bitsquare

The decentralized bitcoin exchange

Version 1.2 (last edited: January 03 2016)

Introduction

Bitsquare is an **open source** peer-to-peer application that allows anyone to buy and sell Bitcoin in exchange to **national currencies** or **alternative crypto currencies.**

Unlike existing exchanges, Bitsquare is **fully decentralized** and **censorship resistant** using alternative protection mechanisms:

- escrow transaction employing 2-of-3 multisignature address
- security deposits to incentivise following the trade protocol
- a decentralized arbitration system helps resolve disputes

Bitsquare protects user's **privacy** by using a custom **P2P network over Tor**, in which every user is a participating node. An all-in-one **desktop application** (for Linux, OS X and Windows) provides an intuitive user interface and executes the trading protocol.

Motivation

Bitcoin is a **censorship resistant** payment system, because it avoids dependence on trusted third parties. Currently, the process of acquiring Bitcoin does not follow the same principles due to the lack of a fully decentralized solution. Bitsquare aims to fill this gap.

Core values

There is a variety of Bitcoin exchanges out there, but all of those are operating in a traditional way where the user needs to trust a centralized system with his funds and expose his data and financial privacy. The vulnerability of such models has been demonstrated numerous times - most notably by MtGox. But theft and server hacks are not the only issue: centralized exchanges are vulnerable to coin-tracing on a mass scale, which is a serious violation for users' privacy.

The key point of **decentralization** is the lack of single points of failure, control or censorship. Bitsquare holds these values in every aspect of the project:

- Infrastructure (P2P network - there are no servers)
- Never hold user's funds (neither bitcoins nor fiat)
- Never hold user's data (no account registration)
- The software is developed open source, there is no controlling company
- No individual persons have leverage over the developers, as the project is self-funded and in part through donations

Furthermore we consider **privacy** as a fundamental human right which needs to be protected as far as possible.

- The P2P network operates over Tor (using Tor hidden services)
- All private data sent over the wire is end-to-end encrypted
- No privileged access to any data (public data is public to everyone, private data only accessible to the traders)

Comparison to related projects

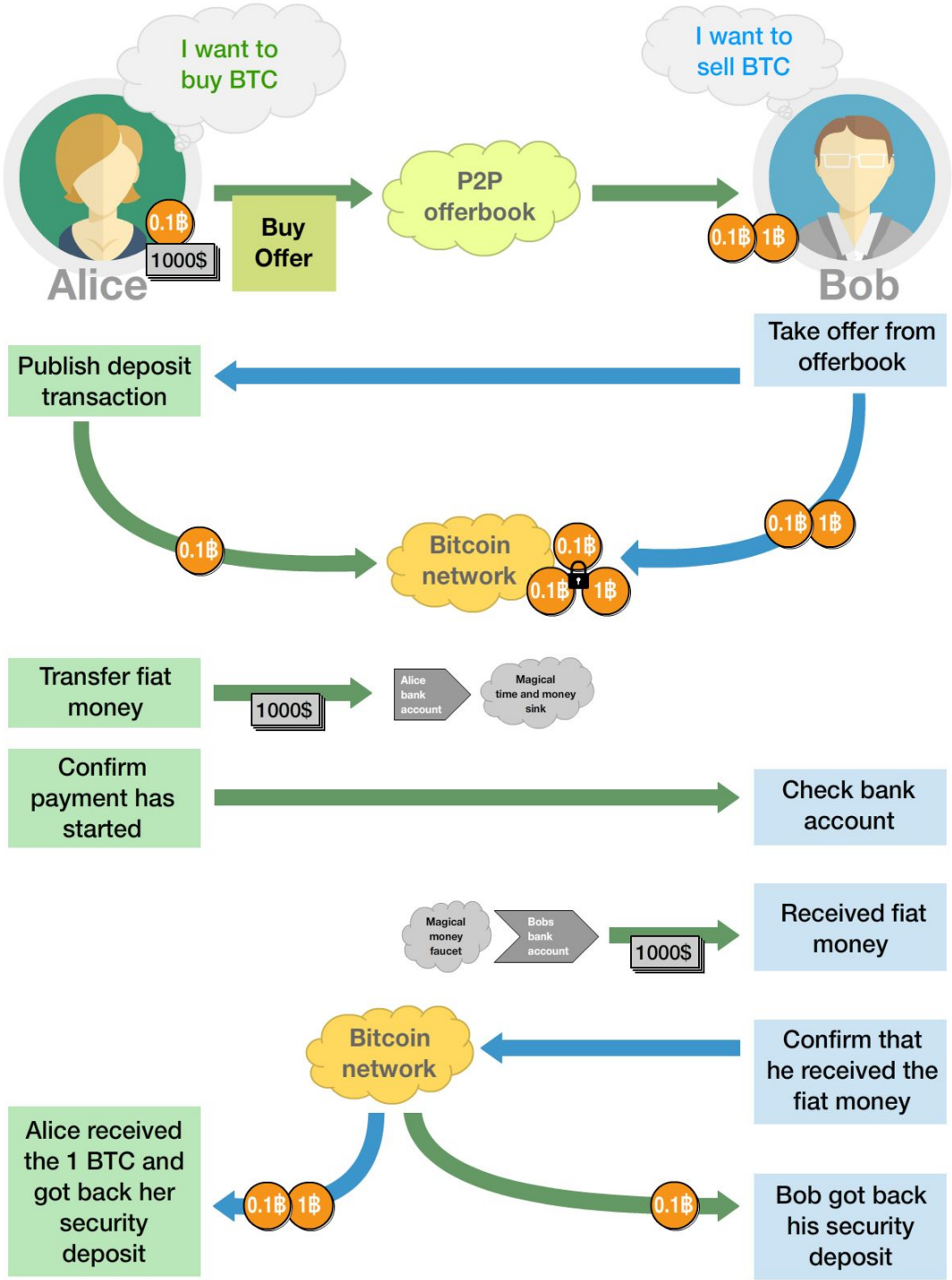
One may describe Bitsquare is as a **fully decentralized** version of LocalBitcoins, where:

- no central place exists to collect user data
- no servers exist to attract adversaries
- no trust is needed in the service provider (Bitsquare)
- users have exclusive ownership of their funds
- users do not rely on a reputation system, which can be manipulated

Bitsquare resembles other decentralized projects, such as OpenBazaar or Bitmarkets, which employ similar protection mechanisms. However, those projects behave as Ebay-style marketplaces rather than (crypto-)currency exchanges.

Overview

This graphical overview shows the basic high-level flow of the trade process. See the **detailed version** for more information.



These **videos** demonstrate the current software and give a more detailed explanation of the trade process. A detailed graphical representation of the **trade protocol** should help to explain

the way the payment process is executed. A document also discusses the possible **risks, attacks and protection mechanisms**. An **arbitration system** will serve as primary protection mechanism and is also described in a separate document.

Main characteristics

- P2P infrastructure without servers: No single point of failure and no privacy breach due transaction monitoring possible.
- National (or alternative crypto) currency are transferred directly from one user's payment account to the others payment account without any intermediate party.
- Support for alternative crypto currencies to be exchanged with Bitcoin.
- No registration or identification process
- Decentralized arbitrator system as primary protection mechanism
- Security deposit as additional incentive for following the trade protocol
- A atomic deposit transaction locks up both traders funds to a 2 of 3 multisig address
- Trading fees as protection against spam and market manipulation
- A limit on the trade amount (1 BTC) to reduce the overall risk exposure
- Open source license (AGPL)
- Contract holds all trade details and is signed by both traders, it will be used as evidence in case of a dispute
- Fraud reports as protection against bank charge backs and crime (stolen payment account)

Protection mechanisms

For protecting against several fraud and attack scenarios we use different solutions:

- Trader's security deposit - refunded after successful trade or used as payment for the arbitrator in case of a dispute.
- Arbitrator - anonymous and randomly assigned. Resolves disputes between traders.
- Arbitrator's security deposit - locked when the arbitrator is registered and released upon stepping down.
- Contract - blinded non-refutable proof of trade details
- Fraud report - reports by arbitrators with proof of clear cases of fraud
- Trade volume limitation - limits to maximum trade volume in order to reduce potential gain from fraud

Business model

Bitsquare is not a company, but an open-source project that aims to fill a gap in the cryptocurrency ecosystem: to provide an exchange platform which follows the same principles as Bitcoin itself. A unique incentive mechanism is set up to support the project:

- transaction fees go in part to the developers and in part to the arbitrators
- in the event of disputes, arbitrators collect the security deposit of the losing party (or in some cases half the deposit of each party)

Technology

The Bitsquare application is built in Java 8 with JavaFX for the GUI. For interaction with the Bitcoin network the BitcoinJ library is used. For decentralized messaging and data storage a custom flooding (gossiping) network over Tor is used.

P2P network

There are a few main use cases for the P2P network:

- Broadcast data (typically offers - public data)
- Messaging between trading peers (private and end-to-end encrypted)
- Data storage if trading peer is offline (mailbox- like system)

Key features of the P2P network technology:

- Highly accessible (NAT traversal, firewalls,...)
- Protect privacy (Tor hidden services)
- Redundant data storage (flooded to all peers)
- Data access protection (using signatures)
- Resistant against spam/flooding
- Scalable

You can find more details about the P2P network here.

Wallet

Bitsquare protects the privacy between trades by separating each trade with a different set of addresses. No addresses will be used across multiple trades avoiding coin merge and de-anonymisation vectors. The user needs to further take care when doing the deposit from and withdrawal to his external wallet to avoid loss of privacy due coin merge (e.g. usage of Coin Join solutions).

Wallet key features:

- Manage the key pairs (HD wallet)
- Create regular and pay-to-script-hash (P2SH) transactions
- Sign transactions
- Broadcast transactions
- Add hash of contract to a transaction (eg. OP_RETURN)

Security Deposit

The security deposit will be derived from the arbitration fee which will be used as payment to the arbitrator only in case of a dispute resolution. If no dispute is opened, this deposit is returned in whole to each trader.

The security deposit serves also as an incentive to follow the protocol (e.g. to ensure Bob is not lazy or careless and forgets to release the payout transaction) as well as a mechanism to ensure a dishonest trader is forced to pay the costs for arbitration.

Fees

The fees are necessary for protection against offer book spam, market manipulation and identity harvesting. They are also needed as payment to the arbitrators for their services. Arbitrators are compensated for agreeing in advance to be available to arbitrate a trade even in the case the trade is not disputed.

Initially the fees will be kept to a minimum. Later as the trading community grows the fees will be adjusted as needed to make the arbitration system sustainable and to adjust to the level of observed fraud activity.

To make the payment process fast we do not wait for transaction confirmation of fees. A double spend of the fees is potentially possible but highly unlikely, due to the difficulty of its execution and its low profitability. There will be a second verification at the end of the trade process where a double spend would be detected and that could be used for local blacklisting.

Bitsquare operates with the following fees:

- Create offer fee: 0.001 BTC (paid to the arbitrators, mining fee is included)
- Take offer fee: same as create offer fee (and also paid to the arbitrators)
- Bitcoin mining fee: 0.0003 BTC (A mining fee is included in a transaction three times: Deposit from external wallet, trade, and withdrawal to external wallet. So the sum is 0.0009 BTC)
- Security deposit (might be used as arbitration fee): 0.1 BTC, which is returned in whole to the trader after the transaction in case he is not found to have behaved dishonestly. The security deposit from dishonest trader will be used to pay the arbitrator for his efforts. In rare cases half the security deposit of each trader may be collected instead. The active arbitration fee is not related to the size of the trade and does not affect the time required to mediate a dispute as the amount of work an arbitrator must perform is roughly constant even when small amounts are exchanged.
- (only for arbitrators) arbitrator's security deposit: 2 BTC. In addition, a part of each collected arbitration fee from dishonest traders is locked in the security deposit. This (accumulated) amount is returned in whole to the arbitrator upon stepping down from arbitration.

Trading protocol

The desktop application implements the protocol for the trading process. When broadcasting an offer, the offering peer agrees to accept any take-offer request which fulfills the terms defined in the offer. The take-offer process requires that the Bitsquare applications of both traders are running (it can run in background). They do not need to be physically present at their computer, but the software needs to be online to react to the take offer request.

The Bitcoin buyer should wait for at least 1 blockchain confirmation as protection against double spend, before starting the transfer of the national currency (or alternative cryptocurrency). The Bitcoin seller will release the deposit after he has confirmed the receipt of the national currency. Here is a detailed graphical overview of the trade protocol.

Arbitration

Bitsquare relies on a decentralized arbitration system to ensure that traders fulfill their obligations. See the "Arbitration System" document for more details on how this system works.

Fraud reports

A fraud report is used to warn about fraud from bank chargebacks, stolen payment accounts or arbitration fee fraud. The arbitration system can not help in these cases because the Bitcoin payment has already been released by the time the fraud is discovered. The fraud report only serves to prevent repeated scam with the same payment account and Tor onion address. More details can be found in the "Risk Analysis" document.

Limitations and risks

within Bitsquare

- Only non-reversible payment transfer methods are supported to minimize the risk of chargebacks
- You can trade at most 1 Bitcoin per transaction
- You must already have a small amount of Bitcoin to execute a trade (for paying the security deposit, trade fee and Bitcoin mining fee)
- The Bitsquare application must be running (can run in background), in order to allow the user's offer to be taken.
- Bitcoin is always one part of the exchanged currencies. One cannot trade alternative cryptocurrencies for national currencies.
- Arbitrators need to lock away 2 Bitcoins, which are only returned when they step back from their service.

outside Bitsquare

- Depending on the payment method: Personally identifying information will be revealed to the trading partner and stored in the contract as part of the payment transfer.
- The speed of the trade process depends on the duration of the payment transfer.
- Application should not be used in jurisdictions where Bitcoin is illegal (risk from trading with undercover agents).

Remarks

Identity verification

Bitsquare does not carry out identity verification of users. However, in the event of a dispute, the assigned arbitrator may need to check the identity of the traders. This information is only visible

to that arbitrator and to at most one senior arbitrator. Users may request that identity verification is carried out over encrypted channels, e.g. using Tox instead of Skype. See the "Risk Analysis" document for more information.

Reputation system

Bitsquare does not use a reputation system, as such systems can easily be manipulated, e.g. by a Sybil attack.

Example use cases

Standard exchange process

1. Trader selects the arbitrators he want to accept in case of disputes or stick with the default selection of all matching arbitrators.
2. Trader sets up a payment method account.
3. Buyer deposits bitcoins from external wallet (for security deposit, create-offer fee and mining fee)
4. Buyer publishes the offer. Create-offer-fee gets paid to one of his selected arbitrators. The security deposit will be locked in his local Bitsquare trading wallet in case someone takes the offer.
5. Seller deposits bitcoins from external wallet (for security deposit, take-offer fee, mining fee and the trade amount)
6. Seller takes offer. The software sends his security deposit and Bitcoin trade amount to a 2-of-3 multisig address.
7. Buyer transfers the national currency (or alternative cryptocurrency) amount directly to Seller outside Bitsquare (e.g. via online banking web page or altcoin wallet)
8. Seller confirms upon payment receipt and releases Bitcoin from the escrow address
9. Buyer withdraws trade amount and his refunded security deposit to an external wallet
10. Seller withdraws his refunded security deposit to an external wallet

Resolving a dispute

1. The traders started a trade but for whatever reason it got stalled.
2. After the max. allowed trade period (depends on the payment method: e.g. OKPay: 1 day, SEPA: 8 days) the software displays an "Open dispute" button, which is otherwise not visible. Any trader can requests arbitration by pressing that button.
3. Bitsquare provides a chat like communication system for disputes (and support tickets in case of software bugs) only between the trader and the arbitrator. The initiating trader will see his first (system) message he has sent to the arbitrator requesting a dispute.
4. The arbitrator receives the dispute request and the software send a dispute message to the other trader, informing him that his peer has started a dispute. The two traders cannot communicate directly with each other and cannot see the communication of the other trader with the arbitrator.
5. Traders and arbitrator communicate in real time, end-to-end encrypted.
6. Arbitrator follows a protocol to request additional information from both parties and

renders his decision based on acquired evidence.

7. Arbitrator unlocks the multi-signature address using his key and the key of the winning party, transferring the Bitcoin amount to the “rightful owner” based on the available evidence. Typically the arbitrator collects the security deposit of the losing party and refunds the deposit of the other party (there are also alternative payout possibilities as well).
8. When criminal fraud is detected: Arbitrator publishes and signs a digital report containing all data about the criminal trader to the public fraud list. These reports will only be created in clear cases of fraud like bank chargeback or use of a stolen bank account.
9. If either trader is not satisfied with the decision of the arbitrator, he may request a second and final arbitration round, performed by a senior arbitrator. The latter reviews the available evidence and renders his decision. If the original arbitrator is found to have behaved dishonestly, further steps are taken to penalize his behavior, based on the severity of his fault.

The details of an exchange transaction

Alice wants to buy Bitcoin for national currency. When Alice creates a new offer she needs to define the amount of Bitcoin to buy or sell, the price and a minimum amount she is willing to trade. The other data included in an offer, like the acceptable arbitrators or the acceptable payment account countries and method, will be derived from the account settings.

To avoid potential collusion between the arbitrator and one of the trading parties the arbitrator will be selected in an unbiased and verifiable way. This will minimize the chance that a trader forces the selection to a preferred arbitrator. The selection mechanism is described in the “Arbitration System” document.

Create offer

Alice broadcasts a cryptographically signed offer to buy a set amount of BTC with a specific currency at a set rate. She also has to specify which national currency transfer methods and which registered arbitrators she agrees to use. The offer only reveals her P2P network ID (onion address), not any personal information. The offer will be broadcasted to the P2P network. The offer storage is access protected so that she is the only one who can remove her offer. There will be a maximum time to live (10 min.) for the offer storage in the P2P network. If she stays online her software will automatically re-publish the offer to ensure the offer does not get removed. If she goes offline her offer gets immediately removed. In cases the software crashes or if she loses internet connectivity the time to live ensures that the offer will not stay long time as “dead offer” in the public offer book.

Offer book

At startup every trader loads all offers for his selected national currency from the P2P network peers he connects to.
The offer book displays all offers matching the selected currency. Offers which are not matching the user’s payment account or selected arbitrators are displayed as inactive (grey out).

Informative feedback is provided upon user interaction why that offer is inaccessible (e.g. “the offerer uses a payment method you do not support”).

The trader can filter offers by currency and payment method to customize his offer book as well as sort all relevant table columns.

Take offer

When Bob takes an offer, the software verifies that the offer fee was paid by Alice. He used the onion address in the offer to connect to Alice’s Tor hidden service to start the trade protocol.

After that there is a check that the offer is still available, i.e. no other trader has taken the offer in the meantime. The offer will remain in the distributed offer book until an escrow deposit is created and funded by both peers. Bob’s software then pays the take-offer fee. Until this point neither peer has revealed any private information to the other peer.

Deposit transaction

Upon taking an offer, a deposit transaction is created using a 2-of-3 multi-signature pay-to-script-hash (P2SH) output script to fund the escrow address. The deposit transaction is passed for completion and signing between the traders over the messaging channel. Finally it is published to the Bitcoin blockchain by the offerer.

The deposit transaction to the escrow address contains:

- Input from Alice: Security deposit + mining fee
- Input from Bob: Security deposit + mining fee + trade amount
- Output to escrow address: 2*Security deposit + mining fee + trade amount
- Output to record contract hash: OP_RETURN + hash of contract (20 bytes).

Contract

After acceptance of an offer and the payment of the corresponding take-offer fee, the taker creates and signs a digital contract. The contract contains all relevant data about the trade (payment details) and both traders. The contract will be verified and locally stored by both peers and will only be used and needed in case of a dispute but is available to be displayed in the application. The hash of the contract will be included in the deposit transaction as proof that both parties have accepted the trade details.

During the trade protocol the software of each trader verifies the fee payments and that the other peer is not listed in the fraud list.

National currency transaction

After the escrow deposit transaction is published, Alice waits for at least 1 confirmation, then she starts the transfer of national currency to the Bitcoin seller’s payment account (eg. by bank transfer).

Create the payout transaction

Alice creates the payout transaction.

The payout transaction contains:

- Input: Funds from multisig escrow address, signed by Alice with her private key (1 of 2 necessary signatures)
- Output to Alice: Security deposit refund + release of payment to Alice
- Output to Bob: Security deposit refund

Alice signs her part and sends the partially signed payout transaction to Bob and tells him that she has started the national currency transfer.

Bob waits until he receives the national currency payment

Bob receives the payout transaction and the message from Alice that she has started the national currency transfer. He will periodically check his payment account until the transaction is complete or a predetermined amount of time has elapsed.

Bob signs and publishes the payout transaction

After receiving the money into his payment account, he signs the payout transaction and publishes it to the Bitcoin network.
He gets back his security deposit and can withdraw it to his external wallet.
For Bob all has been successfully completed.

As soon as Bob has published the payout transaction Alice gets a message and as soon the transaction is visible in the bitcoin network she can withdraw the Bitcoin payment and the refunded security deposit to her external wallet. For Alice all has now been successfully completed.

Cancel offer

The creator of an offer can remove the offer at any time, as long as the offer is not taken by another trader. When removing the offer a message will be broadcasted to the P2P network so all users get updated the offer book with the removed offer. The reserved security deposit in the trade wallet will be available for withdrawal to an external wallet. The create-offer fee, which is paid when creating the offer, cannot be redeemed.

Dispute

At the middle of the timeout period for completing a trade a warning notification is displayed to both traders, reminding them to check the status of their transaction. As soon the timeout is reached (depending on the payment method) either trader can open a dispute and contact the assigned arbitrator. When opening a dispute, the software sends a request to the arbitrator with the contract attached. The chat-like communication system allows encrypted real time messaging between the traders and the arbitrator. The traders cannot communicate directly to

each other..

The arbitrator will investigate the case and request additional information and proofs to each trader. After the arbitrator has rendered his decision, he unlocks the multi-signature address using his key and the key of the winning party, transferring the Bitcoin amount to the “rightful owner” based on the available evidence. The arbitrator collects the security deposit of the losing party and refunds the deposit of the other party. Thus, the winning party will have no costs, while the losing party will lose his security deposit.
In cases where the problem was caused by external circumstances (e.g. bank has blocked the transfer, etc.), the arbitrator can decide, based on the available evidence, to take half of each security deposits as his payment and refund the rest back to the traders. More details about the arbitration system can be found in the “Arbitration System” document.

Disclaimer

In countries where Bitcoin use is illegal it is not recommended to use this platform as it comes with severe risks. Undercover agents can act as peer traders.

Banks might also block a payment account if they discover involvement in Bitcoin trades.
If that risk exists in your national banking environment it is recommended that you open a payment account dedicated to Bitcoin trading to prevent the hassles of a primary payment account being blocked.

There will never be 100% safety when using any exchange; the same is true for centralized exchanges or any kind of money transfer for that matter.

To limit potential losses the maximum trading volume is restricted. This will help reduce the risk of a stolen bank account being used because only a small amount of the money could be exchanged for Bitcoin before the theft is discovered, so the platform is less attractive for criminals. A limit of 1 BTC is initially applied. If real life experience allows us we will raise that limit over time.

While Bitsquare is developed to offer the right to privacy, it is not intended to facilitate criminal behavior and the team does not endorse such activities. In the event of disputes, arbitrators may need to verify the identity of the traders.