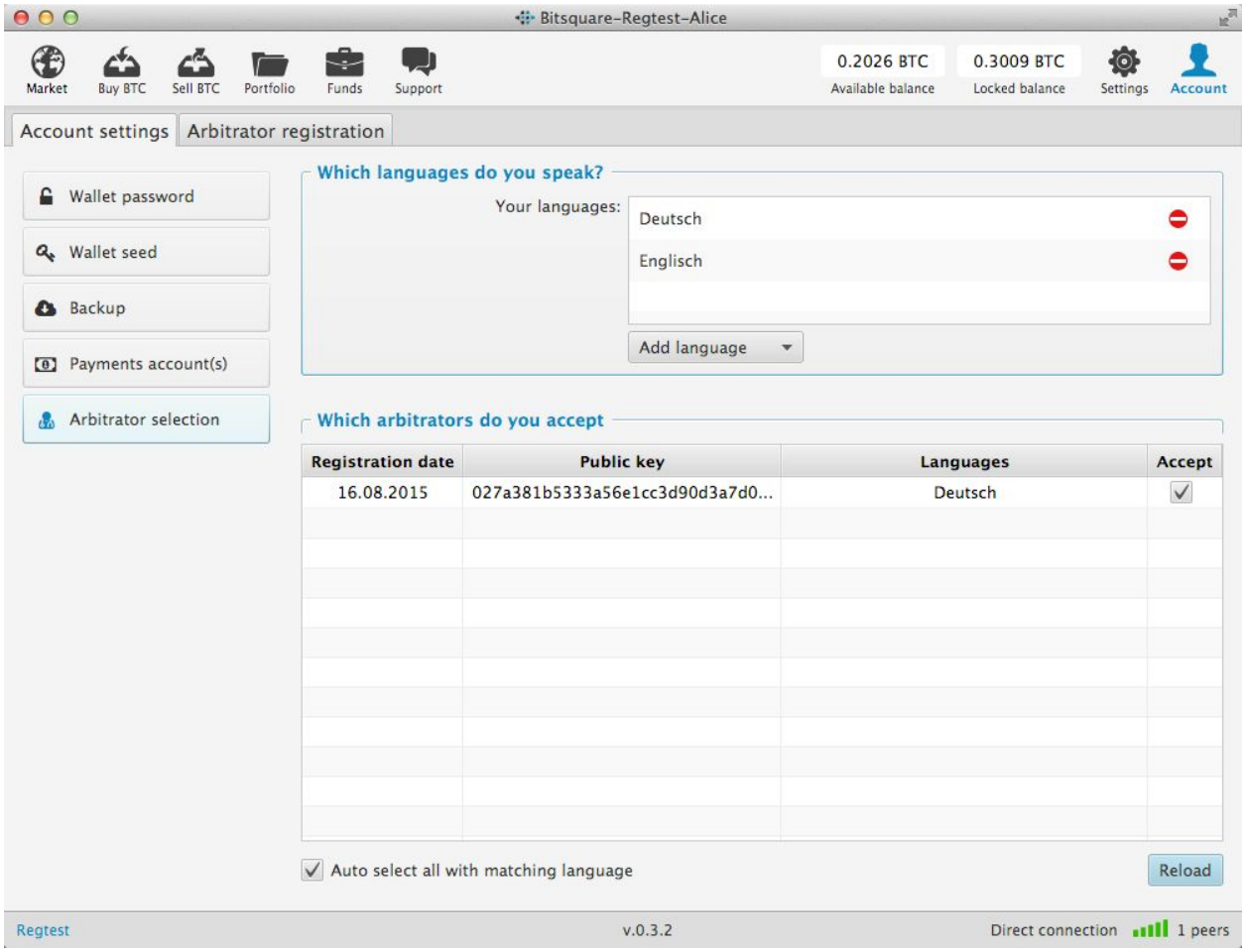
Bitsquare arbitration system

Version 1.0 (last edited: January 03 2016)

Arbitrator selection

The user must select at least one arbitrator when doing a trade. He[1] can only select among arbitrators with whom he shares a language. By default the checkbox for auto-selection of matching arbitrators is enabled. That way the user will always have the maximum set of arbitrators matching his language. As there is no concept of arbitrator reputation, it makes no sense to deselect arbitrators, as this will only reduce his trading possibilities. Traders will only be able to take offers of users with whom they have at least one overlapping selected arbitrator.



When creating an offer, the offerer will pay the create-offer-fee (trading fee) to one of the arbitrators he has accepted. The selection is automated and derived from the hash of the offer ID (which is random). The taker will pay the take-offer-fee to one of the arbitrators in the

[1] Throughout the rest of the document “he” refers to “he/she”

intersection set of both traders (offerer: A1, A2, A3: taker: A2, A3, A4 -> intersection set: A2, A3). The hash of the offer ID will be used for the selection rule and will be automatically verified by each trader's software. Naturally, an arbitrator cannot be selected for his own trades.

Fees and security deposits

The trading fees serve as passive income to the arbitrators. So even if there are no disputes the arbitrator has a motivation to stay available for the system. In case of a dispute the security deposit will be used as payment for the active dispute resolution efforts. The height of the fees is static and is the same for all trades independent of the trade amount. The trading fee for each trader is 0.001 BTC (0.1% of 1 BTC - the max. trade volume). The security deposit (active arbitration fee) is 0.1 BTC. This fee will be adjusted during the initial course of operation and in case of larger BTC price changes.

Dispute process

First warning notification

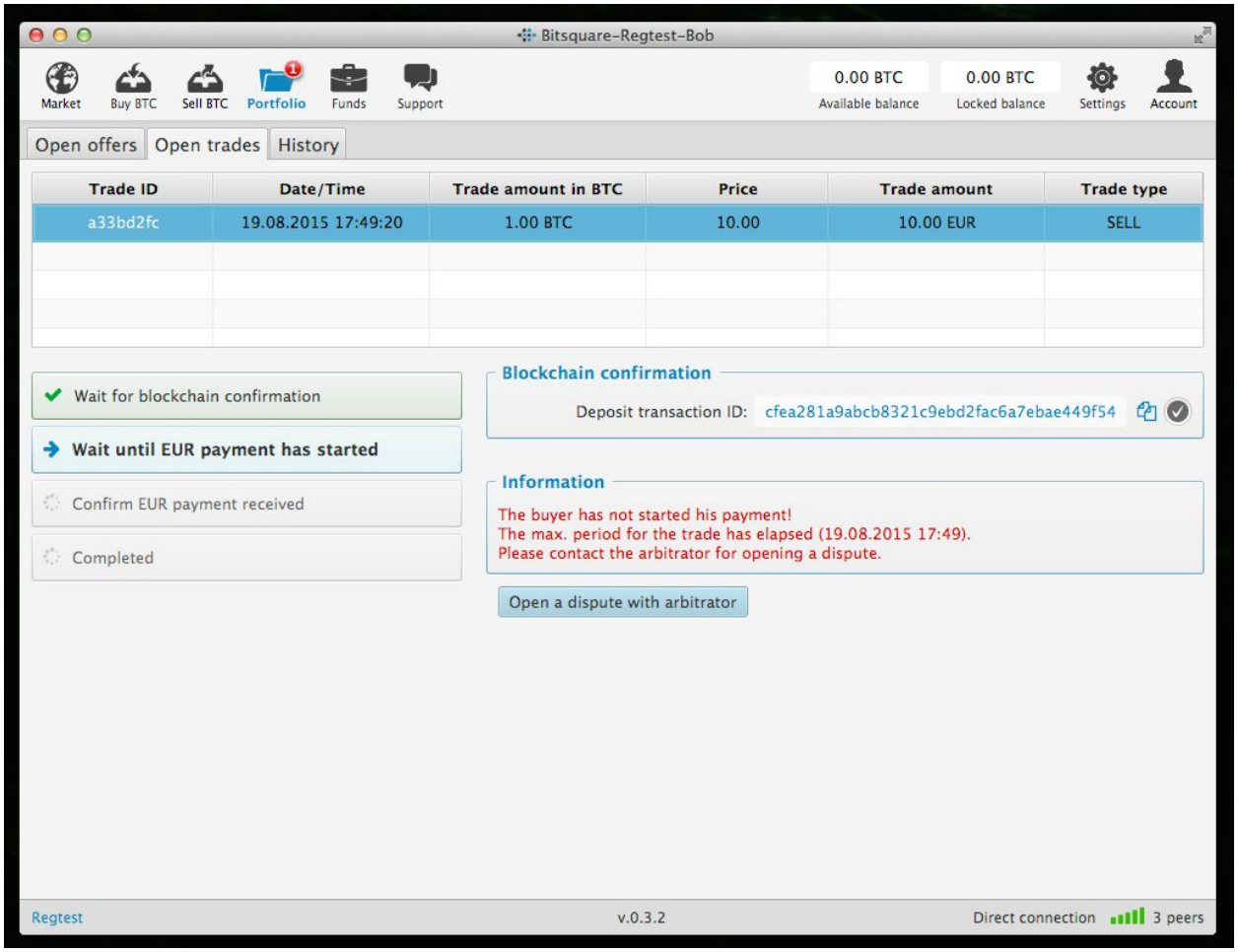
Every payment method has a different max. duration for the trade, which is derived from the max. period that payment method might take. For example, a Sepa transaction takes 1-3 business days on average. The max. period after a trade started and the BTC seller received the Fiat payment will be 8 days. For OKPay, which has instant transaction period, the max. trade period will be 24 hours. Most other payment methods will have 1 day as well.
After half of the max. period both traders will get an automatic notification with request for checking their fiat payment/receipt.
If the BTC seller has not received the Fiat payment after that period he gets displayed a message and a button to contact the arbitrator for resolving the problem.

Dispute

At the start of the dispute, both users get displayed a system message where the basic rules are defined and containing a link to the webpage explaining the process in more details.
In the communication there will be a max. time defined for any party to respond, which is 48 hours. Not responding leads to losing the case and the associated deposit. There will be an overall max. arbitration time period of 14 days, to avoid endless disputes. After that period a final decision will be taken by the arbitrator. If one or both traders are not satisfied with the decision, they can then request a second and final arbitration round. In that round the case and decision of the previous arbitrator will be reviewed by a senior arbitrator, who will render his decision in a timely manner.

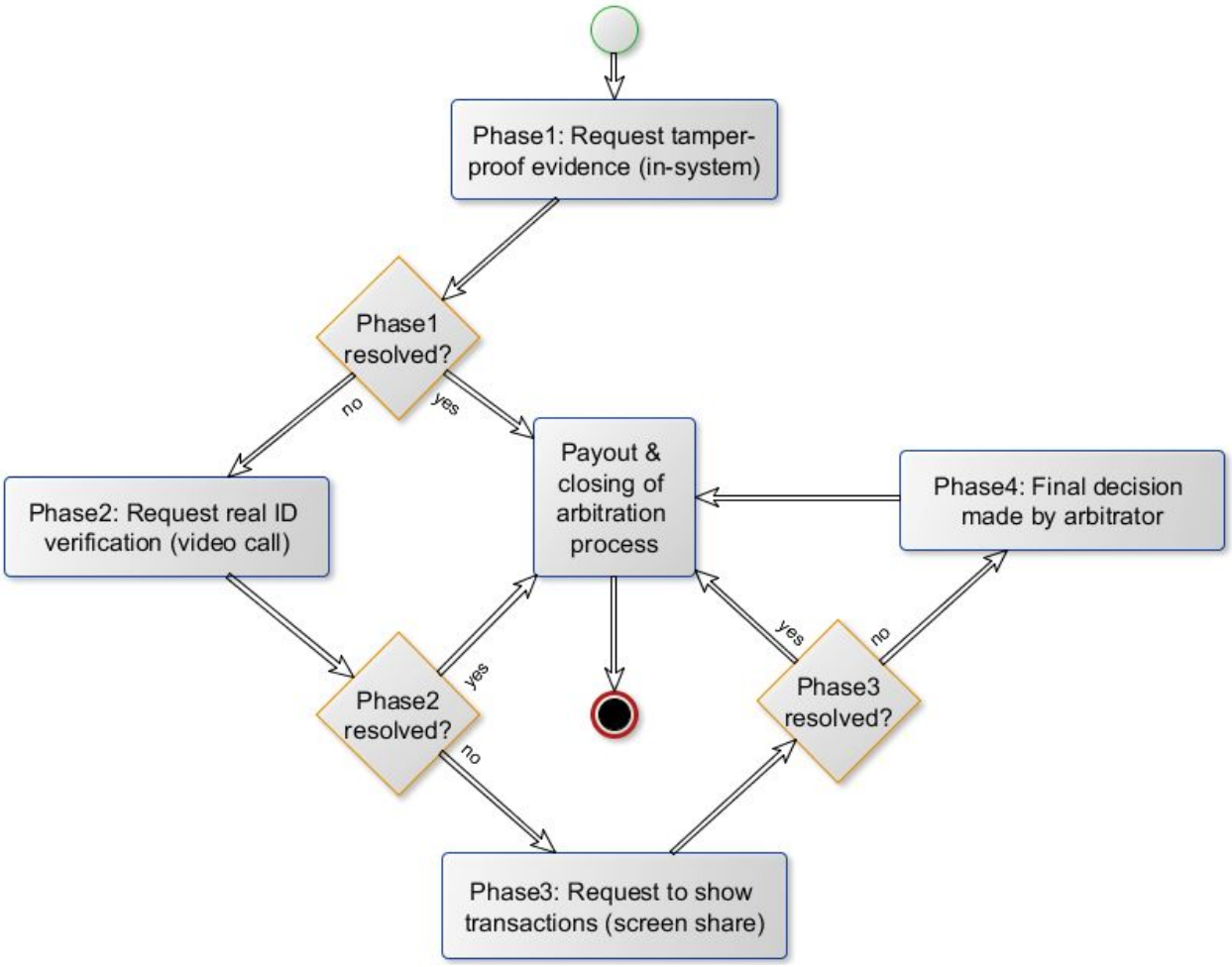
Screenshots

Open dispute screen:



Arbitration process

The arbitration process proceeds in phases. In each phase the arbitrator requests the traders to deliver certain proofs.



Phase 1

PageSigner

When the user enters the arbitration time frame, the arbitrator will ask both parties to send a tamper proof evidence of their trade using PageSigner - a Firefox/Chrome extension.

- The BTC buyer needs to show that the amount has been transferred with the correct reference text. He should navigate to his online banking web page and filter his transactions by the reference text in order to not leak more private data than needed, and do a page-signing of that single web page.
- The BTC seller should filter his history for the reference text (offer ID) to prove that he has not received the payment. Additionally he needs to filter by date to cover the period from the trade day to the current day. That might leak a bit of privacy, but we get a more confident result. So he should send 2 page signed proofs to the arbitrator.

The page must also show evidence that it matches the payment method, Fiat amount, reference text and account number used in the trade (the contract contains both users payment details).

There are no security sensitive data included in that signed page, i.e. no bank credentials. Each trader sends their evidence, generated by PageSigner, to the arbitrator as an attachment, using the built-in interface.

Digitally signed bank statement

If the user does not accept to use PageSigner or his banking web page does not work with PageSigner, the arbitrator will ask the user to request from his bank a digitally signed statement which delivers evidence for his complaint.
If he does not do that either, he risks that in case the other trader delivers tamper proof evidence he will lose the dispute.

In the case that there is no obvious resolution (e.g. both peers did not deliver tamper proof evidence, or deliver conflicting evidence) the arbitrator will request the traders to check with their bank whether the transaction is not blocked. If one peer suspect a problem caused by his bank (blocking or delayed transfer) the arbitrator can give him more time to resolve the issue with his bank. However, the maximum dispute period still applies.

Phase 2

Real life ID verification

First each trader needs to scan 2 governmental issues IDs front and back. At least one of the documents needs to have a photo. The arbitrator will then request traders to make a selfie photo together with the documents and send those photos to the arbitrator.
After that the arbitrator will request a video session via any commonly used and freely available video conference tool (Skype, Hangout, Tox...) and ask the trader to show both documents and also to show his face so the arbitrator can compare with the photo and the scans. Sufficiently good resolution should be selected for the video call to allow verification. The video session will be recorded by the arbitrator for documentation reasons in case of a second round.

The arbitrator does not need to be visible himself in the video session and doesn’t need to provide any identification to the traders.

If one trader fails to successfully verify himself, the other peer will be the winner, provided he can verify himself.

Phase 3

Screensharing or video casting

After the ID verification was successful, the next step is to get a proof of the Fiat transaction in question. The arbitrator asks each trader to navigate to his online banking web page and filter the transaction in question (same as above with PageSigner). Each trader will then show this page to the arbitrator using screen sharing or a mobile camera using sufficiently high video quality. The video or screen sharing session will be recorded by the arbitrator for documentation reasons in case of a second round.

Phase 4

If the dispute is not resolved by phase 3, or the maximum dispute period is over, the arbitrator will render his final decision considering all available evidence. Alternatively, he may propose to leave it up to the traders. In that case he would only receive at any time later the result both traders have agreed on and will execute the payout, but he should not be active part in the dispute resolution anymore to limit his effort. His payment (from the security deposit) will be derived from the payout decision (if split payout the fee will also be split).

Payout phase

After a decision has been made, the arbitrator will publish a new payout transaction from the 2 of 3 MultiSig deposit with the winning party as receiver of the trade amount and the refund of the security deposit (so the winning party does not lose anything) and the security deposit of the losing party will be used as payment for the arbitrator.
Both traders will get the result communicated. Each trader may dispute arbitrator's decision and go to the second round, once that is implemented. The payout process and the dispute closing is handled inside the application in an encrypted chat system with mailbox functionality in case the user is offline.

Incorrect data or payment amount (bank fees)

If the bitcoin buyer transfers an incorrect Fiat amount or does not use the exact reference text (offer ID) it is considered a breach of contract.
If a trader uses the words "Bitcoin", "BTC", "Trade" or "Bitsquare" in the reference text it will also be considered as contract breach, as some banks are very hostile against Bitcoin related transactions and the other peer might get serious problems with his bank.
The software UI will alert the user to take care for all those issues at the moment when the Fiat payment is required.
Any additional fees occurring on the sending side must be covered by the Fiat sender. If the receiving bank takes extra fee (should not be the case in our supported payment methods) it has to be accepted by the BTC seller. If currency exchange fees are charged by either the sending or receiving bank, the fees has to be covered by the account holder where the fee is charged. We don't support mixed currency exchange (buy bitcoin with paying in EUR but receiving in USD). OKPay offers internal exchange and Sepa supports a series of non-Euro currencies. But those cases are handled as the trade currency which is defined in the trade, and the conversion costs are paid by the one with the non matching trade currency.

Second arbitration round

For the full version it is planned to offer a second arbitration round in case the loser wants to dispute the result. He has to pay in advance a fee and one of the senior arbitrators will be chosen to check the case again. The height of the security deposit is taken as main factor,

additionally the arbitrators which are personally invited in the bootstrap phase are considered as senior arbitrators.
The second arbitration round is not supported in the current version. In cases a user feels unfairly treated he can get in touch with the team and they will decide how to deal with the situation.
Further details are described in the arbitration system paper.

Summary of parameters:

Maximum duration for a trader to reply to arbitrator's request: 48 hours
Maximum duration for the overall dispute process: 14 days
Maximum duration for Sepa bank transfer: 8 days
Maximum duration for OKpay transfer: 1 day
Create-offer-fee/take-offer-fee: 0.001 BTC
Security deposit: 0.1 BTC