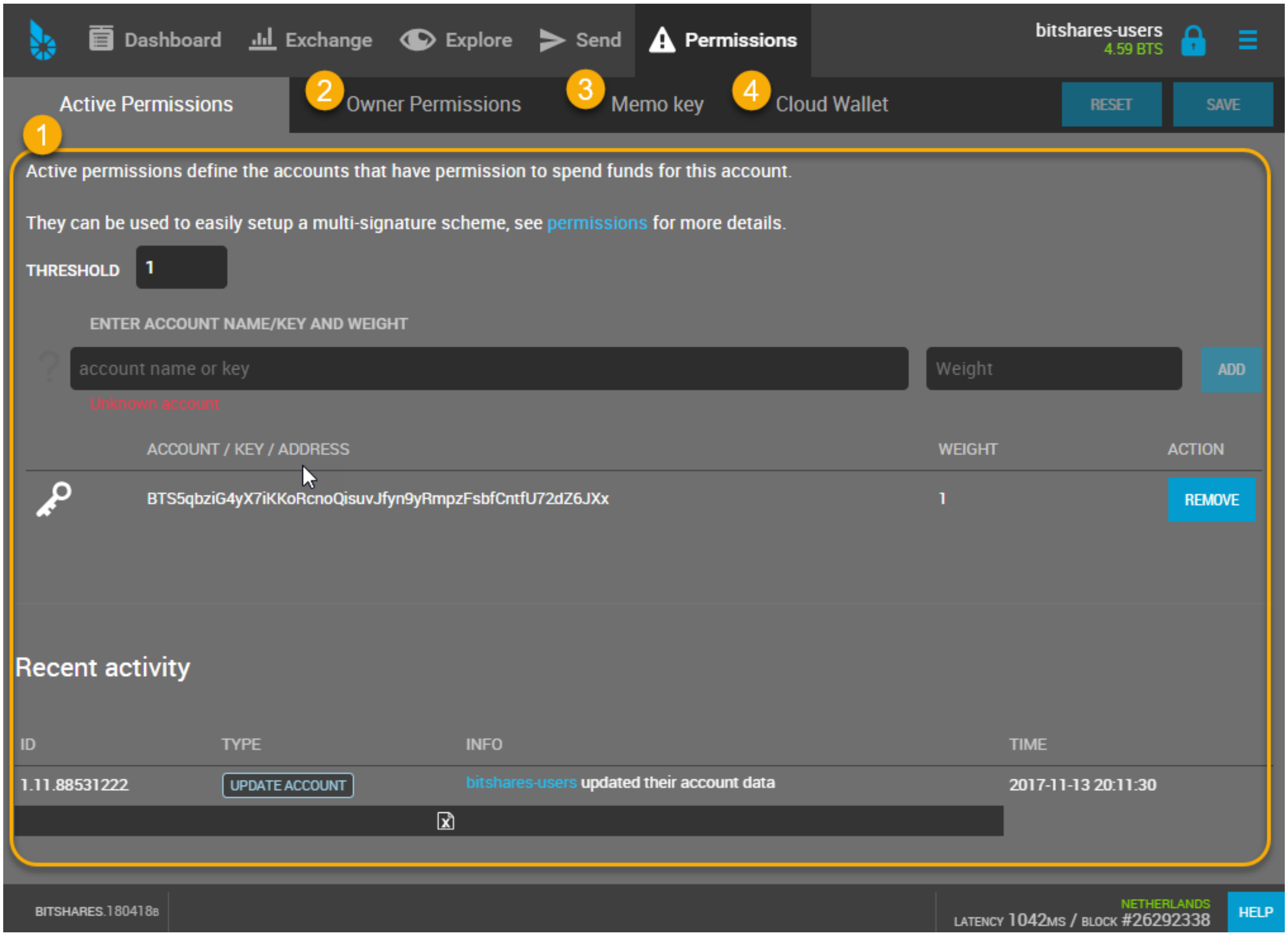
BitShares designs permissions around people, rather than around cryptography, making it easy to use. Every account can be controlled by any weighted combination of other accounts and private keys. This creates a hierarchical structure that reflects how permissions are organized in real life, and makes multi-user control over funds easier than ever. Multi-user control is the single biggest contributor to security, and, when used properly, it can virtually eliminate the risk of theft due to hacking.

Read more about *Multi-Signature*

14.6.2 Permissions - in Wallet Settings

The Permission page locates in a side menu.

- Go to [**Settings**] and click [**Permissions**]



Active permissions define the accounts that have permission to spend funds for this account.

They can be used to easily setup a multi-signature scheme, see permissions for more details.

THRESHOLD 1

ENTER ACCOUNT NAME/KEY AND WEIGHT

account name or key | Weight | ADD

Unknown account

ACCOUNT / KEY / ADDRESS	WEIGHT	ACTION
BTS5qbziG4yX7iKKoRcnoQisuvJfyn9yRmpzFsbfCntfU72dZ6JXx	1	REMOVE

Recent activity

ID	TYPE	INFO	TIME
1.11.88531222	UPDATE ACCOUNT	bitshares-users updated their account data	2017-11-13 20:11:30

14.6.3 Permissions Tabs

Active Permissions Active permissions define the accounts that have permission to spend funds for this account.

Owner Permissions Owner permissions define who has control over the account. Owners may overwrite all keys and change any account settings.

Memo Key The memo key is where you receive memos, in order to decode the memos you need to control the private key for the public key. By using a public/private key pair without spending authority, you may give read-only access to your memos to third parties.

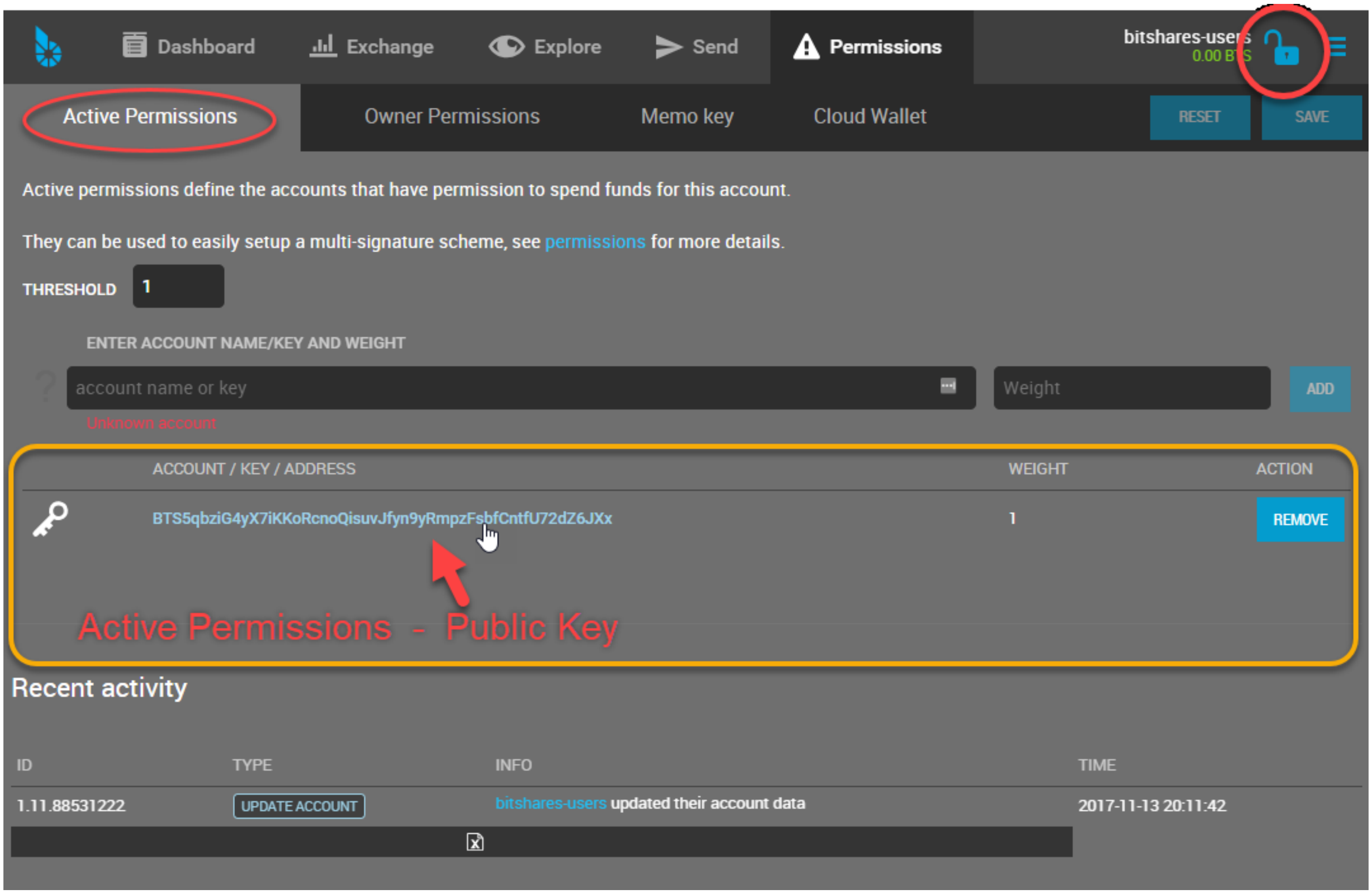
Cloud Wallet You can use this feature, if you want to change your **Cloud wallet** password.

14.7 Public Key and Private Key

14.7.1 Where are public/private keys?

In this section, we will show you how to find your private key.

You can find each **Public key** and **Private key** on the Permissions page.



Active permissions define the accounts that have permission to spend funds for this account.

They can be used to easily setup a multi-signature scheme, see permissions for more details.

THRESHOLD 1

ENTER ACCOUNT NAME/KEY AND WEIGHT

account name or key

Weight

Unknown account

ACCOUNT / KEY / ADDRESS	WEIGHT	ACTION
BTS5qbziG4yX7iKKoRcnoQisuvJfyn9yRmpzFsbfCntfU72dZ6JXx	1	REMOVE

Recent activity

ID	TYPE	INFO	TIME
1.11.88531222	UPDATE ACCOUNT	bitshares-users updated their account data	2017-11-13 20:11:42

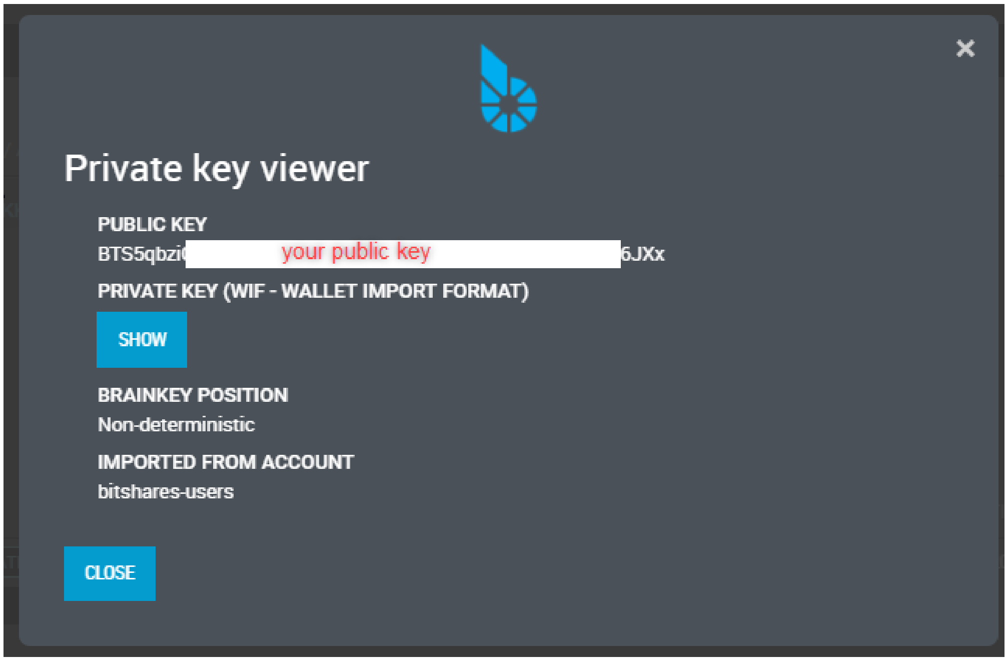
14.7.2 How to find each private key

Note: If you cannot click nor find a link, *login* to your wallet.

1. **Active and Owner – Private keys**

- Go to [**Settings**] - [**Permissions**]

- Click a private key number or a key image.
- A Private key viewer form opens. You will find a Public Key and a [**SHOW**] button like below.
- Click the [**SHOW**] button. You will find your Private key under the Public key.



Private key viewer

PUBLIC KEY

BTS5qbzi[redacted]6JXx

PRIVATE KEY (WIF - WALLET IMPORT FORMAT)

BRAINKEY POSITION

Non-deterministic

IMPORTED FROM ACCOUNT

bitshares-users

2. **Memo – Private keys**

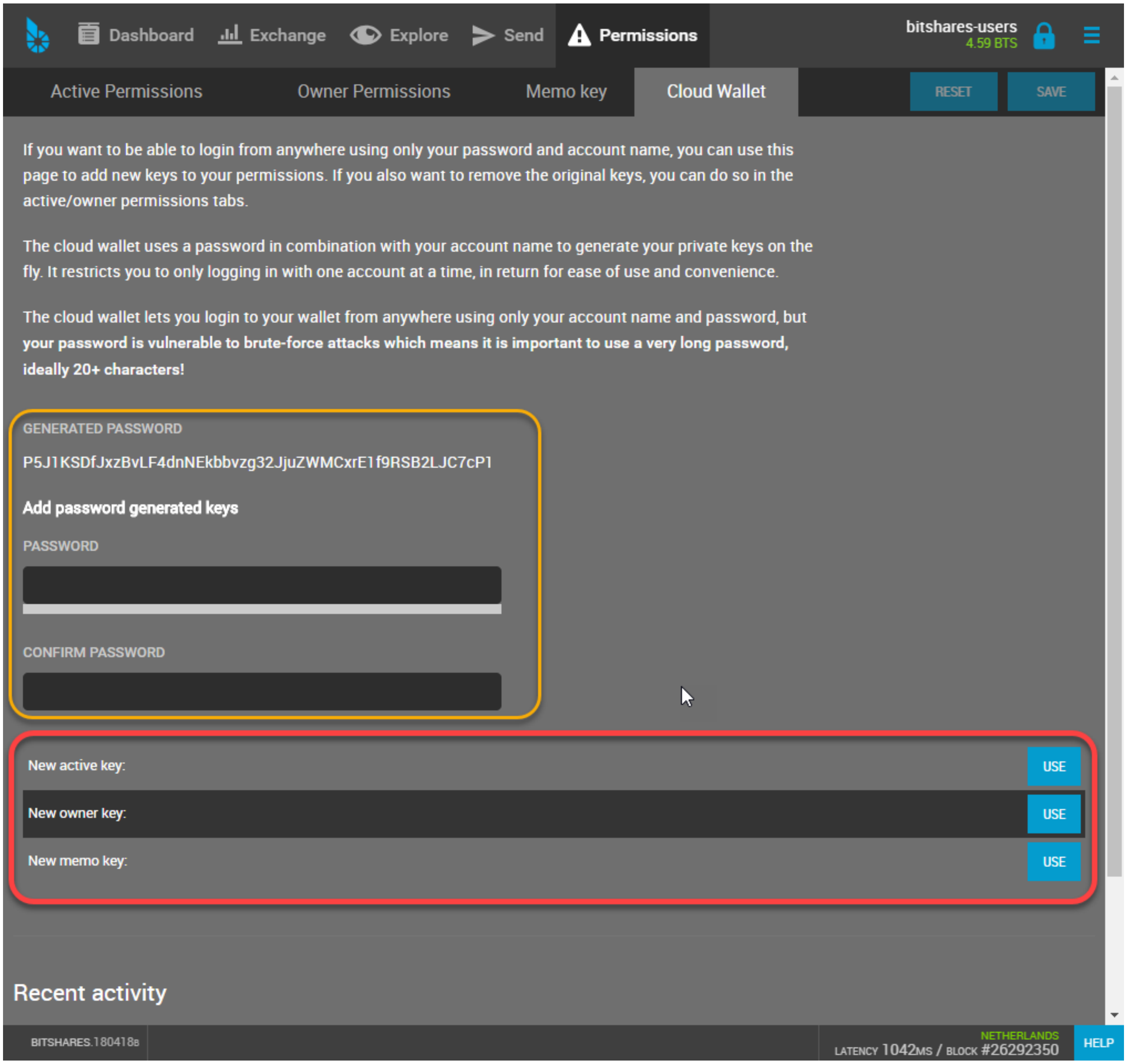
- Go to [**Settings**] - [**Permissions**] - [**Memo key**] tab
- Click a key image. (It seems a private key number does not have a link.)
- A Private key viewer form opens. You will find a Public Key and a [**SHOW**] button like below.
- Click the [**SHOW**] button. You will find your Private key under the Public key.

14.7.3 How to change Cloud wallet password

In this section, we will show you how to change your Cloud Wallet password.

- Go to [**Settings**] - [**Permissions**] - [**Cloud Wallet key**] tab

If you want to change your **Cloud Wallet** password, use this page. You will change your password and your keys during this process.



If you want to be able to login from anywhere using only your password and account name, you can use this page to add new keys to your permissions. If you also want to remove the original keys, you can do so in the active/owner permissions tabs.

The cloud wallet uses a password in combination with your account name to generate your private keys on the fly. It restricts you to only logging in with one account at a time, in return for ease of use and convenience.

The cloud wallet lets you login to your wallet from anywhere using only your account name and password, but **your password is vulnerable to brute-force attacks which means it is important to use a very long password, ideally 20+ characters!**

GENERATED PASSWORD

P5J1KSDfJxzBvLF4dnNEkbbvzg32JjuZWMCxrE1f9RSB2LJC7cP1

Add password generated keys

PASSWORD

CONFIRM PASSWORD

New active key:

New owner key:

New memo key:

Steps

1. **Save your old Memo key (optional)**

   When you replace the memo key you will not be able to see old memos, so if you have a lot of those we recommend saving the old memo private key.

   - Go to [**Settings**] - [**Permissions**] - [**Memo key**] tab
   - Click a key image.
   - A Private key viewer form opens. You will find a Public Key and a [**SHOW**] button like below.
   - Click the [**SHOW**] button. Log in to your wallet if necessary. You will find your Private key under the Public key.
   - Write down and save the Private key.

2. **Set new password**

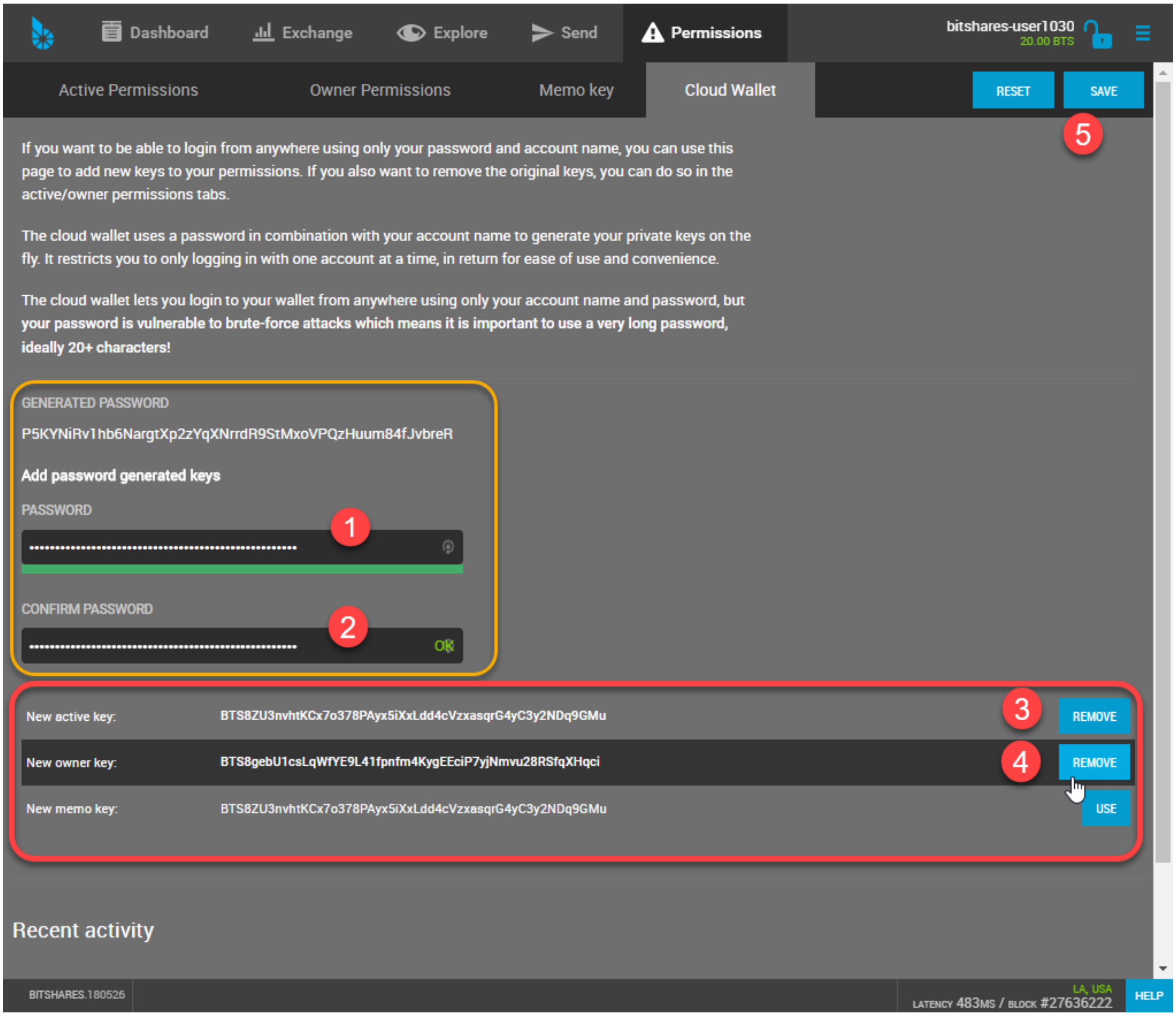
   You can use your desired new password or use the auto-GENERATED PASSWORD.

   - (#1)Type in [**PASSWORD**]
   - (#2)Conform the password [**CONFIRM PASSWORD**]

3. **Generate new keys**

   In this example, we decided to keep old Memo keys.

   - (#3)Click [**USE**] to generate new Active key
   - (#4)Click [**USE**] to generate new Owner key
   - (#5)Click [**SAVE**]
   - Confirm the Transaction



If you want to be able to login from anywhere using only your password and account name, you can use this page to add new keys to your permissions. If you also want to remove the original keys, you can do so in the active/owner permissions tabs.

The cloud wallet uses a password in combination with your account name to generate your private keys on the fly. It restricts you to only logging in with one account at a time, in return for ease of use and convenience.

The cloud wallet lets you login to your wallet from anywhere using only your account name and password, but **your password is vulnerable to brute-force attacks which means it is important to use a very long password, ideally 20+ characters!**

GENERATED PASSWORD

P5KYNiRv1hb6NargtXp2zYqXNrrdR9StMxoVPQzHuum84fJvbreR

Add password generated keys

PASSWORD

••

CONFIRM PASSWORD

•• OK

New active key: BTS8ZU3nvhtKCx7o378PAyx5iXxLdd4cVzxasqrG4yC3y2NDq9GMu

New owner key: BTS8gebU1csLqWfYE9L41fpnfm4KygEEciP7yjNmvu28RSfqXHqci

New memo key: BTS8ZU3nvhtKCx7o378PAyx5iXxLdd4cVzxasqrG4yC3y2NDq9GMu

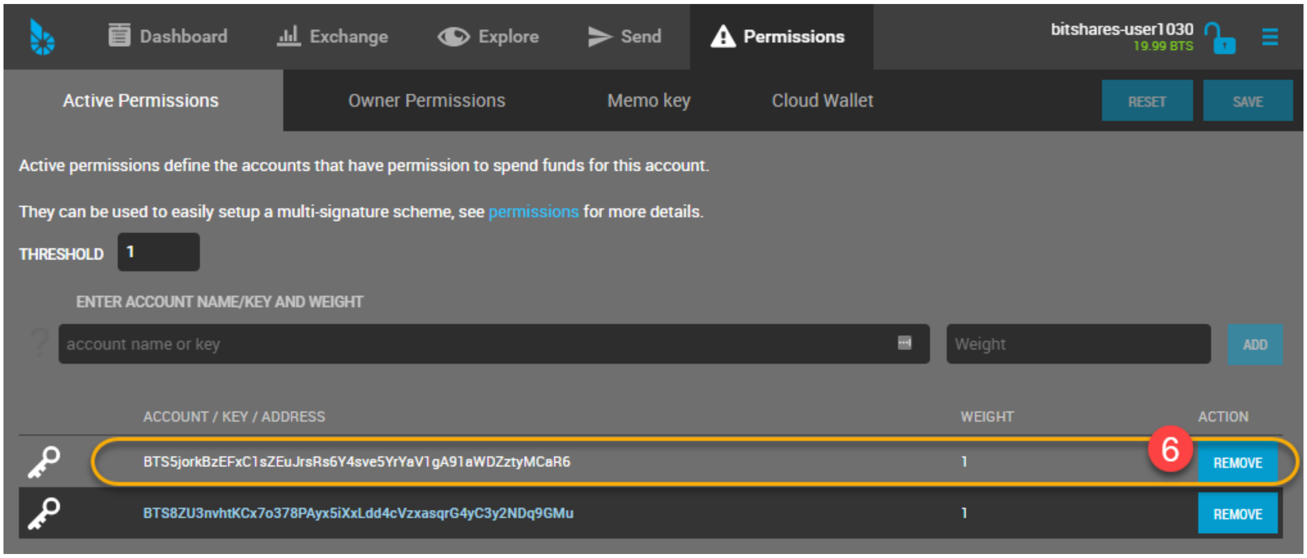
4. **Remove old keys**

   In order to remove access using your old password, you need to remove the keys corresponding to the old password.

- Log out, and log back in with **your new password**.
- Go to [**Settings**] - [**Permissions**] - [**Active key**] tab

You will see the two public keys. The light blue colored key is your new public key that is belongs to your new password. You want to keep only this key!

- (#6)Click [**REMOVE**] next to the plain colored key. In this case, remove "P5J3maQ7kCDxaUfbBCRKwTwWnPwCp6h5sZU6va7C9sYW6".
- Now go to the Owner tab and do the same for the old owner key.
- (#7)Click [**SAVE**] – *Do not forget to save!*
- Confirm the Transaction



Active permissions define the accounts that have permission to spend funds for this account.

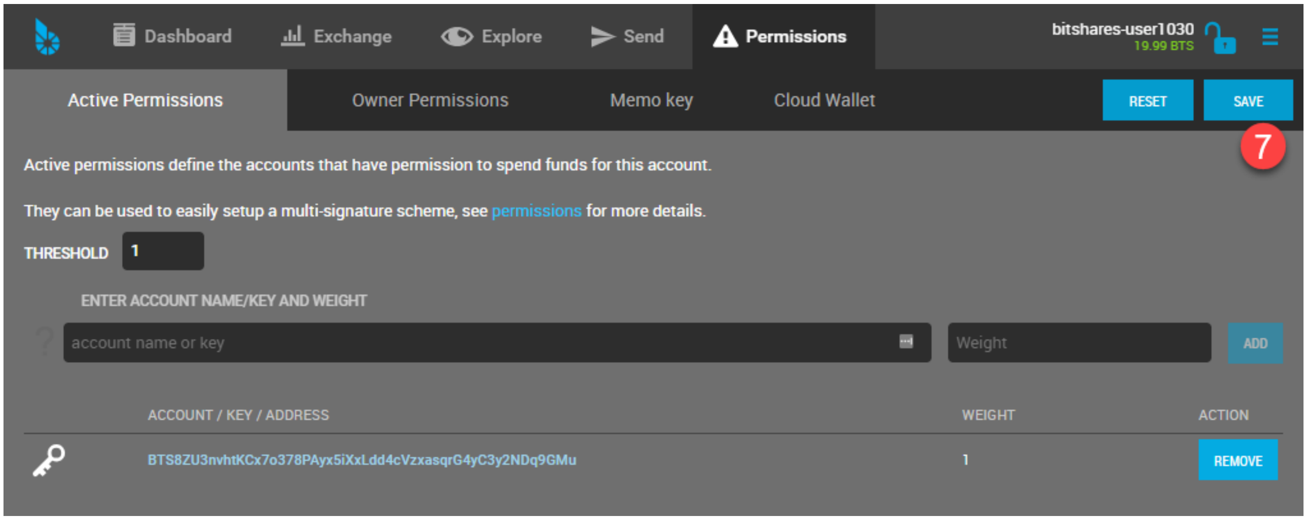
They can be used to easily setup a multi-signature scheme, see permissions for more details.

THRESHOLD 1

ENTER ACCOUNT NAME/KEY AND WEIGHT

account name or key | Weight

ACCOUNT / KEY / ADDRESS	WEIGHT	ACTION
BTS5jorkBzEFxC1sZEuJrsRs6Y4sve5YrYaV1gA91aWDZztyMCaR6	1	REMOVE
BTS8ZU3nvhtKCx7o378PAyx5iXxLdd4cVzxasqrG4yC3y2NDq9GMu	1	REMOVE



Active permissions define the accounts that have permission to spend funds for this account.

They can be used to easily setup a multi-signature scheme, see permissions for more details.

THRESHOLD 1

ENTER ACCOUNT NAME/KEY AND WEIGHT

account name or key | Weight

ACCOUNT / KEY / ADDRESS	WEIGHT	ACTION
BTS8ZU3nvhtKCx7o378PAyx5iXxLdd4cVzxasqrG4yC3y2NDq9GMu	1	REMOVE

14.8 Multi-Signature

Table of Contents

14.8.1 Authorities

In BitShares an *authority* consists of one or many entities that authorize an action, such as transfers or trades.

- An authority consists of one or several pairs of an account name with a *weight*.
- In order to obtain a valid transaction, the sum of the weights from signing the parties has to exceed the threshold as defined in the permissions.

Examples We explain some examples to shed some light on the used terminology and the use-cases. We assume that a new account is created with it's active permissions set as described below. **Note** that the same scheme also works for the owner permissions.

14.8.2 (Flat) Multi-Signature

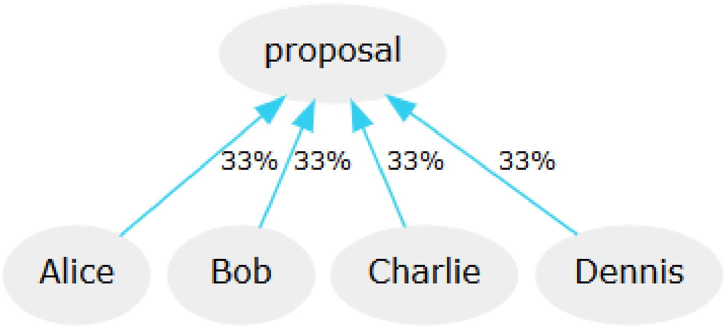
A flat multi-signature scheme is composed of `M` entities of which `N` entities must sign in order for the transaction to be valid. Now, in BitShares, we have *weights* and a *threshold* instead of `M` and `N`. Still we can achieve the very same thing with even more flexibility as we will see now.

Let's assume, Alice, Bob, Charlie and Dennis have common funds. We want to be able to construct a valid transaction if only two of those agree. Hence a **2-of-4** (N-of-M) scheme can look as follows:

Account	Weight
Alice	1
Bob	1
Charlie	1
Dennis	1
Threshold:	3

This means that each party has the same weight of 1 while 3 parties need to sign the transaction/proposal.

In other words: Alice, Bobe, Charlie and Dennis, each have 33% weight while 100% must be reached.



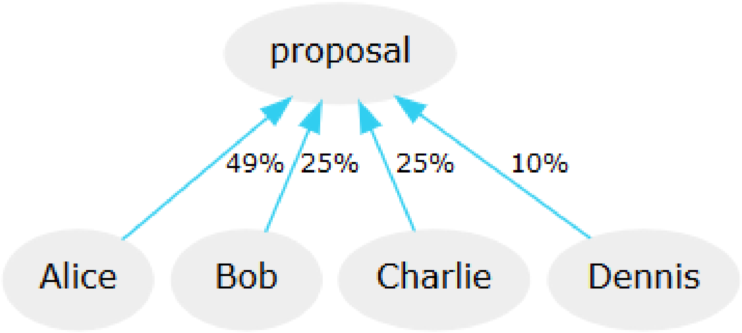
All four participants have a weight of 33% but the threshold is set to 51%. Hence only two out of the four need to agree to validate the transaction.

Alternatively, to construct a 3-of-4 scheme, we can either decrease the weights to 17 or increase the threshold to 99%.

14.8.3 (Flat) Flexible Multi-Signature

With the threshold and weights, we now have more flexibility over our funds, or more precisely, we have more *control*. For instance, we can have separate weights for different people. Let's assume Alice wants to secure here funds against theft by a multi-signature scheme but she does not want to hand over too much control to her friends. Hence, we create an authority similar to:

Account	Weight
Alice	49%
Bob	25%
Charlie	25%
Dennis	10%
Threshold:	51%

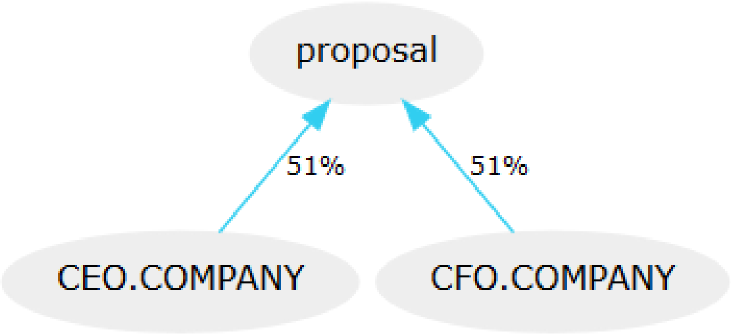


Now the funds can either be accessed by Alice and a single friend or by all three friends together.

14.8.4 Multi-Hierarchical Flexible Multi-Signature

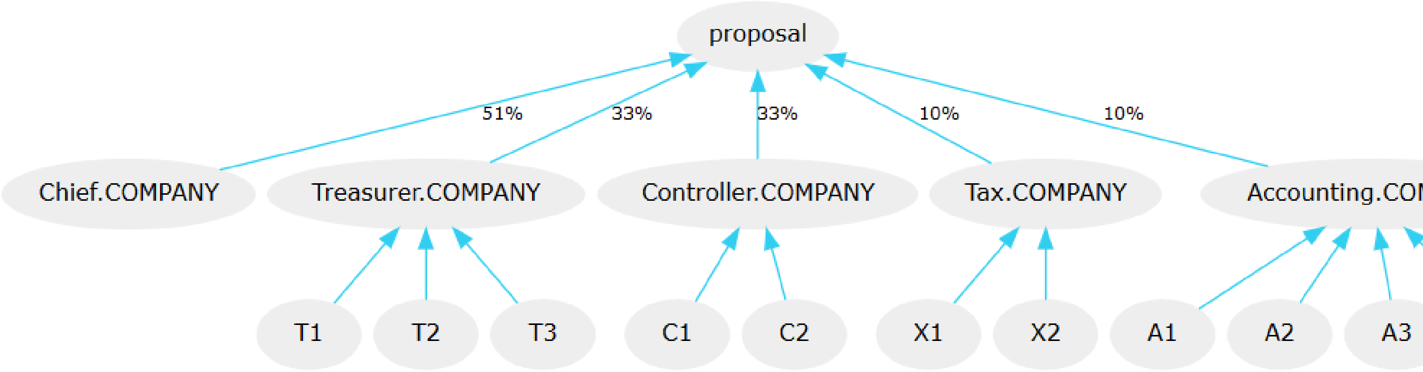
Let's take a look at a simple multi-hierarchical corporate account setup. We are looking at a company that has a Chief of Financial Officer (CFO) and a some departments working for him, such as the Treasurer, Controller, Tax Manager, Accounting, etc. The company also has a CEO that wants to have spending privileges. Hence we construct an authority for the funds according to:

Account	Weight
CEO.COMPANY	51%
CFO.COMPANY	51%
Threshold:	51%



whereas CEO.COMPANY and CFO.COMPANY have their own authorities. For instance, the CFO.COMPANY account could look like:

CFO.COMPANY	Weight
Chief.COMPANY	51%
Treasurer.COMPANY	33%
Controller.COMPANY	33%
Tax Manager.COMPANY	10%
Accounting.COMPANY	10%
Threshold:	51%



This scheme allows:

- the CEO to spend funds
- the Chief of Finance Officer to spend funds
- Treasurer together with Controller to spend funds
- Controller or Treasurer together with wither the Tax Manager or Accounting to spend funds.

Hence, a try of arbitrary depth can be spanned in order to construct a flexible authority to reflect mostly any business use-case.

14.9 Voting

Table of Contents

If you hold some BTS tokens, you are considered a BTS Holder of the BitShares business and thus have a say in where it should be heading in future. As a BTS Holder you can cast a vote for three different entities within the network:

Block producers Block producers bundle transactions into blocks and sign them with their signing key. These so called *witnesses* keep the blockchain alive by producing one block every few seconds and get paid by newly issued BTS shares similar to Bitcoin. Their second job is to produce reliable and accurate price feeds for the smartcoins.

Committee Members Committee Members *govern the blockchain and the business parameters*, and define the transaction fees.

Workers Workers are freelancers or businesses that provide a non-profitable service for the BitShares ecosystem. Essentially, they apply for a job in the ecosystem by providing actual work and get paid accordingly (if the BTS Holders approve).

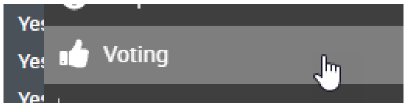
Since voting might be a too time-consuming task for many BTS Holders, BitShares offers them a way to committee their voting power to so called **proxies**. The sole purpose of proxies is to follow the ecosystem and be vote according to their *followers*. This is similar to many political votes where citizens vote for representatives which vote on their behalf.

Voting itself is **very simple** with the User interface and requires only a few clicks.

14.9.1 Voting by using BitShares UI

You can cast your vote or set your proxy by BitShares User interface.

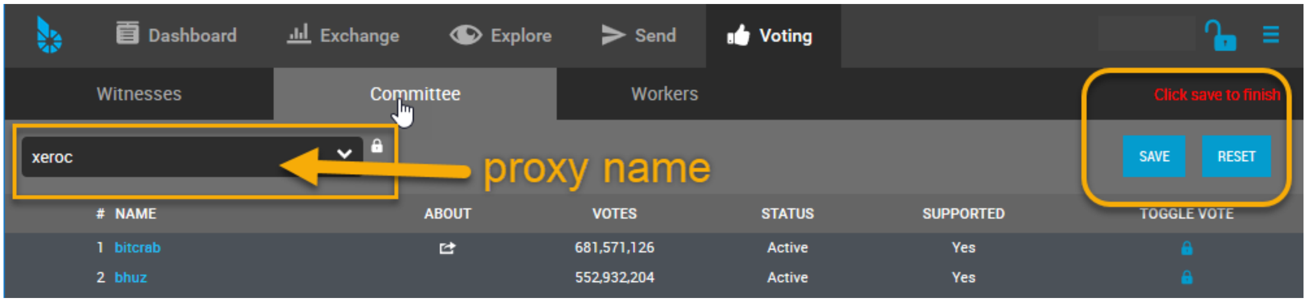
Open the side dropdown menu and select **[Voting]**



Setting a proxy

The picture below shows how to set your trusted proxy:

1. Type a proxy name
2. Click [SAVE]
3. Login to a wallet if you have not logged in
4. Confirm the Transaction



xeroc

proxy name

Click save to finish

#	NAME	ABOUT	VOTES	STATUS	SUPPORTED	TOGGLE VOTE
1	bitcrab	⇗	681,571,126	Active	Yes	🔒
2	bhuz		552,932,204	Active	Yes	🔒

Voting for Witness, Committee Member or Worker

If you have not set a proxy, you can cast your own vote for witnesses, committee members or workers.

1. Select a Witnesses, Committee, or Workers tab
2. Click and check **TOGGLE VOTE**
3. Click [SAVE]
4. Login to a wallet if you have not logged in
5. (vote for each entity)

CHAPTER 15

Create a BitShares Wallet

Table of Contents

15.1 Terminology

In this section, we want to describe Terminologies and guide you to create and register your BitShares Account.

Wallet

Wallets interacts with the blockchain to process accounts and funds functionalities. Users register to create a single wallet. The single wallet can carry many accounts. Users who have a lifetime membership (LTM) can register multiple accounts in parallel; all of them are stored in a single wallet. Also, users can create multiple wallets to organize their accounts properly.

Accounts

In BitShares, you can create own **unique account name**, so, you can remember easily. And you will use the account name to communicate (e.g. Send fund) with other BitShares account users (BTS Holders) like an email address. The advantage of using account name is that people can identify you by using a readable and memorable word instead of cryptographic addresses.

Each user has at least one account that can be used to interact with the blockchain. The account can be seen as a single banking account with an individual balance, transaction history, etc. Since these accounts are registered on the blockchain and are open to the public, we recommend to pick a pseudonym to achieve some privacy.

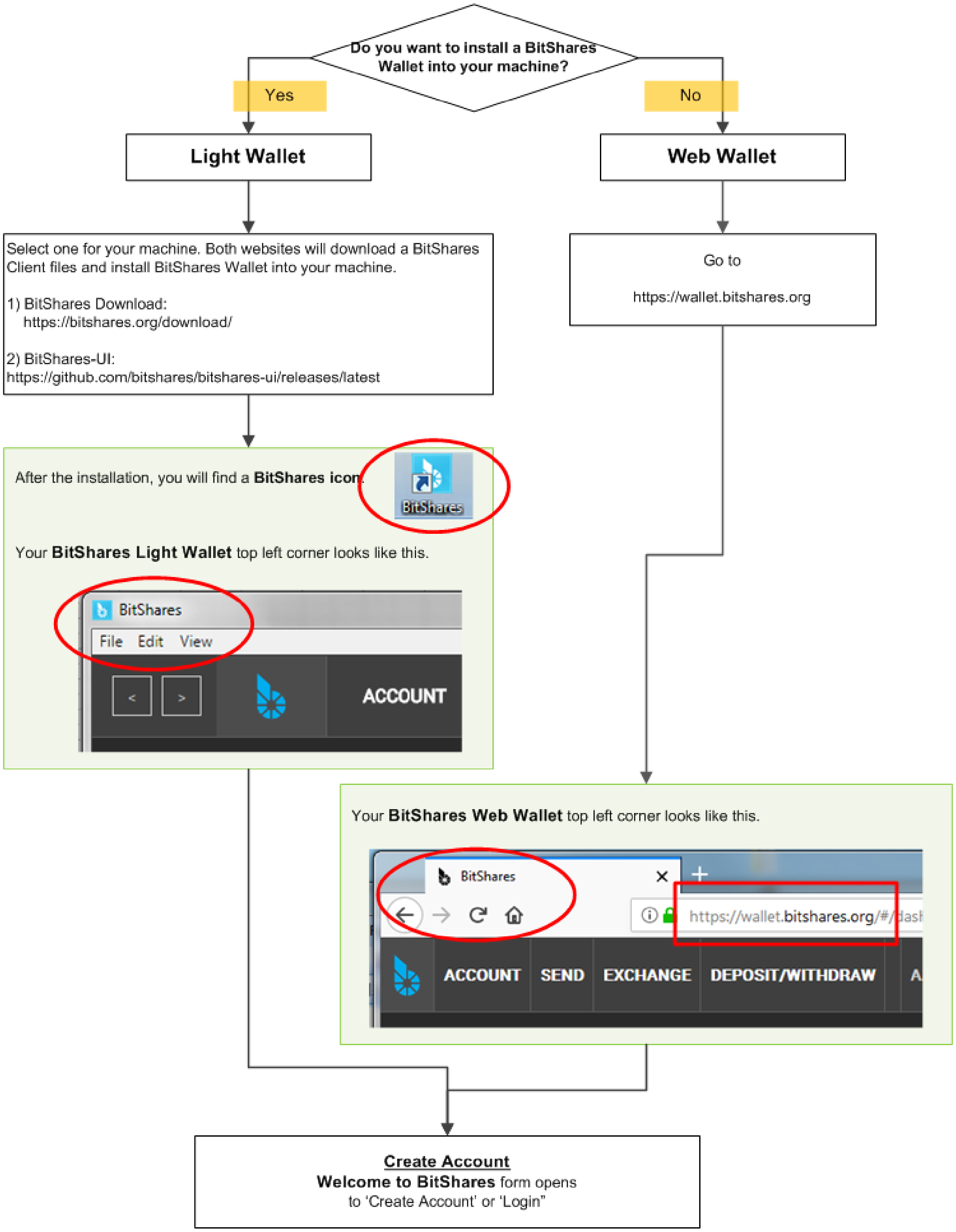
Keys

Keys refer to the cryptography used to secure access to your account and funds. It is of importance to prevent others from gaining access to these keys.

BitShares has *owner, active and memo keys*. And each key has *public key and private key*. It's important to know that Owner permission has administrative powers over the whole account. Active Permission is considered as an "online" permission that allows to access funds and some account settings.

15.2 Light wallet or Web wallet?

Before we create a wallet, let's check what type of wallet you can have as your BitShares wallet. Quick check the below chart.



Select one for your machine. Both websites will download a BitShares Client files and install BitShares Wallet into your machine.

1) BitShares Download:
https://bitshares.org/download/

2) BitShares-UI:
https://github.com/bitshares/bitshares-ui/releases/latest

Go to

https://wallet.bitshares.org

After the installation, you will find a **BitShares icon**.

Your **BitShares Light Wallet** top left corner looks like this.

Your **BitShares Web Wallet** top left corner looks like this.

Create Account
Welcome to BitShares form opens
to 'Create Account' or 'Login"

Did you find out which type of wallet you want to have?

- **If you want to install Light Wallet (BitShares UI), download BitShares UI Releases file and install it to your machine.**

  - *This does not mean you will have a Local wallet.*

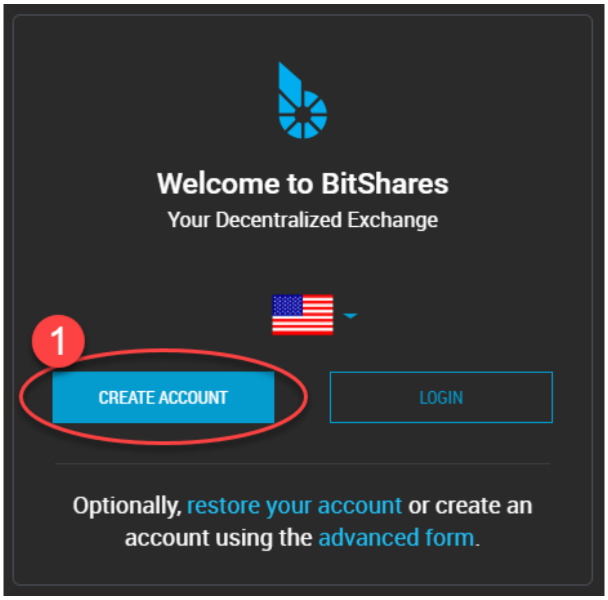
- If you want to use **Web Wallet**, go to this link (https://wallet.bitshares.org).

15.3 Create an Account

In this section, you will create a **Cloud wallet**.

We use the term Cloud Wallet, but technically nothing is stored in the cloud. We call the Cloud Wallet because **you can use your credentials (username and password) from any web browser** at any time to gain access to your account.

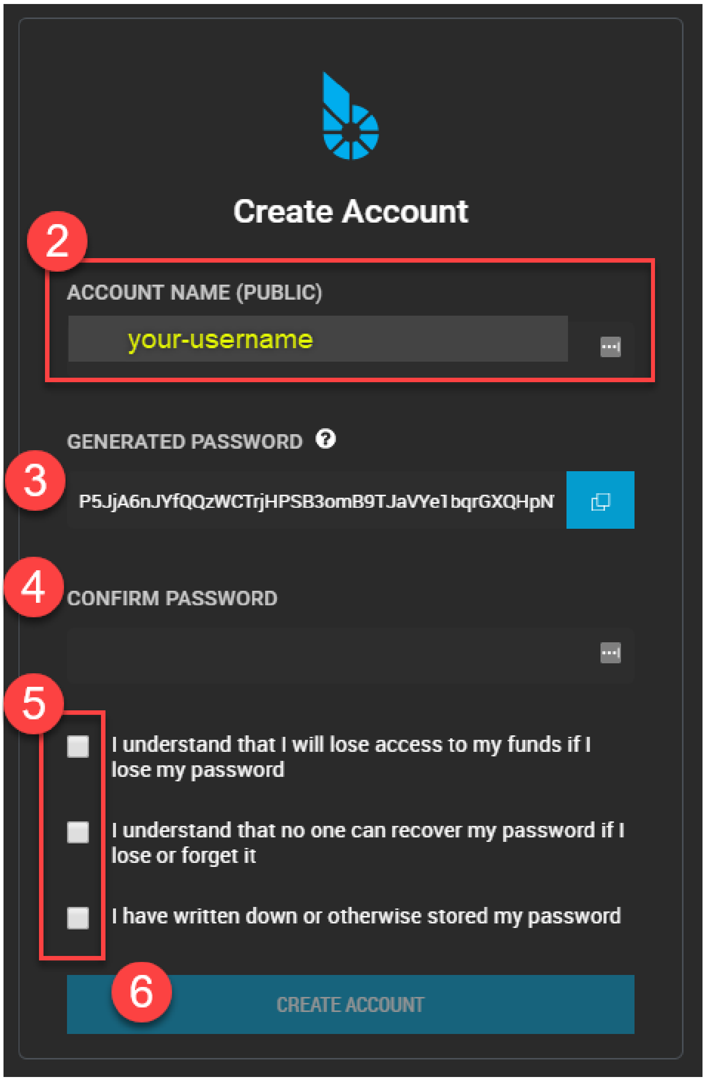
Welcome BitShares - Create Account & Login form



Welcome to BitShares
Your Decentralized Exchange
1
CREATE ACCOUNT
LOGIN
Optionally, restore your account or create an account using the advanced form.

15.3.1 Steps

- 1.Click [**CREATE ACCOUNT**]
- 2.Type in [**ACCOUNT NAME**]. You can create your unique BitShares account name.
- 3.Set a password. Copy and use a **GENERATED PASSWORD**
- 4.Type or paste your password to confirm.
- 5.Check the check boxes. **Make sure you read before you check!**
- 6.Click [**CREATE ACCOUNT**]



Create Account

ACCOUNT NAME (PUBLIC)

your-username

GENERATED PASSWORD

P5JjA6nJYfQQzWCTrjHPSB3omB9TJaVYe1bqrGXQHpN

CONFIRM PASSWORD

□ I understand that I will lose access to my funds if I lose my password

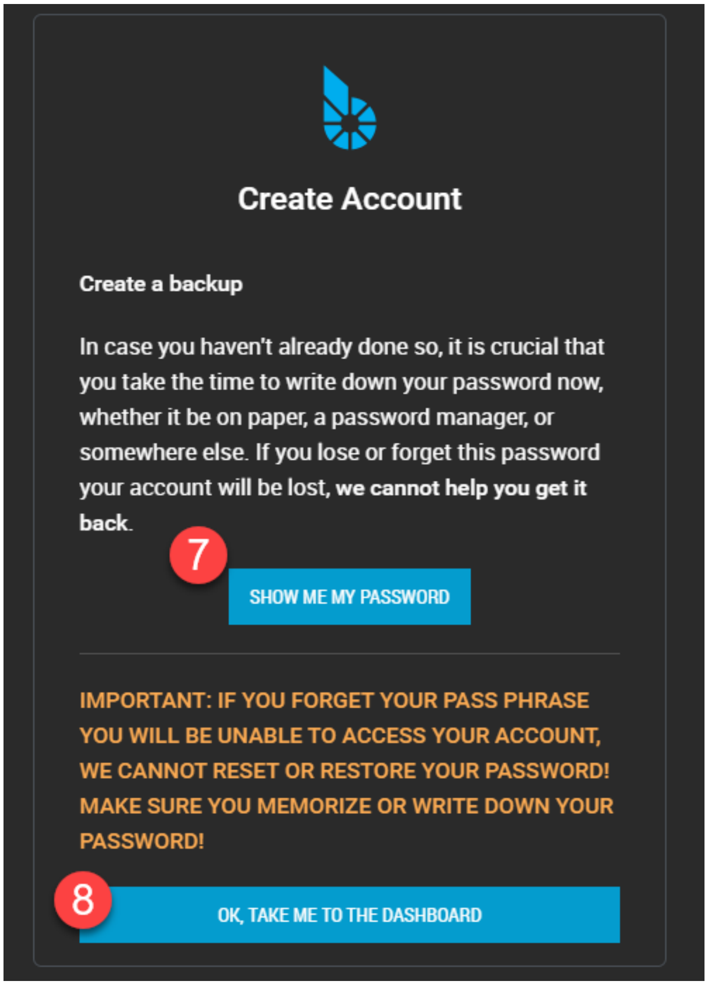
□ I understand that no one can recover my password if I lose or forget it

□ I have written down or otherwise stored my password

Before you submit, check your password one more time if you saved the correct one.

ONLY you can open your wallet again. No one can help. Do not lose it!

- 7.Click **[SHOW ME MY PASSWORD]** and double check if you have a correct password.
- 8.Click [**OK,TAKE ME TO THE DASHBOARD**]



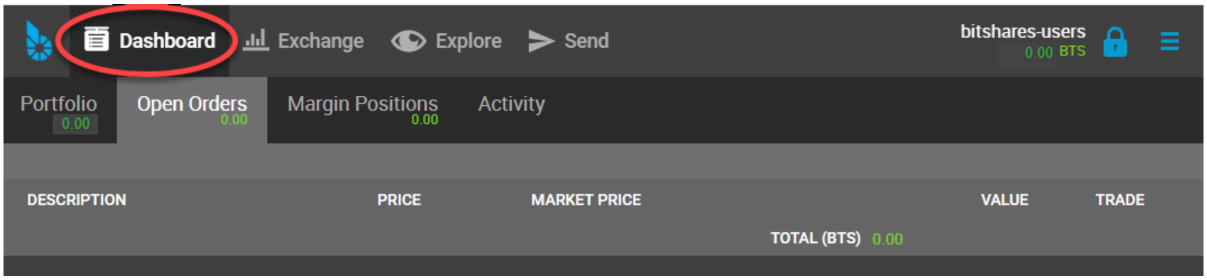
Create Account

Create a backup

In case you haven't already done so, it is crucial that you take the time to write down your password now, whether it be on paper, a password manager, or somewhere else. If you lose or forget this password your account will be lost, **we cannot help you get it back**.

IMPORTANT: IF YOU FORGET YOUR PASS PHRASE YOU WILL BE UNABLE TO ACCESS YOUR ACCOUNT, WE CANNOT RESET OR RESTORE YOUR PASSWORD! MAKE SURE YOU MEMORIZE OR WRITE DOWN YOUR PASSWORD!

- Click the top menu [**Dashbord**] if it did not open.

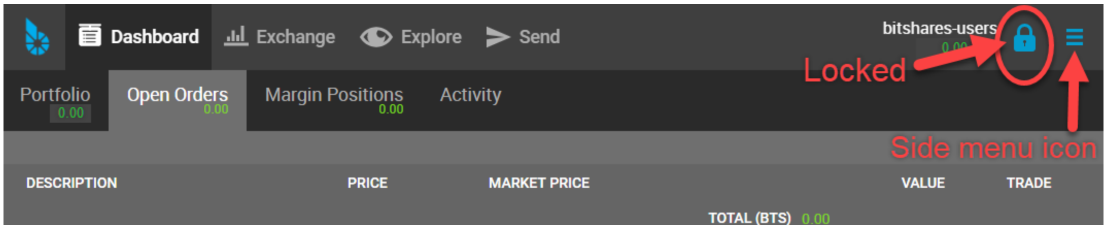


DESCRIPTION	PRICE	MARKET PRICE	VALUE	TRADE
TOTAL (BTS) 0.00				

Now, you have a BitShares **Cloud Wallet**. Before you fund to your account, let's login to make sure if you have a correct password.

15.4 Login

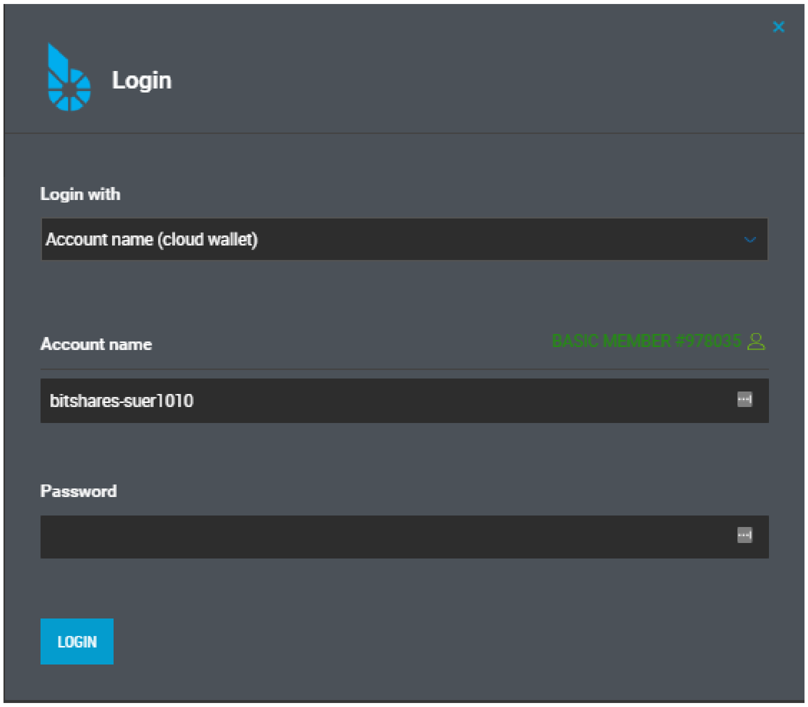
Click a **Locked Key** icon in the top right corner to open a login form.



15.4.1 Cloud Wallet Login form

If you followed the above steps to create a BitShares account, you have a Cloud Wallet as a default wallet.

On the Login form, you can see which wallet Login form for. (i.e., Login with: Account name (cloud wallet))



Login

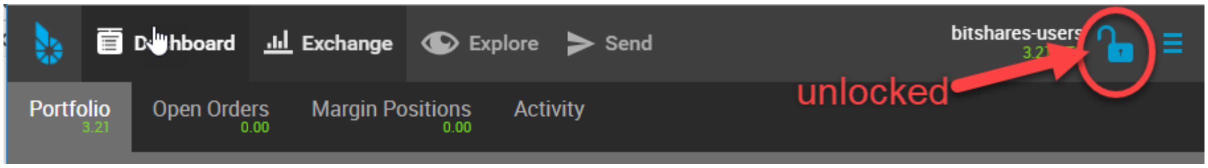
Login with: Account name (cloud wallet)

Account name: bitshares-suer1010

BASIC MEMBER #978035

Password:

If you logged in successfully, you would find a **Unlocked Key**.

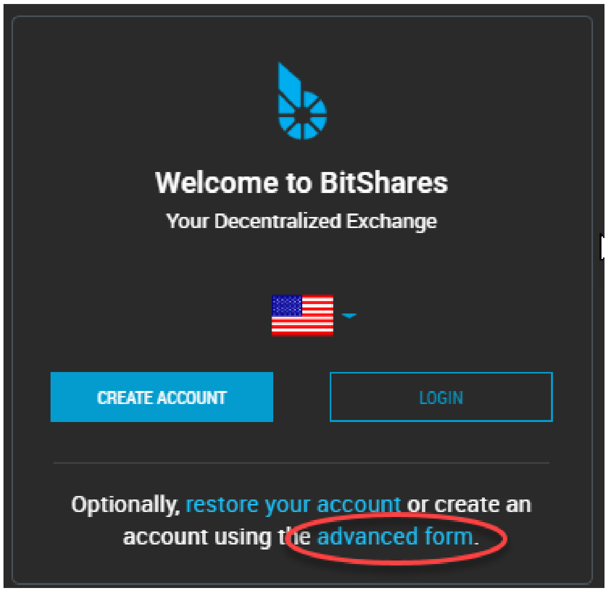


15.5 Advanced: Create an Account

In this section, you will create a **Local Wallet**.

If you have a Cloud Wallet, you can access your wallet from any browsers. However, the Local Wallet, you can only access your funds from **the same computer and web browser** that you have used to register and create your account.

The Local wallet requires you to create **a backup file** to manage your account and funds. The backup file can be used to move



Welcome to BitShares

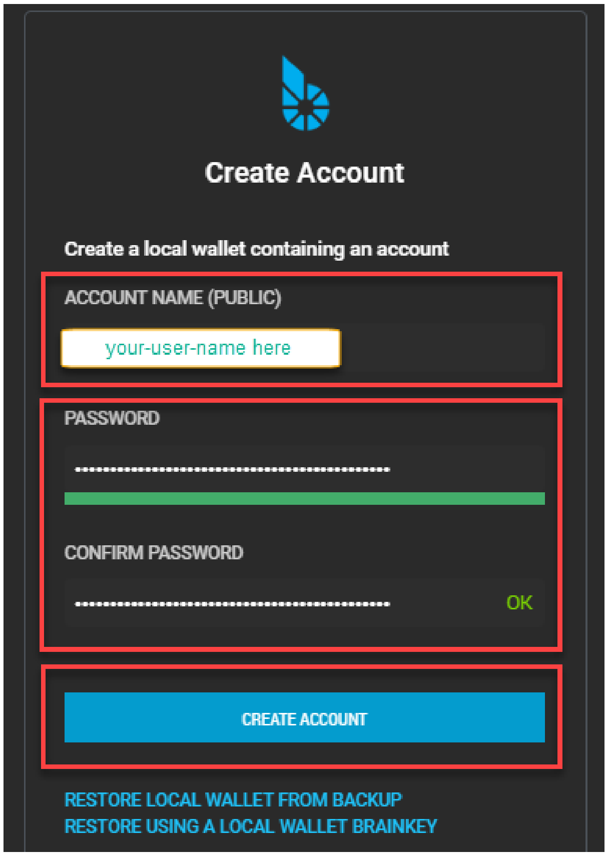
Your Decentralized Exchange

Optionally, restore your account or create an account using the advanced form.

15.5.1 Steps

- 1.Click [**advanced form**]
- 2.Type in [**ACCOUNT NAME**]. You can create your unique BitShares account name.
- 3.Set a password. Create own strong password.
- 4.Type or paste your password to confirm.
- 5.Click [**CREATE ACCOUNT**]

> **If this is yore first account, a faucet will pay the registration fee for you!**



Create Account

Create a local wallet containing an account

ACCOUNT NAME (PUBLIC)

your-user-name here

PASSWORD

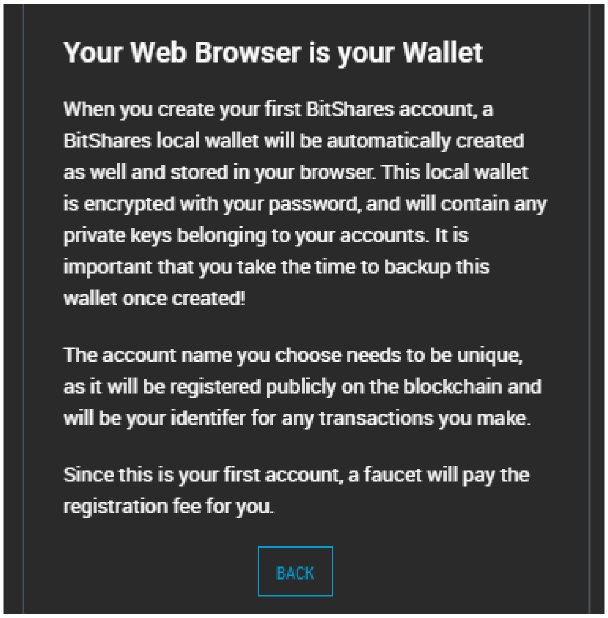
•••

CONFIRM PASSWORD

••• OK

CREATE ACCOUNT
RESTORE LOCAL WALLET FROM BACKUP
RESTORE USING A LOCAL WALLET BRAINKEY

> **Your Web Browser is your Wallet:** Please read the information below.



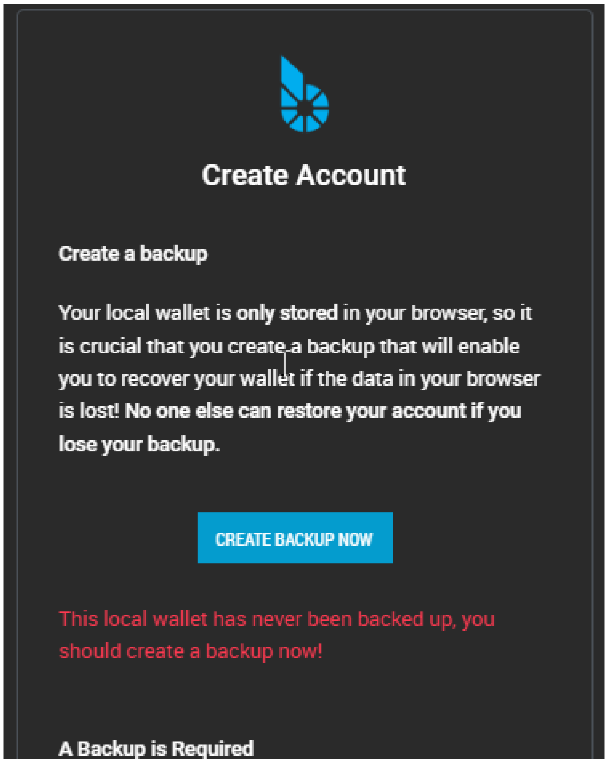
Your Web Browser is your Wallet

When you create your first BitShares account, a BitShares local wallet will be automatically created as well and stored in your browser. This local wallet is encrypted with your password, and will contain any private keys belonging to your accounts. It is important that you take the time to backup this wallet once created!

The account name you choose needs to be unique, as it will be registered publicly on the blockchain and will be your identifer for any transactions you make.

Since this is your first account, a faucet will pay the registration fee for you.

- Click [**CREATE BACKUP NOW**]



Create Account

Create a backup

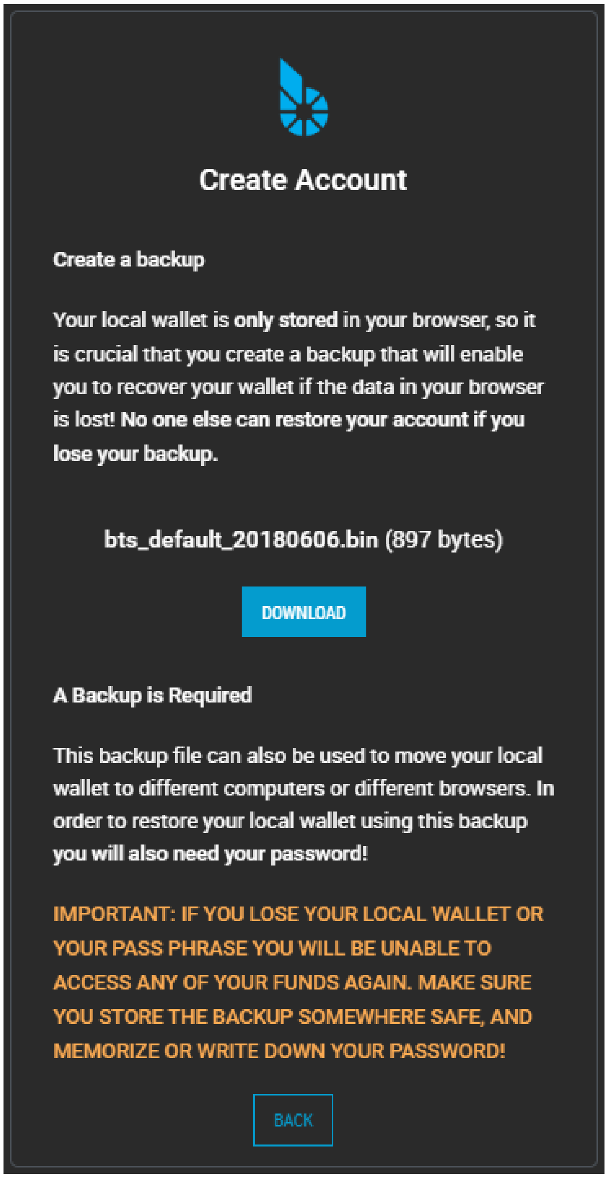
Your local wallet is only stored in your browser, so it is crucial that you create a backup that will enable you to recover your wallet if the data in your browser is lost! No one else can restore your account if you lose your backup.

This local wallet has never been backed up, you should create a backup now!

A Backup is Required

It's extremely important you to create a backup of your account and keep a safe place.

- Click [**DOWNLOAD**] to save a backup (.bin) file.



Create Account

Create a backup

Your local wallet is only stored in your browser, so it is crucial that you create a backup that will enable you to recover your wallet if the data in your browser is lost! No one else can restore your account if you lose your backup.

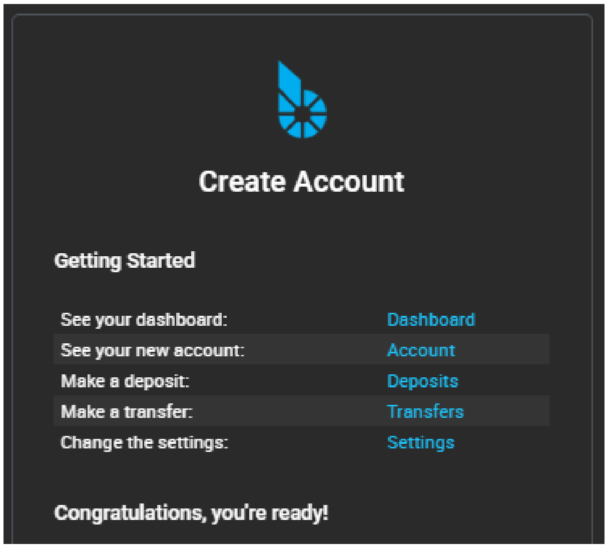
bts_default_20180606.bin (897 bytes)

A Backup is Required

This backup file can also be used to move your local wallet to different computers or different browsers. In order to restore your local wallet using this backup you will also need your password!

IMPORTANT: IF YOU LOSE YOUR LOCAL WALLET OR YOUR PASS PHRASE YOU WILL BE UNABLE TO ACCESS ANY OF YOUR FUNDS AGAIN. MAKE SURE YOU STORE THE BACKUP SOMEWHERE SAFE, AND MEMORIZE OR WRITE DOWN YOUR PASSWORD!

Congratulation, you’re ready!



Create Account

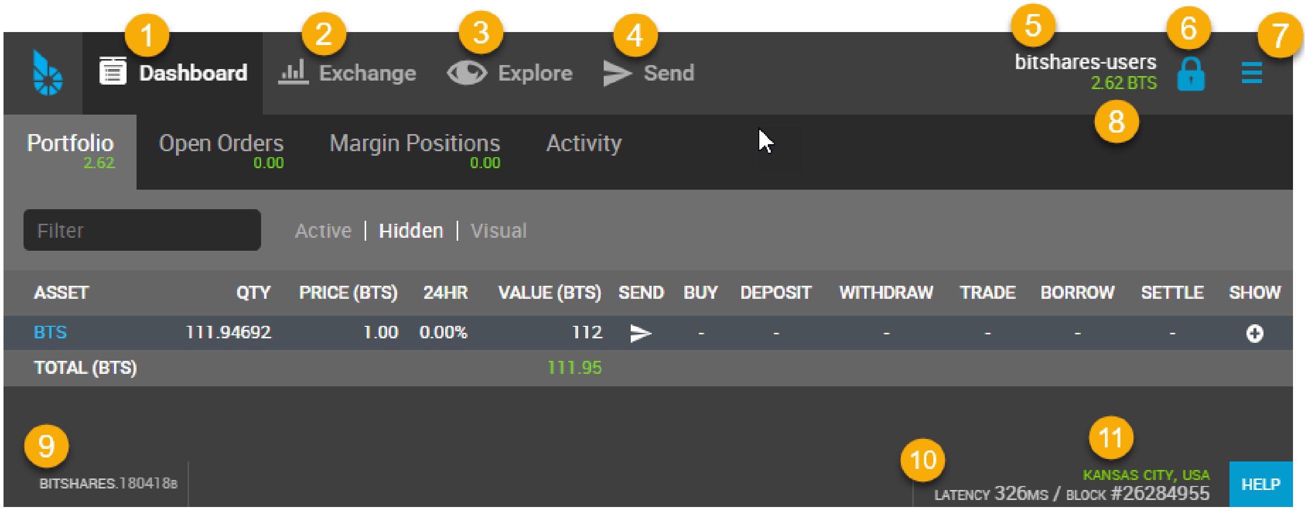
Getting Started

See your dashboard:	Dashboard
See your new account:	Account
Make a deposit:	Deposits
Make a transfer:	Transfers
Change the settings:	Settings

Congratulations, you're ready!

15.6 BitShares Wallet Features

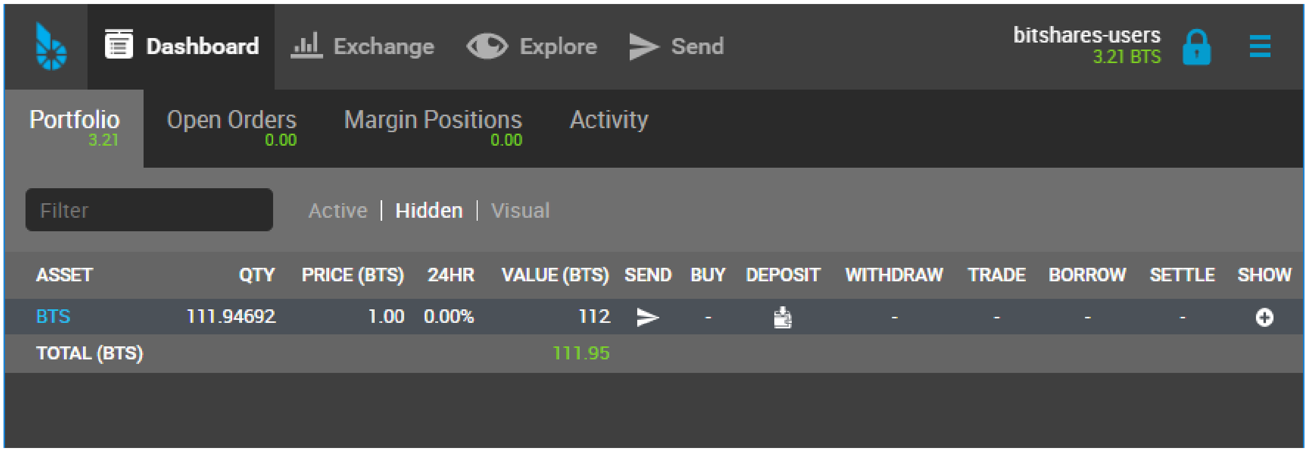
15.6.1 Quick Review Wallet Options



ASSET	QTY	PRICE (BTS)	24HR	VALUE (BTS)	SEND	BUY	DEPOSIT	WITHDRAW	TRADE	BORROW	SETTLE	SHOW
BTS	111.94692	1.00	0.00%	112	➤	-	-	-	-	-	-	⊕
TOTAL (BTS)				111.95								

	Item name	note
1	Dashboard	The Wallet Portfolio, Open Orders, Margin Positions, and Activity information
2	Exchange	BitShares Exchange, Trading information
3	Explore	BitShares Live Blockchain, Assets, Accounts, Witnesses members, Committee members, Markets, and Fee Schedule
4	Send	Opens a Send form. You can send funds to other BitShares Account Holders
5	A BitShares account name	A account name that the data shows on a Dashboard page
6	Key icon	By click, opens a login form. Locked/Unlocked Key icon shows if you've logged in the account currently
7	Side Menu icon	Side Menu icon opens the wallet other menus in a dropdown list
8	Asset Total	Currently showing in a Dashboard Total Assets
9	BitShares Wallet Version	The Release Version of BitShares UI Wallet
10	Latency	The delay of Network connection
11	Server Node name	A server node name that you are connecting

Dashboard

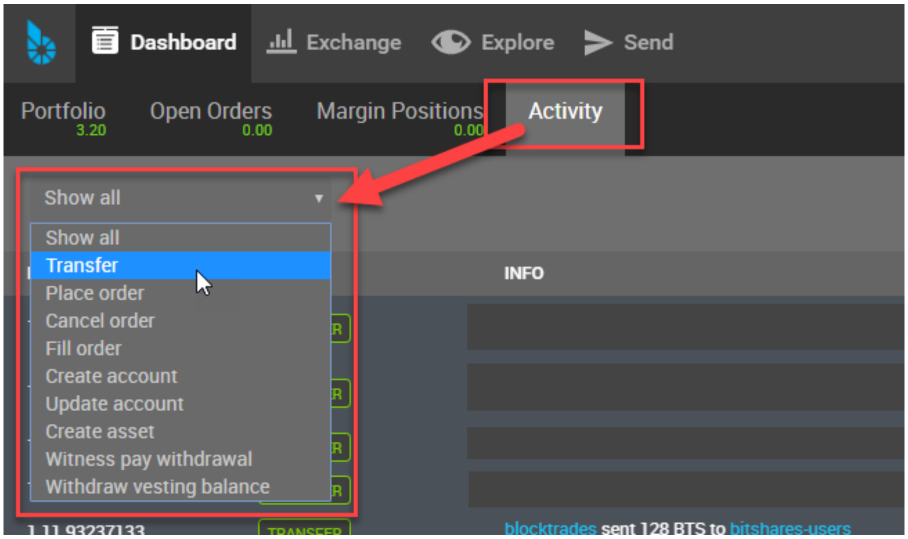


ASSET	QTY	PRICE (BTS)	24HR	VALUE (BTS)	SEND	BUY	DEPOSIT	WITHDRAW	TRADE	BORROW	SETTLE	SHOW
BTS	111.94692	1.00	0.00%	112	➤	-		-	-	-	-	⊕
TOTAL (BTS)				111.95								

Dashboard Tabs

Tab name	note
Portfolio	Your Assets list. You can filter the assets and hide some assets if you don't need to watch.
Open Orders	
Margin Positions	
Activity	Show your all transactions. (i.e., The below shows a type of transactions to choose from.)

Activity - Filters



blocktrades sent 128 BTS to bitshares-users

Side Menus - Dropdown items

option	
login	By click, opens a login form.
Create Account	Users who have a lifetime membership (LTM) can register multiple accounts in parallel;
	all of them are stored in a single wallet
Send(legacy)	Transfer details (Original page). **Send** on the top menu is new form.
Deposit	Deposit funds from other parties (Original Deposit page)
Deposit(beta)	Select an asset you want to deposit and provide you a sending address, Gateway, identicon, and notes.
Withdraw	(Original Withdraw page)
Withdraw(beta)	Search an asset to withdraw
Settings	You can manage your wallet appearance and other settings.
	Settings - CLOUD Wallet Login Mode:
	• General • Accounts • Restore/Import • Nodes • Faucet • Reset settings
	Settings - LOCAL Wallet Login Mode:
	• General • Local Wallet • Accounts • Password • Backup • Restore/Import • Access • Faucet
News	BitShares Blockchain Foundation and other News
Help	Open a Help page
Voting	You can vote for Witnesses, Committee or Workers. Or you can set a Proxy to case a vote.
	Voting is important: in Bitshares in the same way it is important to the community in which you live. The weight of your vote is directly correlated to the number of BTS you own.
	If you aren't heavily involved in the community, you are encouraged to choose a proxy who represents your interests.
Asset	Issued Assets
Signed Message	
Membership stats	Basic Member is a default membership. You can upgrade to Lifetime Membership here.
Vesting balances	Vesting balances contain any fees earned through the referral program or from worker pay,
	For example. They have a tain vesting period and are continually unlocked during that vesting period until all of the balances are available
Whitelist	You can set Whitelist and/or Blicklist. Also, you can view 'Whitelisted by' and 'Blacklisted by'.

CHAPTER 16

BitShares Client and Login Mode

Table of Contents

16.1 BitShares Client

You have sole control of your accounts and funds and they are created on your computer (within the light-client or the browser web-client).

- If you created a **Clout wallet**, you will be able to access to your wallet by using your credentials (username and password) from any browser or computers. You do not need to worry about a backup files. (*You do not have the functionality.*)
- If you created a **Local wallet**, you will be able to access your account **only** on the computer that you have used to register and create your account. If you have created a backup file, you can import it and restore your wallet somewhere else.

16.1.1 Light Client

Download client files and install BitShares Wallet to your computer.

> Note: This download does not mean that you will have a Local wallet.

- Download the Official Light Client
- BitShares-UI – Latest Release

BitShares-UI: This is a web application and runs in a browser. A connection is established to a trusted node in the network that serves as a gateway to the rest of the ecosystem.

16.1.2 Web Client

Access the network and open the wallet in the browsers via one of our partners.

- wallet.bitshares.org https://wallet.bitshares.org
- (more. . .)

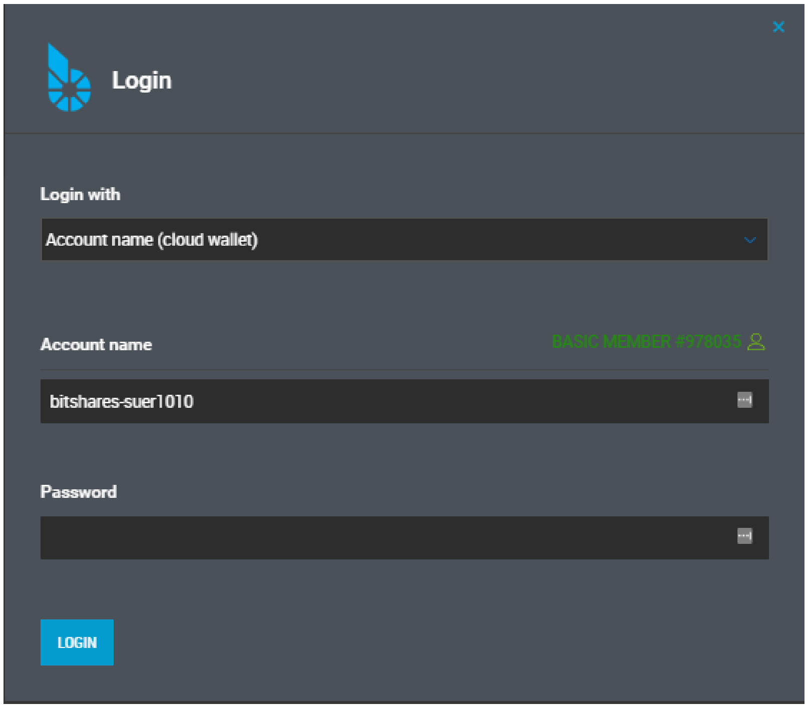
16.2 Login Forms

16.2.1 Cloud Wallet Login

The cloud wallet only allows for a single account to be accessed at a time. This wallet is generally the correct choice for a new user.

Login Form

You login with your account name and your password. The login form shows which type of wallet you login to. (i.e., Login with: **Account name (cloud wallet)**)



Login

Login with

Account name (cloud wallet)

Account name

BASIC MEMBER #978035

bitshares-suer1010

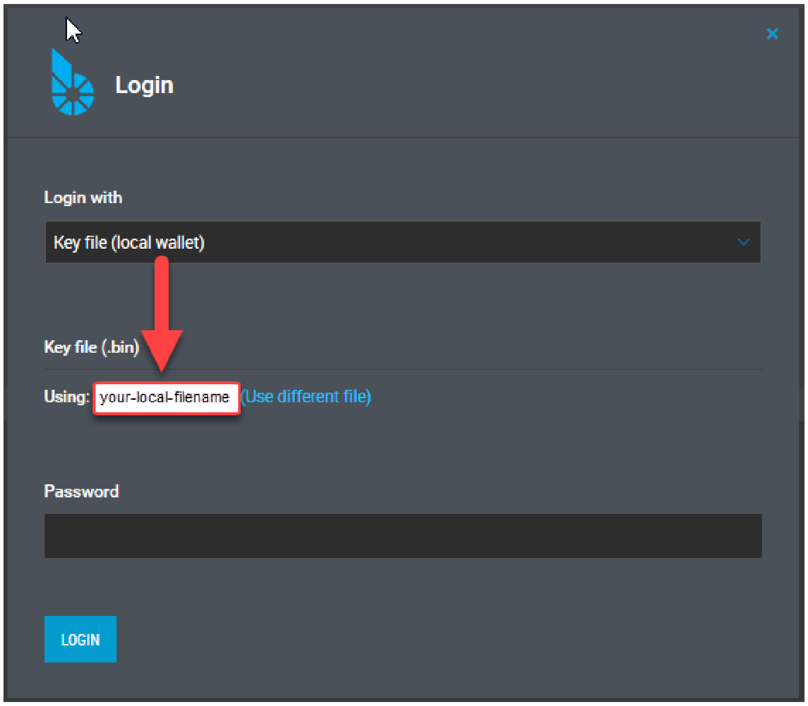
Password

16.2.2 Local Wallet Login

A Big difference between a Cloud wallet and a Local wallet is the local wallet creates a database within your browser. This means that access to your funds is tied to the browser only. If you attempt to access your local wallet from any other computer, or any other browser, it will fail unless you actively import your backup file from the original browser backup file.

Login Form

You select your Local wallet backup file name and type your password to login a Local wallet. The **Key file(.bin)** should be your wallet backup file name. The backup file contains all your keys information.



Login with

Key file (local wallet)

Key file (.bin)

Using: your-local-filename (Use different file)

Password

16.3 Summary

The difference between a Cloud wallet and a Local Wallet.

16.3.1 Cloud Wallet

- BitShare UI wallet will create a **Cloud wallet** as a default wallet. (i.e., [CREATE ACCOUNT])
- The Cloud wallet allows you to login from any web browser at any time to gain access to your account by using your credentials (username and password).
- The Cloud wallet only allows for a single account to be accessed at a time.
- If you have a Cloud wallet, you don't need to worry about a backup. (*You don't have the functionality in the Cloud wallet*).
- **You can switch the INTERFACE by using the [Settings] - [General] - [Login Mode], however your account won't switch, only the *interface* switches.**
- **Even you import Private keys (was in the Cloud wallet) to the Local wallet, you do not have a brain key to associate with the Private keys you imported. Therefor, a brainkey restore won't find those Private keys. (In this case, no meaning to do a brainkey backup and restore.)**
- **The Cloud wallet has no brainkey.** The password is basically the equivalent of the brainkey, but it's only used for that one account.

16.3.2 Local Wallet

- **If you know you want to have a Local wallet, use an [advanced form] link on the Welcome to BitShares form and create a backup file. This is the only way to create a Local wallet.**
- The Local wallet creates a correct pair of keys (a brainkey and private keys) and save the information to your browser.
- The Local wallet creates a database with in your browser. This means that you can only access your funds from the same computer and web browser that you have used to register and create your account. If you attempt to access your local wallet from any other computer, or any other browser, it will fail unless you actively import your backup file from the original browser backup file.
- You have to create a backup files to manage the Cloud wallet account.
- The Cloud wallet has Backup options. Go to [Settings] - [Backup] to find. - **Create local wallet backup** : create a Binary File (.bin) backup. - **Create brainkey backup** : give you long random phrases. You need to write down and keep it in a safe place.
- The backup files can be used to move your local wallet to different computers or different browsers. In order to restore your local wallet you will need the backup file and your password! Therefor, it's extremely important you create a backup and keep a safe place.

16.3.3 Settings - LOGIN MODE

Users often misunderstand about this feature.

This setting feature allows you to select the LOGIN MODE. You can just switch the *interface*. You are **not** switching your account from one to another.

Go to [Settings] - [General] - **LOGIN MODE** to find the feature.

> This feature only switch the *interface*! Not your account self.

16.4 Frequently asked Questions

- **Can I switch (by changing the Wallet Mode or importing private keys) my Cloud wallet to a Local wallet?**
  - No. Your account won't switch, only the *interface* switches.
- **I have a Cloud wallet. Can I have a Local wallet?**
  - Yes. But you will have to create new account for the Local wallet.
- **How can I move my funds from a Cloud wallet to a Local wallet?**
  - We mentioned before. You have to create new account for the Local wallet. You can create the Local wallet by using an [**advanced form**] link on Welcome to BitShares form. After you created new Local wallet, send your funds from your old account (Cloud wallet) to new account (Local wallet). And create a backup!!
- **I have a Cloud wallet. Do I have to save my private keys information somewhere?**
  - Not necessary. Because the Could wallet always do it for extra security. Also lets you login without exposing your owner key, you can login using only the active key.

- **Can I change a Cloud wallet password?**
  - Yes.
  - Go to How to change a password if using a Cloud Wallet : from BitShares UI wiki
- **Can I change a Local wallet password?**
  - Yes.
  - Go to [**Settings**] - [**Password**] - Change your password. Use this page

.

- **There is [Create Account] in a Side navigation menu. Can I create and add new account in the same wallet I logged in?**
  - Yes. However, the account you logged in must have a LifeTime Membership (LTM) stats.

CHAPTER 17

Backups and Restore your Wallet

Table of Contents

> If you use a Cloud Wallet, you do not need to create a backup. **You do not have the option also.**

17.1 Create Local Wallet Backup

It is recommended to make regular backups of your Local wallet. Please note that in order to recover from a backup you will also need to provide the passphrase (password) because backups are encrypted. If you lose your wallet backup file or your passphrase, you will not be able to access any of your funds again.

You are the only individual that has access to your account and funds, it is your responsibility to make a secure backup of your registered Local wallet account.

17.1.1 Backup Types

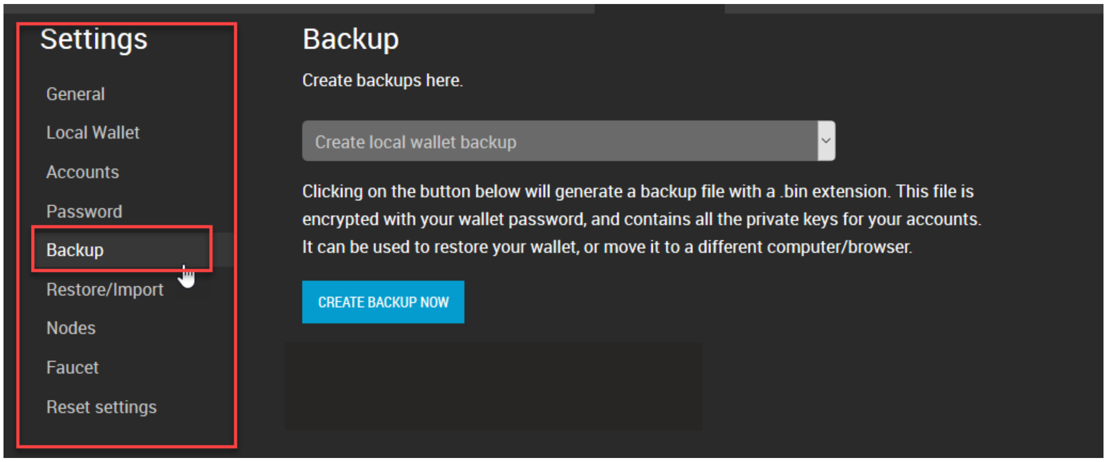
There are three types of backups.

type	
Create local wallet backup	create a Binary File (.bin)
Create brainkey backup	give you long random phrases. You need to write down.
Create favorites backup	

17.1.2 How to Create a backup (.bin) file

1. Open a Side menu and select [**Settings**]
2. In [**Settings**], select [**Backup**].
3. Make sure the backup type is *Create local wallet backup*
4. Click [**CREATE BACKUP NOW**]
5. Check your backup file name (e.g. bts_somrthing_20180420.bin)
6. Click [**DOWNLOAD**]

Store this backup in at least two secure locations only accessible by you

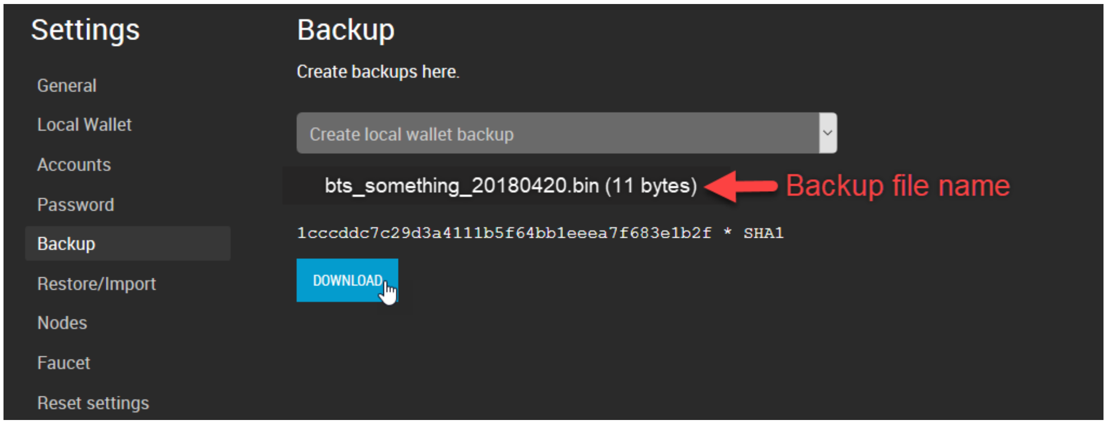


Backup

Create backups here.

Create local wallet backup

Clicking on the button below will generate a backup file with a .bin extension. This file is encrypted with your wallet password, and contains all the private keys for your accounts. It can be used to restore your wallet, or move it to a different computer/browser.



bts_something_20180420.bin (11 bytes)

1cccddc7c29d3a4111b5f64bb1eeea7f683e1b2f * SHA1

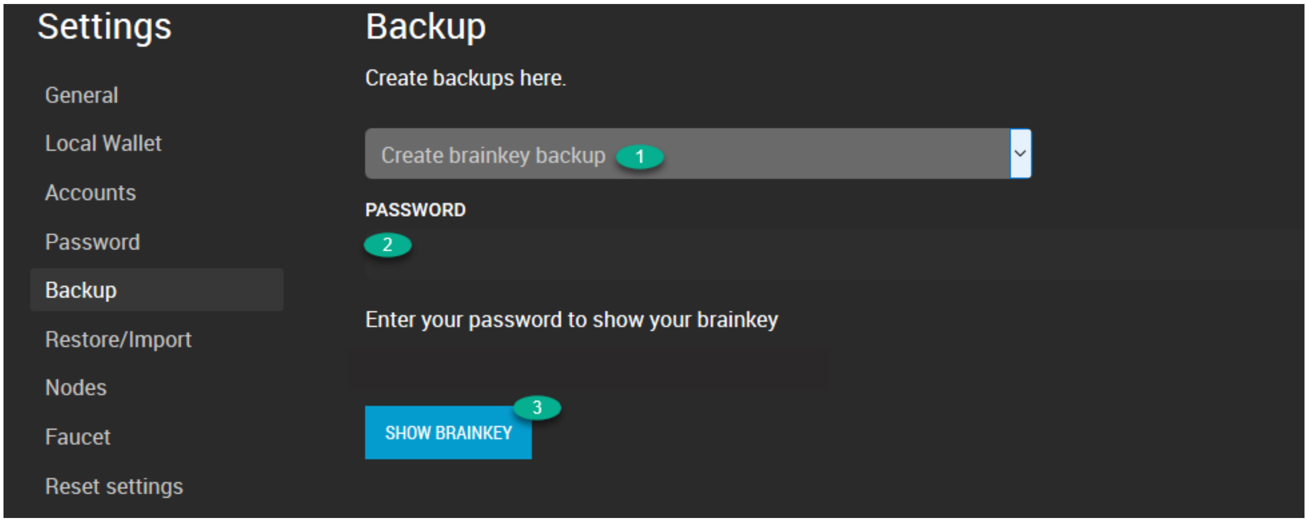
17.1.3 About the Brain Key

The brain key is used as source for all cryptographic keys generated in the wallet. If you have it secured, you will be able to regain access to your accounts and funds (unless the access keys have been changed)

17.1.4 How to Create a Brainkey backup (Advanced User Only)

1. Open a Side menu and select [**Settings**]
2. In [**Settings**], select [**Backup**].
3. (#1) Make sure the backup type is *Create brainkey backup*
4. (#2) Type in a password
5. (#3) Click [**SHOW BRAINKEY**]
6. (#4) Write down *Brainkey* (i.g. very random long phrases)
7. (#5) Click [**I'VE WRITTEN IT DOWN**]

Write it down!! Anyone with access to your recovery key will have access to funds with in the local wallet.



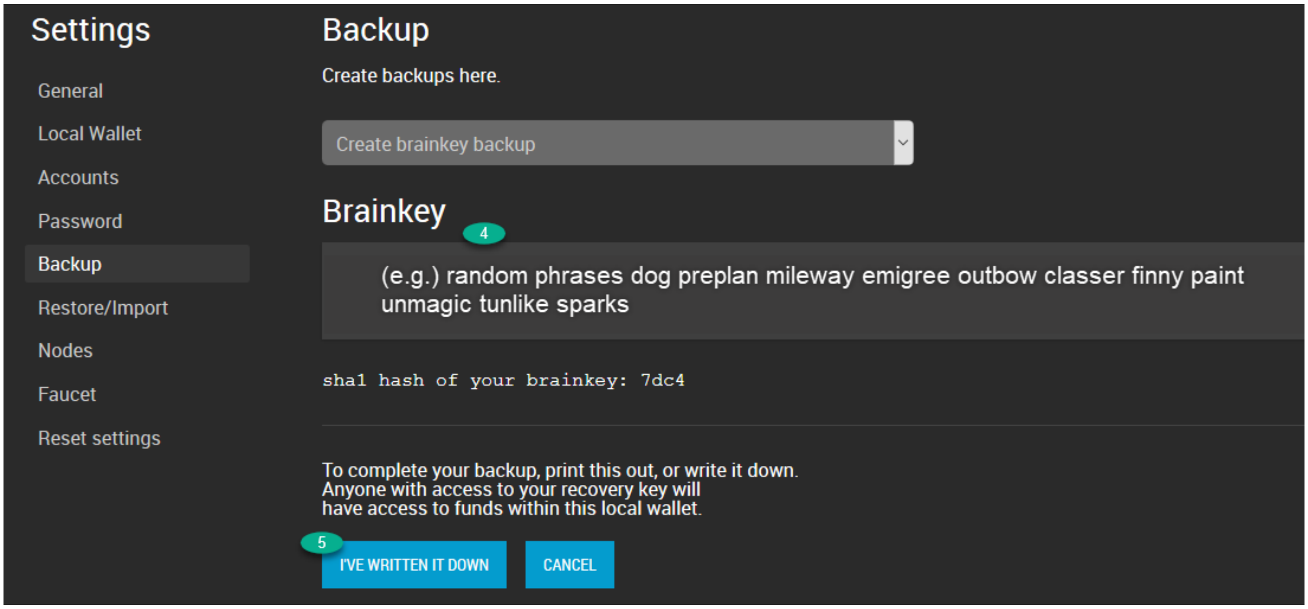
Backup

Create backups here.

Create brainkey backup

PASSWORD

Enter your password to show your brainkey



Backup

Create backups here.

Create brainkey backup

Brainkey

(e.g.) random phrases dog preplan mileway emigree outbow classer finny paint unmagic tunlike sparks

```
sha1 hash of your brainkey: 7dc4
```

To complete your backup, print this out, or write it down.
Anyone with access to your recovery key will
have access to funds within this local wallet.

17.2 Restore / Import

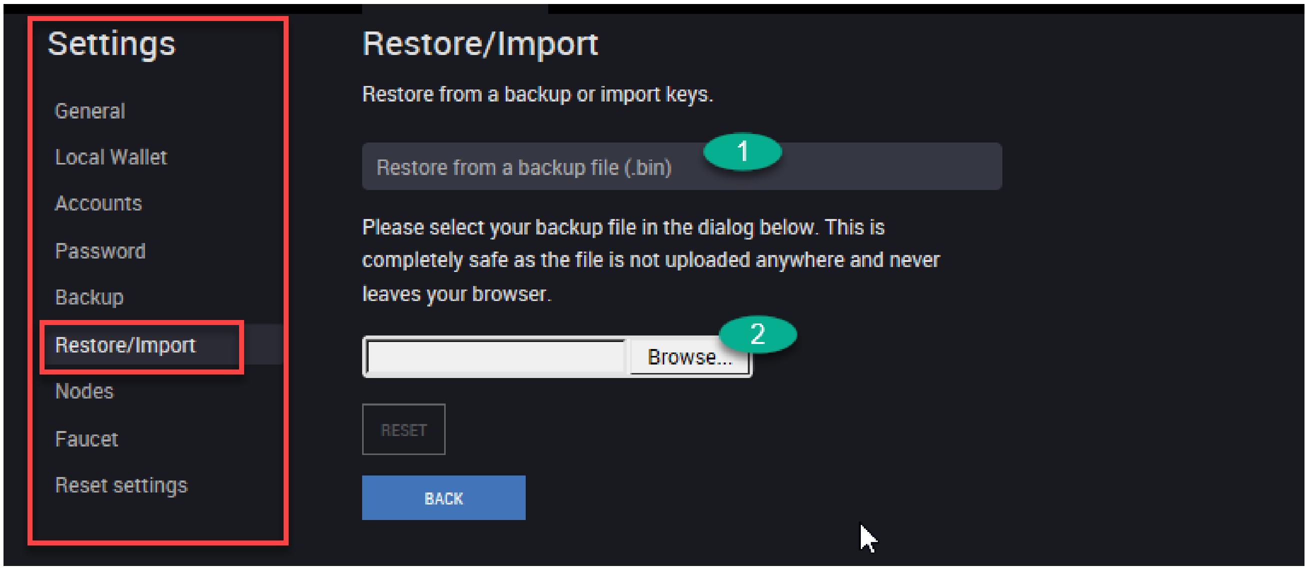
We assume you have created a backup file (.bin) and use a Local wallet.

17.2.1 Restore / Import Options

option	
Restore from a backup file (.bin)	restore from a backup file and a password
Import a private key	import Private keys to a Local wallet. The imported keys will be saved in the bin file. If this happens, you cannot rely on the brainkey for backup after that.
Import a BTS 0.9.3c key export file (.json)	
Restore using a local wallet brainkey	use a password and a Brain key
Restore favorites using a json file	

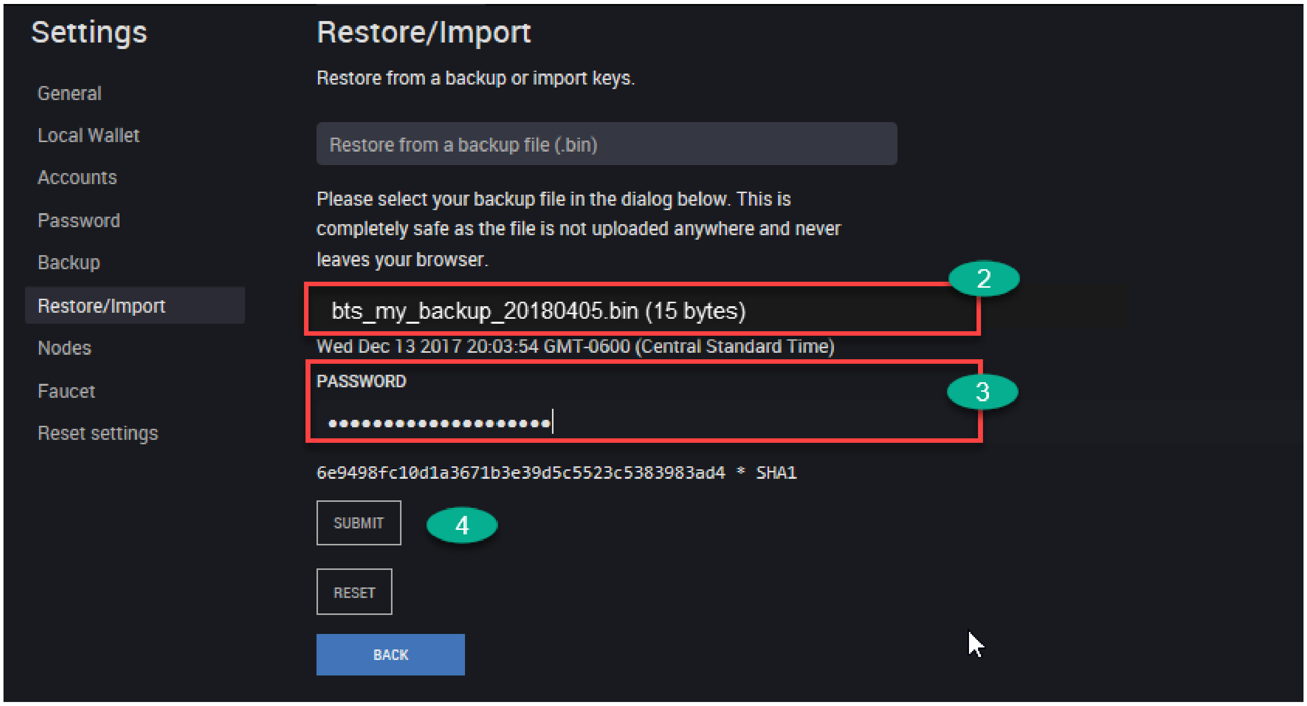
17.2.2 How to Restore from a backup (.bin) file

1. Open a Side menu and select [**Settings**]
2. In [**Settings**], select [**Restore/Import**].
3. (#1) Make sure you selected *Restore from a backup file (.bin)*
4. (#2) Click [**Browse…**] to find a backup file.



Restore from a backup or import keys.

Please select your backup file in the dialog below. This is completely safe as the file is not uploaded anywhere and never leaves your browser.



Restore/Import

Restore from a backup or import keys.

Please select your backup file in the dialog below. This is completely safe as the file is not uploaded anywhere and never leaves your browser.

bts_my_backup_20180405.bin (15 bytes)

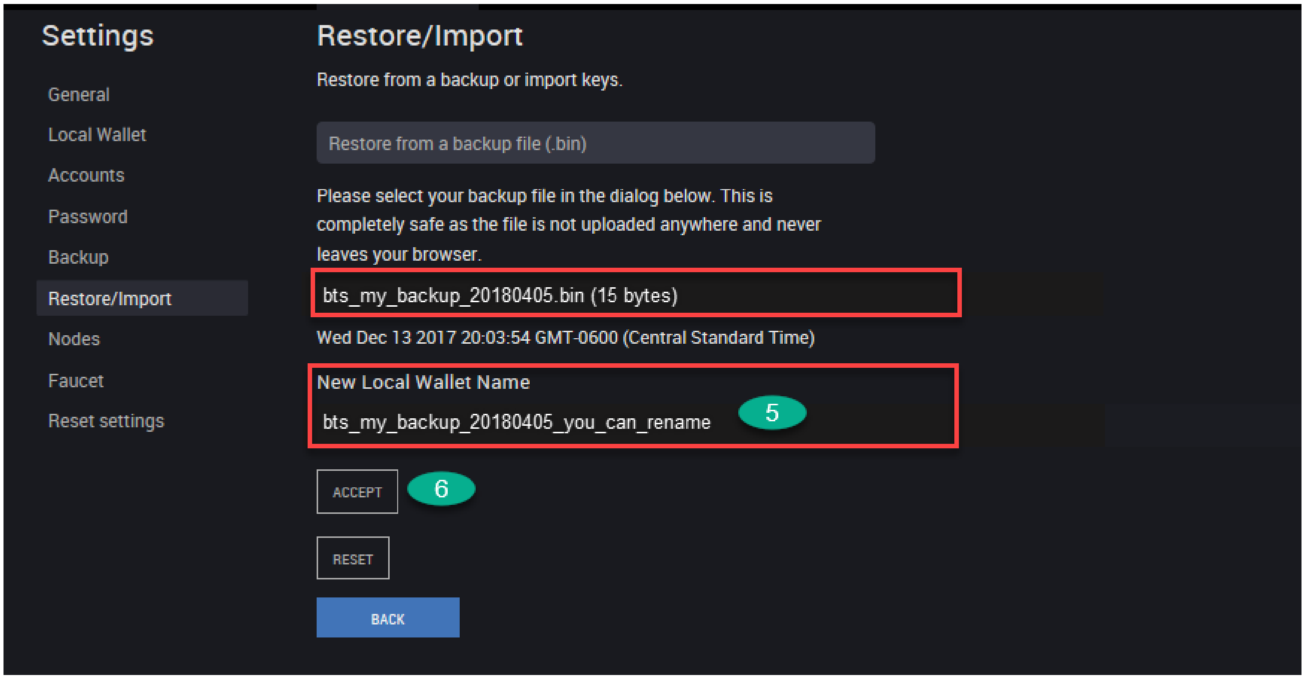
Wed Dec 13 2017 20:03:54 GMT-0600 (Central Standard Time)

PASSWORD

•••••••••••••••••••

6e9498fc10d1a3671b3e39d5c5523c5383983ad4 * SHA1

5. (#3) Type in a password
6. (#4) Click [**SUBMIT**]



Restore/Import

Restore from a backup or import keys.

Please select your backup file in the dialog below. This is completely safe as the file is not uploaded anywhere and never leaves your browser.

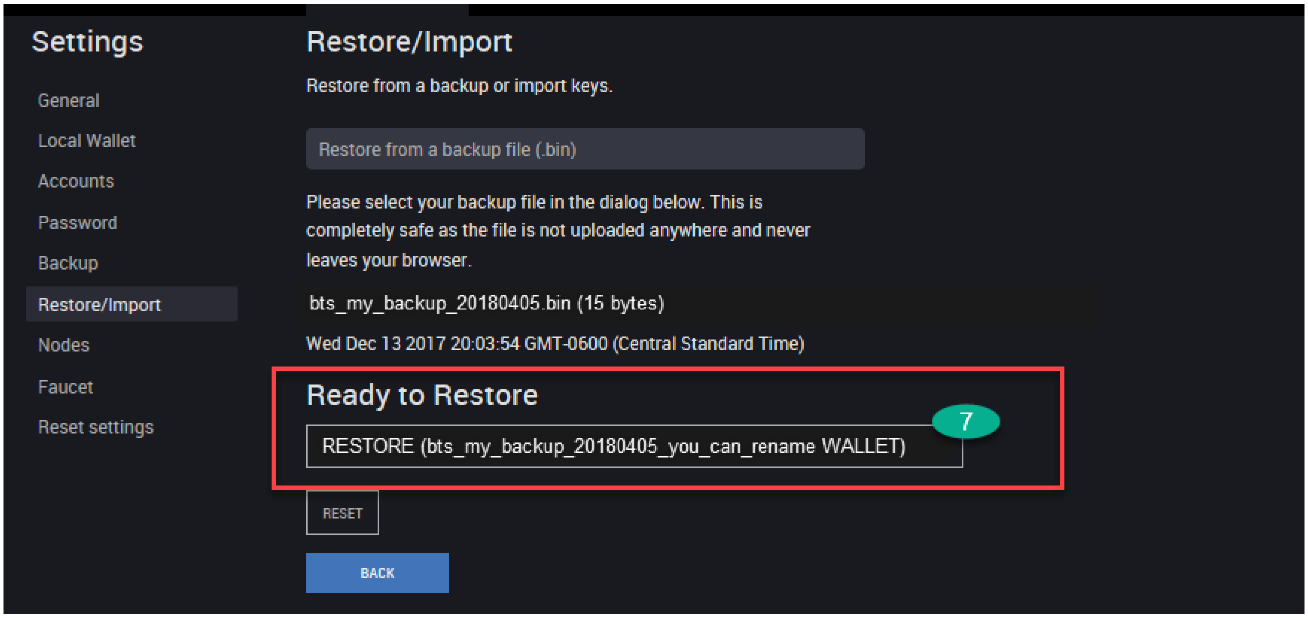
bts_my_backup_20180405.bin (15 bytes)

Wed Dec 13 2017 20:03:54 GMT-0600 (Central Standard Time)

New Local Wallet Name

bts_my_backup_20180405_you_can_rename

7. (#5) Type in *New Local Wallet Name* if you want to change the backup file name.
8. (#6) Click [**ACCEPT**]
9. (#7) **Ready to Restore** - below “RESTORE(. . . .. WALLET)” is a button. Click it.
10. You will find “Successfully restored (. . . .)wallet. Done!!
11. (#8) Click [**DASHBOARD**]



Restore/Import

Restore from a backup or import keys.

Restore from a backup file (.bin)

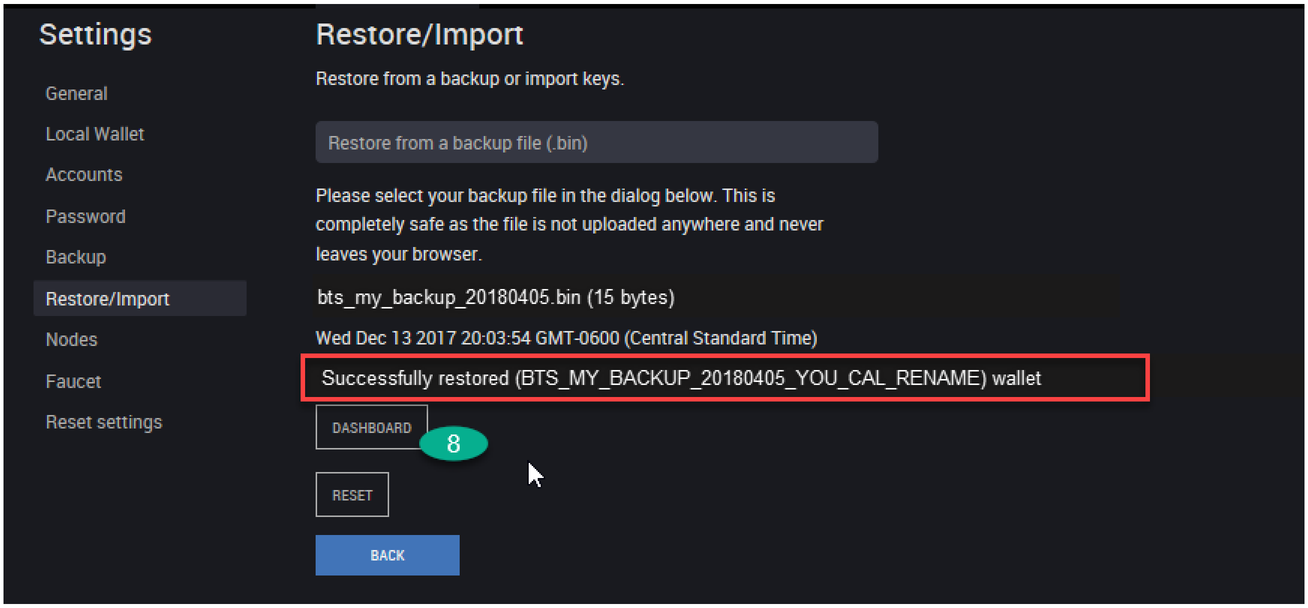
Please select your backup file in the dialog below. This is completely safe as the file is not uploaded anywhere and never leaves your browser.

bts_my_backup_20180405.bin (15 bytes)

Wed Dec 13 2017 20:03:54 GMT-0600 (Central Standard Time)

Ready to Restore

RESTORE (bts_my_backup_20180405_you_can_rename WALLET)



Restore/Import

Restore from a backup or import keys.

Restore from a backup file (.bin)

Please select your backup file in the dialog below. This is completely safe as the file is not uploaded anywhere and never leaves your browser.

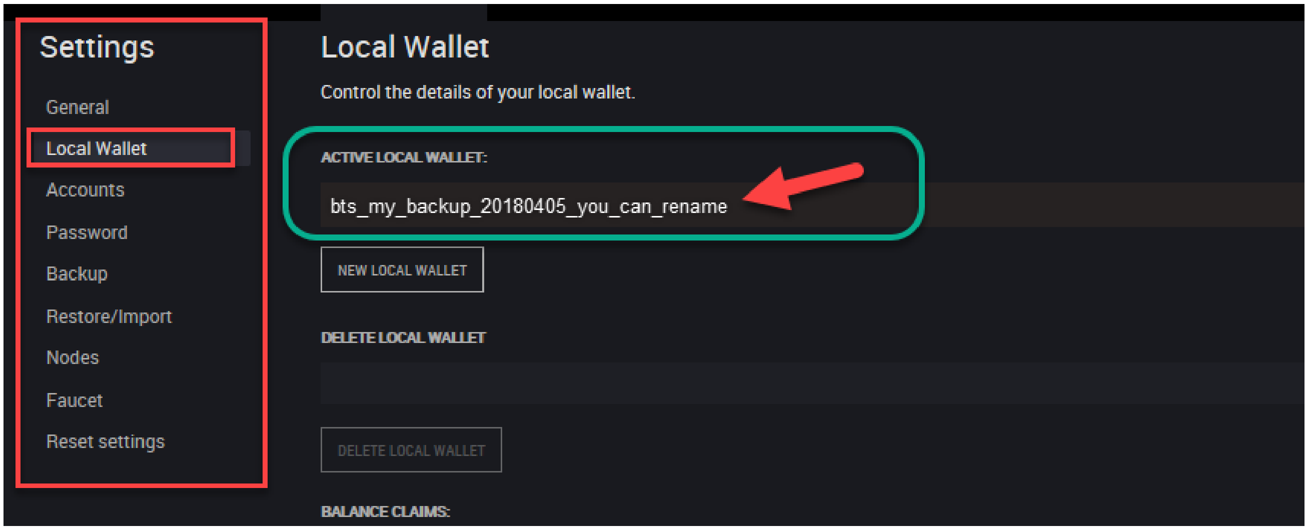
bts_my_backup_20180405.bin (15 bytes)

Wed Dec 13 2017 20:03:54 GMT-0600 (Central Standard Time)

Successfully restored (BTS_MY_BACKUP_20180405_YOU_CAL_RENAME) wallet

17.2.3 How to Check Active Local Wallet backup file name

- [**Settings**] - [**Local Wallet**] - Active Local Wallet



Local Wallet

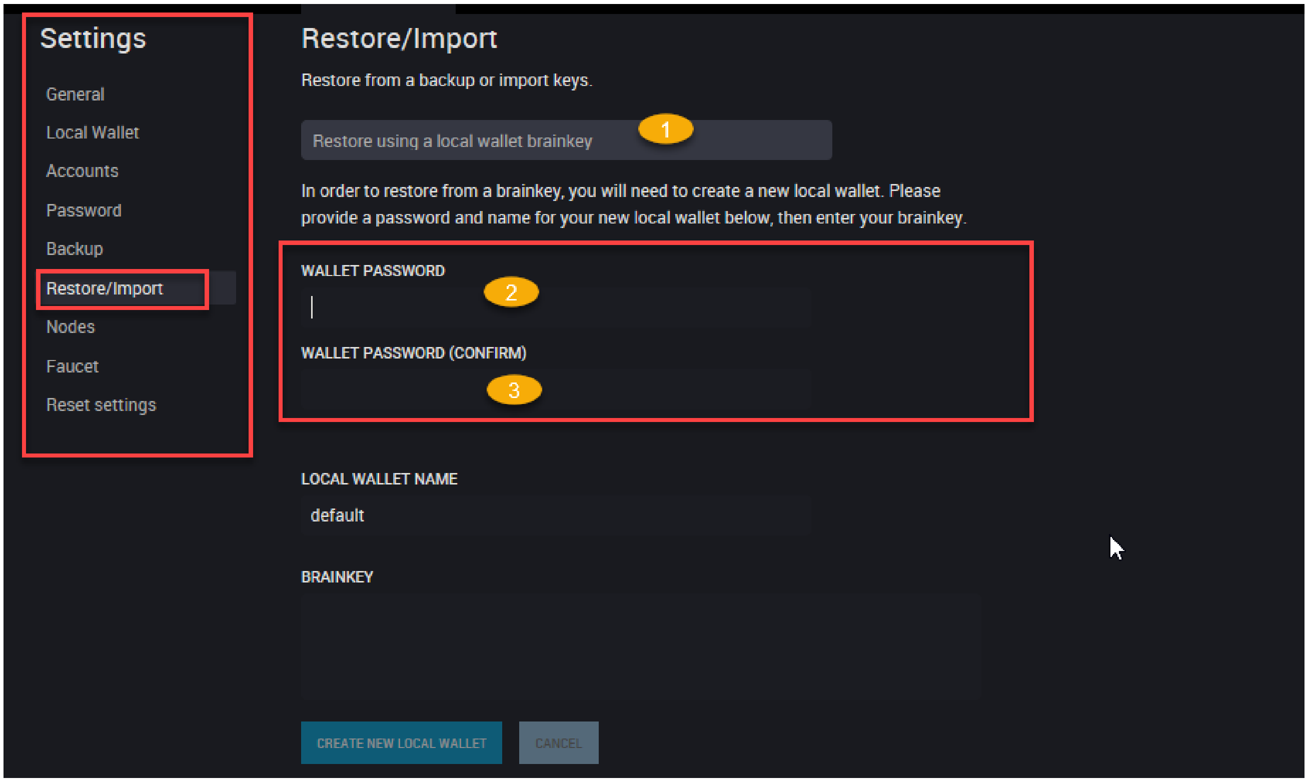
Control the details of your local wallet.

ACTIVE LOCAL WALLET:

bts_my_backup_20180405_you_can_rename

17.2.4 How to Recover Account with Brain key

1. Open a Side menu and select [**Settings**]
2. In [**Settings**], select [**Restore/Import**].
3. (#1) Make sure you selected *Restore using a local wallet brainkey*
4. (#2) Type in a password
5. (#3) Type in a password (Confirm)



Settings

Restore/Import

Restore from a backup or import keys.

Restore using a local wallet brainkey

In order to restore from a brainkey, you will need to create a new local wallet. Please provide a password and name for your new local wallet below, then enter your brainkey.

WALLET PASSWORD

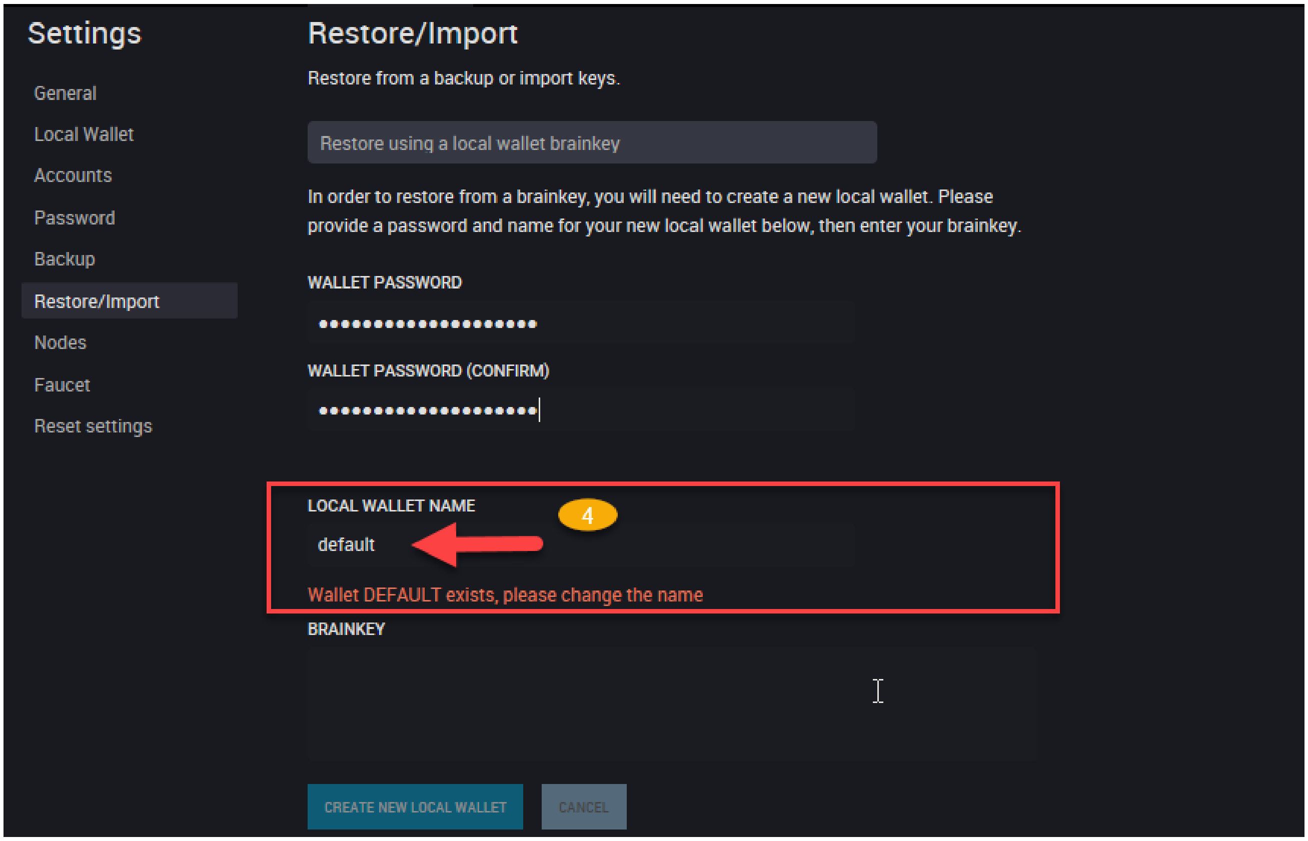
WALLET PASSWORD (CONFIRM)

LOCAL WALLET NAME

default

BRAINKEY

6. (#4) Type in new *Local Wallet Name* if needed. (e.g. “default-test-brainkey-restore”)



Settings

Restore/Import

Restore from a backup or import keys.

Restore using a local wallet brainkey

In order to restore from a brainkey, you will need to create a new local wallet. Please provide a password and name for your new local wallet below, then enter your brainkey.

WALLET PASSWORD

••••••••••••••••••••

WALLET PASSWORD (CONFIRM)

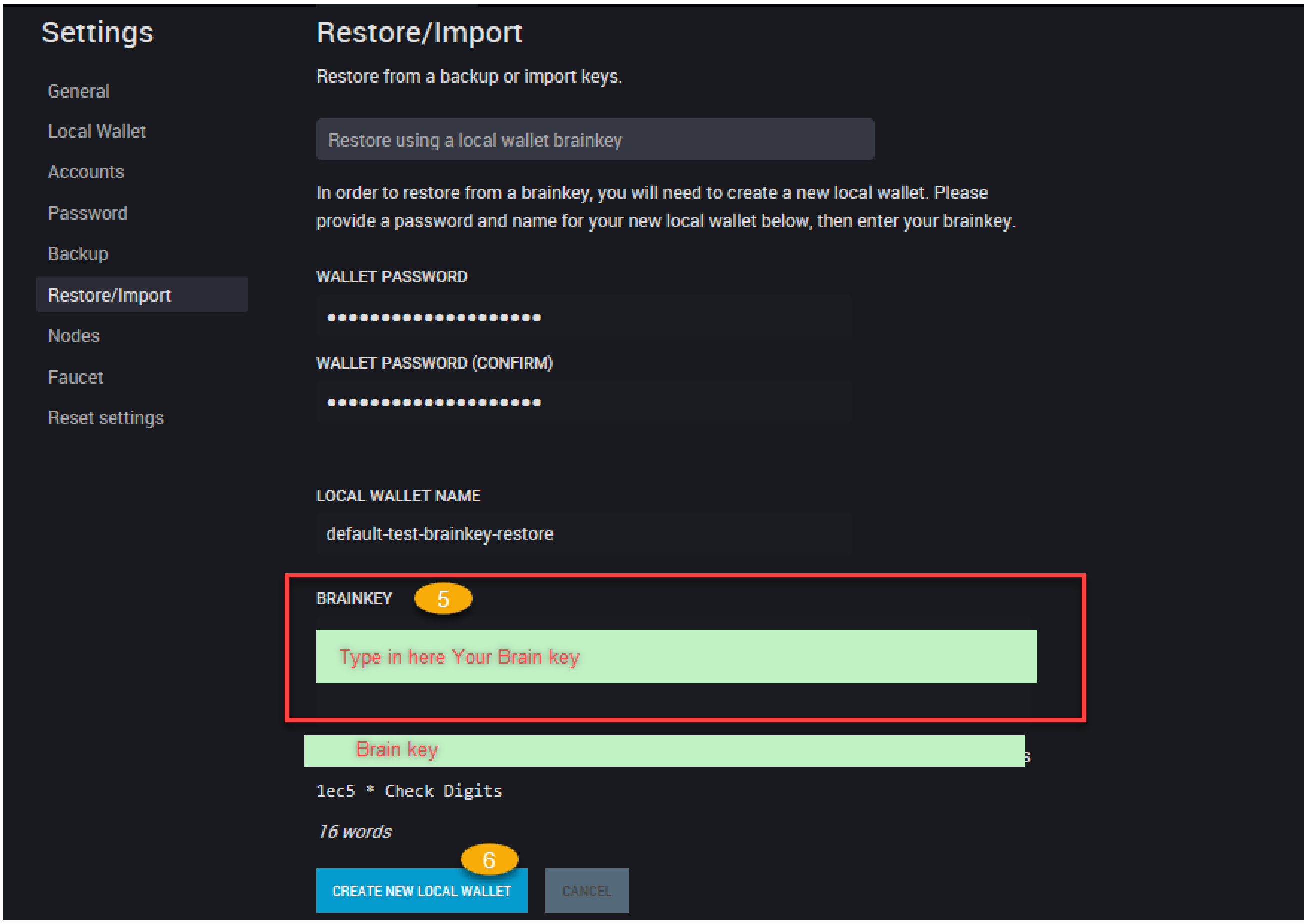
••••••••••••••••••••

LOCAL WALLET NAME

default

Wallet DEFAULT exists, please change the name

BRAINKEY



Restore/Import

Restore from a backup or import keys.

Restore using a local wallet brainkey

In order to restore from a brainkey, you will need to create a new local wallet. Please provide a password and name for your new local wallet below, then enter your brainkey.

WALLET PASSWORD

••••••••••••••••••••

WALLET PASSWORD (CONFIRM)

••••••••••••••••••••

LOCAL WALLET NAME

default-test-brainkey-restore

BRAINKEY

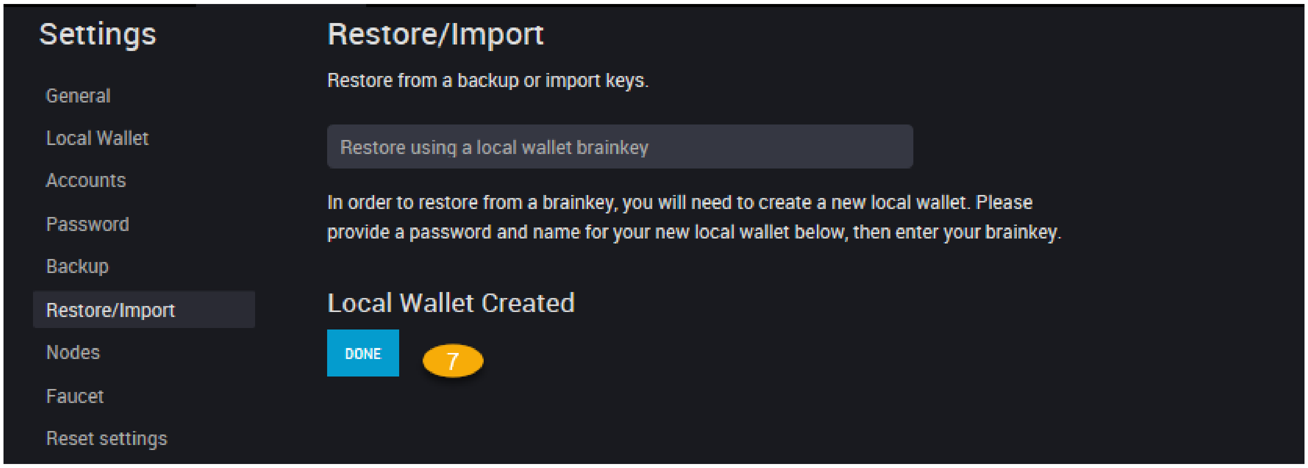
Type in here Your Brain key

Brain key

1ec5 * Check Digits

16 words

7. (#5) Type in **BRAINKEY**
8. (#6) Click [CREATE NEW LOCAL WALLET]



Restore/Import

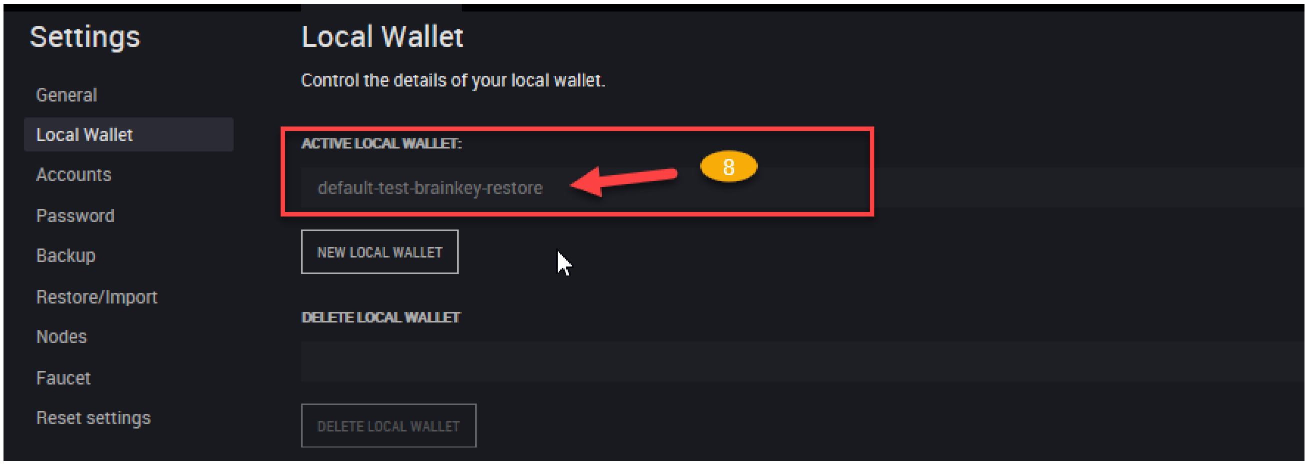
Restore from a backup or import keys.

Restore using a local wallet brainkey

In order to restore from a brainkey, you will need to create a new local wallet. Please provide a password and name for your new local wallet below, then enter your brainkey.

Local Wallet Created

9. (#7) Click [DONE]
10. (#8) Let's check *ACTIVE LOCAL WALLET* name (Go to [Settings] - [Local Wallet])



Settings

General
Local Wallet
Accounts
Password
Backup
Restore/Import
Nodes
Faucet
Reset settings

Local Wallet

Control the details of your local wallet.

ACTIVE LOCAL WALLET:

default-test-brainkey-restore

CHAPTER 18

Fund (Send) & Transactions

Table of Contents

18.1 Fund your Account

18.1.1 Two Options to Fund your Account

- **Send (Transfer)**: This is for between BitShares account holders to send funds. On the BitShares Blockchain , people never need to deal with *addresses* or *public keys*. BitShares account holders can use their *account names* for communication.
- **Deposits**: BitShares account holders can use one of our partners to move over existing funds into your BitShares account.

18.2 Send (Transfer)

Currently, there are two forms to send funds. One is **Send** on the top menu. Another one is **Send (legacy)** on the side menu. Both work the same.

First, we want to list what information on the Send form. Next, you can check each item in the Send form images.

18.2.1 Send Forms items and descriptions

	Item	Description
1	Sender's BitShares Account name	This would be your BitShares Account Name (e.g. *bitshares-users*)
2	TO	Another BitShares Account name whom you want to send funds
3	QUANTITY	• This is a dropdown list and will show all assets you have in the wallet account.
		• Type in a sending amount - AVAILABLE: a selected asset available total amounts
4	MEMO/MESSAGE	(option)
5	FEE	Transaction fee you pay
6	SEND	(button)
7	PASSWORD	If you have not logged in to the wallet, you will be asked to login
8	LOGIN	(button)
9	CONFIRM	(button) last check before you send founds

18.2.2 Form: Send

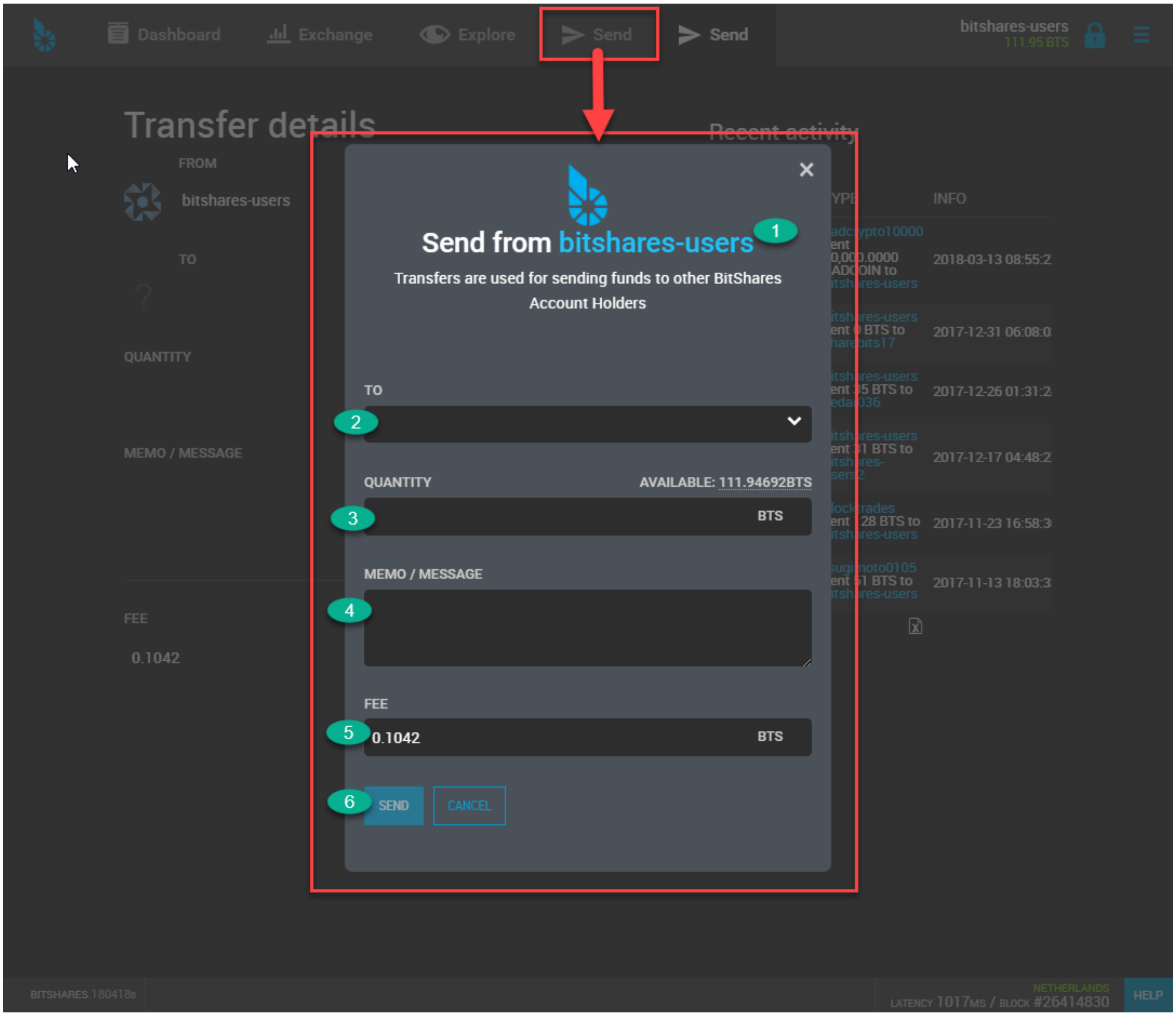
A send (transfer) operation moves funds from user `A` to user `B`. In contrast to most other blockchain-based financial networks, we do **not** use *addresses* or *public keys* for transfers.

Instead, all that is needed for transfers is:

- source account name: From
- destination account name: To
- funds (amount and asset): Quantity
- asset/token type
- memo (optional)

A transfer may contain a memo with arbitrary text.

Note: The `memo` is **encrypted** by default can only be decrypted by the participants of the transfer! The transfer fee depends on the length of the memo!



Send from bitshares-users

Transfers are used for sending funds to other BitShares Account Holders

TO

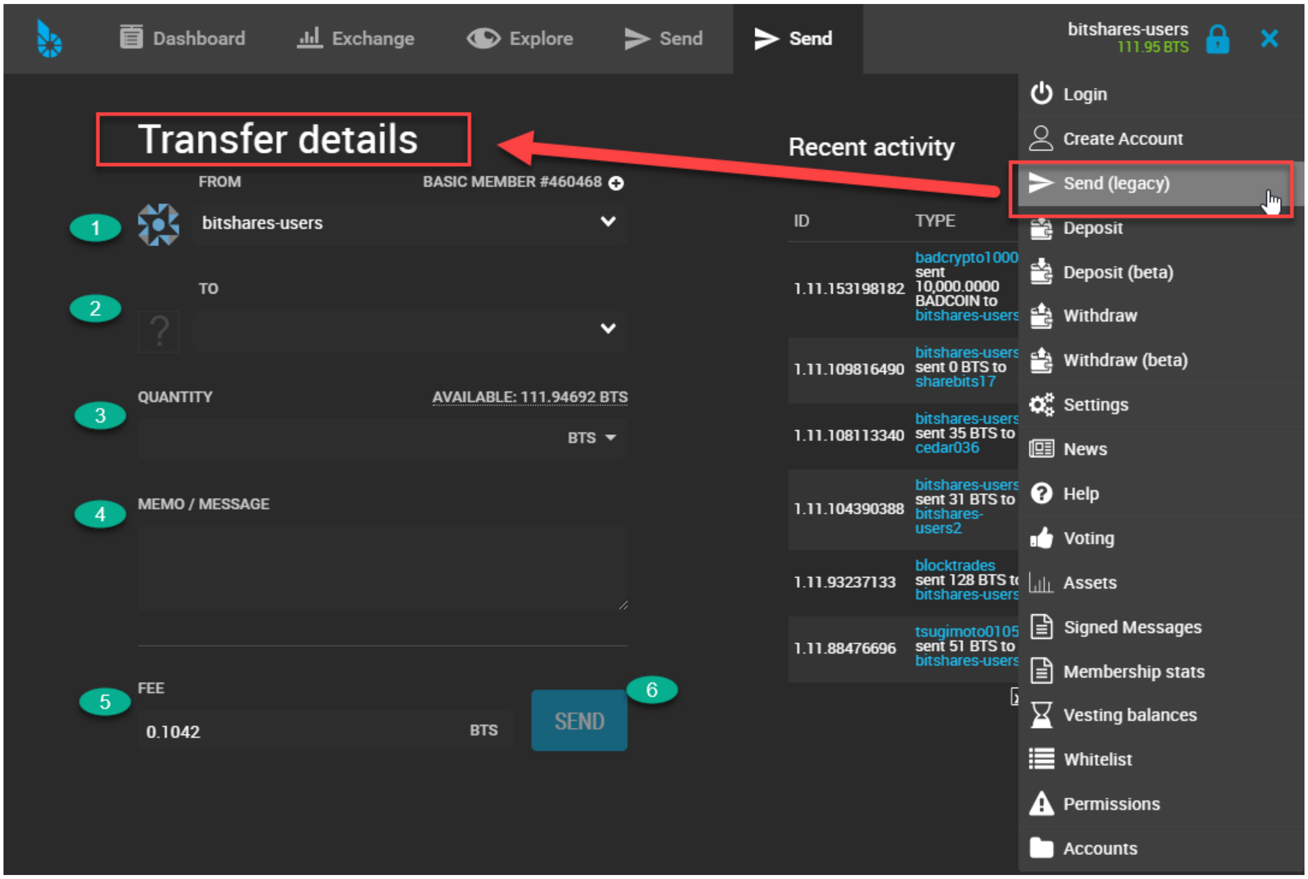
QUANTITY AVAILABLE: 111.94692BTS

MEMO / MESSAGE

FEE 0.1042 BTS

> After click [SEND], you need to login (if it's not yet) and [CONFIRM] the Transaction.

Form: Send - Transfer details (legacy form)



Transfer details

FROM BASIC MEMBER #460468

bitshares-users

TO

QUANTITY AVAILABLE: 111.94692 BTS

BTS

MEMO / MESSAGE

FEE

0.1042 BTS

Recent activity

ID	TYPE
1.11.153198182	badcrypto1000 sent 10,000.0000 BADCOIN to bitshares-users
1.11.109816490	bitshares-users sent 0 BTS to sharebits17
1.11.108113340	bitshares-users sent 35 BTS to cedar036
1.11.104390388	bitshares-users sent 31 BTS to bitshares-users2
1.11.93237133	blocktrades sent 128 BTS t bitshares-users
1.11.88476696	tsugimoto0105 sent 51 BTS to bitshares-users

18.3 Deposit

Currently, there are two forms to deposit funds. One is **Deposit** and another one is **Deposit (Beta)**. Both locate on the side menu.

BitShares has partners to provide Transfer (i.g. Gateway/Bridge) services which you can choose from. Each Transfer service has own instruction and available coins to handle. When you select a Transfer Service, please follow the instruction. In the next section, we will show you several examples and patterns to compare the deposit forms.

Note: On the BitShares blockchain, people never need to deal with *addresses* or *public keys* but can instead use account names. Your account name becomes the *email address* for your funds.

18.3.1 Deposit Forms Items and Descriptions

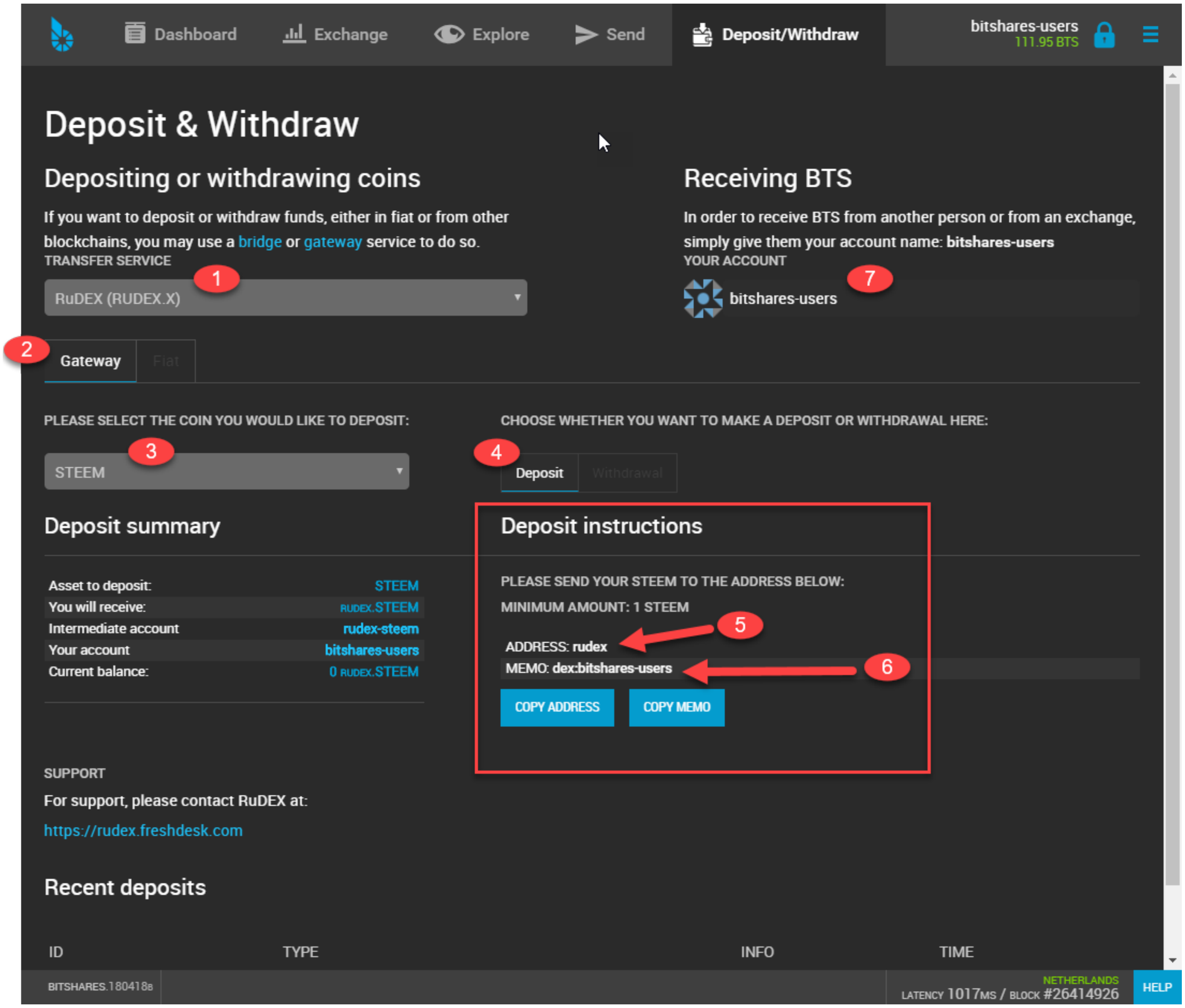
	Item	Description
1	Transfer Service	A dropdown list - Select a transfer service
2	Service Type	A service you use
3	Coin Name	A dropdown list - Select the coin name you want to deposit
4	Deposit / Withdraw tabs	Select *Deposit* tab
5	Address	Your deposit address to transfer funds.
6	Memo	Your Memo information to transfer funds. (*Not all coins' transfers use 'Memo'*)
7	BitShares Account Name	This would be your BitShares Account name

If you cannot select an Asset on the Deposit(Beta) form, try to login to your wallet first.

Examples

(Example 1) Deposit STEEM by using a Gateway service

You use *ADDRESS* and *MEMO* to deposit funds. The below images show a Deposit and a Deposit(Beta) forms.



Deposit & Withdraw

Depositing or withdrawing coins

If you want to deposit or withdraw funds, either in fiat or from other blockchains, you may use a bridge or gateway service to do so.

TRANSFER SERVICE

RuDEX (RUDEX.X)

Receiving BTS

In order to receive BTS from another person or from an exchange, simply give them your account name: **bitshares-users**

YOUR ACCOUNT

bitshares-users

PLEASE SELECT THE COIN YOU WOULD LIKE TO DEPOSIT:

STEEM

CHOOSE WHETHER YOU WANT TO MAKE A DEPOSIT OR WITHDRAWAL HERE:

Deposit summary

Asset to deposit:	STEEM
You will receive:	RUDEX.STEEM
Intermediate account	rudex-steem
Your account	bitshares-users
Current balance:	0 RUDEX.STEEM

Deposit instructions

PLEASE SEND YOUR STEEM TO THE ADDRESS BELOW:

MINIMUM AMOUNT: 1 STEEM

ADDRESS: rudex

MEMO: dex:bitshares-users

SUPPORT

For support, please contact RuDEX at:

https://rudex.freshdesk.com

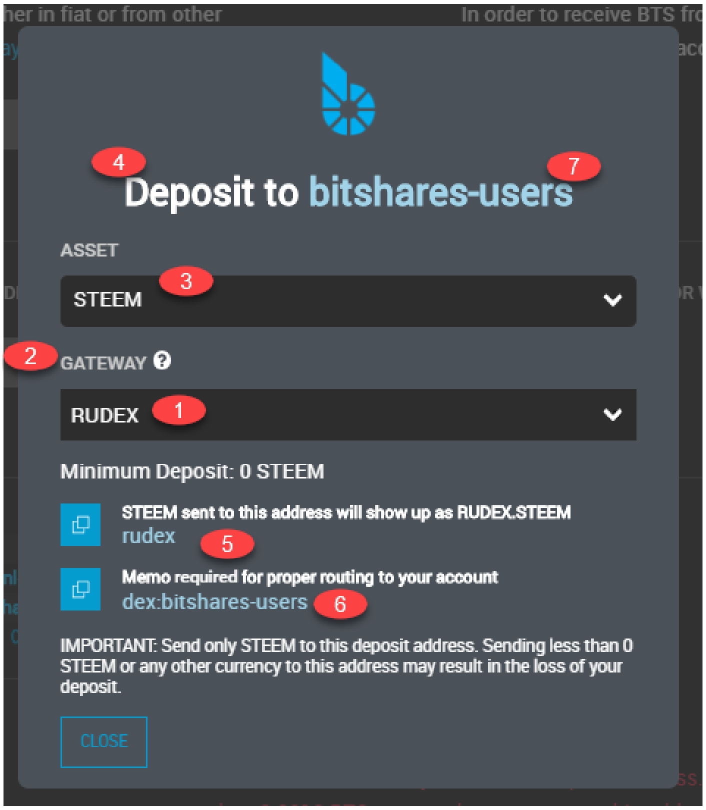
Recent deposits

ID	TYPE	INFO	TIME

BITSHARES.180418B

NETHERLANDS

LATENCY 1017MS / BLOCK #26414926



Deposit to bitshares-users

ASSET

STEEM

GATEWAY

RUDEX

Minimum Deposit: 0 STEEM

STEEM sent to this address will show up as RUDEX.STEEM

rudex

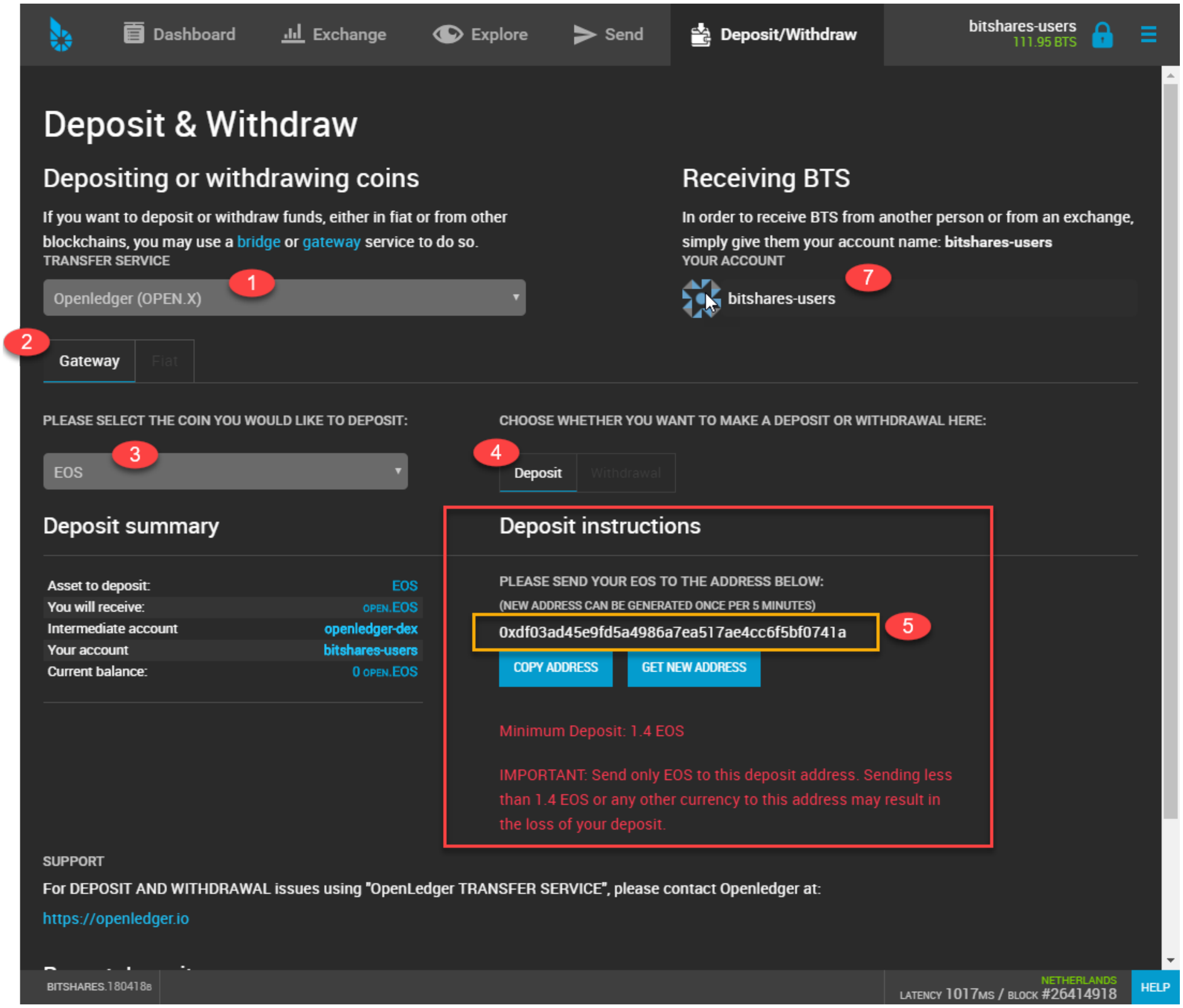
Memo required for proper routing to your account

dex:bitshares-users

IMPORTANT: Send only STEEM to this deposit address. Sending less than 0 STEEM or any other currency to this address may result in the loss of your deposit.

(Example 2) Deposit EOS by using a Gateway service

You use *ADDRESS* to deposit funds. The below images show a Deposit and a Deposit(Beta) forms.



Deposit & Withdraw

Depositing or withdrawing coins

If you want to deposit or withdraw funds, either in fiat or from other blockchains, you may use a bridge or gateway service to do so.

TRANSFER SERVICE: Openledger (OPEN.X)

Receiving BTS

In order to receive BTS from another person or from an exchange, simply give them your account name: **bitshares-users**

YOUR ACCOUNT: bitshares-users

PLEASE SELECT THE COIN YOU WOULD LIKE TO DEPOSIT: EOS

CHOOSE WHETHER YOU WANT TO MAKE A DEPOSIT OR WITHDRAWAL HERE:

Deposit summary

Asset to deposit:	EOS
You will receive:	OPEN.EOS
Intermediate account	openledger-dex
Your account	bitshares-users
Current balance:	0 OPEN.EOS

Deposit instructions

PLEASE SEND YOUR EOS TO THE ADDRESS BELOW:
(NEW ADDRESS CAN BE GENERATED ONCE PER 5 MINUTES)

0xdf03ad45e9fd5a4986a7ea517ae4cc6f5bf0741a

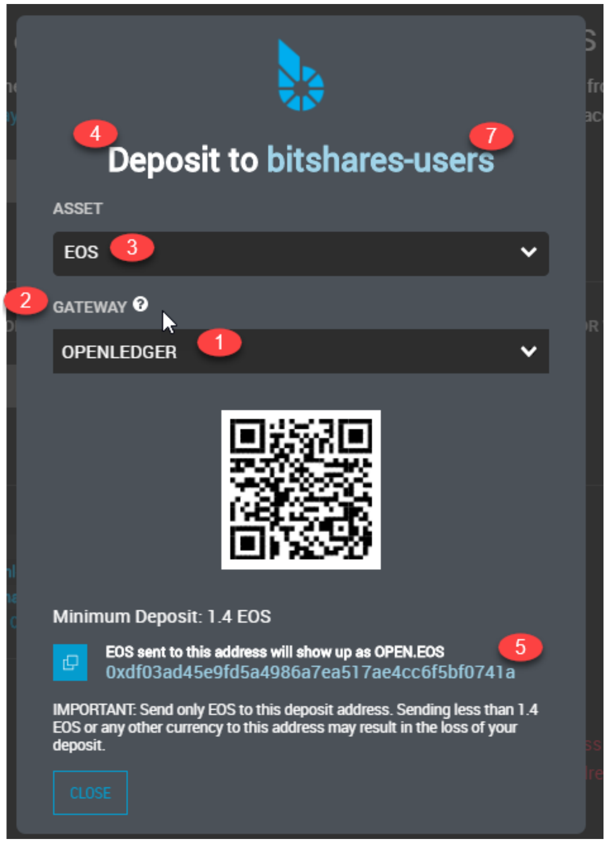
Minimum Deposit: 1.4 EOS

IMPORTANT: Send only EOS to this deposit address. Sending less than 1.4 EOS or any other currency to this address may result in the loss of your deposit.

SUPPORT

For DEPOSIT AND WITHDRAWAL issues using "OpenLedger TRANSFER SERVICE", please contact Openledger at:

https://openledger.io



Deposit to bitshares-users

ASSET

EOS

GATEWAY

OPENLEDGER

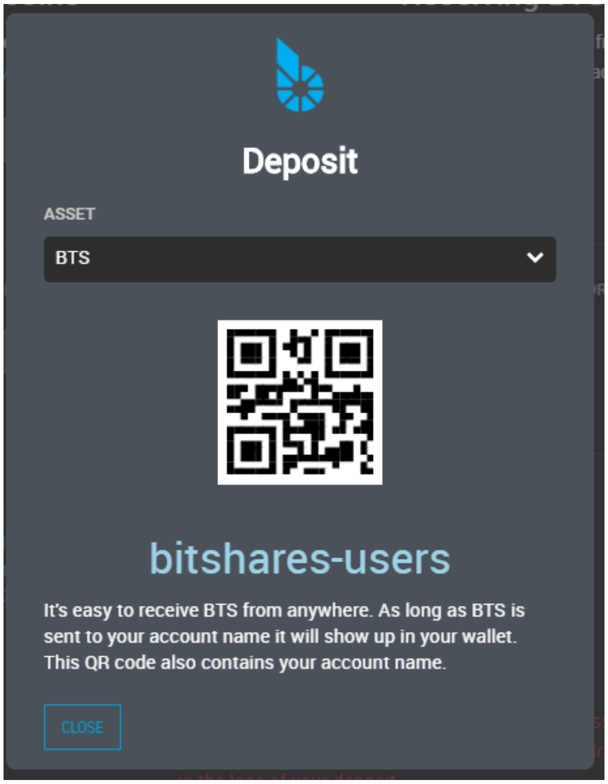
Minimum Deposit: 1.4 EOS

EOS sent to this address will show up as OPEN.EOS
0xdf03ad45e9fd5a4986a7ea517ae4cc6f5bf0741a

IMPORTANT: Send only EOS to this deposit address. Sending less than 1.4 EOS or any other currency to this address may result in the loss of your deposit.

(Example 3) Deposit BTS

You use BitShares Account Name as *ADDRESS* to deposit funds. The below image shows a Deposit(Beta) form.



Deposit

ASSET

BTS

bitshares-users

It's easy to receive BTS from anywhere. As long as BTS is sent to your account name it will show up in your wallet. This QR code also contains your account name.

18.4 Transactions

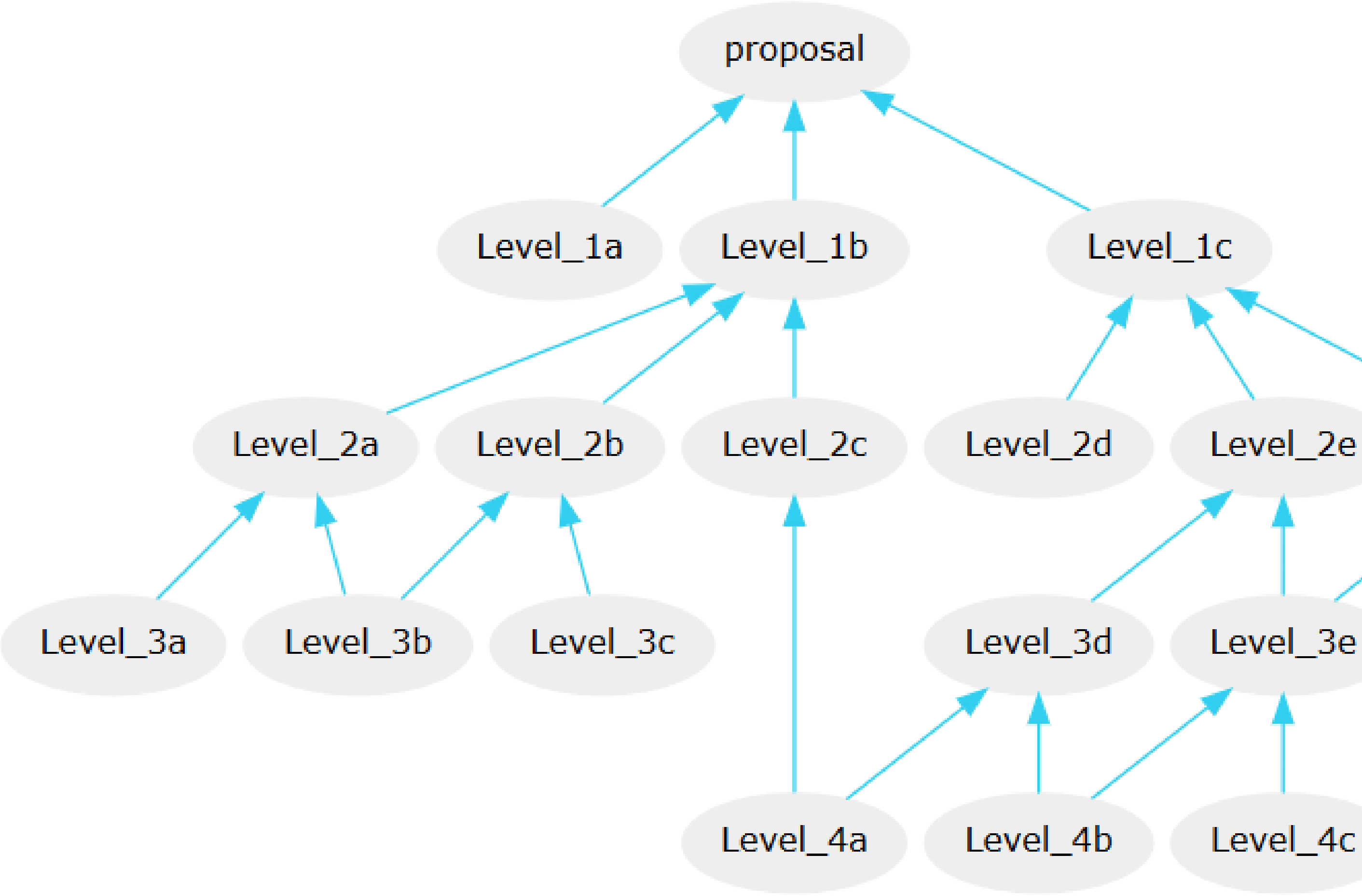
18.4.1 Proposed Transactions

The Graphene technology allows users to *propose* a transaction on the blockchain which requires approval of multiple accounts in order to execute.

At any time, a proposal can be approved in a single transaction if sufficient signatures are available (see `proposal_update_operation` as constructed by the `approve_proposal` call), as long as the authority tree to approve the proposal does not exceed the maximum recursion depth. In practice, however, it is easier to use proposals to acquire all approvals, as this leverages on-chain notification of all relevant parties that their approval is required. Off-chain multi-signature approval requires some off-chain mechanism for acquiring several signatures on a single transaction. This off-chain synchronization can be avoided using proposals.

The user proposes a transaction, then signatory accounts use add or remove their approvals from this operation. When a sufficient number of approvals have been granted, the operations in the proposal are evaluated. Even if the transaction fails, the proposal will be kept until the expiration time, at which point, if sufficient approval is granted, the transaction will be evaluated a final time. This allows transactions which will not execute successfully until a given time to still be executed through the proposal mechanism. The first time the proposed transaction succeeds, the proposal will be regarded as resolved, and all future updates will be invalid.

The proposal system allows for arbitrarily complex or recursively nested authorities. If a recursive authority (i.e. an authority which requires approval of 'nested' authorities on other accounts) is required for a proposal, then a second proposal can be used to grant the nested authority's approval. That is, a second proposal can be created which, when sufficiently approved, adds the approval of a nested authority to the first proposal. This multiple-proposal scheme can be used to acquire approval for an arbitrarily deep authority tree.



Note that each account in the figure can carry a **different weight**. An example of how to setup your permissions accordingly is given in account-permissions.

18.4.2 Confidential Transactions

A confidential transfer is one that hides the amount being sent. Confidential transfers are also referred to as blinded transfers. It makes use of Oleg Andreev's blind signatures.

When privacy is important no account is ever used twice and it is impossible for any third party to identify how money is moving through blockchain analysis alone.

CHAPTER 19

Bridge and Gateway

If you want to deposit or withdraw funds, either in fiat or from other blockchains, You may use a bridge or gateway service to do so. The next section describes *Bridge* and *Gateway* services.

19.1 Bridge and gateway services

Both bridges and gateways allow you to deposit and withdraw coins, but there is a difference in the amount of trust you need to place in the service providers.

19.2 Bridges: trust-free model

A bridge service provides a way to deposit an amount of a crypto-currency other than BitShares, and in turn receive a SmartCoin equivalent. SmartCoins have no counterparty risk, so the only risk you experience when using a bridge is during the short time it takes to complete the transfer. This is better than a centralized exchange such as Poloniex, where you are always at risk of the exchange being hacked, going bankrupt, or experiencing any number of other issues.

19.3 Gateways: trust-based model

Gateways are basically equivalent to the standard exchange model where you depend on the solvency of the exchange to be able to redeem your coins. Generally gateways issue assets prefixed with their symbol, like OPEN, TRADE, or META. These assets are backed 100% by the real BTC or ETH or any other coin that people deposit with the gateways.

An OPEN.BTC is thus in theory equivalent to the BTC you get on Poloniex, which could be prefixed POLO.BTC. In both cases you rely on the service provider, CCEDK for OPEN. assets and Poloniex for POLO. assets, to remain solvent in order to back the value of the assets they've issued. Because gateways only provide this one service which is normally only one part of running an exchange, one might even argue that they have an easier job of securing their holdings.

(ref: https://wallet.bitshares.org/#/help/introduction/bridges_gateways)

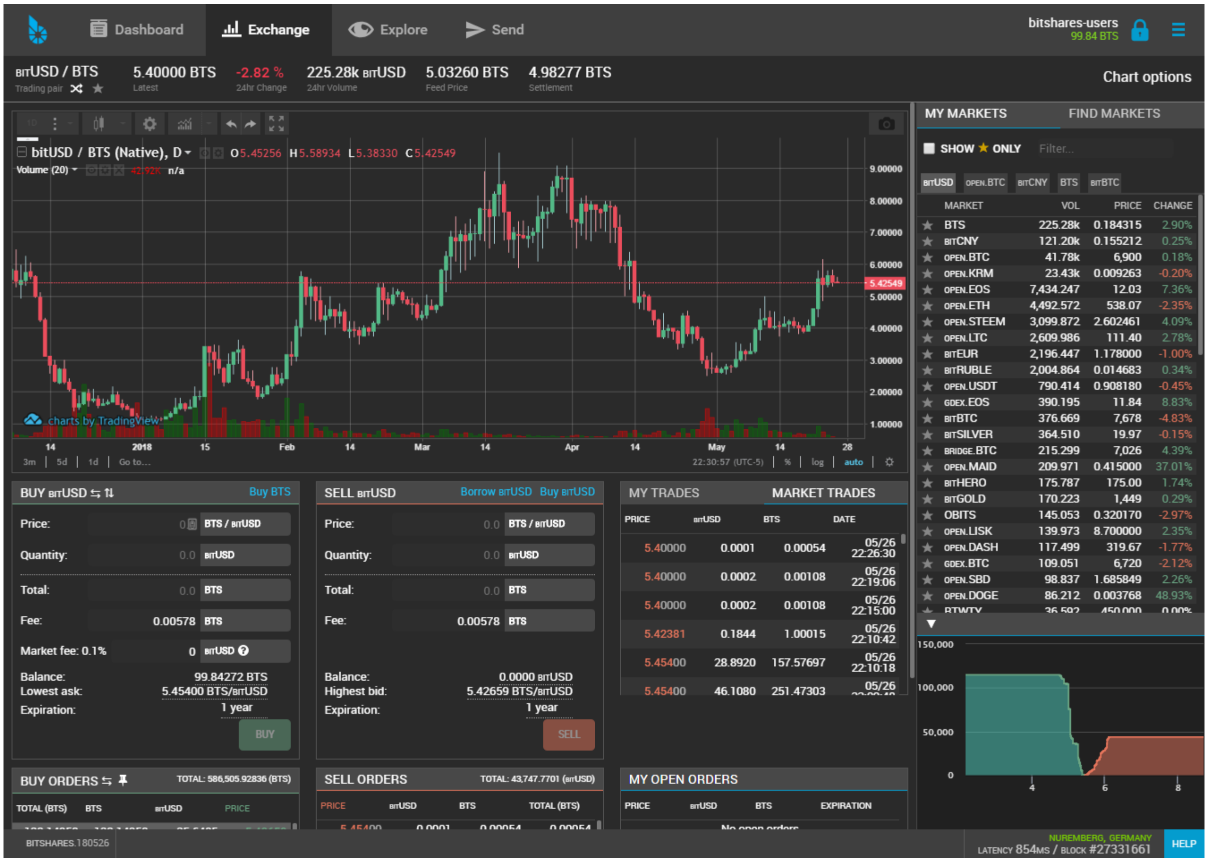
CHAPTER 20

Exchange and Explore

Table of Contents

20.1 Exchange

https://wallet.bitshares.org/#/market/USD_BTS



MARKET	VOL	PRICE	CHANGE
BTS	225.28k	0.184315	2.90%
BITCNY	121.20k	0.155212	0.25%
OPEN.BTC	41.78k	6,900	0.18%
OPEN.KRM	23.43k	0.009263	-0.20%
OPEN.EOS	7,434.247	12.03	7.36%
OPEN.ETH	4,492.572	538.07	-2.35%
OPEN.STEEM	3,099.872	2.602461	4.09%
OPEN.LTC	2,609.986	111.40	2.78%
BITEUR	2,196.447	1.178000	-1.00%
BITRUBLE	2,004.864	0.014683	0.34%
OPEN.USDT	790.414	0.908180	-0.45%
GDEX.EOS	390.195	11.84	8.83%
BITBTC	376.669	7,678	-4.83%
BITSILVER	364.510	19.97	-0.15%
BRIDGE.BTC	215.299	7,026	4.39%
OPEN.MAID	209.971	0.415000	37.01%
BITHERO	175.787	175.00	1.74%
BITGOLD	170.223	1,449	0.29%
OBITS	145.053	0.320170	-2.97%
OPEN.LISK	139.973	8.700000	2.35%
OPEN.DASH	117.499	319.67	-1.77%
GDEX.BTC	109.051	6,720	-2.12%
OPEN.SBD	98.837	1.685849	2.26%
OPEN.DOGE	86.212	0.003768	48.93%

Price: 0 BTS / bitUSD
Quantity: 0.0 bitUSD
Total: 0.0 BTS
Fee: 0.00578 BTS
Market fee: 0.1% 0 bitUSD
Balance: 99.84272 BTS
Lowest ask: 5.45400 BTS/bitUSD
Expiration: 1 year

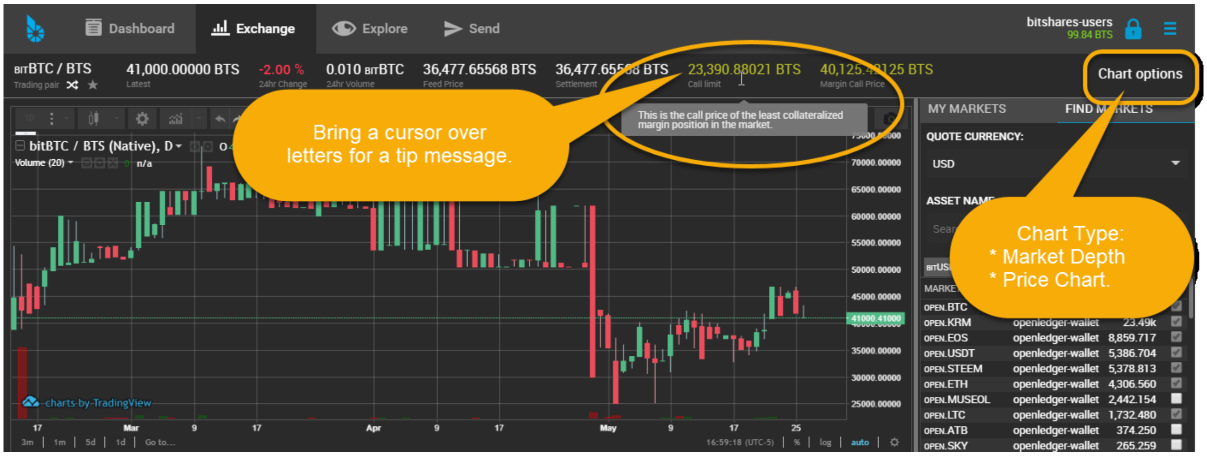
Price: 0.0 BTS / bitUSD
Quantity: 0.0 bitUSD
Total: 0.0 BTS
Fee: 0.00578 BTS
Balance: 0.0000 bitUSD
Highest bid: 5.42659 BTS/bitUSD
Expiration: 1 year

PRICE	bitUSD	BTS	DATE
5.40000	0.0001	0.00054	05/26 22:26:30
5.40000	0.0002	0.00108	05/26 22:19:06
5.40000	0.0002	0.00108	05/26 22:15:00
5.42381	0.1844	1.00015	05/26 22:10:42
5.45400	28.8920	157.57697	05/26 22:10:18
5.45400	46.1080	251.47303	05/26

BUY ORDERS TOTAL: 586,505.92836 (BTS)

SELL ORDERS TOTAL: 43,747.7701 (bitUSD)

20.1.1 Form Features

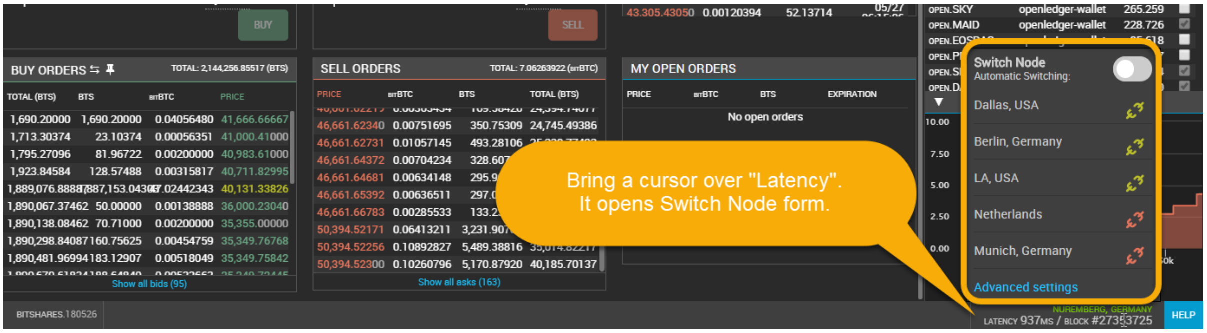


This is the call price of the least collateralized margin position in the market.

Bring a cursor over letters for a tip message.

Chart Type:
* Market Depth
* Price Chart.

OPEN.KRM	openledger-wallet	23.49k
OPEN.EOS	openledger-wallet	8,859.717
OPEN.USDT	openledger-wallet	5,386.704
OPEN.STEEM	openledger-wallet	5,378.813
OPEN.ETH	openledger-wallet	4,306.560
OPEN.MUSEOL	openledger-wallet	2,442.154
OPEN.LTC	openledger-wallet	1,732.480
OPEN.ATB	openledger-wallet	374.250
OPEN.SKY	openledger-wallet	265.259



BUY ORDERS ⇆ TOTAL: 2,144,256.85517 (BTS)

TOTAL (BTS)	BTS	BITBTC	PRICE
1,690.20000	1,690.20000	0.04056480	41,666.66667
1,713.30374	23.10374	0.00056351	41,000.41000
1,795.27096	81.96722	0.00200000	40,983.61000
1,923.84584	128.57488	0.00315817	40,711.82995
1,889,076.8888	1,887,153.04306	47.02442343	40,131.33826
1,890,067.37462	50.00000	0.00138888	36,000.23040
1,890,138.08462	70.71000	0.00200000	35,355.00000
1,890,298.84087	160.75625	0.00454759	35,349.76768
1,890,481.96994	183.12907	0.00518049	35,349.75842

Show all bids (95)

SELL ORDERS TOTAL: 7.06263922 (BITBTC)

PRICE	BITBTC	BTS	TOTAL (BTS)
46,661.62340	0.00751695	350.75309	24,745.49386
46,661.62731	0.01057145	493.28106	
46,661.64372	0.00704234	328.607	
46,661.64681	0.00634148	295.9	
46,661.65392	0.00636511	297.0	
46,661.66783	0.00285533	133.2	
50,394.52171	0.06413211	3,231.907	
50,394.52256	0.10892827	5,489.38816	
50,394.52300	0.10260796	5,170.87920	40,185.70137

Show all asks (163)

MY OPEN ORDERS

PRICE	BITBTC	BTS	EXPIRATION

No open orders

Bring a cursor over "Latency".
It opens Switch Node form.

Switch Node
Automatic Switching:

- Dallas, USA
- Berlin, Germany
- LA, USA
- Netherlands
- Munich, Germany

Advanced settings

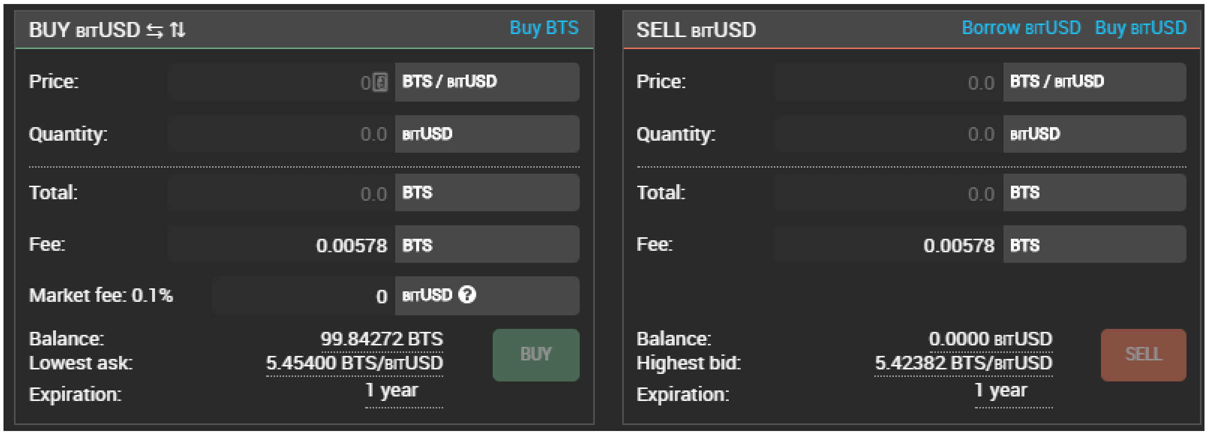
20.2 How to trade in the DEX

The decentralized exchange (DEX) of BitShares has a similar look&feel as traditional centralized exchanges. However, trading in the DEX can have many different appearances, depending on what user-interface is used. We here describe the user interface of the official wallet.

20.2.1 Playing Orders

Orders can be placed in the same way as everywhere else, by providing

- the amount to buy/sell
- the price at which to buy/sell



BUY BITUSD ⇆ ⇅ Buy BTS

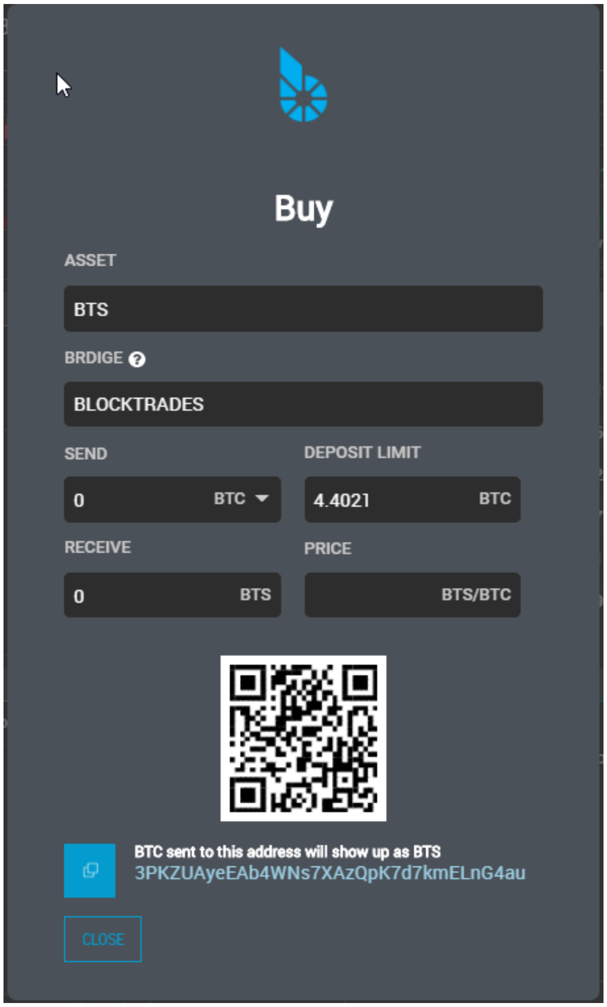
Price:	0	BTS / BITUSD
Quantity:	0.0	BITUSD
Total:	0.0	BTS
Fee:	0.00578	BTS
Market fee: 0.1%	0	BITUSD

Balance: 99.84272 BTS
Lowest ask: 5.45400 BTS/BITUSD
Expiration: 1 year

SELL BITUSD Borrow BITUSD Buy BITUSD

Price:	0.0	BTS / BITUSD
Quantity:	0.0	BITUSD
Total:	0.0	BTS
Fee:	0.00578	BTS

Balance: 0.0000 BITUSD
Highest bid: 5.42382 BTS/BITUSD
Expiration: 1 year



Buy

ASSET

BTS

BRDIGE

BLOCKTRADES

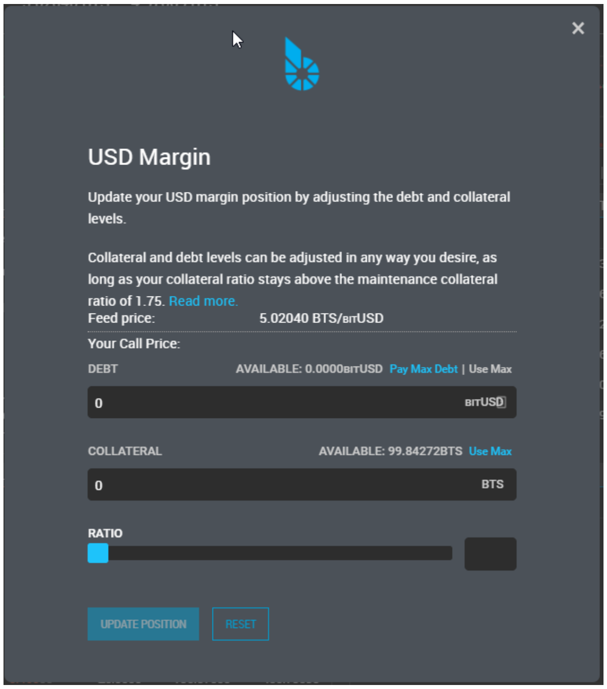
SEND: 0 BTC

DEPOSIT LIMIT: 4.4021 BTC

RECEIVE: 0 BTS

PRICE: BTS/BTC

BTC sent to this address will show up as BTS
3PKZUAyeEAb4WNs7XAzQpK7d7kmELnG4au



USD Margin

Update your USD margin position by adjusting the debt and collateral levels.

Collateral and debt levels can be adjusted in any way you desire, as long as your collateral ratio stays above the maintenance collateral ratio of 1.75. Read more.

Feed price: 5.02040 BTS/bitUSD

Your Call Price:

DEBT AVAILABLE: 0.0000bitUSD Pay Max Debt | Use Max

0 bitUSD

COLLATERAL AVAILABLE: 99.84272BTS Use Max

0 BTS

RATIO

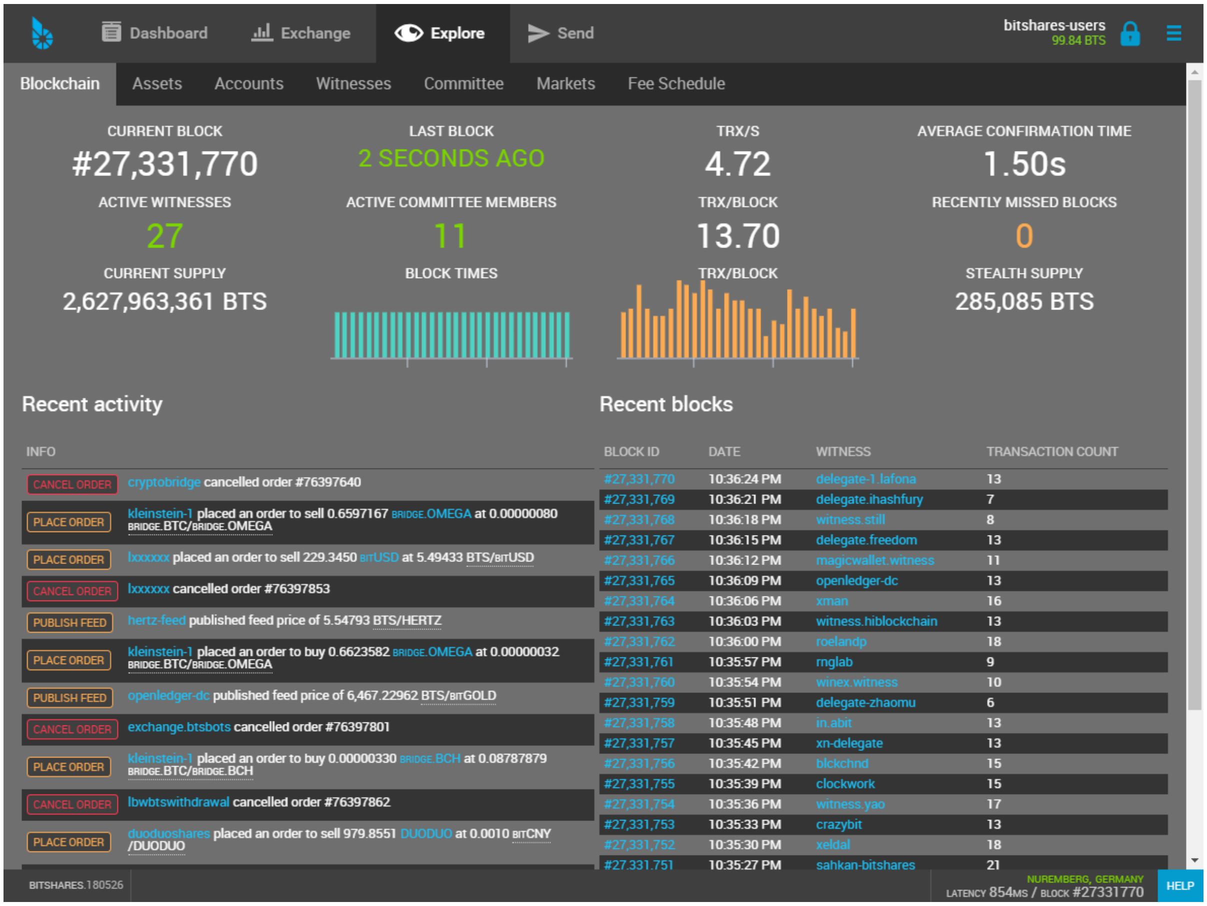
Fees

In contrast to other exchanges, BitShares asks for a tiny **flat fee** for placing an order. This fee can be payed in USD, BTC, or GOLD and is independent of the actual assets that are traded.

If you cancel an order that has not been fully or partially filled, 90% of the fee will be payed back to your account. However, this chargeback will be in *BTS* and not in the asset you have originally paid the fee in.

20.3 Explore

(*Forms layouts*)



CURRENT BLOCK #27,331,770

LAST BLOCK 2 SECONDS AGO

TRX/S 4.72

AVERAGE CONFIRMATION TIME 1.50s

ACTIVE WITNESSES 27

ACTIVE COMMITTEE MEMBERS 11

TRX/BLOCK 13.70

RECENTLY MISSED BLOCKS 0

CURRENT SUPPLY 2,627,963,361 BTS

STEALTH SUPPLY 285,085 BTS

Recent activity

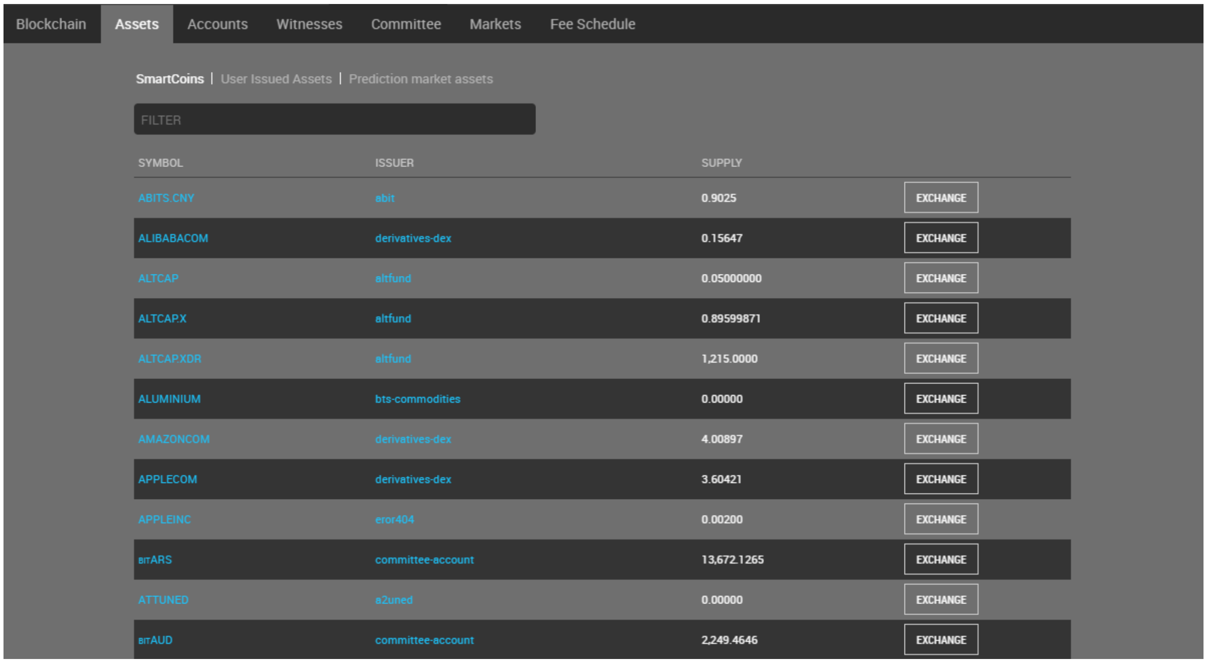
INFO	
CANCEL ORDER	cryptobridge cancelled order #76397640
PLACE ORDER	kleinstein-1 placed an order to sell 0.6597167 BRIDGE.OMEGA at 0.00000080 BRIDGE.BTC/BRIDGE.OMEGA
PLACE ORDER	lxxxxxx placed an order to sell 229.3450 BITUSD at 5.49433 BTS/BITUSD
CANCEL ORDER	lxxxxxx cancelled order #76397853
PUBLISH FEED	hertz-feed published feed price of 5.54793 BTS/HERTZ
PLACE ORDER	kleinstein-1 placed an order to buy 0.6623582 BRIDGE.OMEGA at 0.00000032 BRIDGE.BTC/BRIDGE.OMEGA
PUBLISH FEED	openledger-dc published feed price of 6,467.22962 BTS/BITGOLD
CANCEL ORDER	exchange.btsbots cancelled order #76397801
PLACE ORDER	kleinstein-1 placed an order to buy 0.00000330 BRIDGE.BCH at 0.08787879 BRIDGE.BTC/BRIDGE.BCH
CANCEL ORDER	lbwbtswithdrawal cancelled order #76397862
PLACE ORDER	duoduoshares placed an order to sell 979.8551 DUODUO at 0.0010 BITCNY /DUODUO

Recent blocks

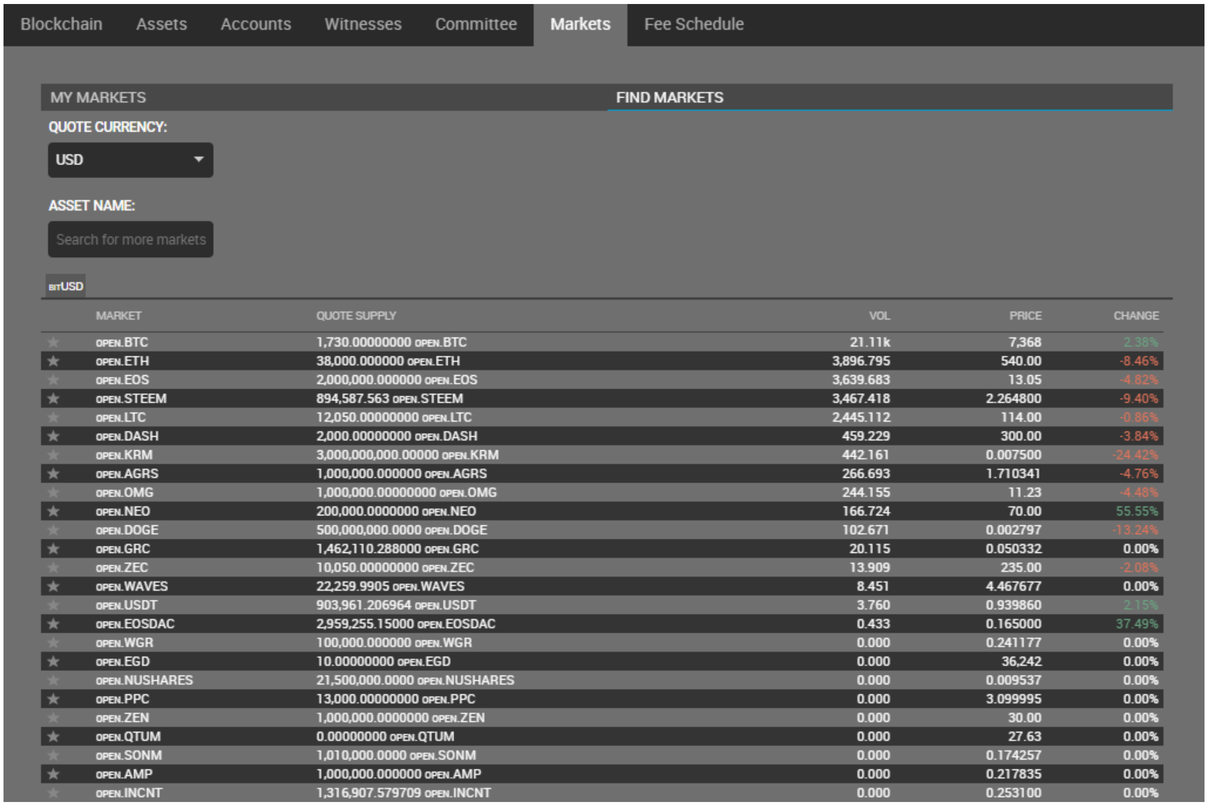
BLOCK ID	DATE	WITNESS	TRANSACTION COUNT
#27,331,770	10:36:24 PM	delegate-1.lafona	13
#27,331,769	10:36:21 PM	delegate.ihashfury	7
#27,331,768	10:36:18 PM	witness.still	8
#27,331,767	10:36:15 PM	delegate.freedom	13
#27,331,766	10:36:12 PM	magicwallet.witness	11
#27,331,765	10:36:09 PM	openledger-dc	13
#27,331,764	10:36:06 PM	xman	16
#27,331,763	10:36:03 PM	witness.hiblockchain	13
#27,331,762	10:36:00 PM	roelandp	18
#27,331,761	10:35:57 PM	rnglab	9
#27,331,760	10:35:54 PM	winex.witness	10
#27,331,759	10:35:51 PM	delegate-zhaomu	6
#27,331,758	10:35:48 PM	in.abit	13
#27,331,757	10:35:45 PM	xn-delegate	13
#27,331,756	10:35:42 PM	blckchnd	15
#27,331,755	10:35:39 PM	clockwork	15
#27,331,754	10:35:36 PM	witness.yao	17
#27,331,753	10:35:33 PM	crazybit	13
#27,331,752	10:35:30 PM	xeldal	18
#27,331,751	10:35:27 PM	sahkan-bitshares	21

BITSHARES.180526

NUREMBERG, GERMANY
LATENCY 854MS / BLOCK #27331770



SYMBOL	ISSUER	SUPPLY	
ABITS.CNY	abit	0.9025	EXCHANGE
ALIBABACOM	derivatives-dex	0.15647	EXCHANGE
ALTCAP	altfund	0.05000000	EXCHANGE
ALTCAP.X	altfund	0.89599871	EXCHANGE
ALTCAP.XDR	altfund	1,215.0000	EXCHANGE
ALUMINIUM	bts-commodities	0.00000	EXCHANGE
AMAZONCOM	derivatives-dex	4.00897	EXCHANGE
APPLECOM	derivatives-dex	3.60421	EXCHANGE
APPLEINC	eror404	0.00200	EXCHANGE
BITARS	committee-account	13,672.1265	EXCHANGE
ATTUNED	a2uned	0.00000	EXCHANGE
BITAUD	committee-account	2,249.4646	EXCHANGE

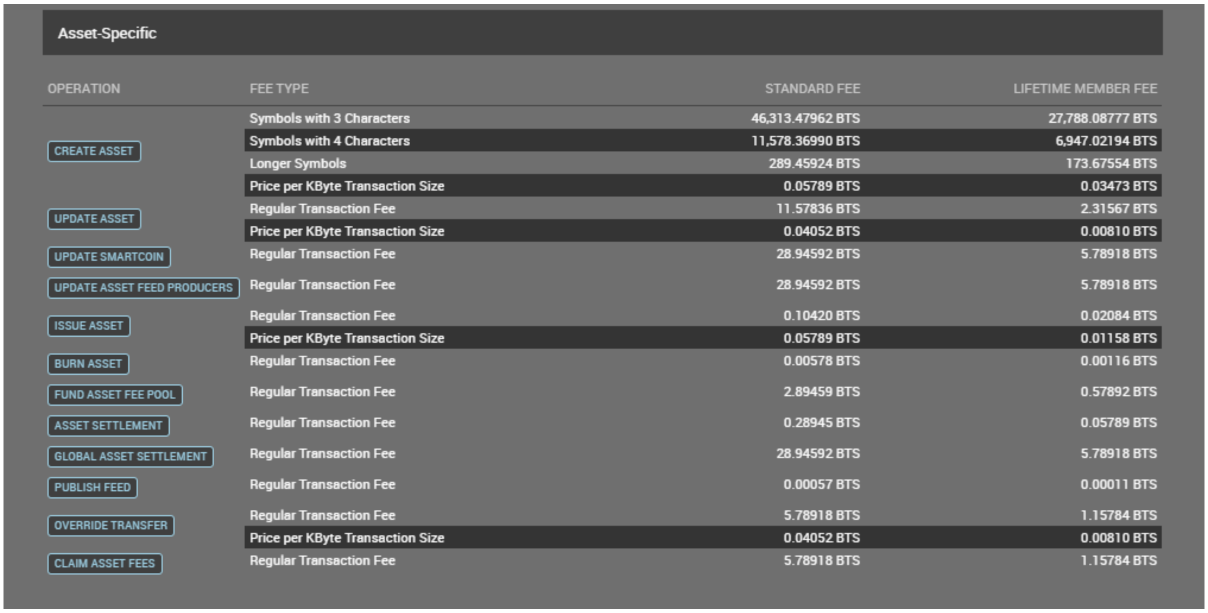


QUOTE CURRENCY: USD

ASSET NAME: Search for more markets

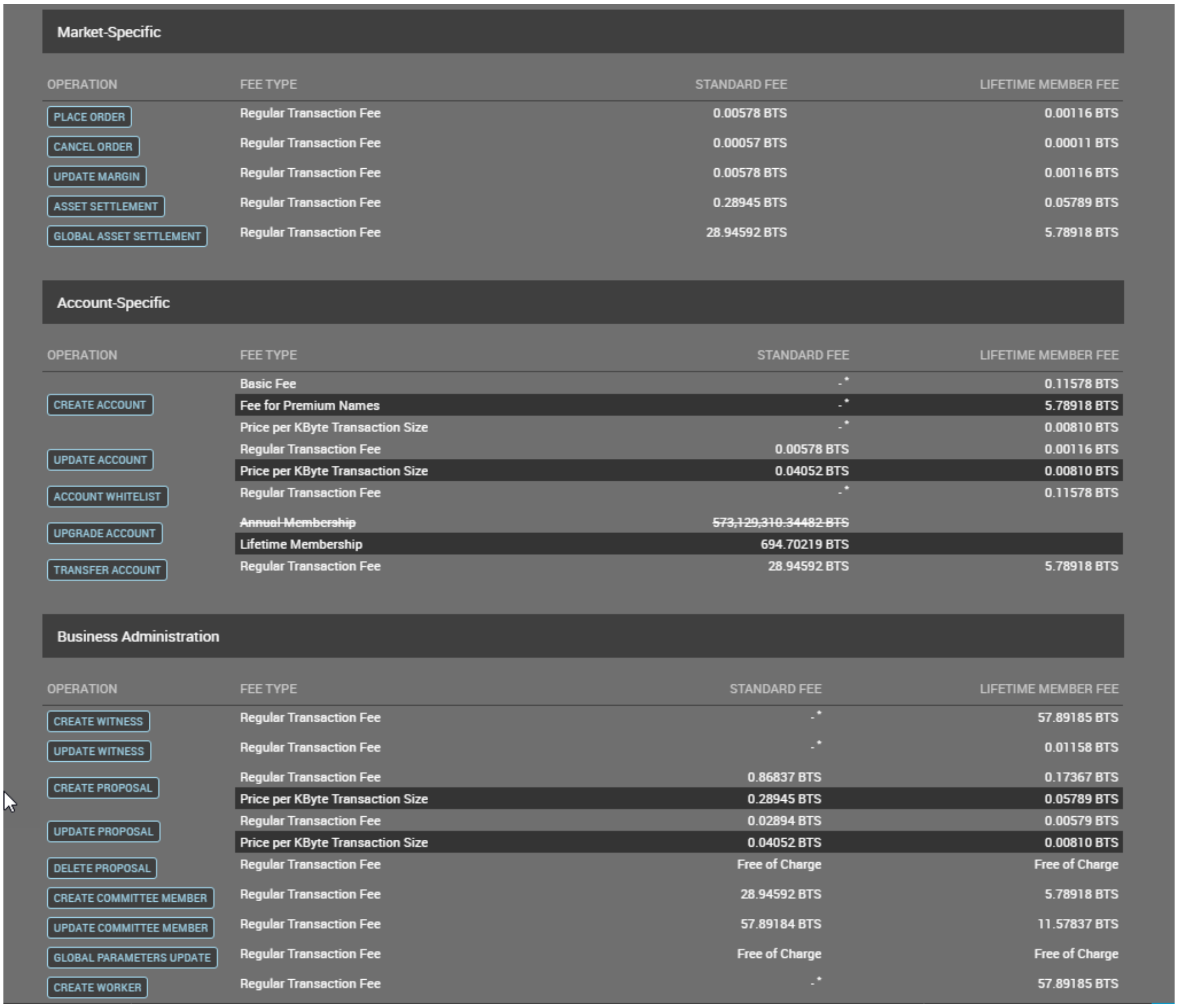
BITUSD

	MARKET	QUOTE SUPPLY	VOL	PRICE	CHANGE
★	OPEN.BTC	1,730.00000000 OPEN.BTC	21.11k	7,368	2.38%
★	OPEN.ETH	38,000.000000 OPEN.ETH	3,896.795	540.00	-8.46%
★	OPEN.EOS	2,000,000.000000 OPEN.EOS	3,639.683	13.05	-4.82%
★	OPEN.STEEM	894,587.563 OPEN.STEEM	3,467.418	2.264800	-9.40%
★	OPEN.LTC	12,050.00000000 OPEN.LTC	2,445.112	114.00	-0.86%
★	OPEN.DASH	2,000.00000000 OPEN.DASH	459.229	300.00	-3.84%
★	OPEN.KRM	3,000,000,000.00000 OPEN.KRM	442.161	0.007500	-24.42%
★	OPEN.AGRS	1,000,000.000000 OPEN.AGRS	266.693	1.710341	-4.76%
★	OPEN.OMG	1,000,000.00000000 OPEN.OMG	244.155	11.23	-4.48%
★	OPEN.NEO	200,000.0000000 OPEN.NEO	166.724	70.00	55.55%
★	OPEN.DOGE	500,000,000.0000 OPEN.DOGE	102.671	0.002797	-13.24%
★	OPEN.GRC	1,462,110.288000 OPEN.GRC	20.115	0.050332	0.00%
★	OPEN.ZEC	10,050.00000000 OPEN.ZEC	13.909	235.00	-2.08%
★	OPEN.WAVES	22,259.9905 OPEN.WAVES	8.451	4.467677	0.00%
★	OPEN.USDT	903,961.206964 OPEN.USDT	3.760	0.939860	2.15%
★	OPEN.EOSDAC	2,959,255.15000 OPEN.EOSDAC	0.433	0.165000	37.49%
★	OPEN.WGR	100,000.000000 OPEN.WGR	0.000	0.241177	0.00%
★	OPEN.EGD	10.00000000 OPEN.EGD	0.000	36,242	0.00%
★	OPEN.NUSHARES	21,500,000.0000 OPEN.NUSHARES	0.000	0.009537	0.00%
★	OPEN.PPC	13,000.00000000 OPEN.PPC	0.000	3.099995	0.00%
★	OPEN.ZEN	1,000,000.0000000 OPEN.ZEN	0.000	30.00	0.00%
★	OPEN.QTUM	0.00000000 OPEN.QTUM	0.000	27.63	0.00%
★	OPEN.SONM	1,010,000.0000 OPEN.SONM	0.000	0.174257	0.00%
★	OPEN.AMP	1,000,000.000000 OPEN.AMP	0.000	0.217835	0.00%
★	OPEN.INCNT	1,316,907.579709 OPEN.INCNT	0.000	0.253100	0.00%



Asset-Specific

OPERATION	FEE TYPE	STANDARD FEE	LIFETIME MEMBER FEE
CREATE ASSET	Symbols with 3 Characters	46,313.47962 BTS	27,788.08777 BTS
	Symbols with 4 Characters	11,578.36990 BTS	6,947.02194 BTS
	Longer Symbols	289.45924 BTS	173.67554 BTS
	Price per KByte Transaction Size	0.05789 BTS	0.03473 BTS
UPDATE ASSET	Regular Transaction Fee	11.57836 BTS	2.31567 BTS
	Price per KByte Transaction Size	0.04052 BTS	0.00810 BTS
UPDATE SMARTCOIN	Regular Transaction Fee	28.94592 BTS	5.78918 BTS
UPDATE ASSET FEED PRODUCERS	Regular Transaction Fee	28.94592 BTS	5.78918 BTS
ISSUE ASSET	Regular Transaction Fee	0.10420 BTS	0.02084 BTS
	Price per KByte Transaction Size	0.05789 BTS	0.01158 BTS
BURN ASSET	Regular Transaction Fee	0.00578 BTS	0.00116 BTS
FUND ASSET FEE POOL	Regular Transaction Fee	2.89459 BTS	0.57892 BTS
ASSET SETTLEMENT	Regular Transaction Fee	0.28945 BTS	0.05789 BTS
GLOBAL ASSET SETTLEMENT	Regular Transaction Fee	28.94592 BTS	5.78918 BTS
PUBLISH FEED	Regular Transaction Fee	0.00057 BTS	0.00011 BTS
OVERRIDE TRANSFER	Regular Transaction Fee	5.78918 BTS	1.15784 BTS
	Price per KByte Transaction Size	0.04052 BTS	0.00810 BTS
CLAIM ASSET FEES	Regular Transaction Fee	5.78918 BTS	1.15784 BTS



Market-Specific

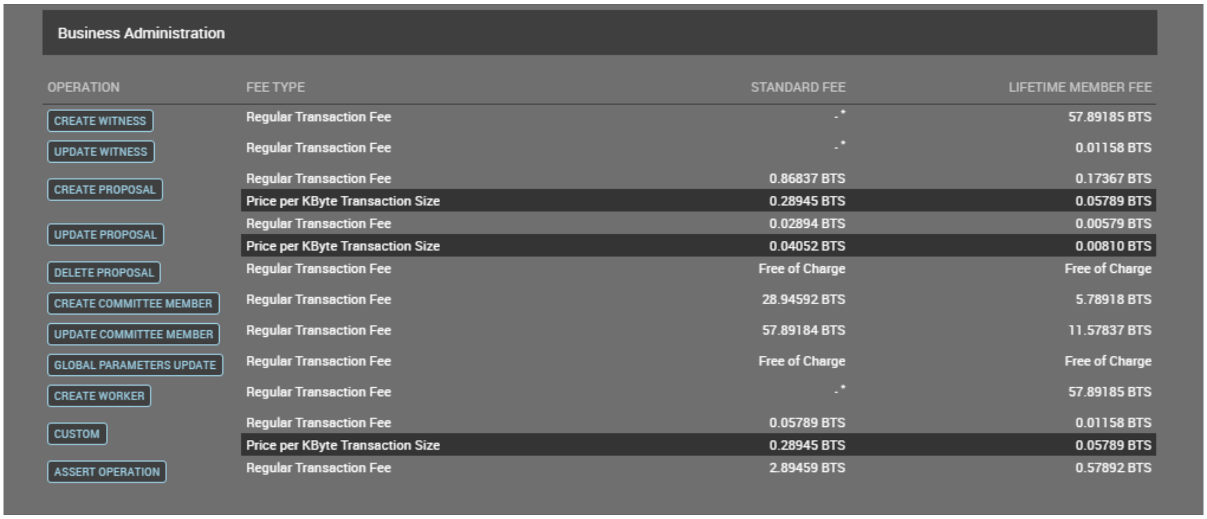
OPERATION	FEE TYPE	STANDARD FEE	LIFETIME MEMBER FEE
PLACE ORDER	Regular Transaction Fee	0.00578 BTS	0.00116 BTS
CANCEL ORDER	Regular Transaction Fee	0.00057 BTS	0.00011 BTS
UPDATE MARGIN	Regular Transaction Fee	0.00578 BTS	0.00116 BTS
ASSET SETTLEMENT	Regular Transaction Fee	0.28945 BTS	0.05789 BTS
GLOBAL ASSET SETTLEMENT	Regular Transaction Fee	28.94592 BTS	5.78918 BTS

Account-Specific

OPERATION	FEE TYPE	STANDARD FEE	LIFETIME MEMBER FEE
CREATE ACCOUNT	Basic Fee	-*	0.11578 BTS
	Fee for Premium Names	-*	5.78918 BTS
	Price per KByte Transaction Size	-*	0.00810 BTS
UPDATE ACCOUNT	Regular Transaction Fee	0.00578 BTS	0.00116 BTS
	Price per KByte Transaction Size	0.04052 BTS	0.00810 BTS
ACCOUNT WHITELIST	Regular Transaction Fee	-*	0.11578 BTS
UPGRADE ACCOUNT	~~Annual Membership~~	~~573,129,310.34482 BTS~~	
	Lifetime Membership	694.70219 BTS	
TRANSFER ACCOUNT	Regular Transaction Fee	28.94592 BTS	5.78918 BTS

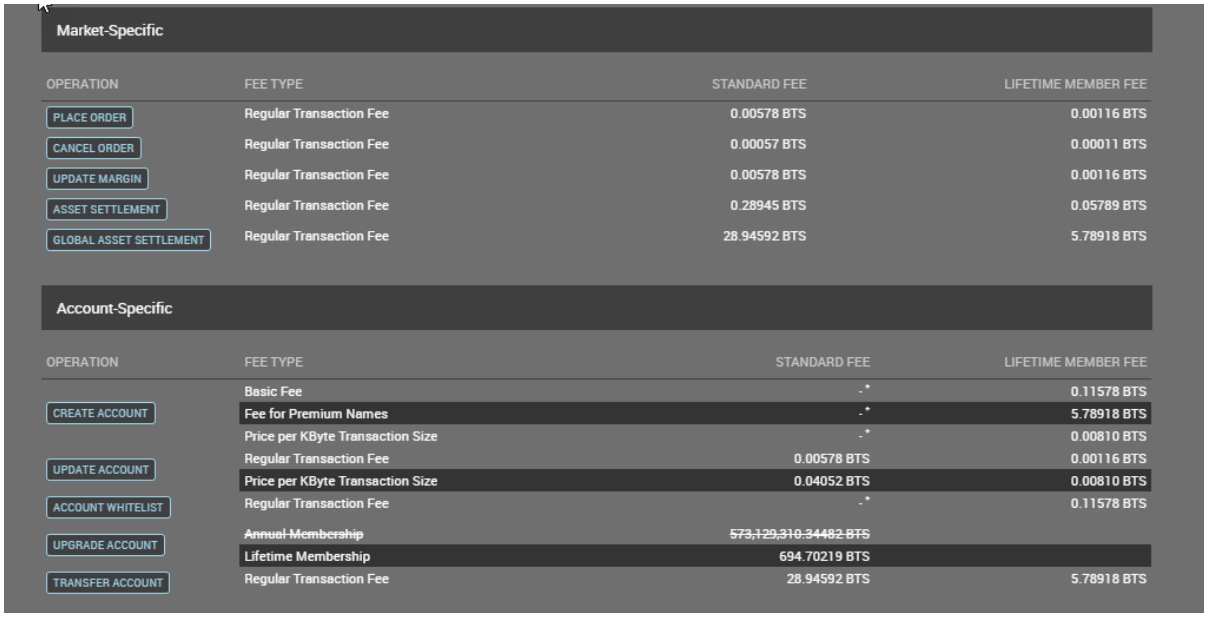
Business Administration

OPERATION	FEE TYPE	STANDARD FEE	LIFETIME MEMBER FEE
CREATE WITNESS	Regular Transaction Fee	-*	57.89185 BTS
UPDATE WITNESS	Regular Transaction Fee	-*	0.01158 BTS
CREATE PROPOSAL	Regular Transaction Fee	0.86837 BTS	0.17367 BTS
	Price per KByte Transaction Size	0.28945 BTS	0.05789 BTS
UPDATE PROPOSAL	Regular Transaction Fee	0.02894 BTS	0.00579 BTS
	Price per KByte Transaction Size	0.04052 BTS	0.00810 BTS
DELETE PROPOSAL	Regular Transaction Fee	Free of Charge	Free of Charge
CREATE COMMITTEE MEMBER	Regular Transaction Fee	28.94592 BTS	5.78918 BTS
UPDATE COMMITTEE MEMBER	Regular Transaction Fee	57.89184 BTS	11.57837 BTS
GLOBAL PARAMETERS UPDATE	Regular Transaction Fee	Free of Charge	Free of Charge
CREATE WORKER	Regular Transaction Fee	-*	57.89185 BTS



Business Administration

OPERATION	FEE TYPE	STANDARD FEE	LIFETIME MEMBER FEE
CREATE WITNESS	Regular Transaction Fee	-*	57.89185 BTS
UPDATE WITNESS	Regular Transaction Fee	-*	0.01158 BTS
CREATE PROPOSAL	Regular Transaction Fee	0.86837 BTS	0.17367 BTS
	Price per KByte Transaction Size	0.28945 BTS	0.05789 BTS
UPDATE PROPOSAL	Regular Transaction Fee	0.02894 BTS	0.00579 BTS
	Price per KByte Transaction Size	0.04052 BTS	0.00810 BTS
DELETE PROPOSAL	Regular Transaction Fee	Free of Charge	Free of Charge
CREATE COMMITTEE MEMBER	Regular Transaction Fee	28.94592 BTS	5.78918 BTS
UPDATE COMMITTEE MEMBER	Regular Transaction Fee	57.89184 BTS	11.57837 BTS
GLOBAL PARAMETERS UPDATE	Regular Transaction Fee	Free of Charge	Free of Charge
CREATE WORKER	Regular Transaction Fee	-*	57.89185 BTS
CUSTOM	Regular Transaction Fee	0.05789 BTS	0.01158 BTS
	Price per KByte Transaction Size	0.28945 BTS	0.05789 BTS
ASSERT OPERATION	Regular Transaction Fee	2.89459 BTS	0.57892 BTS



Market-Specific

OPERATION	FEE TYPE	STANDARD FEE	LIFETIME MEMBER FEE
PLACE ORDER	Regular Transaction Fee	0.00578 BTS	0.00116 BTS
CANCEL ORDER	Regular Transaction Fee	0.00057 BTS	0.00011 BTS
UPDATE MARGIN	Regular Transaction Fee	0.00578 BTS	0.00116 BTS
ASSET SETTLEMENT	Regular Transaction Fee	0.28945 BTS	0.05789 BTS
GLOBAL ASSET SETTLEMENT	Regular Transaction Fee	28.94592 BTS	5.78918 BTS

Account-Specific

OPERATION	FEE TYPE	STANDARD FEE	LIFETIME MEMBER FEE
CREATE ACCOUNT	Basic Fee	-*	0.11578 BTS
	Fee for Premium Names	-*	5.78918 BTS
	Price per KByte Transaction Size	-*	0.00810 BTS
UPDATE ACCOUNT	Regular Transaction Fee	0.00578 BTS	0.00116 BTS
	Price per KByte Transaction Size	0.04052 BTS	0.00810 BTS
ACCOUNT WHITELIST	Regular Transaction Fee	-*	0.11578 BTS
UPGRADE ACCOUNT	~~Annual Membership~~	~~573,129,310.34482 BTS~~	
	Lifetime Membership	694.70219 BTS	
TRANSFER ACCOUNT	Regular Transaction Fee	28.94592 BTS	5.78918 BTS

CHAPTER 21

Securing BitShares with Ledger Nano

Your BitShares account can be secured by a Ledger Nano S hardware wallet. Hardware wallets secure crypto assets by protecting private keys. With a hardware-secured account, transaction signing occurs on the hardware device, rather than the host computer, isolating private keys from exposure to malware or other threats.

This tutorial explains how to create a new BitShares account and set its Active and Owner authorities to keys managed by the Ledger Nano S hardware wallet, using the *BitShares App for Ledger Nano S* and a companion GUI app called *SimpleGUIWallet*.

Contents:

21.1 Requirements

- A Ledger Nano S hardware wallet, with latest firmware.
- An existing BitShares account (optional).
- Ledger-aware wallet software, such as SimpleGUIWallet (described below), for managing your hardware-secured BitShares accounts.

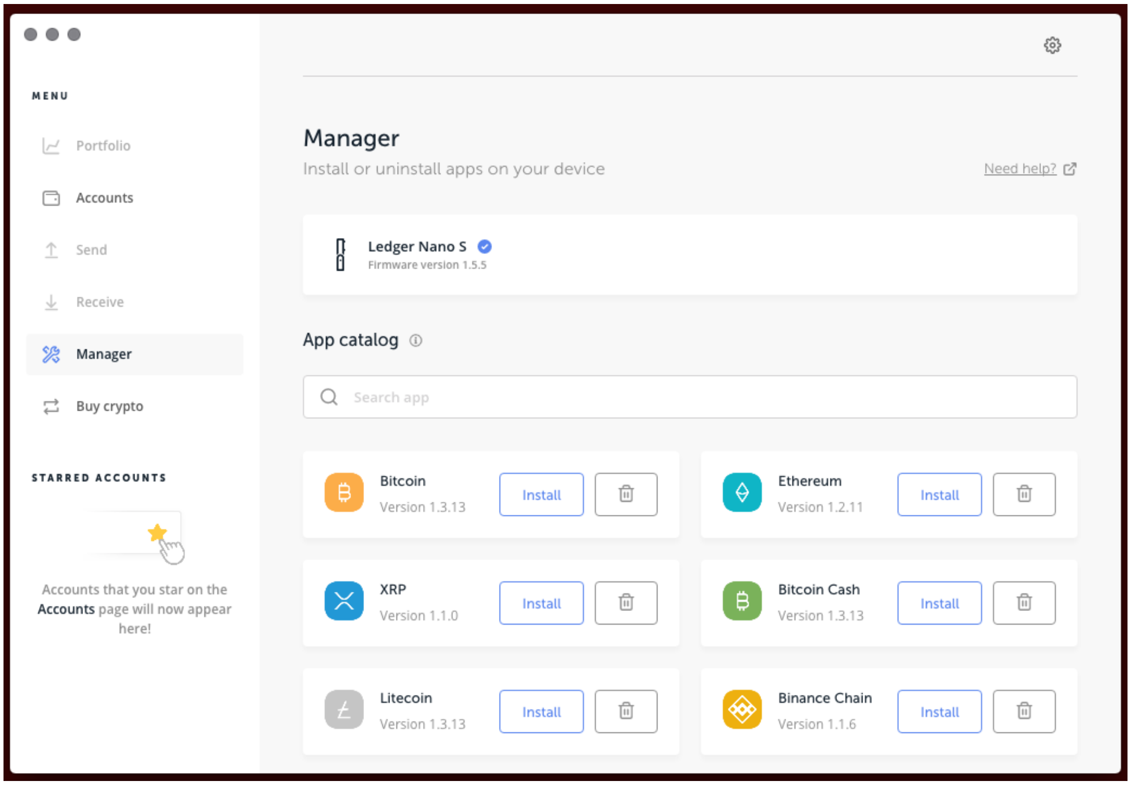
21.2 Installation and Setup

This section covers installation of the BitShares app on the Ledger Nano S hardware device, and the installation of the companion GUI wallet app called SimpleGUIWallet for managing your hardware-secured BitShares accounts from a host computer running Windows, OS X, or Linux.

21.2.1 Installation of BitShares app from Ledger Live

The BitShares App for Ledger Nano can be installed on your Ledger Nano S device from a host computer via the Ledger Live device management app.

1. Select the "Manager" tab from the menu in Ledger Live.
2. Search for the BitShares app in the App Catalog.
3. Click "Install" to install the BitShares app, following on-screen instructions



Manager

Install or uninstall apps on your device

Ledger Nano S
Firmware version 1.5.5

Bitcoin Version 1.3.13

Ethereum Version 1.2.11

XRP Version 1.1.0

Bitcoin Cash Version 1.3.13

Litecoin Version 1.3.13

Binance Chain Version 1.1.6

Accounts that you star on the **Accounts** page will now appear here!

Fig. 1: Ledger Live "Manager" tab, showing installation of BitShares app.

21.2.2 Installing SimpleGUIWallet companion app on host computer

A companion app, compatible with Windows, Mac, and Linux, for communicating with the the BitShares Nano app, is available from:

- SimpleGUIWallet (ledger-app-bitshares)

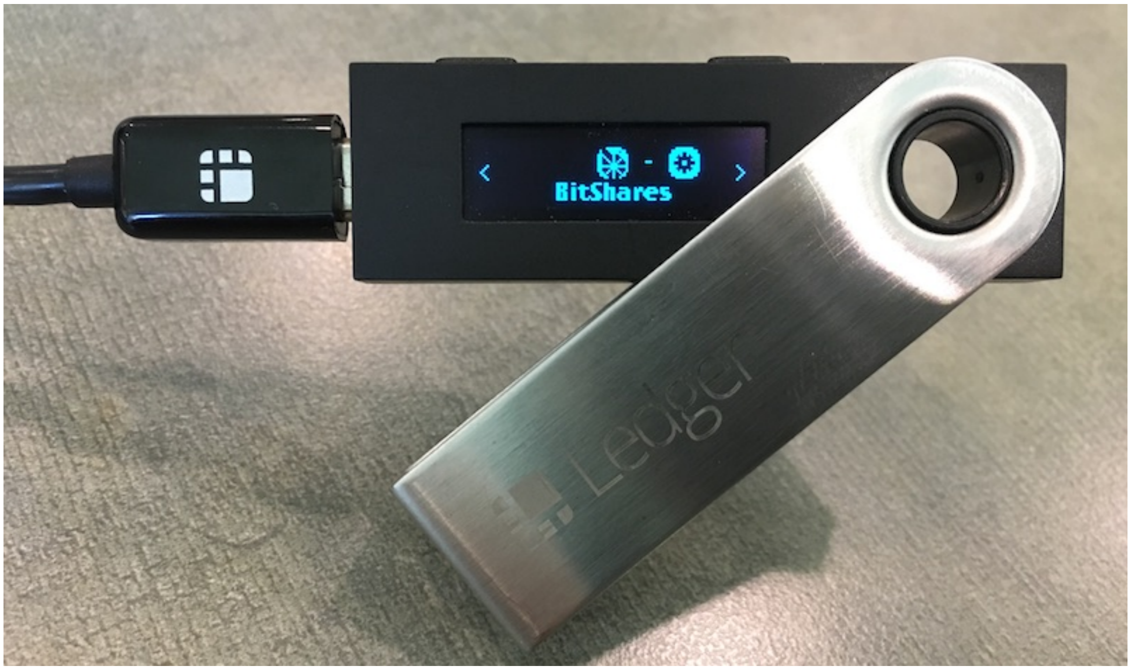


Fig. 2: Ledger Nano S Dashboard showing BitShares app installed.

21.3 Securing a BitShares Account with the Ledger Nano

BitShares accounts work differently from Bitcoin wallets in that a named account must be registered on the BitShares blockchain. The account will declare one or more public keys to act as "authorities" capable of signing transactions.

BitShares accounts are very capable and flexible. The platform supports over 40 operation types. The most commonly used operations center around trading on the decentralized exchange (DEX), and of course simple transfers of tokens. The BitShares "Reference" UI wallet (web wallet: https://wallet.bitshares.org; standalone wallet: https://github.com/bitshares/bitshares-ui/releases) supports the full functionality of a BitShares account. By contrast, the Ledger Nano BitShares app is primarily geared towards simple transfers and holding of tokens, although it is technically capable of signing any operation type.

This tutorial assumes that you already have an existing BitShares account for use in a standard, full-featured BitShares UI, and that you will be creating a new, separate account, to hold tokens secured by your Ledger Nano S hardware wallet device. Essentially, we assume your existing account will be the "hot wallet," and the new account will be your hardware-secured "cold wallet."

21.3.1 Step 1: Create an account to associate with the Nano

If you already have a BitShares account and it has "lifetime membership" status, you can easily create a new account by selecting "Create Account" from the main drop-down menu ("Burger" menu) in the upper-right corner of the Reference UI.

If you do not already have a BitShares account, or if your account does not have lifetime-membership status, then you can use either the standalone wallet or one of the web-hosted wallets (e.g. https://wallet.bitshares.org) to register the account, and a faucet will pay the registration fee for you. A tricky thing though is that most such wallets will only pay the registration fee for ONE account per wallet instance. So if you used the standalone wallet to register your primary account, then you may wish to use the web-hosted wallet to register your new account, or vice-versa. Or you can just load the web wallet from a different device, (or a different browser), to get back to the faucet-subsidized account registration screen.

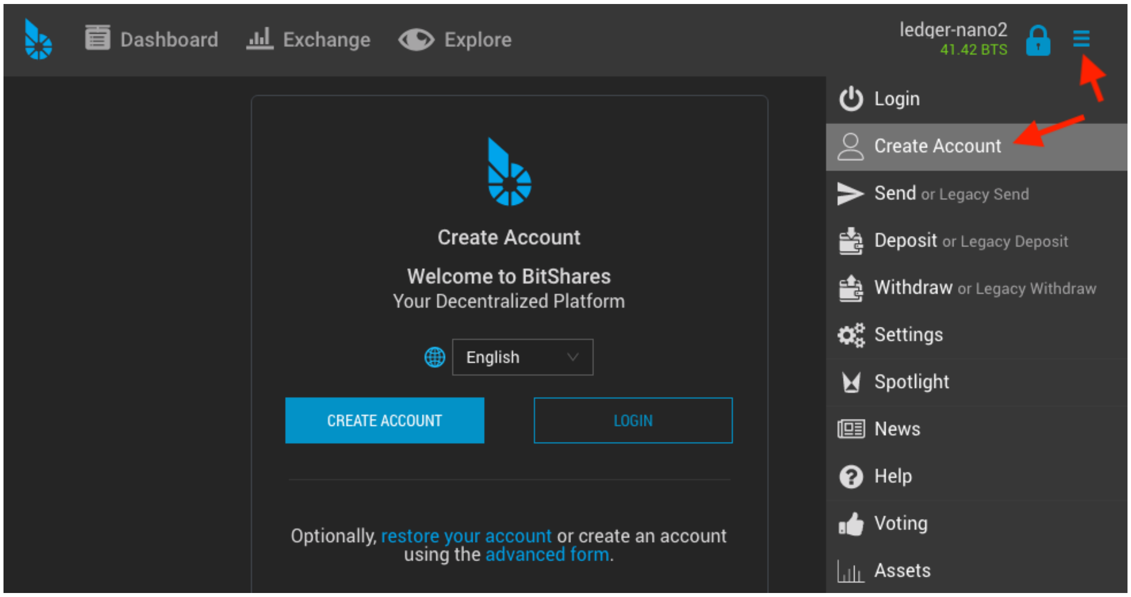


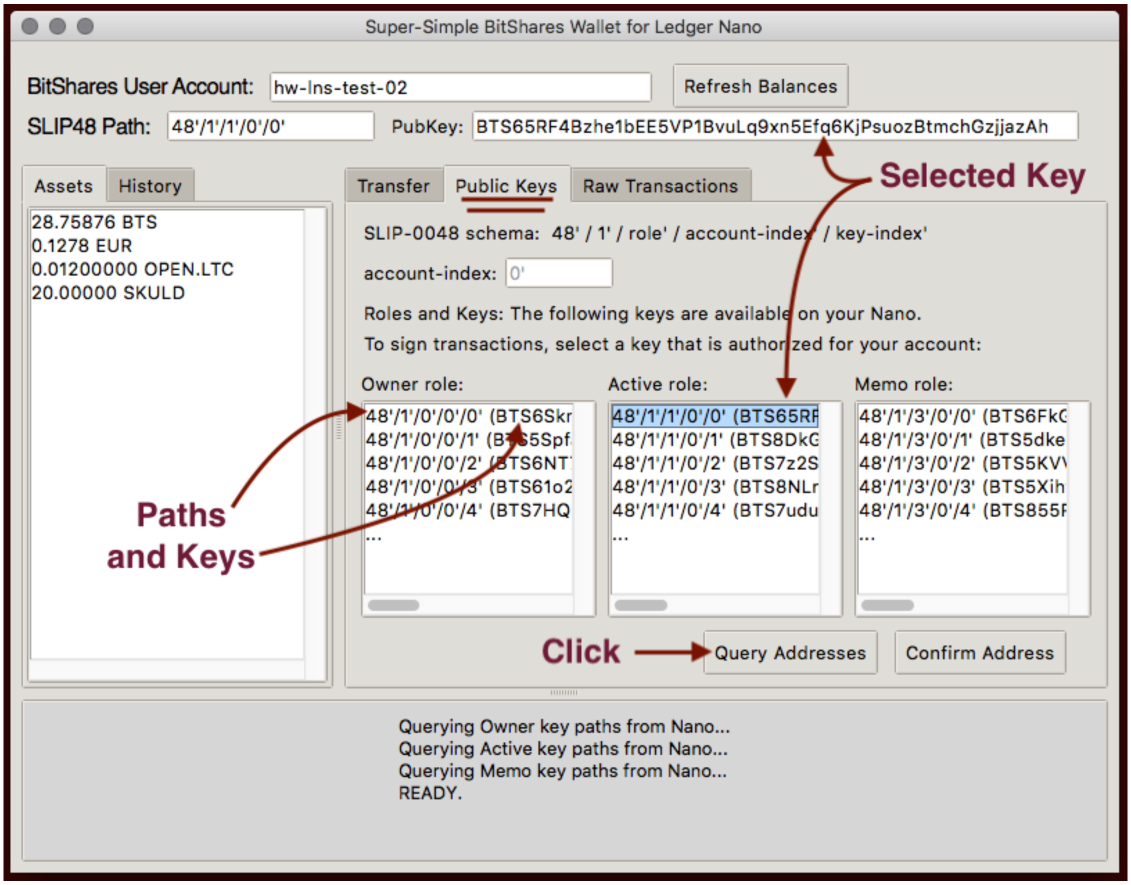
Fig. 3: Account Create form in the BitShares reference UI Wallet.

Once you have created this account, you will next need to retrieve **two** public keys from your Ledger Nano S hardware wallet, and set them as your account's "owner" and "active" authorities. Once the original account keys are removed and replaced with these new keys, the account will be controlled solely by the Ledger Nano S hardware device.

21.3.2 Step 2: Get Public Keys from the Ledger Nano

A BitShares account specifies two types of authorities: "Owner," and "Active," which each declare a weighted list of public keys needed to sign transactions. (The weights allow for multi-signature arrangements. Here we will only consider a single key per authority.) For the majority of transaction types, either the "owner" authority or the "active" authority may sign the transaction. Your newly-created account will have had default keys generated for it during registration. We will replace these keys with public keys retrieved from the Ledger Nano device. We do this as follows:

1. Start up the companion app, *SimpleGUIWallet*.
2. Connect your Ledger Nano S hardware wallet device, unlock with PIN code, and start the BitShares app.
    - The Nano should display the BitShares logo and the words **Use wallet to view accounts**.
3. In the companion app, select the "Public Keys" tab from the main tab array.
    - The window will show list boxes of SLIP-0048 derivation paths for three different "roles": Owner role, Active role, and Memo role.
    - (Note: SLIP-0048 is a key derivation scheme analogous to Bitcoin's BIP-44, but tailored for the key roles used in Graphene-based blockchains such as BitShares.)
    - Each path will not yet show a public key, but instead will show "(??)".
4. Click the "Query Addresses" button to retrieve the public keys corresponding to each derivation path from the Nano device.
    - The list boxes will now be populated with paths and public keys.
5. Now we wish to select one key to use for our account's Owner role and one for the Active role. You may of course choose any key, but the recommendation is to choose the first key on the "Owner role" list (path



BitShares User Account: hw-lns-test-02

SLIP48 Path: 48'/1'/1'/0'/0'

PubKey: BTS65RF4Bzhe1bEE5VP1BvuLq9xn5Efq6KjPsuozBtmchGzjjazAh

28.75876 BTS
0.1278 EUR
0.01200000 OPEN.LTC
20.00000 SKULD

SLIP-0048 schema: 48' / 1' / role' / account-index' / key-index'

account-index: 0'

Roles and Keys: The following keys are available on your Nano.
To sign transactions, select a key that is authorized for your account:

Owner role:	Active role:	Memo role:
48'/1'/0'/0'/0' (BTS6Skr	48'/1'/1'/0'/0' (BTS65RF	48'/1'/3'/0'/0' (BTS6FkG
48'/1'/0'/0'/1' (BTS5Spf	48'/1'/1'/0'/1' (BTS8DkG	48'/1'/3'/0'/1' (BTS5dke
48'/1'/0'/0'/2' (BTS6NT	48'/1'/1'/0'/2' (BTS7z2S	48'/1'/3'/0'/2' (BTS5KV
48'/1'/0'/0'/3' (BTS61o2	48'/1'/1'/0'/3' (BTS8NLr	48'/1'/3'/0'/3' (BTS5Xih
48'/1'/0'/0'/4' (BTS7HQ	48'/1'/1'/0'/4' (BTS7udu	48'/1'/3'/0'/4' (BTS855F
...	...	...

```
Querying Owner key paths from Nano...
Querying Active key paths from Nano...
Querying Memo key paths from Nano...
READY.
```

Fig. 4: The Public Keys tab can be used to list public keys controlled by the Ledger Nano device, organized by derivation path.

48’/1’/0’/0’/0’) for the owner authority and the first key from the “Active role” list (path 48’/1’/1’/0’/0’) for the active authority. When an item from the list box is selected, the public key appears in the PubKey box at the top of the window, where it can be copied to your computer’s clipboard.

21.3.3 Step 3: Confirm keys on Ledger Nano device

It is highly recommended to *confirm* your selected keys on the Ledger Nano device prior to importing them as authorities into your new BitShares account. This is to ensure that the *SimpleGUIWallet* companion app has not been tampered with to give you a decoy key. Confirm keys as follows:

1. In the “Public Keys” tab of *SimpleGUIWallet*, query addresses as in the subsection above. Then select the key you wish to confirm from the list, and click the “Confirm Address” button.
2. On your Ledger Nano device, look to see that the device says “**Confirm public key**” and displays the exact same public key as you see in the *SimpleGUIWallet* app. If the keys do not match, DO NOT trust the key from *SimpleGUIWallet*. If the keys do match, then you know that the Ledger Nano device can sign transactions using the key, and you may import the key into your account, as described in the next subsection.

21.3.4 Step 4: Add the keys to your new account

In the BitShares UI wallet where you created your new account, navigate to the “Permissions” area by clicking the Menu icon (upper right), selecting “Settings,” then “Accounts,” and then “View Keys” for the appropriate account, as illustrated below:

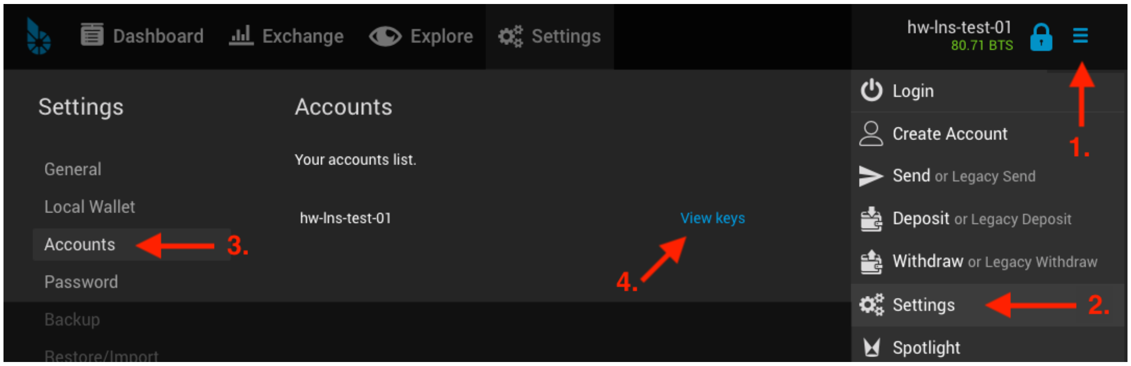
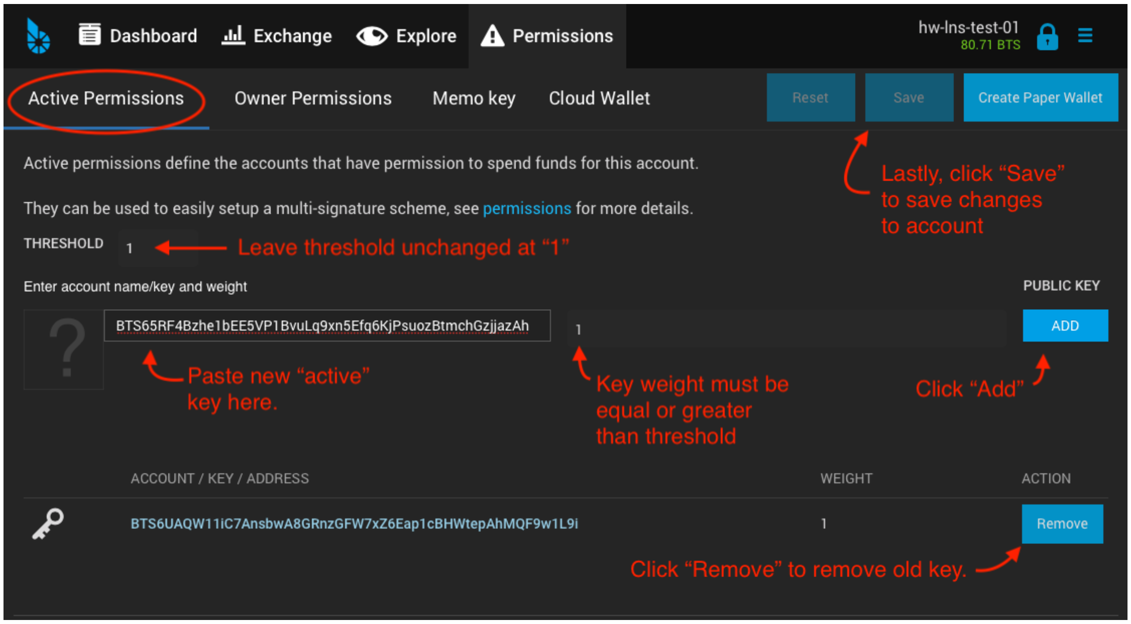


Fig. 5: Keys are managed under Settings —> Accounts —> View Keys.

Once in the “Permissions” tab, you should see the screen below, where we will first replace the Active authority key, and then the Owner authority key.

Steps:

1. Select the “Active Permissions” sub-tab, (if not already selected).
2. Observe the “Threshold” value. If this is a new account, registered in the standard way, this value should be “1”. Do not change it.
3. In the “Enter account name/key and weight” field, paste an appropriate key copied from the “Public Keys” tab in *SimpleGUIWallet*. (E.g. a key from the “Active role” list, if this is for the account’s active authority.)
4. For the key weight, enter “1”. (This is equal to the threshold, meaning this key can unilaterally sign transactions as the account’s active authority.)



Active permissions define the accounts that have permission to spend funds for this account.

They can be used to easily setup a multi-signature scheme, see permissions for more details.

THRESHOLD 1

Enter account name/key and weight

BTS65RF4Bzhe1bEE5VP1BvuLq9xn5Efq6KjPsuozBtmchGzjjazAh 1

ACCOUNT / KEY / ADDRESS	WEIGHT	ACTION
BTS6UAQW11iC7AnsbwA8GRnzGFW7xZ6Eap1cBHWtepAhMQF9w1L9i	1	Remove

Lastly, click "Save" to save changes to account

Leave threshold unchanged at "1"

Paste new "active" key here.

Key weight must be equal or greater than threshold

Click "Add"

Click "Remove" to remove old key.

Fig. 6: Adding a new Active key and removing the old one.

5. Click "Add" to add the key to the list of keys recognized by the account. You will now see two keys listed under "Account / Key / Addresses". They are the new key just added, and the old key that was generated when the account was registered.
6. Click the "Remove" button next to the old key. This will remove the ability of the old key to sign transactions for the account, leaving only the key derived from the Ledger Nano device to sign as the account's active authority.
7. At the top of the window, click the "Save" button to apply these changes to the account. You will be asked to confirm the "account update" transaction, and may be asked to type the password you chose when you created the account, in order to unlock the UI wallet. When the transaction is broadcast and confirmed on the blockchain, your account's Active authority will have been successfully replaced with the new key managed by the Nano.

Once these steps are complete, repeat the above steps, but this time for the "Owner Permissions" tab, and select a Nano key from the "Owner role" list box.

When both the Active and Owner keys have been replaced, your new account can *ONLY* sign transactions with the aid of your Ledger Nano hardware device, and your account is now secured.

(Note: The BitShares UI wallet Permissions tab will also let you replace the Memo key. However, this is not recommended in this tutorial. Although SLIP-0048 does define a key path for memo keys, and these public keys can be retrieved from the Nano, the Ledger Nano S BitShares app does not currently support encrypting or decrypting memos with the Nano. Leaving this key unchanged means you can still use the regular BitShares UI wallet to read memos attached to transactions.)

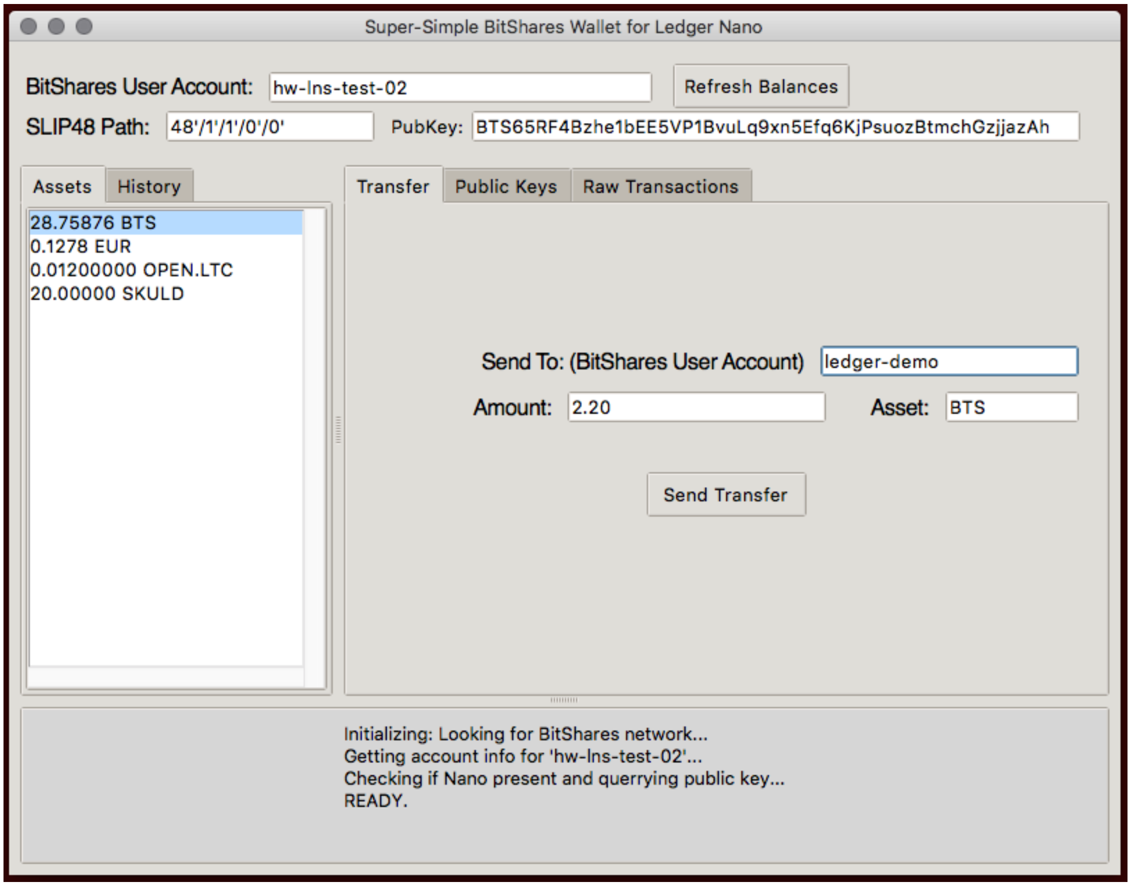
21.4 Using the Companion app with Nano BitShares app

SimpleGUIWallet is a very bare-bones, rudimentary GUI interface to the Ledger Nano BitShares app. It does not maintain a database of keys or accounts, and will not write any data or configuration files to disk. When you start *SimpleGUIWallet*, you will need to tell it which BitShares account you wish to use, and which key (specified as a SLIP-0048 derivation path) to use when signing transactions.

The *SimpleGUIWallet* window is divided into four general areas:

- **Top**: This is where you type the name of a BitShares account that you wish to act as, and which key will be used to sign transactions.
- **Middle Left**: Here there are two tabs that show information about the selected account. After clicking “Refresh Balances,” the Assets tab will populate with a list of assets (tokens) held by the account, and the History tab will populate with a list of recent transactions conducted by the account.
- **Middle Right**: Here are tabs where you can “do things.” There is a tab for transferring tokens, a tab for querying the Ledger Nano to determine what keys it manages, and a tab for Raw Transactions, which can be used for advanced purposes not covered by this tutorial.
- **Bottom**: At the bottom is a status pane that will print messages informing you of how the app is interacting with the BitShares network and with the Ledger Nano hardware device.

When you start up *SimpleGUIWallet*, it will automatically connect to the BitShares network by locating a public API node to communicate with.



BitShares User Account: hw-lns-test-02

SLIP48 Path: 48'/1'/1'/0'/0'

PubKey: BTS65RF4Bzhe1bEE5VP1BvuLq9xn5Efq6KjPsuozBtmchGzjjazAh

28.75876 BTS
0.1278 EUR
0.01200000 OPEN.LTC
20.00000 SKULD

Send To: (BitShares User Account) ledger-demo

Amount: 2.20

Asset: BTS

```
Initializing: Looking for BitShares network...
Getting account info for 'hw-lns-test-02'...
Checking if Nano present and querrying public key...
READY.
```

Fig. 7: BitShares SimpleGUIWallet desktop companion app for Ledger Nano S BitShares app.

21.4.1 Viewing account balances

BitShares is a multi-asset platform. The core token on BitShares is the BTS token, but there are also numerous user-issued assets and assets defined by smart contracts. The Ledger Nano S BitShares app can send and receive any tokens that your BitShares account can hold.

The “Assets” tab on the left side of the window shows a list of assets held by the selected account, and their respective balances. After typing a BitShares account name in the “BitShares User Account” field at the top of the window, click the "Refresh Balances" button to refresh this list.

21.4.2 Receiving tokens

Receiving crypto assets is very easy in BitShares. Just give the sending party your BitShares account name, and they can send tokens to you. There is no need to retrieve "addresses" or keys from the wallet in order to receive funds.

21.4.3 Sending tokens

Sending tokens from your account can be done on the "Transfers" tab.

1. Enter your account name in the "BitShares User Account" field.
   - Optional: Click "Refresh Balances" to see asset balances for this account in the Assets tab.
2. Select the "Transfer" tab.
3. Fill out the "Send To", "Amount", and "Asset" fields.
   - The "Asset" field takes a ticker symbol for the token type that you wish to send. See the "Assets" tab for a list of tokens in your account.
   - Tip: Clicking an asset balance in the Assets list will auto-populate the asset symbol field on the Transfer tab.
4. Connect your Ledger Nano and start the BitShares app.
5. Click "Send Transfer".
6. Review transaction details on the Ledger Nano's display screen, and approve the transaction on the device via the "check" button if the details are correct, else reject it via the "x" button.
7. If you confirmed the transaction on the device, then *SimpleGUIWallet* will receive a signature from the Nano, append it to the transaction, and broadcast it to the BitShares network. The status pane will indicate if the transaction was successful or not.

After the transaction is broadcast, the balances in the Assets tab should update. If they do not, click "Refresh Balances" to refresh them. Likewise, the transfer operation should appear on the "History" tab, if the transaction was successful.

21.4.4 Advanced usage

If you have followed this tutorial, then your new account is now solely controlled by keys managed by your Ledger Nano S hardware wallet device. It is possible that you may at some point desire to use some of the other features of the BitShares platform, beyond simple transfers. The *BitShares App for Ledger Nano S* can sign any valid BitShares transaction, provided you can send it to the device for signing. The "Raw Transactions" tab in *SimpleGUIWallet* allows this, provided you can construct the transaction as a JSON string. How to do this is not covered by this tutorial, but the reader is directed to consult the technical documentation for BitShares or to seek the help of the BitShares community via forums or chat rooms.

21.5 Getting Support

- https://bitshares.org
- https://how.bitshares.works/ — BitShares documentation
- Ledger Nano BitShares App Issue Tracker — Submit bug reports here.

- Various Telegram groups:
  - t.me/BitSharesDEX
  - t.me/btsWalletHelp
  - t.me/btstalk

CHAPTER 22

BitShares Community

22.1 Communities

- Forum - BitSharesTalk
- Telagram - BitSharesDAC
- Telagram - BitShares Traders
- **‘Discord - BitShares (to be updated)‘_**
- BitShares on Steemit
- Twitter
- Reddit
- BitSharesTalk.io
- (*will be added more*)

CHAPTER 23

BitShares Blockchain

23.1 BitShares UI Wallet

- BitShare UI wallet

23.2 Bitshares Block Exploer

- Cryptofresh
- bts.ai
- blocksights.info

23.3 Blockchain Activity

- Blocktivity

CHAPTER 24

Resources External

24.1 From steemit

- Community News - by @officialfuzzy
- Bitshares - State of the Network - by @steempower
- Bitshares - by @blockchained
- BitShares Hangout Recordings - by @ash
- Beyond Bitcoin | Bitshares Talk | - by @africa
- Bit20 - The cryptocurrency index fund - by @blocktivity
- Bitshares DEX Thailand- Blog - by @apasia.tech
- Bitshares GUI Release… - by @billbutler

24.2 Articles

- The total noobs guide to Bitshares : by @funkit
- Market Pegged Asset (MPA) backing collateral layers : by @customminer
- BITSHARES HELP DESK & SUPPORT RESOURCES - How to get answers fast! OpenLedger included! : by intelliguy
- BitShares Enterprise Alliance - Part 1 - Alice's Hero Hub : by @stan
- How IOUs like open.BTC work on the DEX …. and yesterday's half billion dollar CEX heist (01/2018) by @apasia.tech
- BitShares Rough Guides – UIA & IOUs – what's the difference and how do they apply to assets like open.BTC ? (12/2017) by @apasia.tech
- BitShares – Tour of the Token Factory (12/2017) by @apasia.tech

- Rough Guide to the DAC – Part 3 – Worker Proposals on the Blockchain (12/2017) by @apasia.tech
- BitShares - Rough Guide to the DAC - Part 2: Witnesses and DPoS (Not Mining) (12/2017) by @apasia.tech
- BitShares: Rough guide to the DAC - Part 1: Committee Members and Governance (12/2017) by @apasia.tech
- BitShares How-to Tutorial Video 1 - Setting up a Wallet on the BitShares DEX (01-2018) by @tonypeacock
- What is BitShares in 35 Seconds (12/2017) by @tonypeacock