ALL THINGS OPEN 2016

CONSUMER PRIVACY IN BLOCKCHAINS

ABOUT KRISTOV

- Author, security engineer, privacy research, advocate of crypto-economics and science based engineering
  - blockchain.info
    - Largest Bitcoin wallet provider in the world
  - openbitcoinprivacyproject.org
    - Research and education, including threat modeling, stat analysis, BIPs, Consumer Reports
- Skeptic of non-Bitcoin blockchains
  - Blockchains resist censorship
  - Money is censored
  - Network effect of currencies
  - Are there enough kinds of monetary behavior to create sustainable niches?

WHAT ARE WE GOING TO DO WITH BLOCKCHAINS?

- Tell the world about our purchases (Bitcoin)
  - Some purchases are sensitive
  - Non-sensitive purchases must be kept private to provide privacy for sensitive ones
- Encode the details of our business contracts (Ethereum)
- Tell the world where we're going (LaZooz)
- Track our ham on the porkchain
- Conclusion: Blockchains will be a treasure trove for analytics, surveillance apparatuses, stalkers, and the Pig's Liberation Front

HOW DO WE GET DATA PRIVACY IN TRANSIT?

- Keep the data to yourself
    - “If you can’t protect it, don’t collect it”
    - “But the peers of my private blockchain are inside my trust boundary!”
        - …until one gets hacked or defects
        - They might be your *competitors*. **Got any trade secrets?**
- If you must send data, make it look the same
- If you can’t make it look the same, make it appear uniformly random to untrusted parties
    - Example of uniformity: padding messages
- Send data in crowds

BLOCKCHAIN TECH STACK (STOLEN FROM ANNA@IBM)

- Database: Shared ledger where **information** is placed
- Consensus algorithms (PoW, PoS, PBFT)
- P2P Communication: Transmitting **information** to peers
- Cryptography
    - Signing and verification
    - Fancy smart contract crypto magick

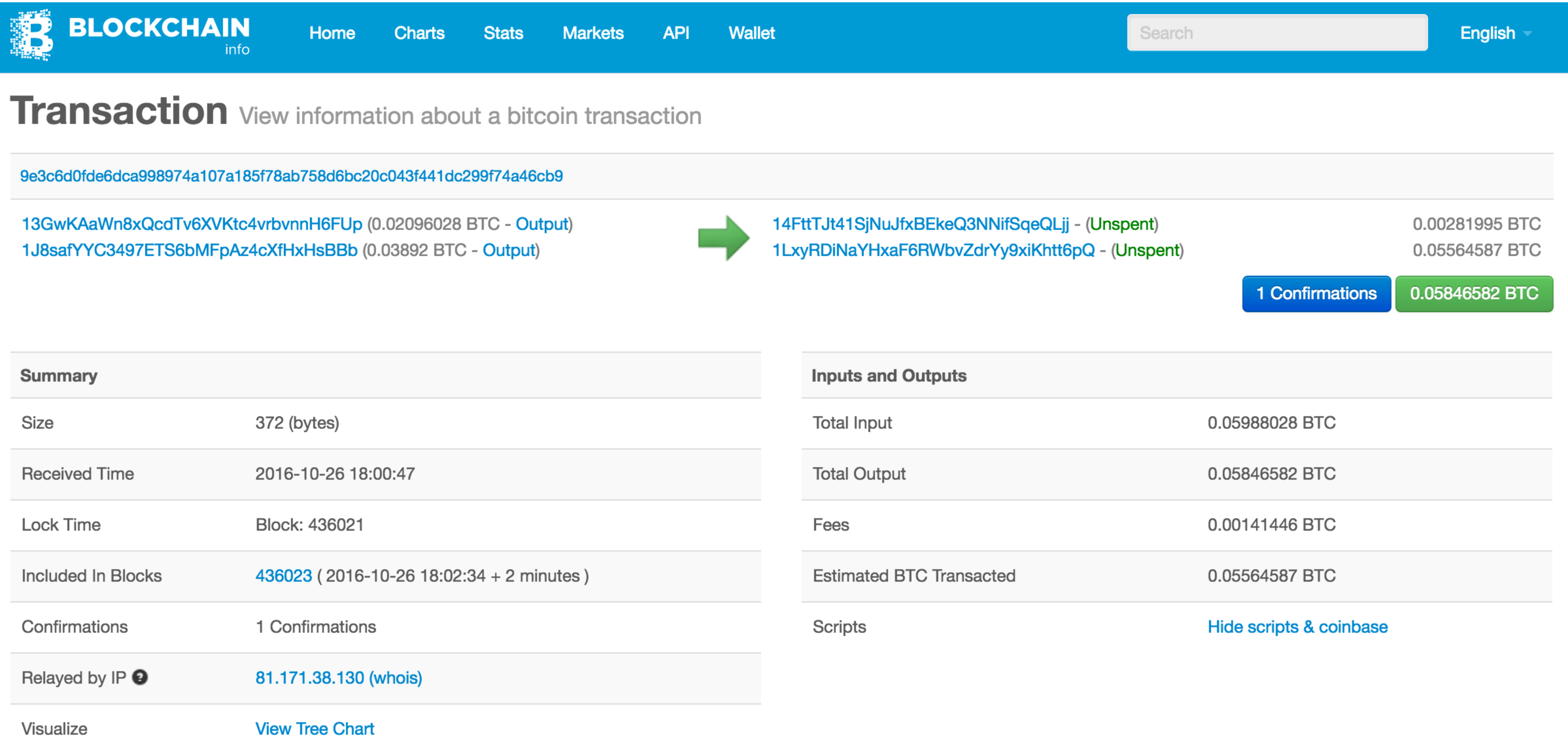
TYPES OF BLOCKCHAINS

- UTXO based: Bitcoin and derivatives
  - Unspent Transaction Output
- Account based: Ethereum
- Other
  - Permissioned blockchains have a different privacy threat model
  - Trust boundaries: Data sent between employees in same department? Inter-department? Inter-company?

TRANSACTIONS IN BITCOIN

- Inputs
  - Quantities of bitcoins spent from previous transactions
  - Inputs correspond to one or more Bitcoin addresses
- Outputs
  - Quantities of bitcoins created in this transaction <= inputs
  - Outputs correspond to one or more Bitcoin addresses
- Fees
  - Payment for transaction-inclusion service to miner
- Miscellaneous fields (locktime, sequence numbers, etc.)

SAMPLE BITCOIN TRANSACTION



Transaction View information about a bitcoin transaction

9e3c6d0fde6dca998974a107a185f78ab758d6bc20c043f441dc299f74a46cb9

13GwKAaWn8xQcdTv6XVKtc4vrbvnnH6FUp (0.02096028 BTC - Output)
1J8safYYC3497ETS6bMFpAz4cXfHxHsBBb (0.03892 BTC - Output)

14FttTJt41SjNuJfxBEkeQ3NNifSqeQLjj - (Unspent) 0.00281995 BTC
1LxyRDiNaYHxaF6RWbvZdrYy9xiKhtt6pQ - (Unspent) 0.05564587 BTC

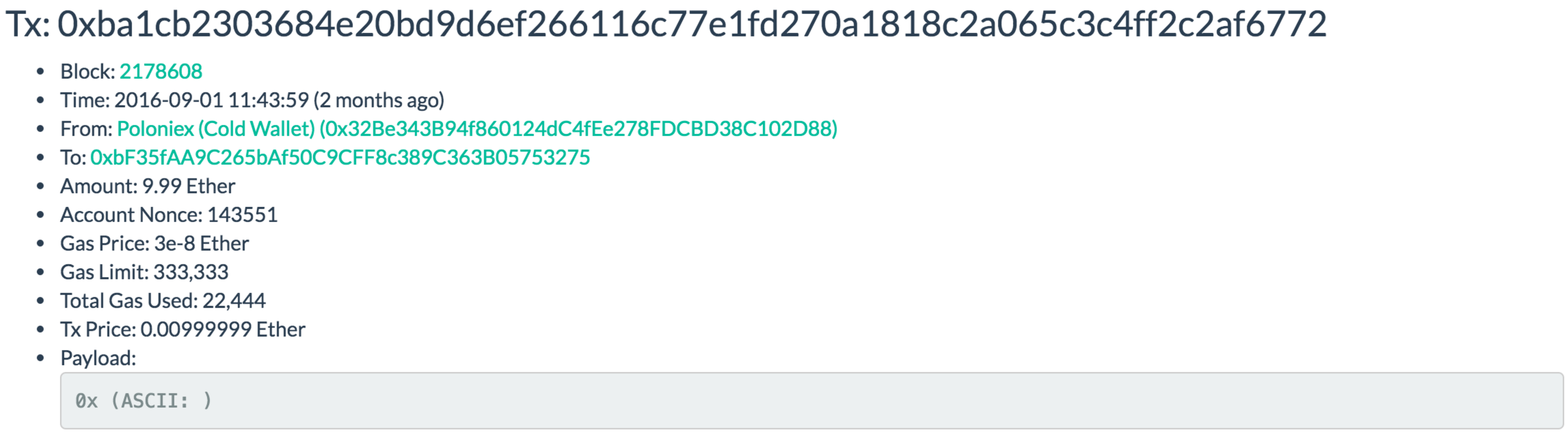
1 Confirmations 0.05846582 BTC

Summary	
Size	372 (bytes)
Received Time	2016-10-26 18:00:47
Lock Time	Block: 436021
Included In Blocks	436023 (2016-10-26 18:02:34 + 2 minutes)
Confirmations	1 Confirmations
Relayed by IP ❓	81.171.38.130 (whois)
Visualize	View Tree Chart

Inputs and Outputs	
Total Input	0.05988028 BTC
Total Output	0.05846582 BTC
Fees	0.00141446 BTC
Estimated BTC Transacted	0.05564587 BTC
Scripts	Hide scripts & coinbase

TRANSACTIONS IN ETHEREUM

- Sender Account (“From”)
- Receiver Account (“To”)
- Amount
- Fees (Gas)



Tx: 0xba1cb2303684e20bd9d6ef266116c77e1fd270a1818c2a065c3c4ff2c2af6772

- Block: 2178608
- Time: 2016-09-01 11:43:59 (2 months ago)
- From: Poloniex (Cold Wallet) (0x32Be343B94f860124dC4fEe278FDCBD38C102D88)
- To: 0xbF35fAA9C265bAf50C9CFF8c389C363B05753275
- Amount: 9.99 Ether
- Account Nonce: 143551
- Gas Price: 3e-8 Ether
- Gas Limit: 333,333
- Total Gas Used: 22,444
- Tx Price: 0.00999999 Ether
- Payload:

```
0x (ASCII: )
```

THREAT MODELING DOCUMENTATION FRAMEWORK

- Express the elements of your threat model (attackers, attacks, countermeasures, criteria)
- Score or weight the elements for importance
- Generate supporting documentation
- Identify weaknesses, prioritize changes, compare approaches
- github.com/openbitcoinprivacyproject/threat-model-scoring-system

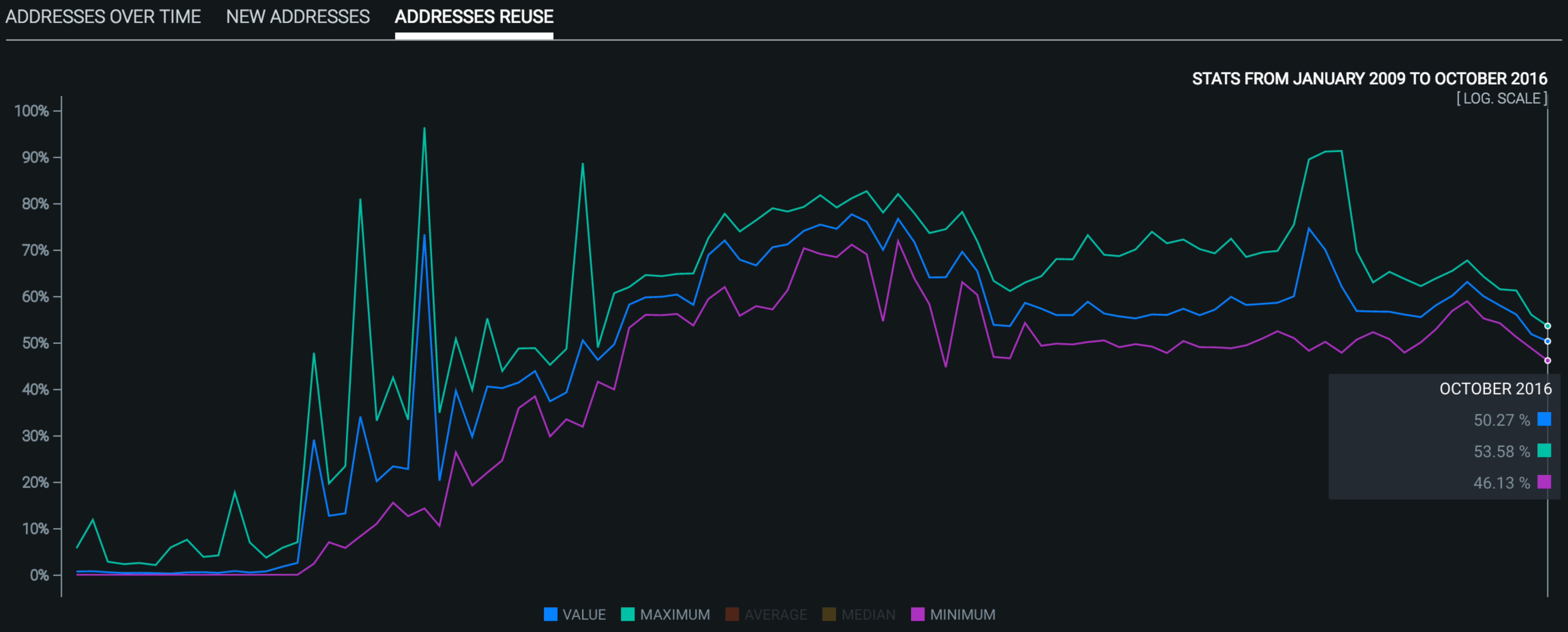
TYPES OF PRIVACY ATTACKERS

- Blockchain observer: Everyone gets a copy!
- Network observer: ISPs, CDNs, etc.
- Protocol peer: P2P traffic
- Transaction participant: People and services you transact with
- Physical adversary: Surveillance cameras
- Software providers: Malicious changes to user software
- "Meta attacks": Seemingly unrelated stuff impacting privacy decisions by users
- Full threat model for Bitcoin: github.com/openbitcoinprivacyproject/wallet-ratings

UTXO- & ACCOUNT-BASED BLOCKCHAIN OBSERVERS

- Identity many transactions belong to a given address cluster (UTXO-based) or account (account-based)
- Cluster addresses based on inputs/sender (UTXO)
- Cluster addresses based on change vs. send discrimination (UTXO)
- Use idiosyncrasies to fingerprint wallet
    - Conceptually similar to browser fingerprinting
- Link transactions to out-of-band behavior taking place at similar time
- Link transactions to a time zone based on consistent periods of activity

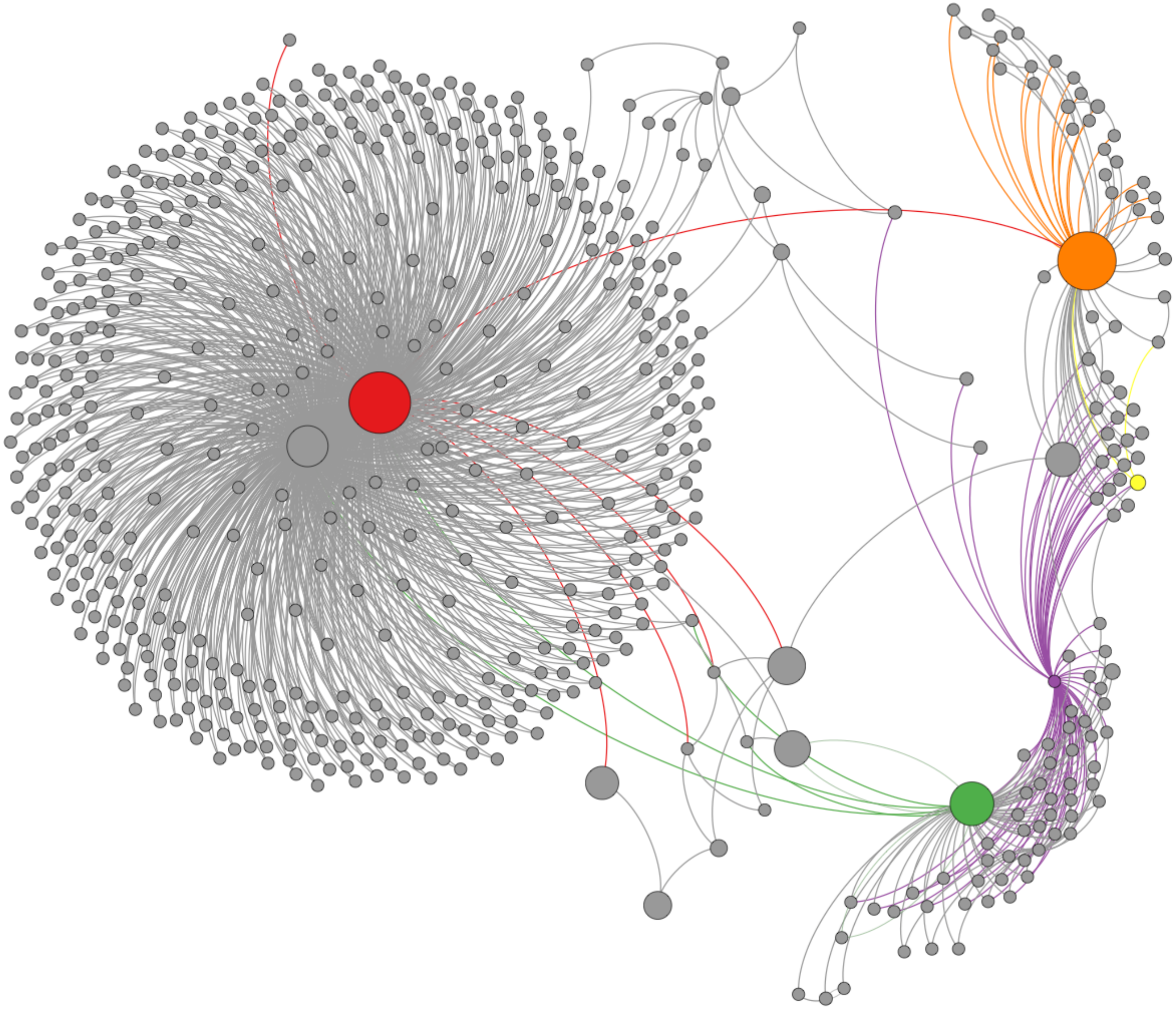
ADDRESS REUSE ON BITCOIN BLOCKCHAIN (DATA VIA OXT.ME)



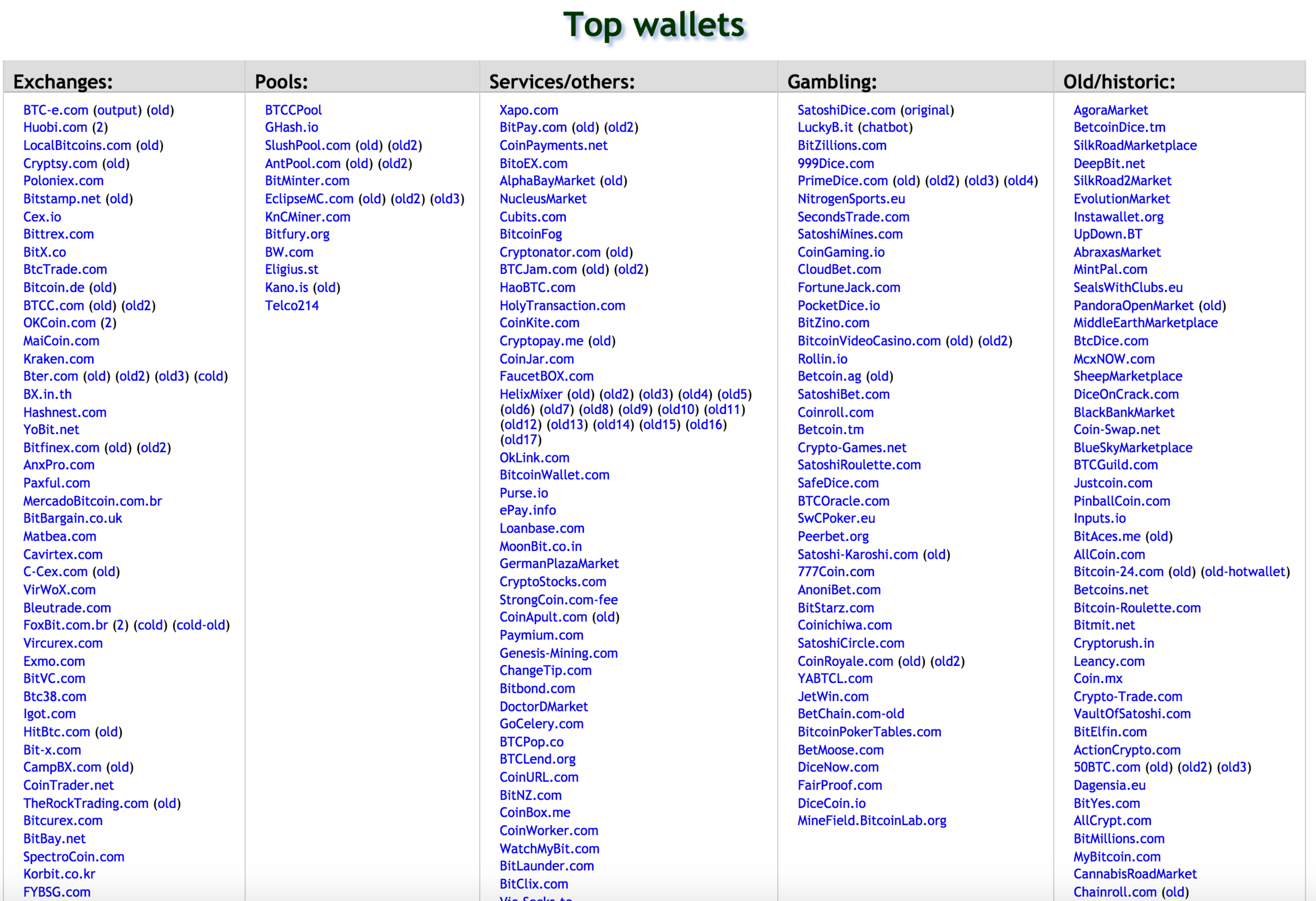
ADDRESS REUSE IN ETHEREUM BLOCKCHAIN

- Probably quite high
- Betrays relationships between users/services and contracts
- Possible solution: HD accounts
  - Common in Bitcoin for a few years
  - Recently adopted by Bitcoin Core
  - Derive many accounts (billions+) from a single seed
  - Improved backup experience

WHY DOES ADDRESS REUSE MATTER?



SERVICE CLUSTERING IN THE BITCOIN BLOCKCHAIN (WALLETEXPLORER.COM)



Top wallets

Exchanges:

BTC-e.com (output) (old)
Huobi.com (2)
LocalBitcoins.com (old)
Cryptsy.com (old)
Poloniex.com
Bitstamp.net (old)
Cex.io
Bittrex.com
BitX.co
BtcTrade.com
Bitcoin.de (old)
BTCC.com (old) (old2)
OKCoin.com (2)
MaiCoin.com
Kraken.com
Bter.com (old) (old2) (old3) (cold)
BX.in.th
Hashnest.com
YoBit.net
Bitfinex.com (old) (old2)
AnxPro.com
Paxful.com
MercadoBitcoin.com.br
BitBargain.co.uk
Matbea.com
Cavirtex.com
C-Cex.com (old)
VirWoX.com
Bleutrade.com
FoxBit.com.br (2) (cold) (cold-old)
Vircurex.com
Exmo.com
BitVC.com
Btc38.com
Igot.com
HitBtc.com (old)
Bit-x.com
CampBX.com (old)
CoinTrader.net
TheRockTrading.com (old)
Bitcurex.com
BitBay.net
SpectroCoin.com
Korbit.co.kr
FYBSG.com

Pools:

BTCCPool
GHash.io
SlushPool.com (old) (old2)
AntPool.com (old) (old2)
BitMinter.com
EclipseMC.com (old) (old2) (old3)
KnCMiner.com
Bitfury.org
BW.com
Eligius.st
Kano.is (old)
Telco214

Services/others:

Xapo.com
BitPay.com (old) (old2)
CoinPayments.net
BitoEX.com
AlphaBayMarket (old)
NucleusMarket
Cubits.com
BitcoinFog
Cryptonator.com (old)
BTCJam.com (old) (old2)
HaoBTC.com
HolyTransaction.com
CoinKite.com
Cryptopay.me (old)
CoinJar.com
FaucetBOX.com
HelixMixer (old) (old2) (old3) (old4) (old5) (old6) (old7) (old8) (old9) (old10) (old11) (old12) (old13) (old14) (old15) (old16) (old17)
OkLink.com
BitcoinWallet.com
Purse.io
ePay.info
Loanbase.com
MoonBit.co.in
GermanPlazaMarket
CryptoStocks.com
StrongCoin.com-fee
CoinApult.com (old)
Paymium.com
Genesis-Mining.com
ChangeTip.com
Bitbond.com
DoctorDMarket
GoCelery.com
BTCPop.co
BTCLend.org
CoinURL.com
BitNZ.com
CoinBox.me
CoinWorker.com
WatchMyBit.com
BitLaunder.com
BitClix.com
VipSocks.to

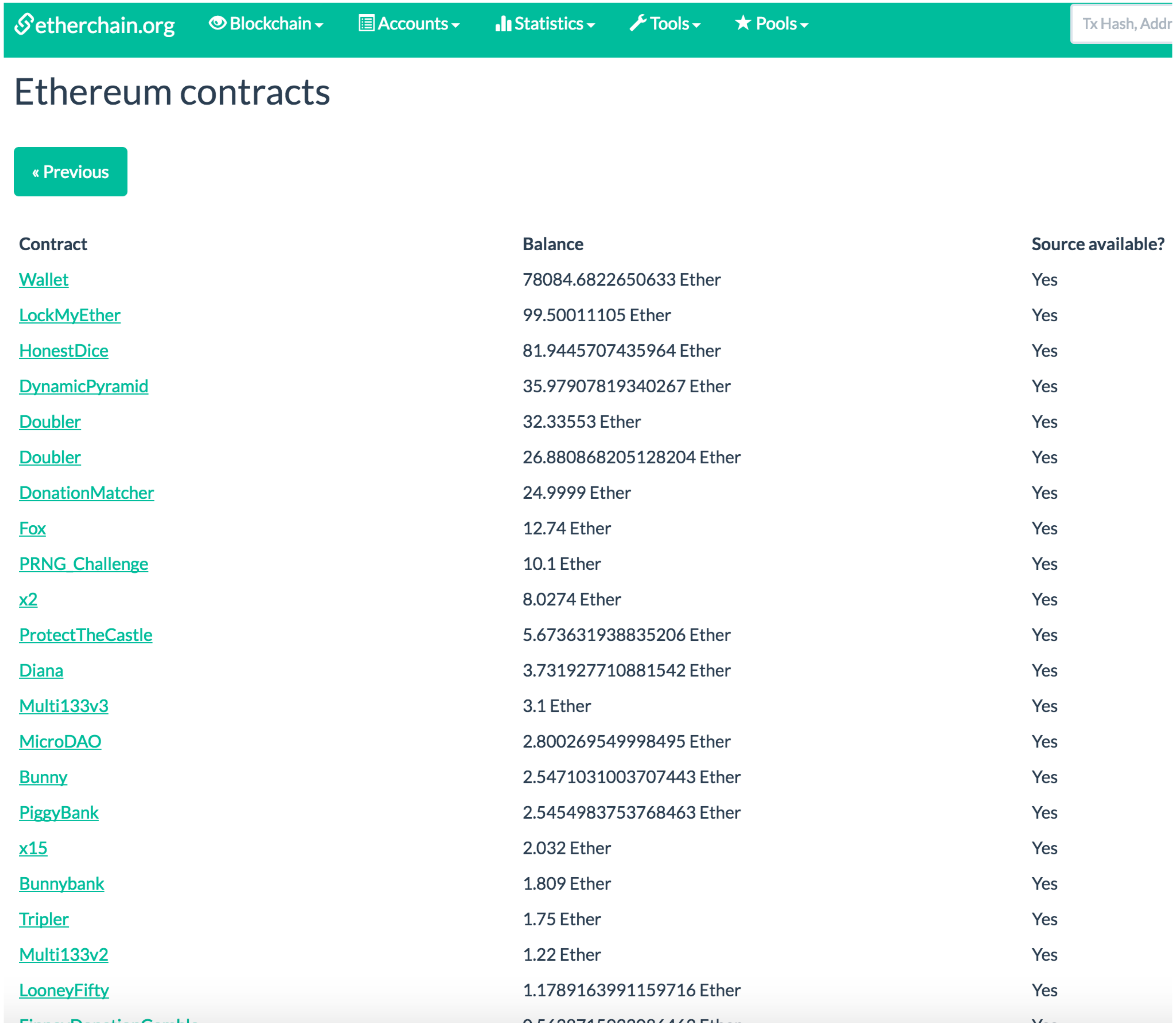
Gambling:

SatoshiDice.com (original)
LuckyB.it (chatbot)
BitZillions.com
999Dice.com
PrimeDice.com (old) (old2) (old3) (old4)
NitrogenSports.eu
SecondsTrade.com
SatoshiMines.com
CoinGaming.io
CloudBet.com
FortuneJack.com
PocketDice.io
BitZino.com
BitcoinVideoCasino.com (old) (old2)
Rollin.io
Betcoin.ag (old)
SatoshiBet.com
Coinroll.com
Betcoin.tm
Crypto-Games.net
SatoshiRoulette.com
SafeDice.com
BTCOracle.com
SwCPoker.eu
Peerbet.org
Satoshi-Karoshi.com (old)
777Coin.com
AnoniBet.com
BitStarz.com
Coinichiwa.com
SatoshiCircle.com
CoinRoyale.com (old) (old2)
YABTCL.com
JetWin.com
BetChain.com-old
BitcoinPokerTables.com
BetMoose.com
DiceNow.com
FairProof.com
DiceCoin.io
MineField.BitcoinLab.org

Old/historic:

AgoraMarket
BetcoinDice.tm
SilkRoadMarketplace
DeepBit.net
SilkRoad2Market
EvolutionMarket
Instawallet.org
UpDown.BT
AbraxasMarket
MintPal.com
SealsWithClubs.eu
PandoraOpenMarket (old)
MiddleEarthMarketplace
BtcDice.com
McxNOW.com
SheepMarketplace
DiceOnCrack.com
BlackBankMarket
Coin-Swap.net
BlueSkyMarketplace
BTCGuild.com
Justcoin.com
PinballCoin.com
Inputs.io
BitAces.me (old)
AllCoin.com
Bitcoin-24.com (old) (old-hotwallet)
Betcoins.net
Bitcoin-Roulette.com
Bitmit.net
Cryptorush.in
Leancy.com
Coin.mx
Crypto-Trade.com
VaultOfSatoshi.com
BitElfin.com
ActionCrypto.com
50BTC.com (old) (old2) (old3)
Dagensia.eu
BitYes.com
AllCrypt.com
BitMillions.com
MyBitcoin.com
CannabisRoadMarket
Chainroll.com (old)

SERVICE TAGGING IN THE ETHEREUM BLOCKCHAIN



Ethereum contracts

« Previous

Contract	Balance	Source available?
Wallet	78084.6822650633 Ether	Yes
LockMyEther	99.50011105 Ether	Yes
HonestDice	81.9445707435964 Ether	Yes
DynamicPyramid	35.97907819340267 Ether	Yes
Doubler	32.33553 Ether	Yes
Doubler	26.880868205128204 Ether	Yes
DonationMatcher	24.9999 Ether	Yes
Fox	12.74 Ether	Yes
PRNG_Challenge	10.1 Ether	Yes
x2	8.0274 Ether	Yes
ProtectTheCastle	5.673631938835206 Ether	Yes
Diana	3.731927710881542 Ether	Yes
Multi133v3	3.1 Ether	Yes
MicroDAO	2.800269549998495 Ether	Yes
Bunny	2.5471031003707443 Ether	Yes
PiggyBank	2.5454983753768463 Ether	Yes
x15	2.032 Ether	Yes
Bunnybank	1.809 Ether	Yes
Tripler	1.75 Ether	Yes
Multi133v2	1.22 Ether	Yes
LooneyFifty	1.1789163991159716 Ether	Yes

NETWORK ATTACKS ON PRIVACY

- Observe the first hop of unencrypted traffic, link to IP address or other distinguishing characteristics of sender
  - Reduce the privacy set of encrypted traffic using timing analysis
- Observe which data nodes query for (P2P or centralized)
- Observe side channel leaks (e.g. transaction triggers email)
- Observe User Agent or other idiosyncrasies to fingerprint client
- Observe updates to transactions (Replace By Fee)

BALANCING DISCLOSURE WITH PRIVACY

- Usually the goal of blockchains is to provide *accountability* and not complete *transparency*
- Avoid address reuse in UTXO-based blockchains
- Combine many transactions into one on-chain
  - CoinJoin
  - TumbleBit
  - Privacy of off-chain transactions TBD
- Use privacy-friendly network channels
  - Tor, I2P, etc.
- Craft transactions in as uniform a fashion as possible to combat software fingerprinting
- Introduce random delays to combat timing analysis
- Use fancy crypto to obfuscate values that do not require disclosure
  - Fully homomorphic encryption (e.g. Confidential Transactions)

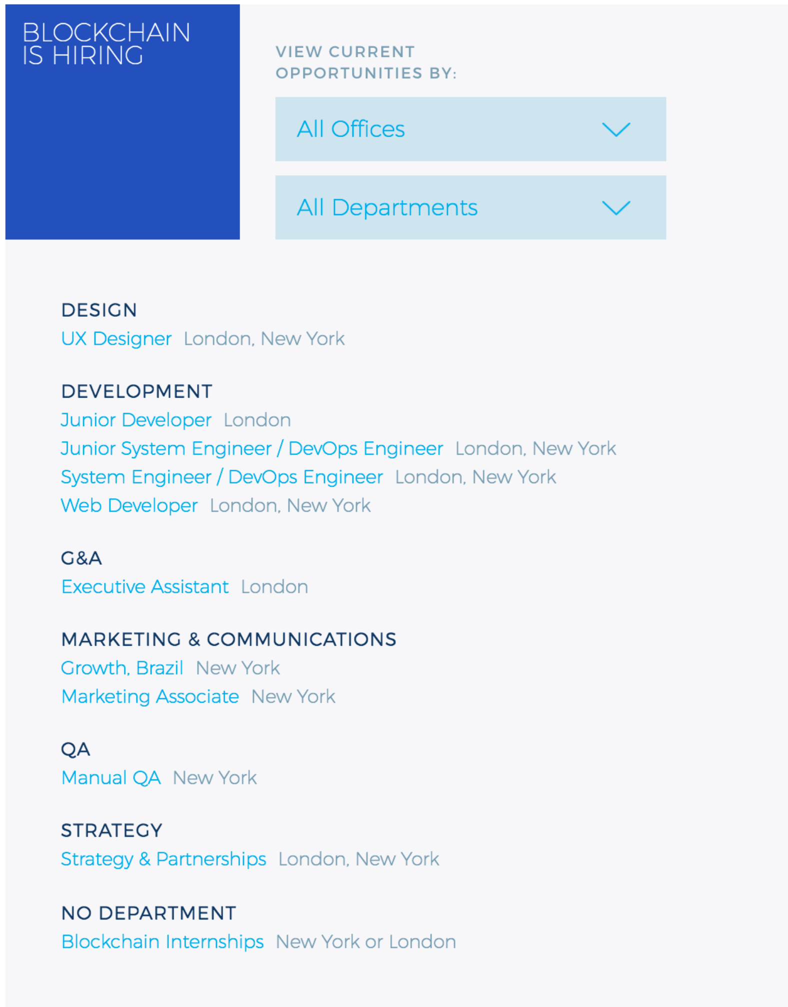
QUESTIONS?

FIND ME ONLINE

- Twitter: @kristovatlas
- Blog: kristovatlas.com
- OBPP
  - @obpp_org
  - OpenBitcoinPrivacyProject.org

BLOCKCHAIN IS HIRING

- blockchain.com
- kristov[at]blockchain.com



BLOCKCHAIN IS HIRING

VIEW CURRENT OPPORTUNITIES BY:

All Offices

All Departments

DESIGN

UX Designer London, New York

DEVELOPMENT

Junior Developer London

Junior System Engineer / DevOps Engineer London, New York

System Engineer / DevOps Engineer London, New York

Web Developer London, New York

G&A

Executive Assistant London

MARKETING & COMMUNICATIONS

Growth, Brazil New York

Marketing Associate New York

QA

Manual QA New York

STRATEGY

Strategy & Partnerships London, New York

NO DEPARTMENT

Blockchain Internships New York or London