Blockchain & Tangle, Topic: IOTA

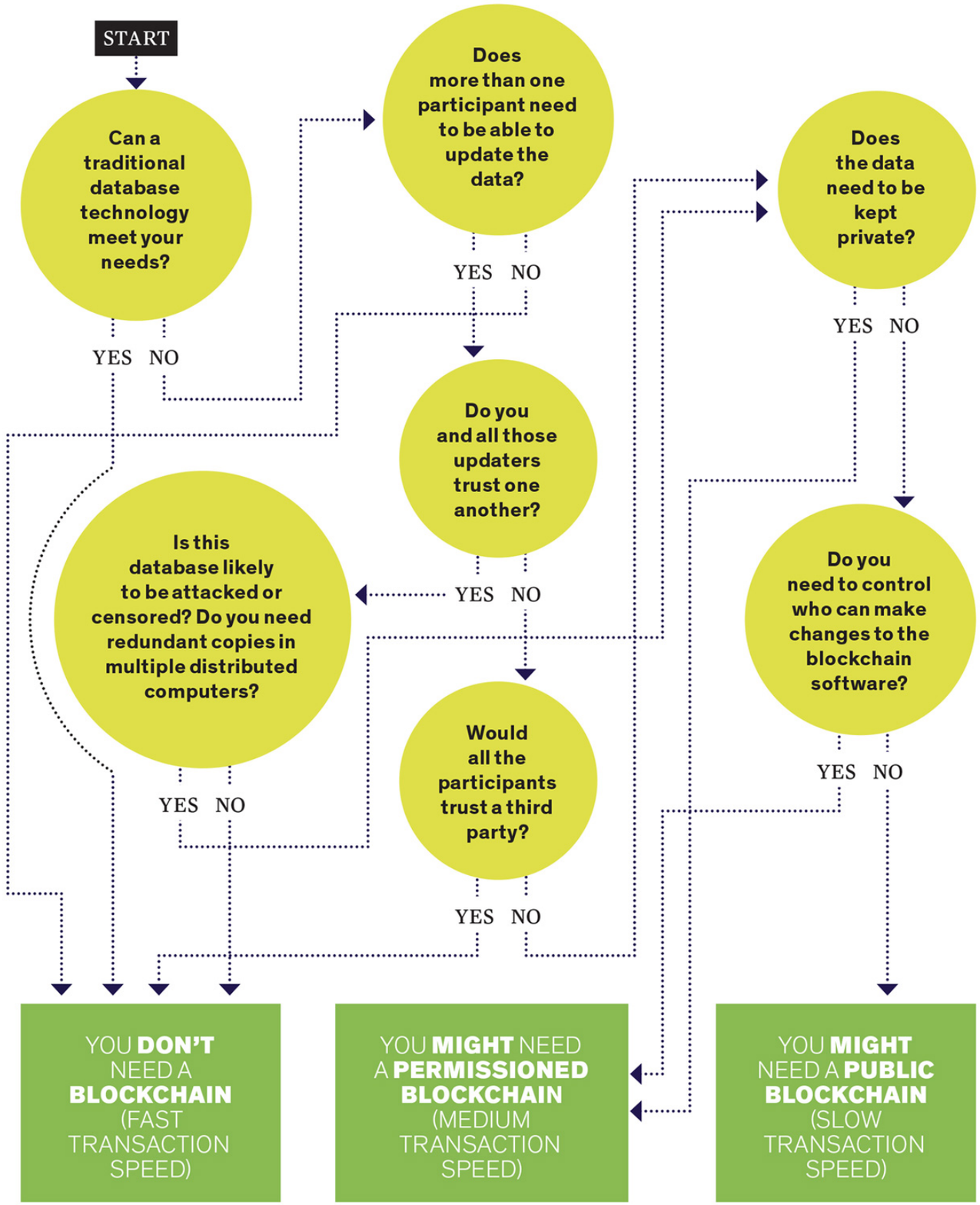
Zurich New ICT Technology Meetup

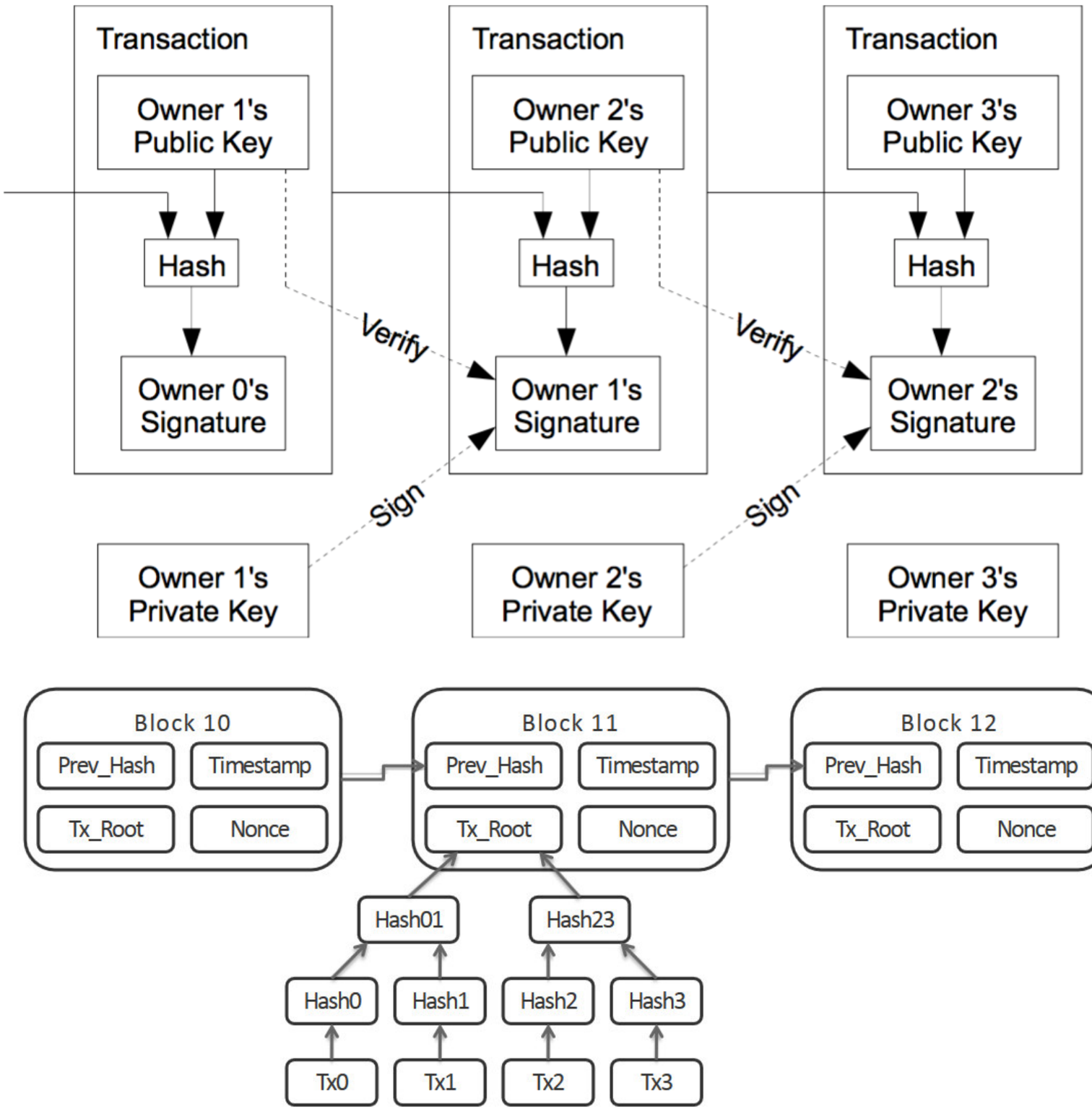
Büro - Züri, Börsenstrasse 9, Zürich, Switzerland; (left next to ZKB)

Ritz Engineering ®

Why Blockchain ?

- Nakamoto 2008
- Blockchain Whitepaper
- Bitcoin
  - Blockchain is a cryptographic secure, immutable storage technology
  - Bitcoin is 1st Application on a Blockchain
- Blockchain (IEEE model) as Storage Technology for further reasons ?
  - Permissoned as Public or Private like Ripple, Hypeledger
  - Permissionless like BTC, ETH, …





Blockchain - Public Singleton - Storage Technology - Immutable
Decentralized, atomar transaction, state transition system

What is a Blockchain Cryptocurrency

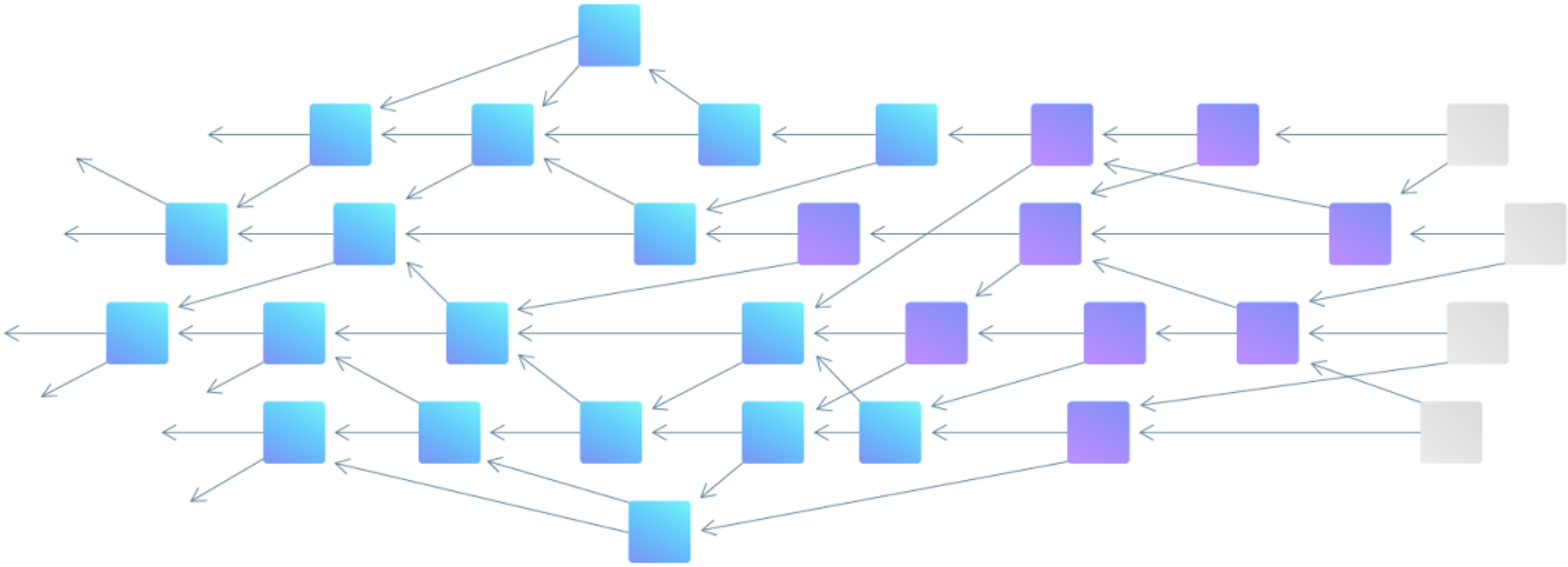
- Blockchain as Distributed Digital Ledger Technology (DLT)
  - Peer to Peer, cryptographic secure Database (Hash)
  - Transactions of trusted values
- Consequence: Trust to 3rd party (Bank, Man in the Middle) unnecessary
  - Trust the open source cryptographic, algorithmic implementation
  - Democratic formal distributed consensus algorithm
- Proof of work / proof of stake
  2nd gen. Blockchain (ETH)
  - Enables a token economy
  - Smart contracts

Problems with BTC / ETH Blockchains

- Miner
  - Consensus
  - Proof of Work (PoW)
  - Energy consumption
  - Price best Bid
    - Maximize Miner Profit
- Tx Speed: 5-25 Tx/s
  - Visa: >2500 Tx/s
  - Paypal: >200 Tx/s
- No Micro payments
  - Fees

IOTA, a Tangle ≠ Blockchain

- Seamless P2P network - Directed Acyclic Graph: loop-less direction of grow
- Site: Details of all Transactions (Sender, Receiver, Value / Data)
- Edge: Connections to other Transactions = validate the Transaction; Proof of Work: validate 2 random connections
- Tips: unconfirmed Transactions (blue=confirmed, violet: partly confirmed (PoW not yet sufficient), grey: Tip)
- Weight = Proof of Work done for Tx; Cumulative Weight = sum of all connected Tx (corresponds to Min Weight Magnitude)



IOTA Cryptocurrency

- Name: 9th letter in greek alphabet
- Max. circulating supply: 2’779’530’283’2767’761 i
- SI Dimensions: i, Ki, Mi, Gi, Ti, Pi
- currently 1Mi = 1.50 €
- Machine to Machine communication
  - IoT
  - Micro Payments
  - no Fees = PoW = verify 2 Tx
- Funded as ICO Dec. 2015
- Public Trust, est. in Germany Dec. 2017
- > 1000 Tx/s

Total amount

2 779 530 283 277 761

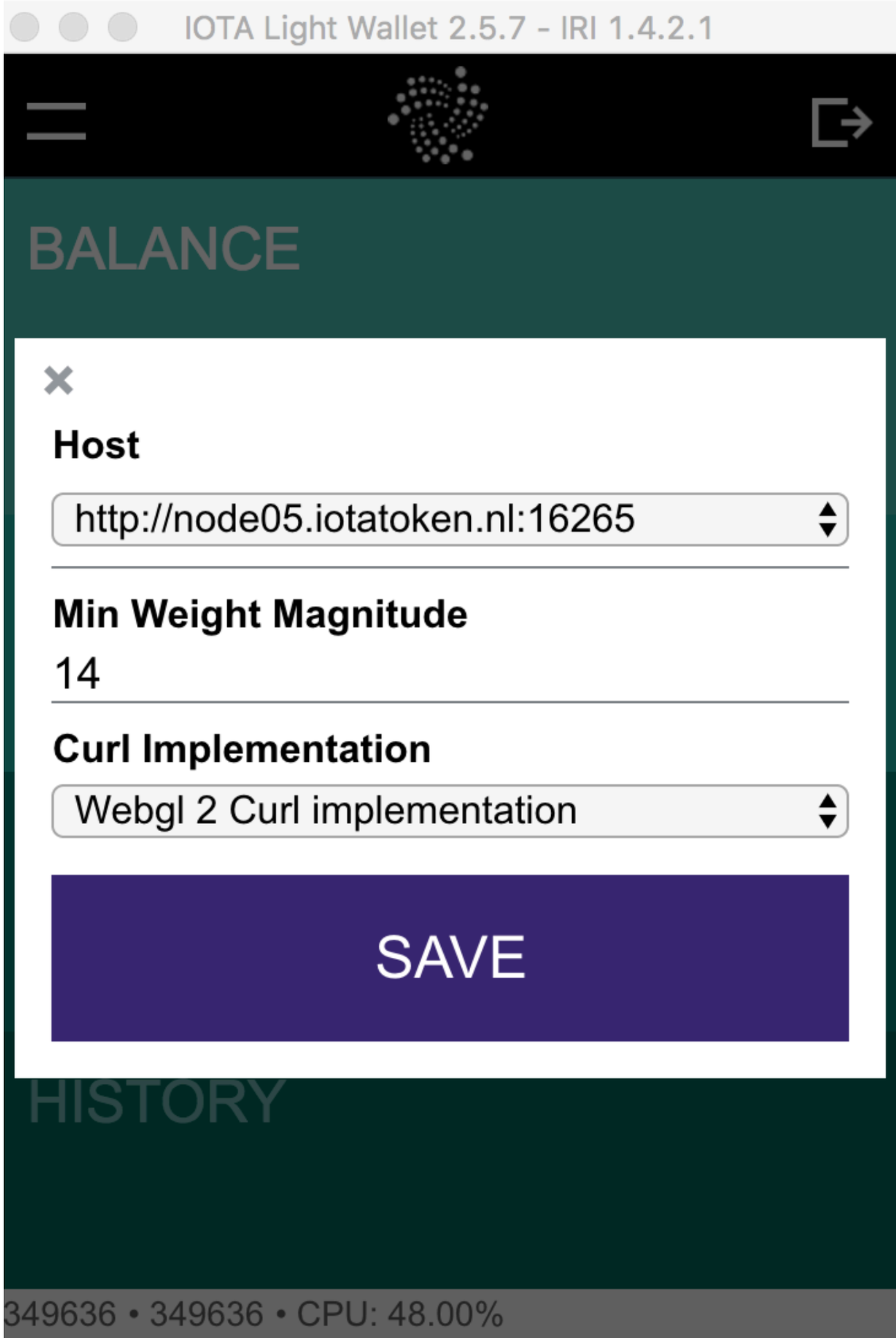
System of Units

Pi	Peta Iota	1.000.000.000.000.000	10^{15}
Ti	Tera Iota	1.000.000.000.000	10^{12}
Gi	Giga Iota	1.000.000.000	10^{9}
Mi	Mega Iota	1.000.000	10^{6}
Ki	Kilo Iota	1.000	10^{3}
i	Iota	1	1

IOTA

Setup

- SEED: 81 char A-Z; 9
  - Private Key and Password
  - IOTA Wallet ! Simple text editor ! Mac:
    cat /dev/urandom |LC_ALL=C tr -dc 'A-Z9' | fold -w 81 | head -n 1
    - Reboot, no network, store secure (keypassx and else)
- Tools —> Edit Node Configuration
  - Host (choose node: Milestone Index = equal)
  - Min. Weight Magnitude (PoW difficulty)
    - default (IRI 1.4.x) is 14; higher: more PoW
  - Curl Implementation (PoW)
    - Webgl 2 Curl: GPU, fast, node.JS
    - Ccurl: CPU, slow, if Webgl 2 Curl fails

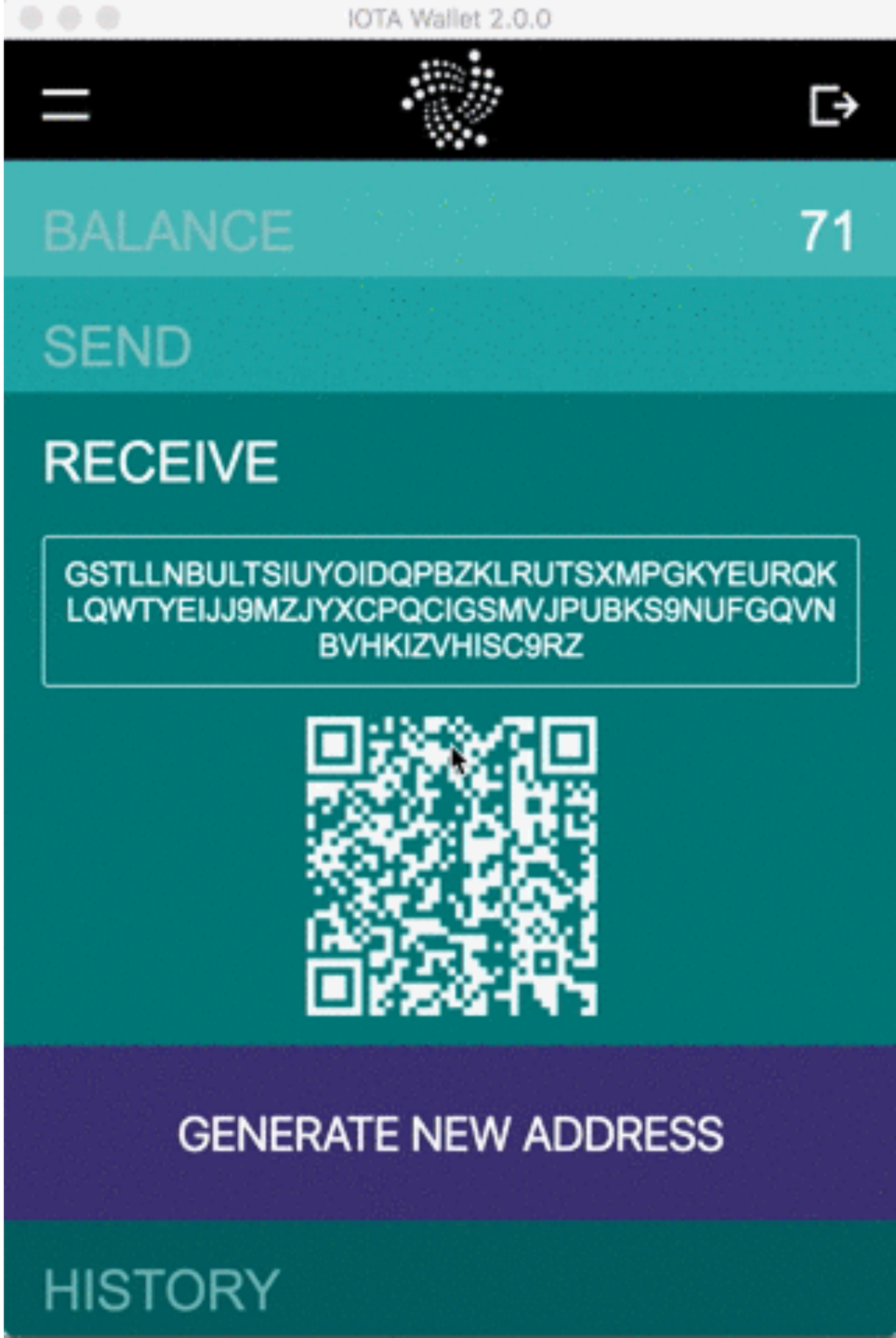


Login

- Seed has to be copied into the field
  - do at best not use any seed generator and if - change a greater number of characters
  - IOTA: Tools —> Generate SEED
  - Do not show the seed to anyone.
- Minimize seed activities to simple copy paste without visibility
  - use password tools like keypassx or else.
- Wallet connects to the tangle and lists the summary and history

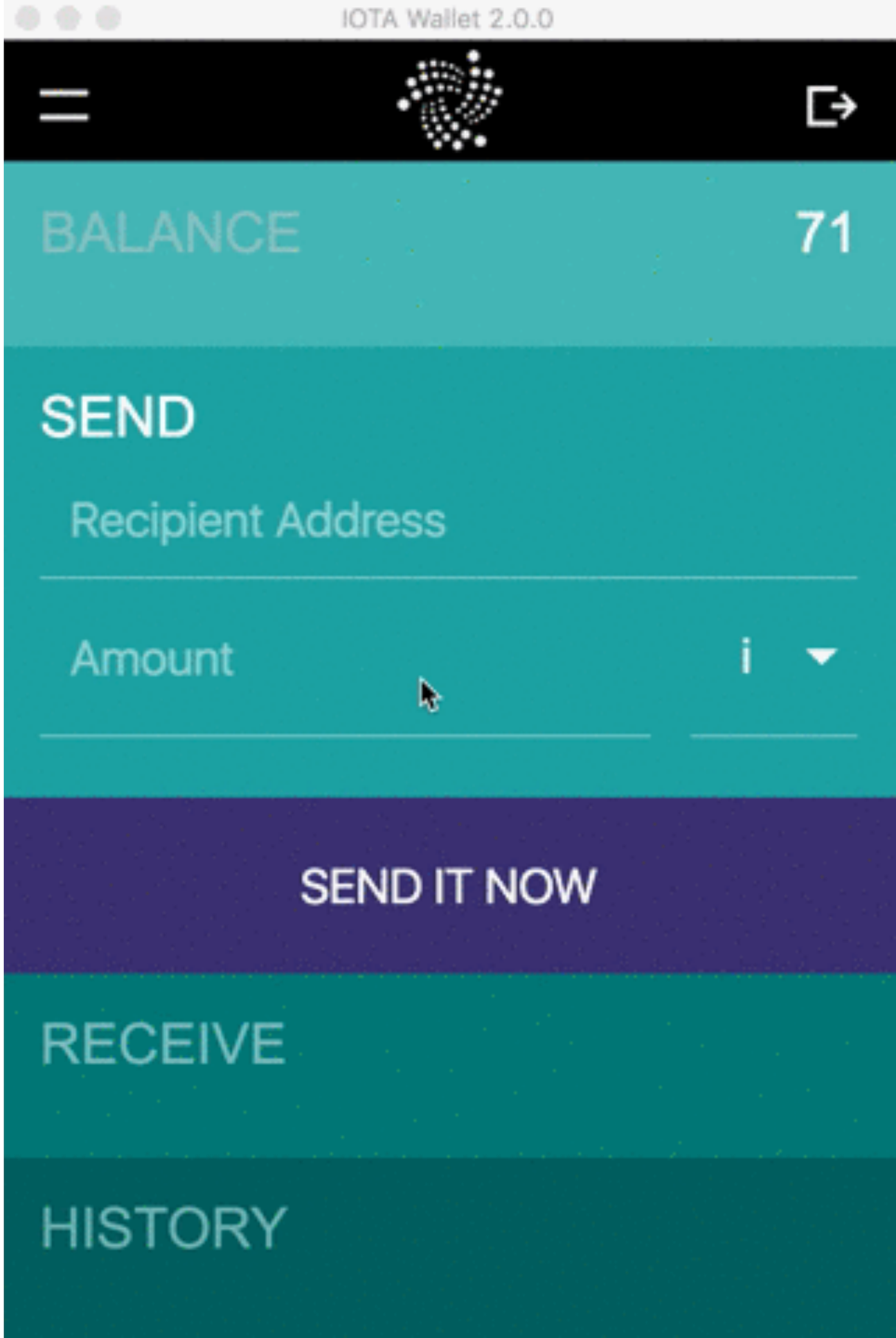
Generate new Address

- Generate a public addresss to receive values
- Generating a new address and attach to the Tangle generate a 0 value transaction
  - 1 Transaction can be seen in the History section.
  - 1 Transaction can be searched (iotasear.ch)
- click on the Receive area copy the address to clipboard



Send IOTA and further operations

- Add the public address of foreign receiver into Recipient Address field
- Add number of IOTA (i, Ki, Mi)
- Send it
- PoW take a time
  - depends on the PoW methods
    - Ccurl or Webgl 2 curl
- „Transfer complete“ doesn’t meant received.
  - History provides Transaction
    - Pending —> Completed



Claim Process to change SEED

- Choose Menu
  Tools —> Claim Process
- Old SEED —> New SEED
- Claimed Value output
- Do not use old SEED anymore.

Recent deposits

ID	Date	Type	Description	Amount	Status
	02-13-18 10:13:47 +0100	Fidor Bank AG (SEPA)	POFICHBEXXX	€10.00	Success

Ledger

Ledger ID	Date	Type	Currency	Amount	Fee	Balance
	02-13-18 11:19:48 +0100	Deposit	Euro (EUR)	€10.00	€0.00	€10.02

kraken bitcoin exchange ETH: Ξ0.45260 EUR: €10.02 ACCOUNT CHARTS HELP LAST LOGIN: 02-12-18 20:03:29 +0000

ETH/EUR	LAST	HIGH	LOW	24 HOUR VOLUME	WEIGHTED AVG
	€681.99	€710.36	€670.55	31,063.38	€684.48

Trade | Funding | Security | Settings | History | Get Verified | MtGox Claim

Current time: 02-14-18 00:09:33 +01:00
Last Updated: 18 seconds ago

Overview | New Order | Orders | Positions | Trades

0.16/0.26% Current Fee | $1,166.88 / $50,000 (2.33%) | 0.14/0.24% Next Fee

Simple | Intermediate | Advanced | New Charting & Trading Tools BETA

Buy | Sell | 0.0147 ETH × 680.00 EUR | Market | Limit = 9.99 EUR

Amount of ETH to buy. Buy at a fixed price per ETH. Estimated amount of EUR to spend.

Buy ETH with EUR » Skip order confirmations.

Zahlungsart: Single Euro Payments Area (SEPA) grafisch

Empfänger

Adress-Code	KRAKEN	
Name	Kraken, Payward Ltd.	
Adresszeile 1	One London Wall, London	
Adresszeile 2	EC2Y 5EB, United Kingdom	
PLZ / Ort	80335	Muenchen
Land	D	Deutschland

Datum	10.02.2018	Ausführen am 12.02.2018
Betrag	10.00 EUR	Euro
Buchungstext	BITCOIN	
Bankname	Fidor Bank AG, München, Deutschland	
SWIFT (BIC)	FDDODEMMXXX	
IBAN	DE31700222000071788512	
Mitteilungen	. Kraken ID	kraken.com
Instruktionen		
Belastungskonto		
Ausgabenkonto	1041	Wertschriften Kraken

Ok | Abbrechen

Address: Bitfinex (IOTA) • 0x1859D3f33Ca1E4870c15780

Choose an Ether address to withdraw to.

Amount: 0.0147

Minimum Ξ0.01000
Maximum Ξ0.45260
Balance Ξ0.45260

Fee: Ξ0.00500

Review Withdrawal »

How to get IOTA: SEPA - Kraken (kraken.com) - Ledger - Trade ETH/EUR - Bitfinex - Withdrawl - Fees

Withdraw > Iota

Address

Amount 6 Mi ≈ USD

Min 127.7 *Help*
Min 250 USD
Equivalent

Wallet Exchange Wallet

Tx Fee (Help) 0.5 Mi

Take fee from amount (Help)

Add a note to this withdrawal for your records. (Saved on Bitfinex only. Not sent to the withdrawal recipient).

I have read, understand, and agree to the conditions for auto-withdrawal processing.

Request Withdrawal

Important: IOTA deposit addresses should not be used more than once. After the first use of a deposit address, subsequent deposits to the same address will not be credited. You can generate new deposit addresses using the [↻] buttons below.

Deposit > Iota

Important: IOTA deposit addresses should not be used more than once. After the first use of a deposit address, subsequent deposits to the same address will not be credited. You can generate new deposit addresses using the [↻] buttons below.

Understanding IOTA, Wallets, Nodes, and Tangle

IOTA is different than other major cryptocurrencies in several important ways. Before using IOTA on Bitfinex, please review the following critical items.

Learn more:
- An introduction to IOTA
- IOTA Node/Wallet Types
- IOTA Technicals and Connection Help
- Connect your light wallet to http://iota.bitfinex.com:80

A Small Deposit Fee of 0.5 IOTA is applied on deposits less than a 1000 USD equivalent. More Info

Please send Iota to one of your deposit addresses displayed below. The deposit will be credited in your corresponding wallet. Learn more about wallets.

You can generate new deposit addresses using the [↻] buttons below.

Exchange Wallet
Click to generate address

Margin Wallet
Click to generate address

Funding Wallet
Click to generate address

Iota deposits are credited after a minimum of 1 confirmations (about 0 minutes, sometimes longer)

ORDER FORM Exchange Margin

Limit OCO HIDDEN POST ONLY

PRICE ETH 0.0021716 ≈ 0.01

AMOUNT MI 6

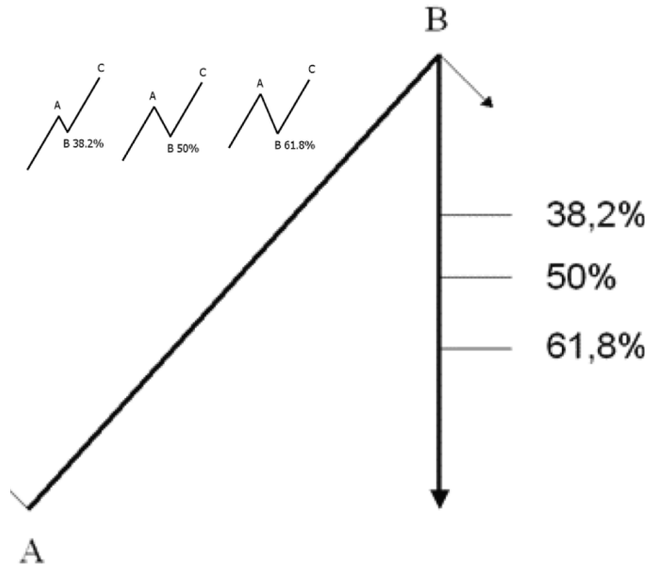
Exchange Buy Exchange Sell

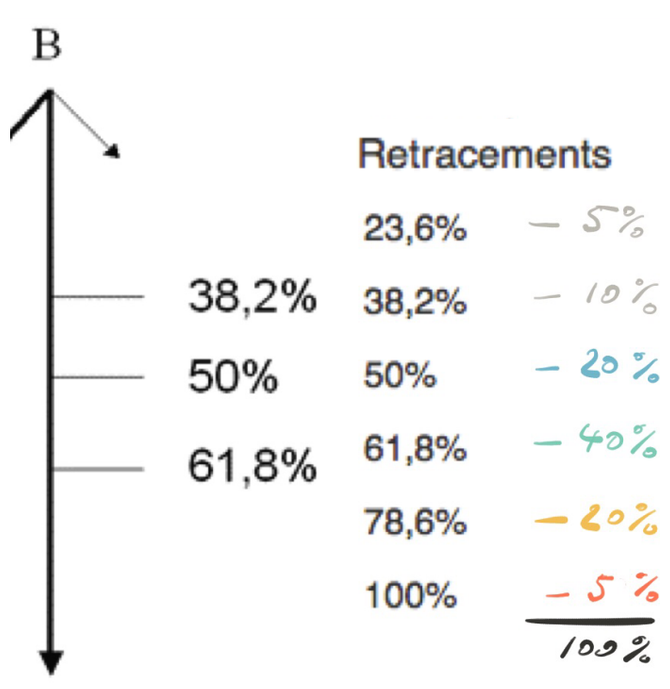
BALANCES

	EXCHANGE	MARGIN	FUNDING
BTC	0.00 0.00	0 0	0 0
DATA	73.93 73.93	0 0	0 0

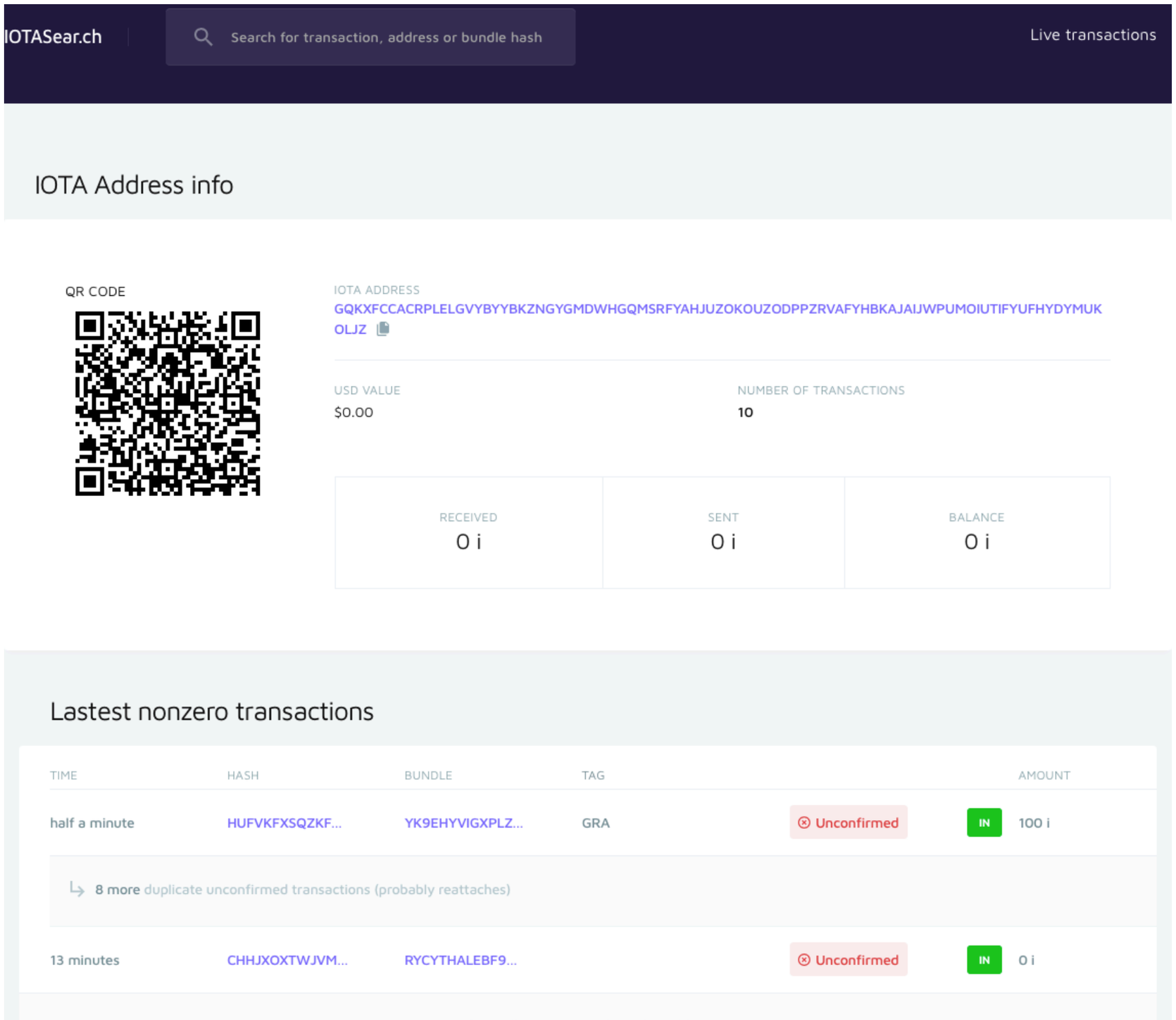
7.24

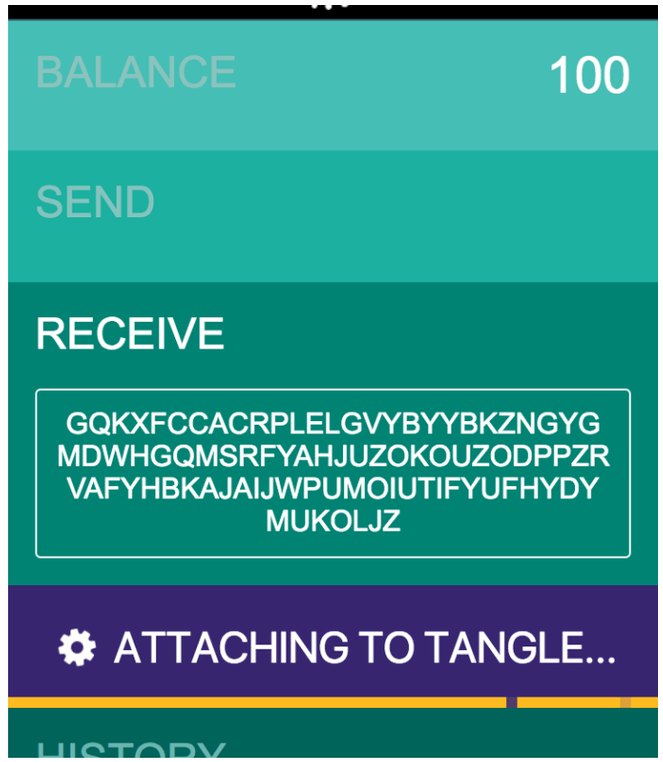
Bitfinex (bitfinex.com) - Ledger - IOTA Trade - Withdrawl to Wallet (IOTA deposit addresses should not used more than once)

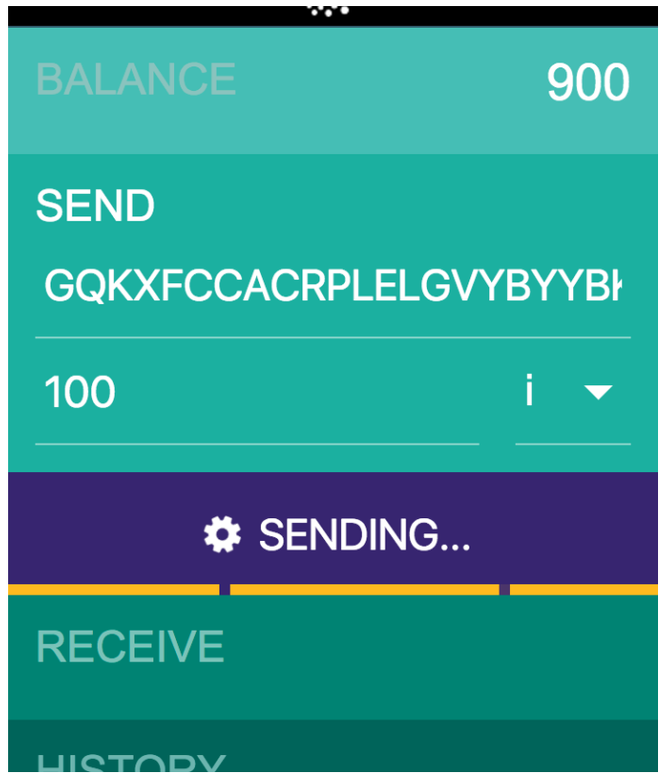




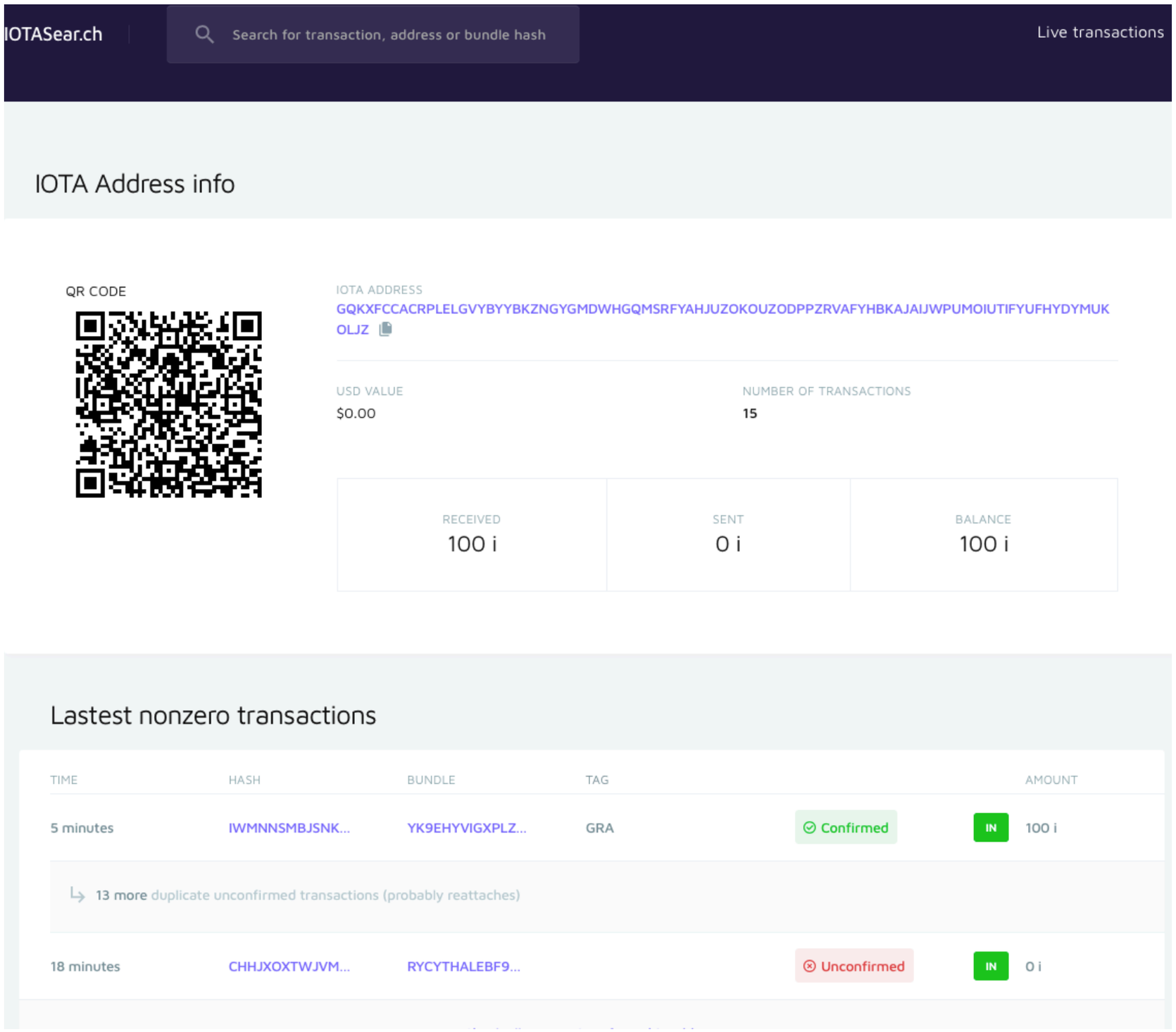
Trading Strategies

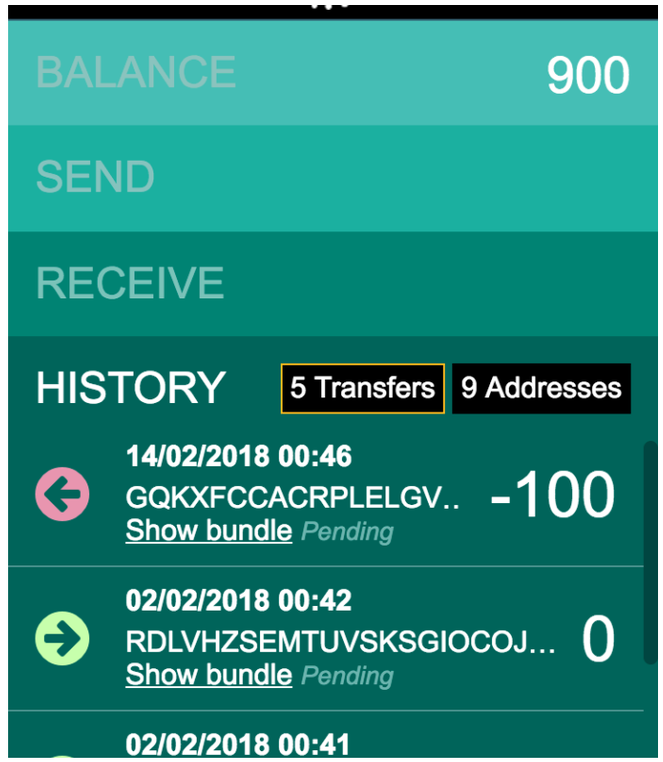


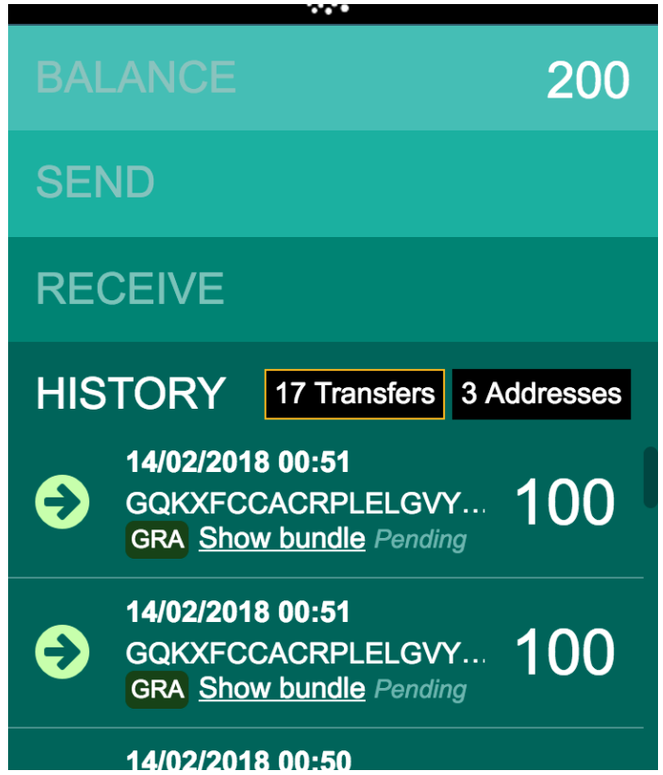




Wallet - Wallet Transaction unconfirmed



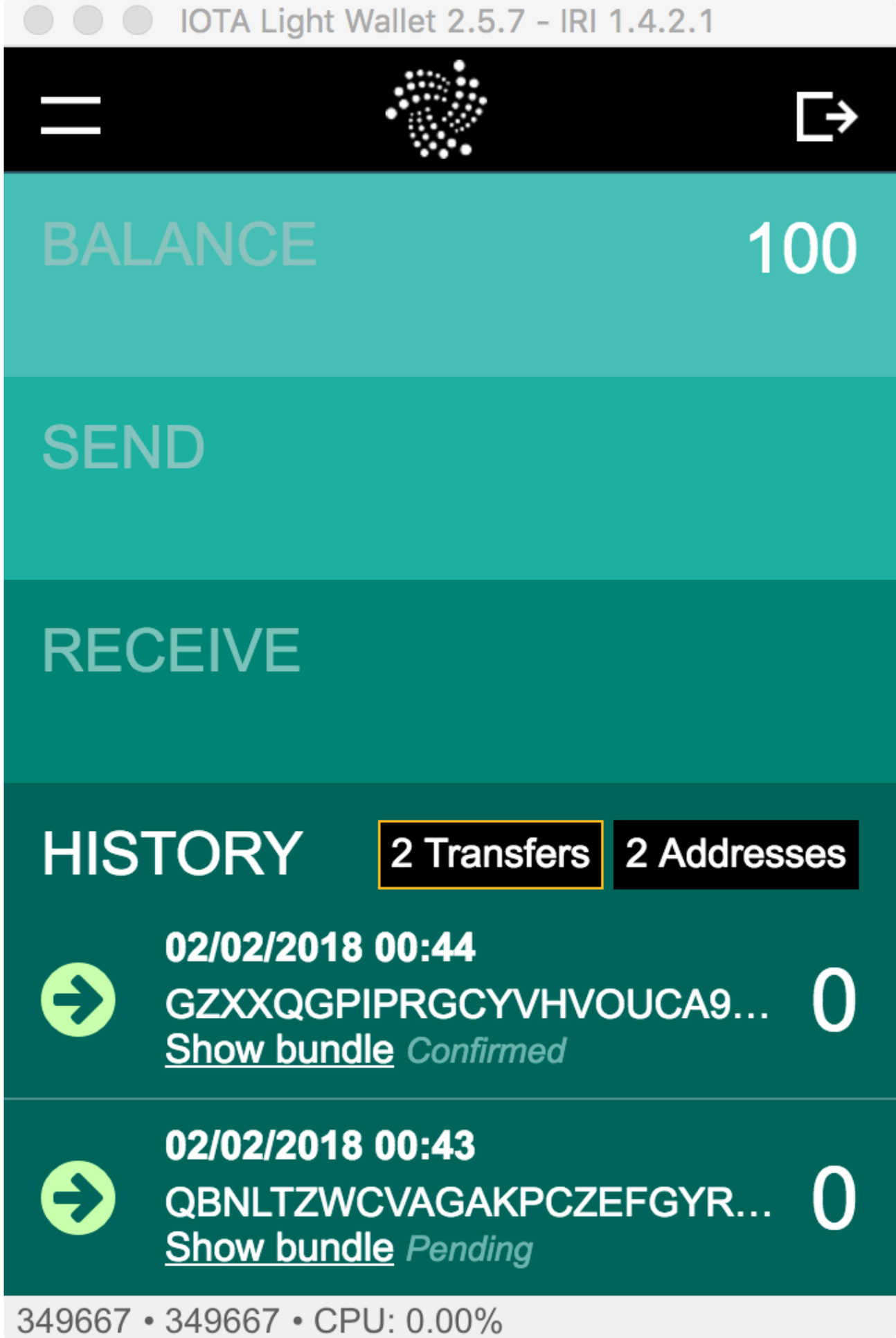




Wallet - Wallet Transaction confirmed

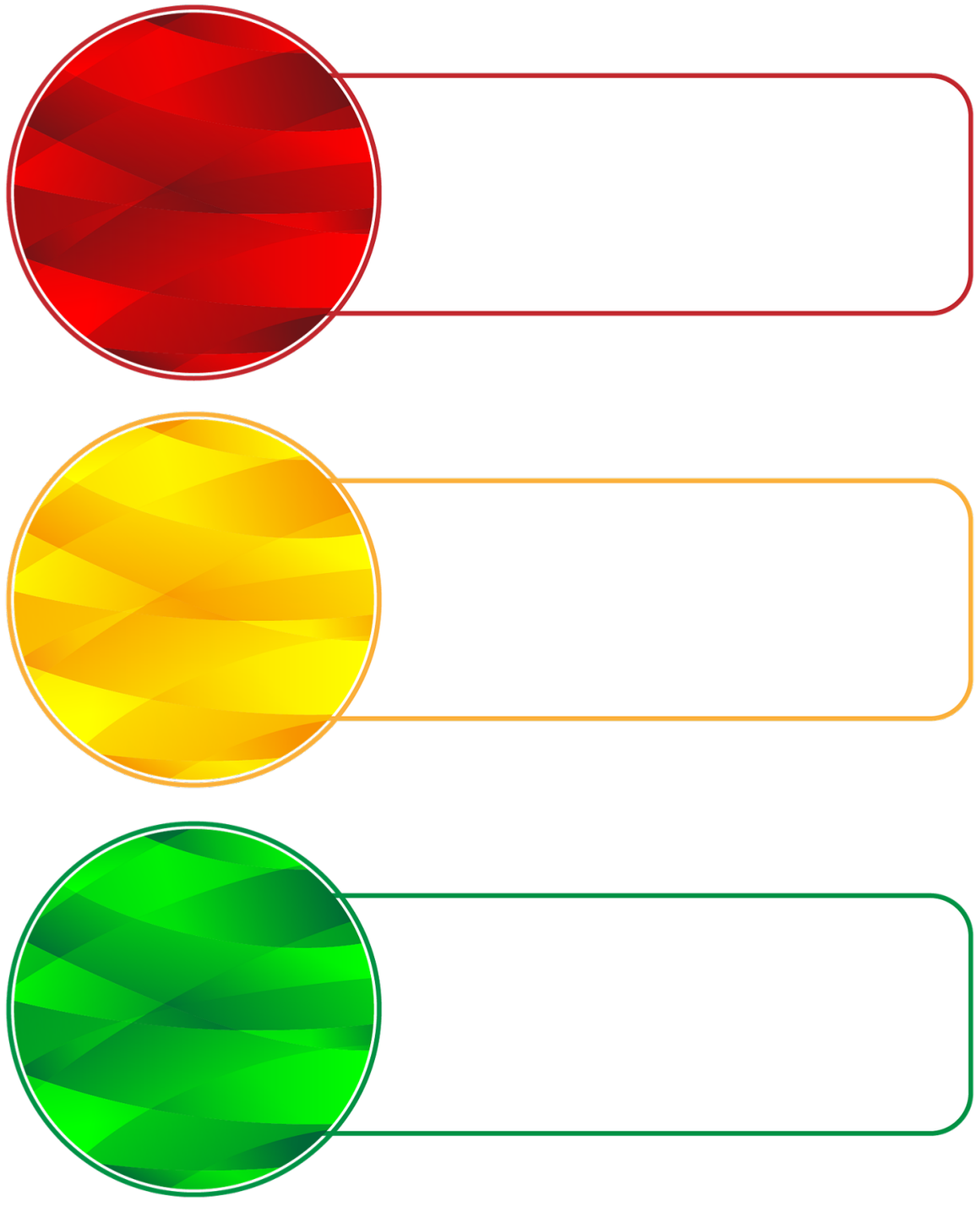
Pending Transactions

- iotasear.ch
- Attach to Tangle
  - creates zero value Transaction
- Rebroadcast
  - Neighbours get same Tx again
- Reattach
  - Tip selection gets new Tx = prefered after 30 min.
- Promote
  - Preferred method if Tx does not get confirmed after 1h
- Snapshot
  - Reduce Tangle size, Record of addresses with corresponding balances
  - after Snapshot: Generate Address



IOTA Rules

- Stay up to date, IOTA is still beta
- Trust only real links, not alias
- Winternitz One Time Signature Scheme:
  - Never reuse an IOTA Address for another outgoing Transaction
  - Wallet is warning so far

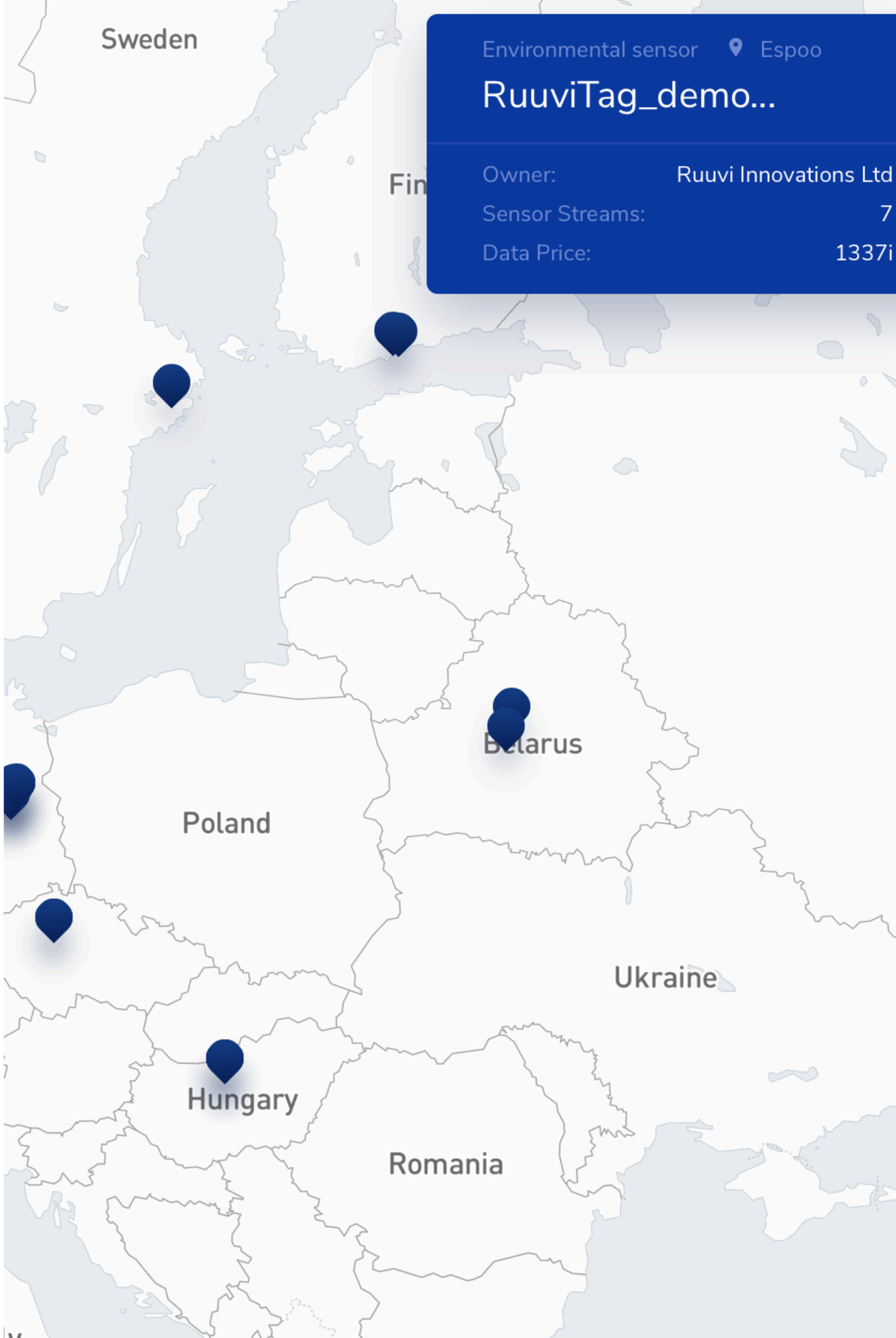


Applications

- Machine to Machine (Sensor - Processor - Actuator), Micropayments
- Donations, PayPal - Business, Fee free Transactions
- Tracking, mesarement and payment of lending products
- Data Market place

Applications

- Desktop Wallet
  - https://github.com/iotaledger/wallet/releases
- Donate with IOTA
  - https://www.tipiota.com
- Data Market
  - data.iota.org
- Ruuvi Tag Sensor Beacon
  - ruuvi.com
- Car recording
  - innogy.de



- Foundation
  - http://iota.org
  - https://blog.iota.org
  - https://data.iota.org
- Developer
  - https://github.com/iotaledger
- GitHub
  - https://github.com/iotaledger/iri
  - https://www.gitbook.com/book/matthewwinstonjohnson/iota-guide-and-faq/details
- Help
  - https://forum.helloiota.com
  - http://iotasupport.com
  - http://www.tangleblog.com/what-is-iota-what-is-the-tangle/
- Prices
  - http://cryptowat.ch
- Youtube
  - https://www.youtube.com/channel/UCQaOR_QLI2tGceGAp3ZWfQw
  - https://www.youtube.com/channel/UCITKvry4fW50iU4FSw9WERQ
  - https://www.youtube.com/channel/UCG5_CT_KjexxjbgNE4lVGkg
  - https://www.youtube.com/channel/UCutCcajxhR33k9UR-DdLsAQ
- Slack
  - https://iotatangle.slack.com
- Reddit
  - https://www.reddit.com/r/Iota/
- Medium
  - https://blog.iota.org/tagged/tangle
- Market
  - http://coinmarketcap.com
- Zürich New ICT Technology Meetup
  - https://github.com/ritzeng/Zurich_New_ICT_Technology_Meetup

Discussion on volatility for value chain processing, Blockchain/Tangle experience, Use Cases, Future of IOTA