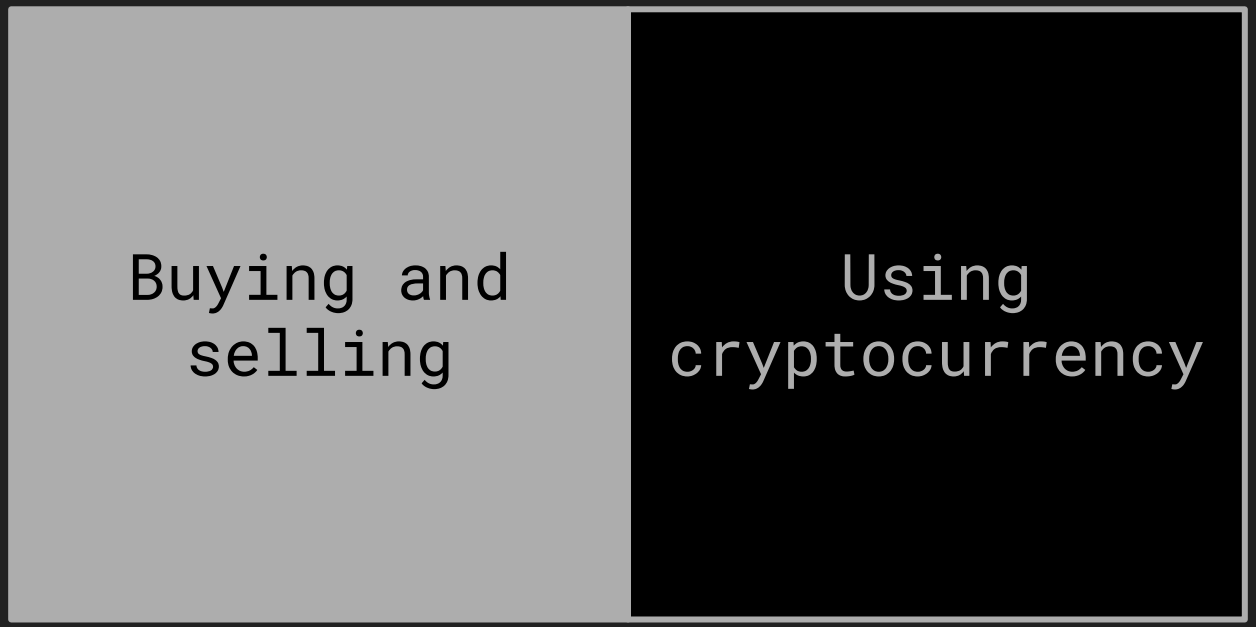
The State of the Art in Cryptocurrency Privacy

An abridged overview
of production systems
by John Light

Areas of privacy to protect



Buying and selling

Cash is king

- Cash marketplaces: Dether, LocalBitcoins, LocalEthereum, Liberalcoins, LocalTrader
- Bitcoin ATMs
  - Coin ATM Radar
- Meetups
  - Network with organizers and other regulars
- Friends

P2P exchanges

- Bisq
- OpenBazaar
- HodlHodl
- On-chain decentralized exchanges (e.g. 0x, Uniswap, etc)
- **Any trust-minimized exchange where ID is not required**

Crypto circles

- One friend buys larger amounts of crypto from exchanges/ OTC traders and distributes to smaller cash buyers, who distribute to their friends, and so on to the smallest buyers, and vice versa for sellers.

- Privacy coins and trust-minimized mixers can be used to break the link between each transaction.

Earn and spend

- Buy and sell goods and services pseudonymously
  - Buy gift cards with cryptocurrency
  - Work in exchange for cryptocurrency
  - Cryptocurrency-accepting merchants and marketplaces
  - Use a pseudonym and throwaway email address if required e.g. for delivery information

Using cryptocurrency

Tor and i2p

- Tools for anonymizing network traffic (browsing history, downloads, cryptocurrency connections)
- Hide the fact that you are using cryptocurrency from your ISP and other computers you connect to on the internet
- Not a silver bullet, use correctly e.g. these tools can’t stop you from connecting your ID to your activity at the application layer by e.g. giving your ID to an exchange or linking your cryptocurrency address to your legal name

Bitcoin

- Wasabi Wallet (ZeroLink)
- JoinMarket (CoinJoin)
- Samourai Wallet
  - Ricochet
  - Stonewall
  - Coin control
  - BIP47 Payment Codes (“stealth addresses”)
  - Future: Whirlpool (ZeroLink)
- On-chain bitcoin privacy techniques rely on obfuscation, not encryption

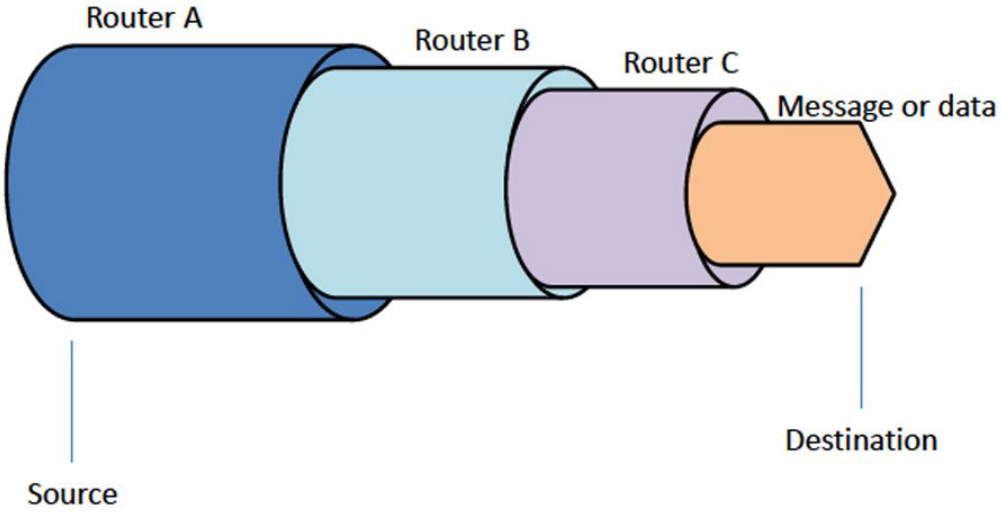
71de16fcab70ab252813914dc56e9a4a36cd9c0e8f1d6f2de6c78dee114dfa03

DETAILS +

bc1qr2fuqctpdfwpwv2zzfe0a44kzand0c3thsg4ku	0.1000127 BTC
bc1q6vq67gfs46klujesqdrjvtzmjtl7228n6hajt7	0.89984182 BTC
bc1qh7vtvff3unvg7z2sct5l9e85nry6h28ue2d9eh	0.10001115 BTC
bc1q9ysv26699daua3zhexqg4negw92j6sarycv4yl	0.24118827 BTC
bc1q6k9dsgu39y4lk33hqnl6l04w2z8qdalu23jyqk	0.10001156 BTC
bc1q4wjpsvm8r7mfyesnmvm672sx2vlg97gpqvzljn	0.10001156 BTC
bc1qmqp0y99jst5su3rah3p9pu7f684mysn8427xgd	0.18216286 BTC
bc1qwxrptj0fw0d2z06qee9ph4tyd53p7nujkszjhe	0.10001971 BTC
bc1qckf3laa4r9xrcc7jkcxc5rkd4uf5jd7n7kkmy8	0.05006037 BTC
bc1q46c7w8euvk6qwttm2lnpdgre7jrt0qfhyj4l60	0.05005881 BTC
bc1qevcru0pctvhwkw6cmnhfwe627c6x2yphcemq86	0.05005642 BTC
bc1q5ptah5cmtngy0fdhvn86p3gf3kpq2e259yp58q	0.05005611 BTC
bc1qflww7ve922e92ssxfhhfagt4gf94spglnry65f	0.10001563 BTC
bc1qka0ydz8390alahs4fy98zjlk55nap3dx5wa9nc	0.10001563 BTC
bc1qsgq969z5dnywe4xeqg76k2zyy007stjkuedry4	0.10001563 BTC
bc1q7rc75a2k4aaa9sjvfh8tkst9ehy626qw9sjmw3	0.10001563 BTC
bc1q90fcswa84ae80tz8htypar4fv9dtjauqm5tcx4	0.10001563 BTC
bc1q0m3rrnqzmyzejzxvx09d5r384ah7h7w2y5n2nw	0.10001563 BTC
bc1q76ght7v26frej3huk53j08mjrwcnalxcugx0et	0.10001563 BTC
bc1qu5rdlds9jwraza95gxq7cefcm2xgyn7p93tzgc	0.10001563 BTC
bc1qh3yjuzqgelxazfz9w3u2gzar76jhrjjvml5vu0	0.10001563 BTC
bc1q3ewat54gnrs9mjseq2zxktwg5yg799yw598gsj	0.10001563 BTC
bc1qs0q4lr840qd0vdww7hkmrv7pnhsusrpg7jy4l9	0.10001563 BTC
bc1qmxrp97rheg9heawypfm0qk44ytdjvxyd4kdmzd	0.10001563 BTC

Lightning

- Off-chain payment network (BTC, LTC, DCR, et al)
- Sphinx onion routing obscures sender and recipient
- Future: Hidden Destination


Router A
Router B
Router C
Message or data
Source
Destination

Zcash

- zk-SNARK encryption (“shielded” or “z” addresses)
- Future: BOLT anonymous off-chain payment network
- Future: Transparent addresses will be deprecated
- Transparent addresses shrink the anonymity set
- Theoretical “toxic waste” could damage monetary property

“Zcash’s privacy tech makes it the most interesting Bitcoin alternative.” - Edward Snowden, whistleblower

Summary

Received Time	Tue 15 Nov 2016 19:29:24 PST (10 months ago)	**Included in Block**	11143
Index	5	**Lock Time**	0
Version	2	**Inputs**	0
Outputs	0	**JoinSplits**	1

Details

Txn 35f6674a1691f21aff6a3819467dbba82aaebf061d50c6ac55f39fbeae73b9a6

Value Transfer

JoinSplits

Input		*Output*
Transparent 0 ZEC + Shielded ? ZEC	► JoinSplit ►	Transparent 0.0001 ZEC + Shielded ? ZEC

Inputs

Outputs

181661 confirmations | 0.0001 ZEC | ≥ 0.0001 ZEC

Monero

- RingCT - encrypted transaction amounts
- Ring Signatures - obfuscate sender and recipient
- Relies on obfuscation - not encryption - for sender and recipient anonymity
- Multiple incidents of accidentally traceable transactions

“Amateur crypto… Mistakes happen and have huge consequences for people like me.” - Edward Snowden, whistleblower

Transaction

Tx hash:	bb72dd162eeef171c37aa071f3ade44ac41a5e6ed8cf35bf9b22fe249bc6fc0e
Tx prefix hash:	a77d0c1a193e73ef09e9dc64f681bff8e2238f85ac61dc70cffcc6f3e27aec8b
Tx public key:	a038e997c58b5b2fb9082e9c68a626ebf0ac314339b53d1eb8d6be0c49fea3d6
Block:	1409324
Output total:	?
Timestamp [UTC]:	2017-09-28 23:56:53
Fee:	0.060000000000
Tx size:	15.7490 Kb
Tx version:	2
# of confirmations:	3
RingCT/type:	yes/2
Extra:	01a038e997c58b5b2fb9082e9c68a626ebf0ac314339b53d1eb8d6be0c49fea3d6

2 output(s) for total of ? xmr

#	Stealth address	Amount	Amount Index
00	3aa5c928d1be9b67bbc0794c8017a137a6745e32ff38475ffccbafd8827c313b	?	2788052 of 2788083
01	26b9bb265c0c54ad1b2022d8df7f01f89dc62e5618697381640181 6d039499f5	?	2788053 of 2788083

8 inputs(s) for total of ? xmr

#	Key image (click row to expand)	Amount
00	e9936fdcc98194f0d3fe93eb5edd2cb15015ae2d51492e65806f2f218027f33a	?

Mixin	stealth address	blk	mixin	in/out	timestamp	age [y:d:h:m:s]
- 00:	5ca5b103b2f708f9cfcf17a59eea7b396cdfa026bd941e087dbb6fce3916f6b2	01298504	5	5/6	2017-04-28 14:02:22	00:153:10:06:03
- 01:	64ea9f9af1619ec53f6fe08ec328adf571450eb811c853c315094623d694d153	01322717	5	37/38	2017-06-01 05:34:36	00:119:18:33:49
- 02:	26d1d08ad684f1da874aac82c538f30baa73b8b79d8be2062b0930b9c177280d	01322903	5	37/38	2017-06-01 11:37:40	00:119:12:30:45
- 03:	42253ac752979ef4bda107e1c14f498c7e128babcdf3ad0309a7ed28d696a4a7	01346263	3	8/9	2017-07-03 19:19:48	00:087:04:48:37
- 04:	78e343387ca43ad4f9e8dac73fc4fe92a21a085088d7be938d2a57e5d0fb41cb	01408945	5	3/2	2017-09-28 11:32:04	00:000:12:36:21

#	Key image (click row to expand)	Amount
01	8373e833c16c03fd3e9088f657221d3bcf9d9f40aea0a127d9ac4e96aaa85584	?

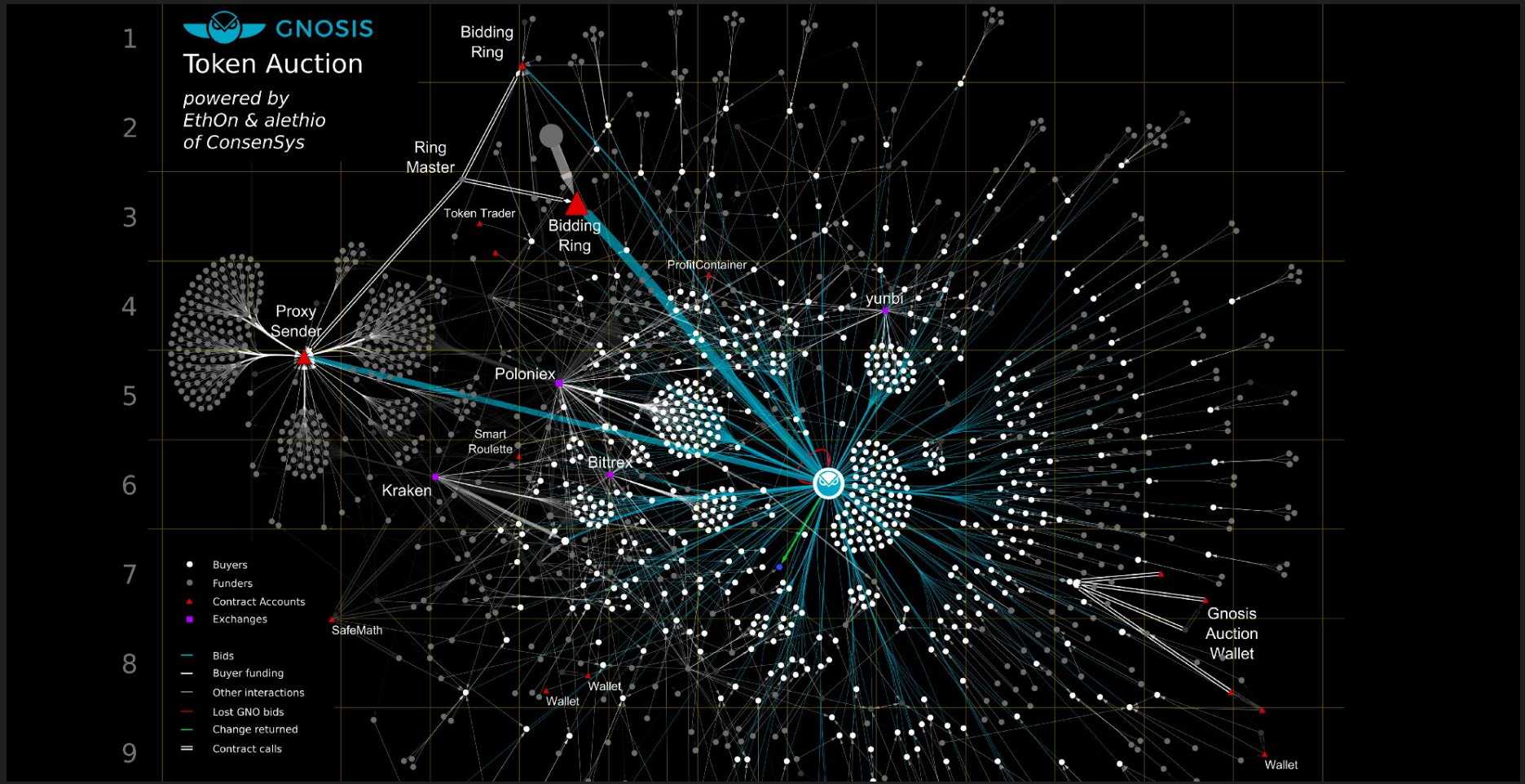
Mixin	stealth address	blk	mixin	in/out	timestamp	age [y:d:h:m:s]
- 00:	2aa941a2566d7dd27e26de4998a0d50eaf708d32f571f0d83f8e060fe6936c77	01315719	0	0/1	2017-05-22 12:37:29	00:129:11:30:56
- 01:	eeb1e536f2157a9cb73bc0a612a287a7419533491d11912fd5e835b31462c86f	01341288	5	1/2	2017-06-26 22:30:11	00:094:01:38:14
- 02:	184d44ba8cb80355f177ee66effa3cda69a4e6882b9744b5a52836c7239bfc14	01348143	5	37/38	2017-07-06 08:03:06	00:084:16:05:19
- 03:	67df8385cfc96050a634679a8257eba064e573e6c11b9a33dce25d774c7847c8	01370063	3	2/3	2017-08-05 17:03:55	00:054:07:04:30
- 04:	96af4f9a1f06ddc87431e810d97700d5c836d7bcc8eaca41af745c73c9492af9	01409096	5	3/2	2017-09-28 16:01:40	00:000:08:06:45

Ethereum

“Privacy on ethereum is bad, really, really bad.”

- Peter Szilagyi, geth core dev

(Hopefully this improves; zk-SNARKs when?)


GNOSIS
Token Auction
powered by
EthOn & alethio
of ConsenSys
Bidding Ring
Ring Master
Token Trader
Bidding Ring
ProfitContainer
yunbi
Proxy Sender
Poloniex
Smart Roulette
Bittrex
Kraken
SafeMath
Wallet
Wallet
Gnosis Auction Wallet
Wallet
Buyers
Funders
Contract Accounts
Exchanges
Bids
Buyer funding
Other interactions
Lost GNO bids
Change returned
Contract calls

A word about full nodes

- A full node is software that downloads and validates the full contents of every block in the blockchain
- Wallets not connected to your own full node share your addresses and balances with third party servers, making it trivial to correlate and track your blockchain activity
- Using a wallet that is connected to your own node is essential - but not sufficient - to using cryptocurrency privately today (but this could change in the future!)

In conclusion

- There is no “privacy silver bullet”
- Privacy and anonymity are a spectrum, not binary
- Privacy with cryptocurrency is still hard (but improving!)
- All else being equal: Cash + Tor + Zcash z-addresses is the most private option today (change my mind!)

Questions?

References and further reading

- Decentralized marketplaces
  - https://github.com/john-light/decentralized-marketplaces/blob/master/README.md
- Decentralized exchanges
  - https://github.com/distribuyed/index
- Buying cryptocurrency with cash
  - https://99bitcoins.com/buy-bitcoin/buy-bitcoin-with-cash/
- Tor and i2p info
  - https://geti2p.net/en/comparison/tor
  - https://www.torproject.org/download/download.html.en#Warning

References and further reading (cont’d)

- Bitcoin info
  - https://www.openbitcoinprivacyproject.org/
  - https://github.com/Samourai-Wallet/Whirlpool
  - https://github.com/JoinMarket-Org/joinmarket#what-is-joinmarket-
- Wasabi Wallet ZeroLink transaction
  - https://blockstream.info/tx/71de16fcab70ab252813914dc56e9a4a36cd9c0e8f1d6f2de6c78dee114dfa03
- Lightning Network Sphinx onion routing
  - https://github.com/lightningnetwork/lightning-rfc/blob/master/04-onion-routing.md

References and further reading (cont’d)

- Zcash info
  - https://z.cash/technology/zksnarks/
  - https://z.cash/support/security/privacy-security-recommendations/
- Monero info
  - https://ww.getmonero.org/resources/research-lab/
  - https://medium.com/@JEhrenhofer/estimating-an-upper-bound-for-the-impact-of-chain-splits-on-monero-64fca7fce918
  - https://www.getmonero.org/2018/03/29/response-to-an-empirical-analysis-of-traceability.html
- Ethereum info
  - https://github.com/AztecProtocol/AZTEC
  - https://github.com/seresistvanandras/MixEth

References and further reading (cont’d)

- Zexe: decentralized private computation
  - https://eprint.iacr.org/2018/962.pdf
- Zcash vs Monero metadata comparison
  - https://twitter.com/lightcoin/status/913560957141397504
- Edward Snowden quotes
  - https://twitter.com/Snowden/status/913544739542241282
  - https://twitter.com/Snowden/status/913557610858778625
- Peter Szilagyi quote
  - https://www.coindesk.com/the-little-known-ways-ethereum-reveals-user-location-data