Blockchains & Cryptocurrencies

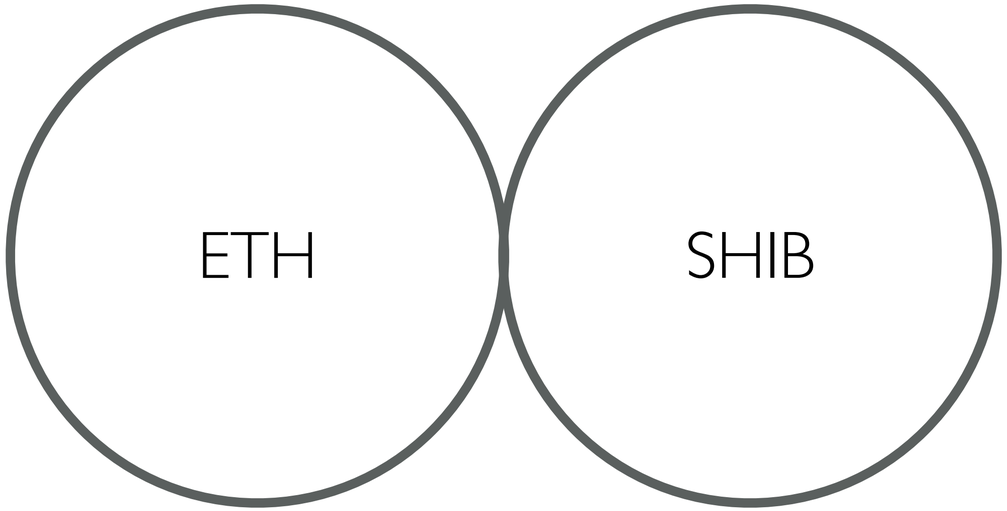
Ethereum Applications / Privacy

Instructor: Matthew Green
Fall 2024

News?

Constant Function Market Makers (AMM)

- A simpler (and much less efficient) type of exchange
  - Built from pairs of assets (e.g., ETH/SHIB)
  - New LPs can increase/reduce the overall size of both pools, without changing the ratio

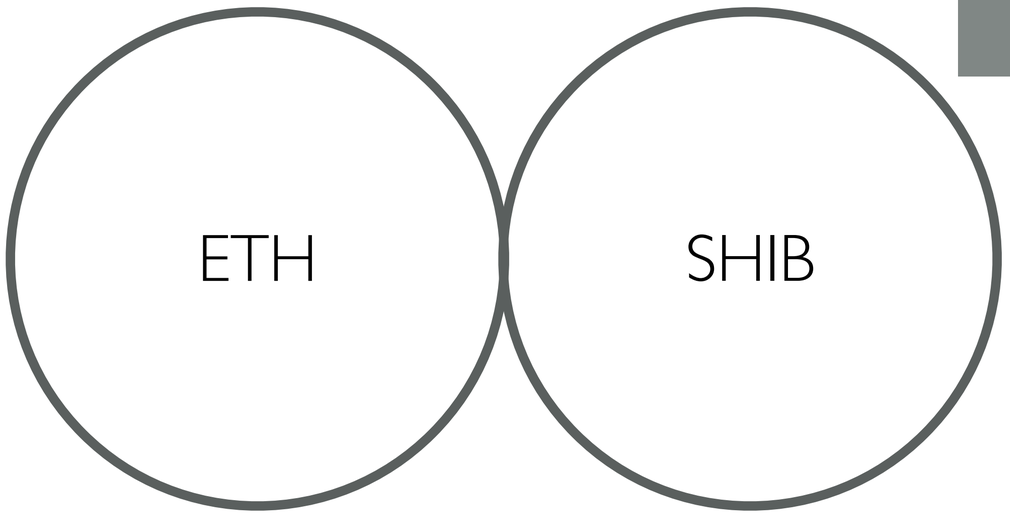


Constant Function Market Makers (AMM)

- A simpler (and much less efficient) type of exchange
  - Built from pairs of assets (e.g., ETH/SHIB)
  - Users can also "swap" (deposit one asset, withdraw the other), in exchange for fees

Overall goal:
Preserve a constant function (e.g., product, sum). E.g.,:

$$A * B = K$$

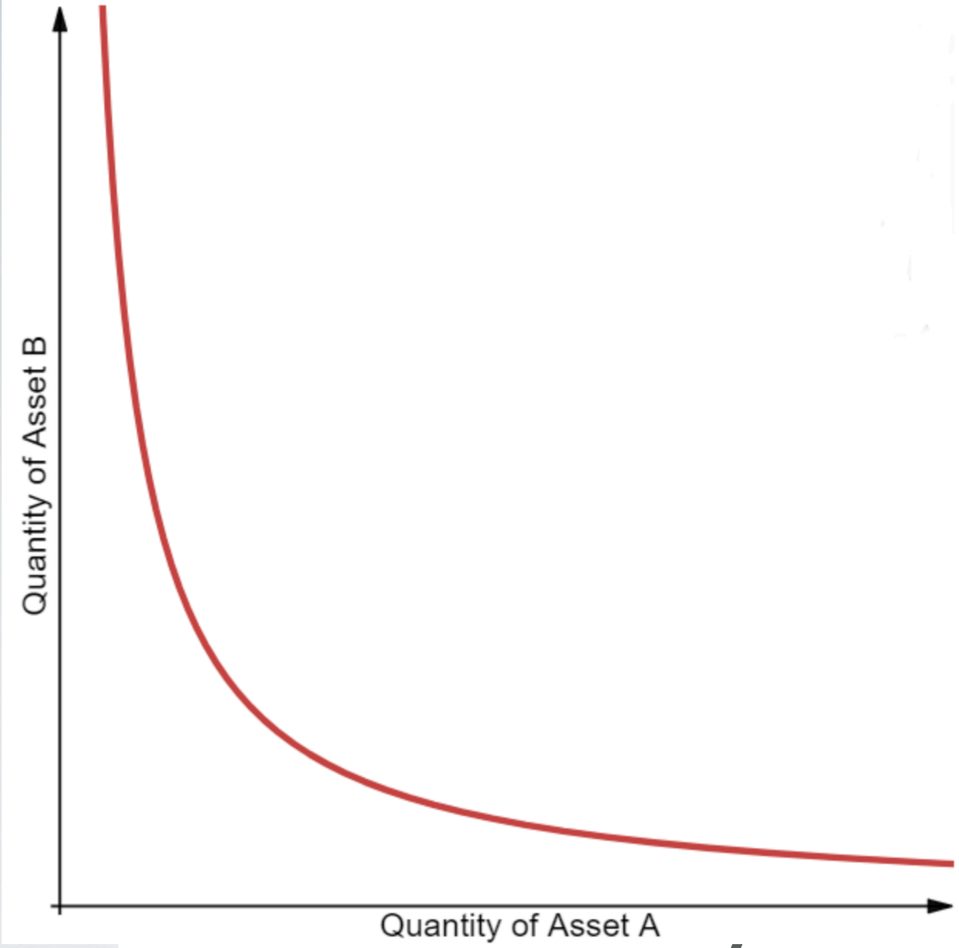


ɔn Market Makers (AMM)

ess efficient) type of exchange

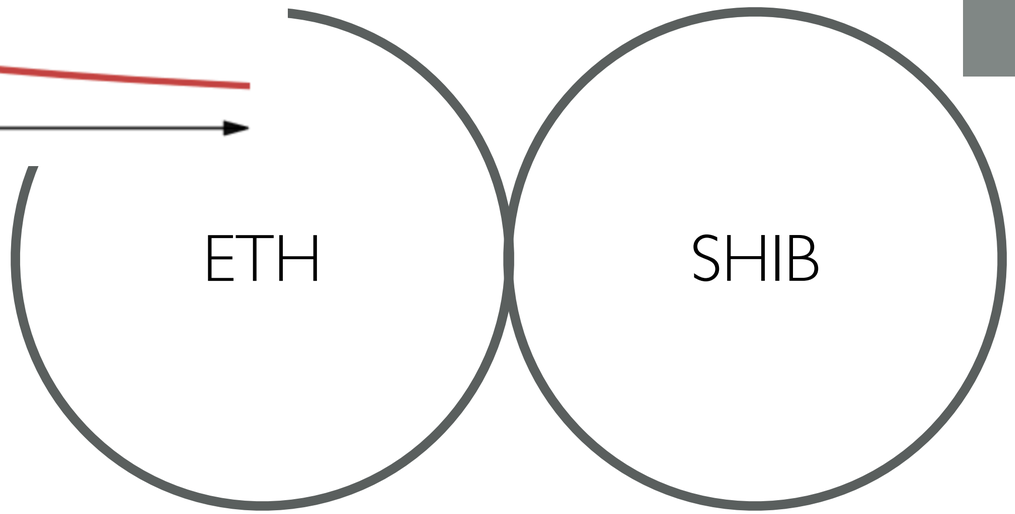
sets (e.g., ETH/SHIB)

d withdraw assets (in vari
ɔol”



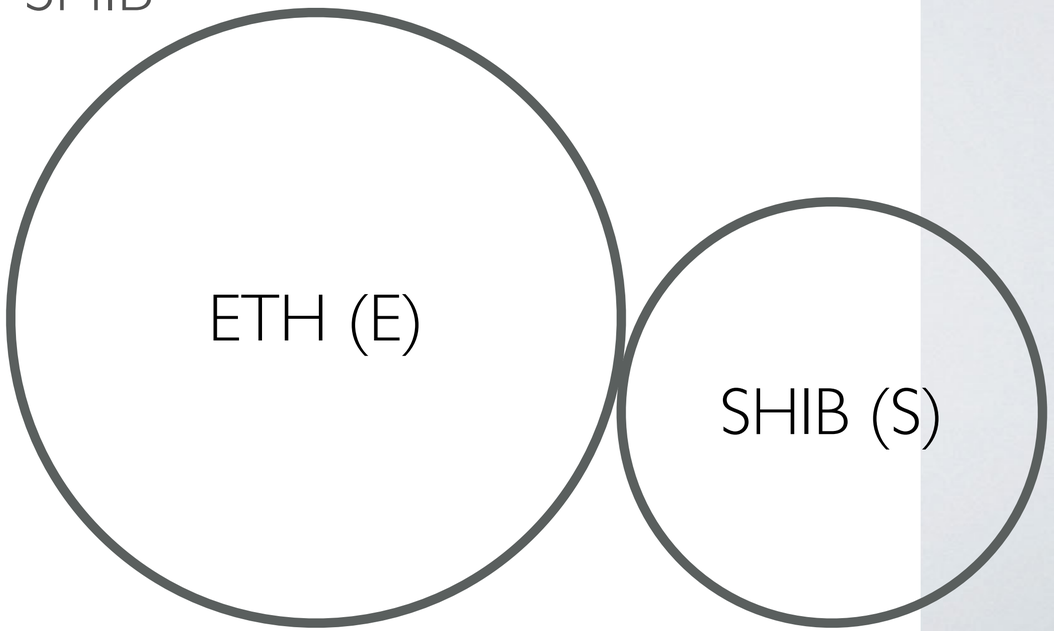
Overall goal:
Preserve a constant function (e.g., product, sum). E.g.,:

$A * B = K$

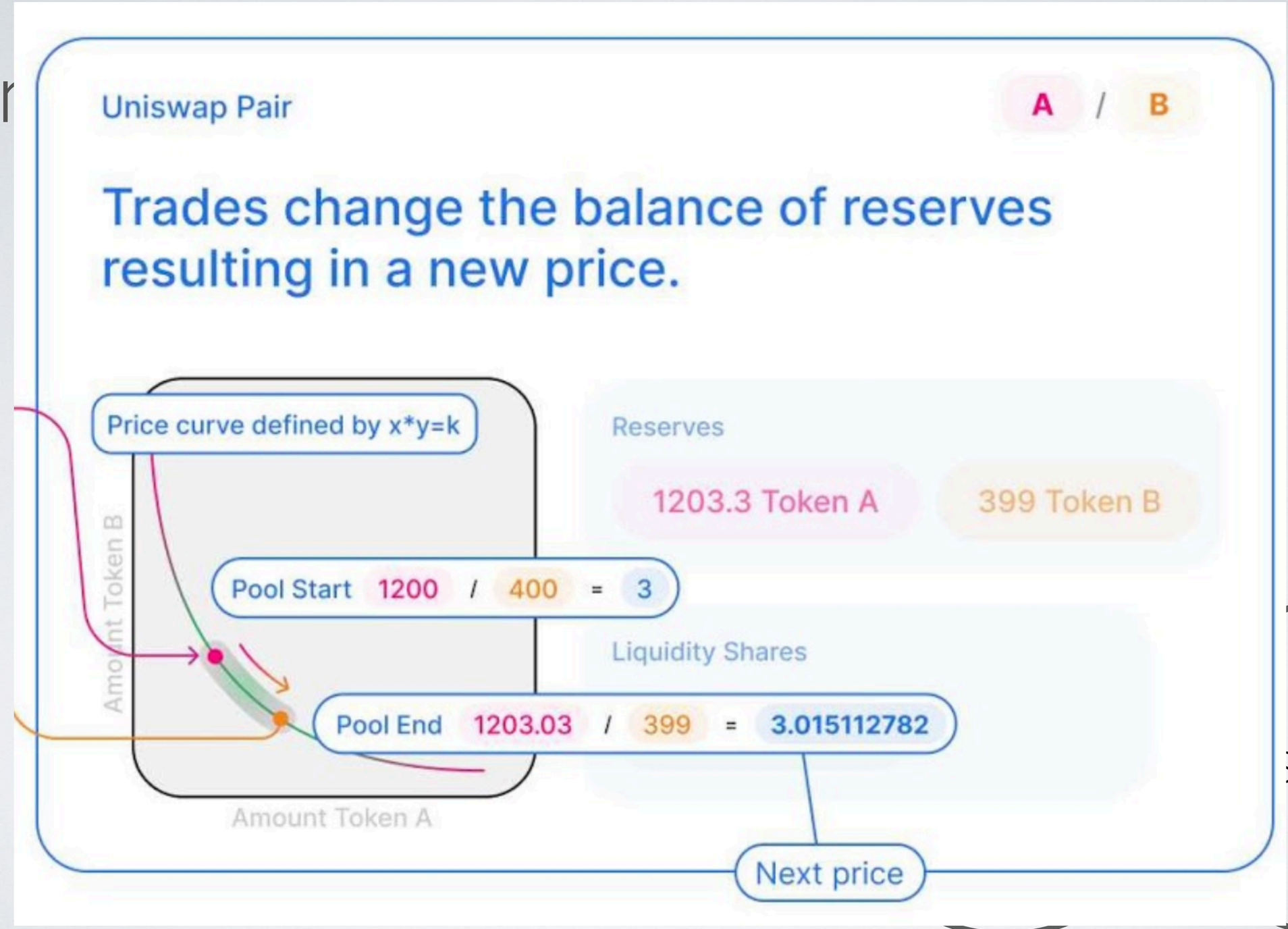


Constant Function Market Makers (AMM)

- User A deposits ETH, wants to “buy" SHIB
  - Initial equation: E * S = K
  - Defines an implicit price (ratio) between the assets
  - They can now deposit ETH & withdraw SHIB at that price (plus pay some fees)
    - This trade changes the market price
    - New price ratio for SHIB: (K / E’) / S’



Cor M)

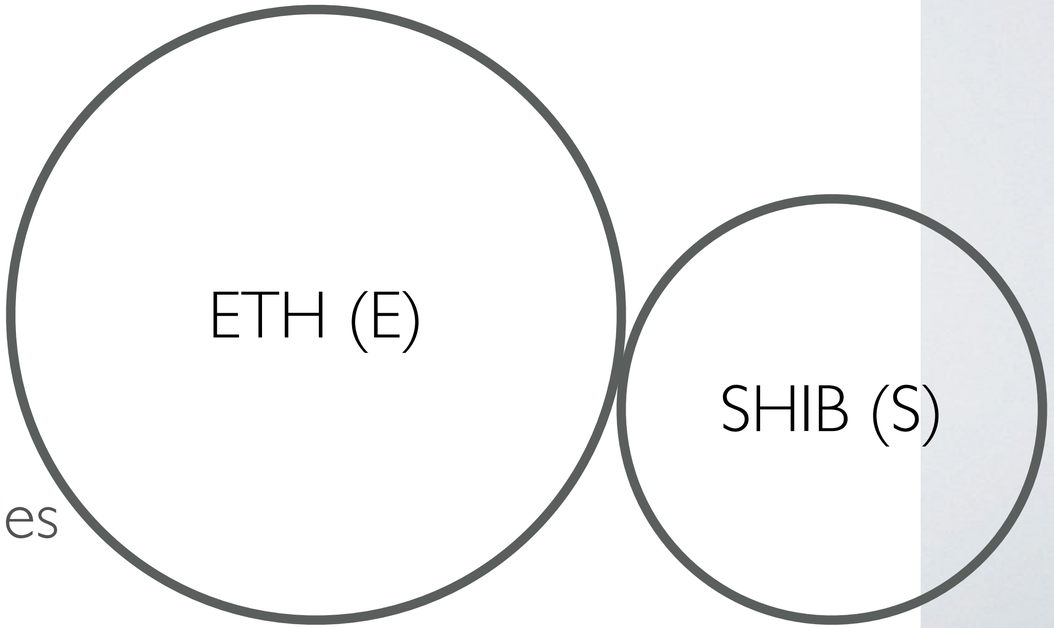


SDC (U)

https://academy.shrimpy.io/lesson/what-is-an-amm-automated-market-maker

Arbitrage / MEV

- In principle, the price of assets should stay "close" to the true price (whatever that is)
  - If the ratio gets far out of whack, hungry traders will "adjust" the pool sizes by executing profitable swaps
  - If there is no pool for an asset pair, systems can "route" trades through multiple pools with more liquidity
    e.g., ETH->USDC, USDC->SHIB
  - Slippage can be quite large
  - Relatively easy to "front-run" public trades

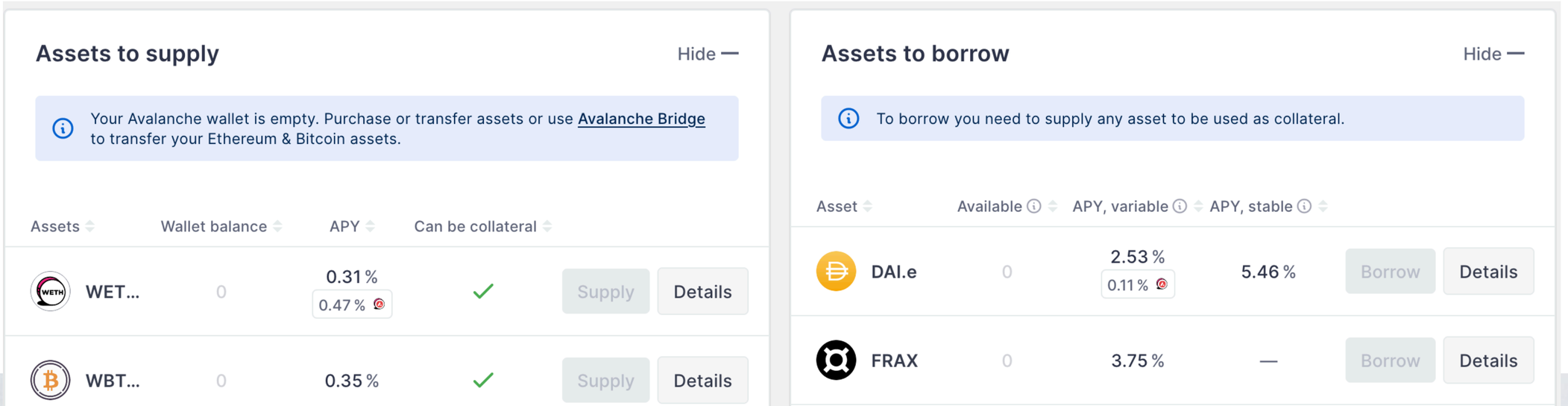


Asset lending

- Another thing smart contracts can do easily is asset lending
  - **Problem:** smart contracts are not great at getting people to repay asset loans
  - This means you need some way to insure those loans
  - Answer: require (over)collateralization

Asset lending

- Another "popular" DeFi service is collaterized asset lending (borrowing)
  - You wish to borrow some amount of Asset B (for whatever)
  - You can deposit and "lock up" some amount of Asset A as collateral for the loan (and pay interest)



Asset lending

- If lenders don't repay the principal, their collateral is automatically liquidated to repay the lenders
  - Hence collateral value must (substantially) exceed loan value
  - If the value of the collateral drops, the system may automatically liquidate it without warning
  - **Question:** How do these smart contracts know the "value" of anything?

Asset lending

- If lenders don't repay the principal, their collateral is automatically liquidated to repay the lenders
  - Hence collateral value must (substantially) exceed loan value
  - If the value of the collateral drops, the system may automatically liquidate it without warning
  - **Question:** How do these smart contracts know the "value" of anything?
  - **Answer:** services provide price "oracles" to these systems, by sending Txes (to some contract) that contain current prices, e.g., ChainLink.
    (Or they can query AMM contracts!)

Asset lending

Assets to supply

Hide —

Your Avalanche wallet is empty. Purchase or transfer assets or use Avalanche Bridge to transfer your Ethereum & Bitcoin assets.

Assets	Wallet balance	APY	Can be collateral		
WET...	0	0.31 % 0.47 %	✓	Supply	Details
WBT...	0	0.35 %	✓	Supply	Details
WAVAX	0	1.65 % 1.15 %	✓	Supply	Details
AVAX	0	1.65 % 1.15 %	✓	Supply	Details

Assets to borrow

Hide —

To borrow you need to supply any asset to be used as collateral.

Asset	Available	APY, variable	APY, stable		
DAI.e	0	2.53 % 0.11 %	5.46 %	Borrow	Details
FRAX	0	3.75 %	—	Borrow	Details
MAI	0	3.51 %	—	Borrow	Details
USDC	0	2.31 % 0.17 %	5.43 %	Borrow	Details

Asset lending (horror stories)

- There are big risks here, if the collateral asset is badly priced (or thinly traded)
  - Show up with some fake nonsense-coin, that has been "wash traded" into appearing to have value
  - Borrow actual money with it
  - Walk away and never come back
- So these systems are not usually unsupervised… and lenders can lose money

Flash loans!

- It is possible to make loans that must be repaid within the course of a single transaction

Account abstraction

- A limitation of smart contracts is that the calling wallet always pays for the "gas" (transaction fees)
- This is annoying for normal users, who don't want to hold ETH
- One solution is to make the service (contract) pay the gas
  - How do we do this in Ethereum?

DeFi / Wallets / Front ends

- Typically a DeFi application begins with a "front end"
  - Usually a JavaScript (or Typescript) application running in a browser
  - Interacts with a wallet (e.g., Metamask) using a standard interface library: web3.js
- Front-end code can make contract calls, payments
  - These need to be signed by the wallet
  - Sent to an Ethereum node for transmission

Where is the Ethereum node?

- Theoretically you can run the node locally
- In practice, most people use a third-party service
  - Popular services include Infura
  - Infura runs Ethereum (and Polygon, Celo, etc.) nodes on a hosted cloud provider
  - You can reach them using an HTTPS-based RPC call

Non-EVM smart contracts

Anonymity

Anonymity in computer science

Anonymity = pseudonymity + unlinkability

Different interactions of the same user with the system should not be linkable to each other

Pseudonymity vs anonymity in forums

Reddit: pick a long-term pseudonym

vs.

4Chan: make posts with no attribution at all

Why is unlinkability needed?

1. Many Bitcoin services require real identity

1. Linked profiles can be deanonymized by a variety of side channels

Defining unlinkability in Bitcoin

- Hard to link different addresses of the same user
- Hard to link different transactions of the same user
- Hard to link sender of a “payment” to its recipient

Quantifying anonymity

Anonymity set: Anonymity set of a transaction T is the set of transactions which an adversary cannot distinguish from T.

To calculate anonymity set:

- define adversary model
- reason carefully about: what the adversary knows, does not know, and cannot know

Why anonymous cryptocurrencies?

Block chain based currencies are totally, publicly, and permanently traceable

Without anonymity, privacy is much worse than traditional banking!

Whale Moves $1.16B Bitcoin in Largest-Ever Dollar Transaction

beincrypto.com | 1d

Trending People

Keith Raniere

Keith Raniere is an Americ
entrepreneur best known a

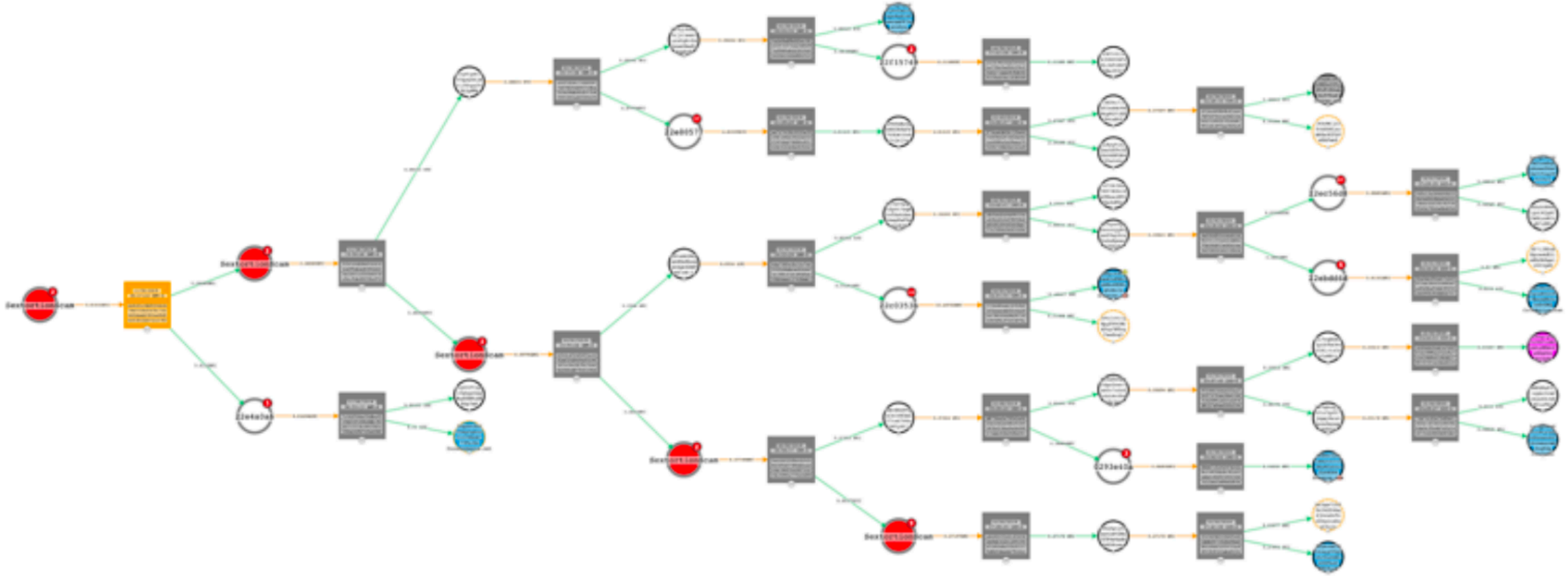
Dez Bryant

Desmond Demond Bryant
American footballer who p

Lindsey Graham

Lindsey Olin Graham (born
1955) is an American polit

Chrissy Teigen



Additionally, 1PXf also sent 0.01359 BTC to GoURL, another 0.0098 BTC to Empire Market (Dark Market), and 0.00507 BTC to Bovada (Gambling). Plus, it sent 0.1405 BTC to 3PFFkzVgbxhwHejFyZeeyXKBFG7dL5gRcj, which still maintained that balance as of December 6.

Several recipients of the emails reported that their payment instructions cited the 1PXf address

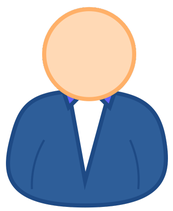
Anonymous e-cash: history

Introduced by David Chaum, 1982

Blind signature: a two-party protocol to create digital signature without signer learning which message is being signed

- An example of secure two-party computation

Anonymous e-cash via blind signatures



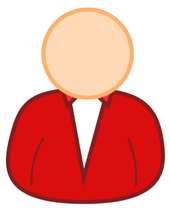
Withdraw anonymous coin

{317038628684424}

Deposit coin # 317038628684424

{317038628684424}

OK



User	Balance
…	…
	9
…	…
	6

Spent coins
…
31703862…

Bank cannot link the two users

Anonymity & decentralization: in conflict

- Interactive cryptographic protocols with bank are hard to decentralize
  - Later: Zerocoin, Zerocash, Monero overcome this challenge by using non-interactive cryptographic techniques
- Decentralization often achieved via public traceability to enforce security

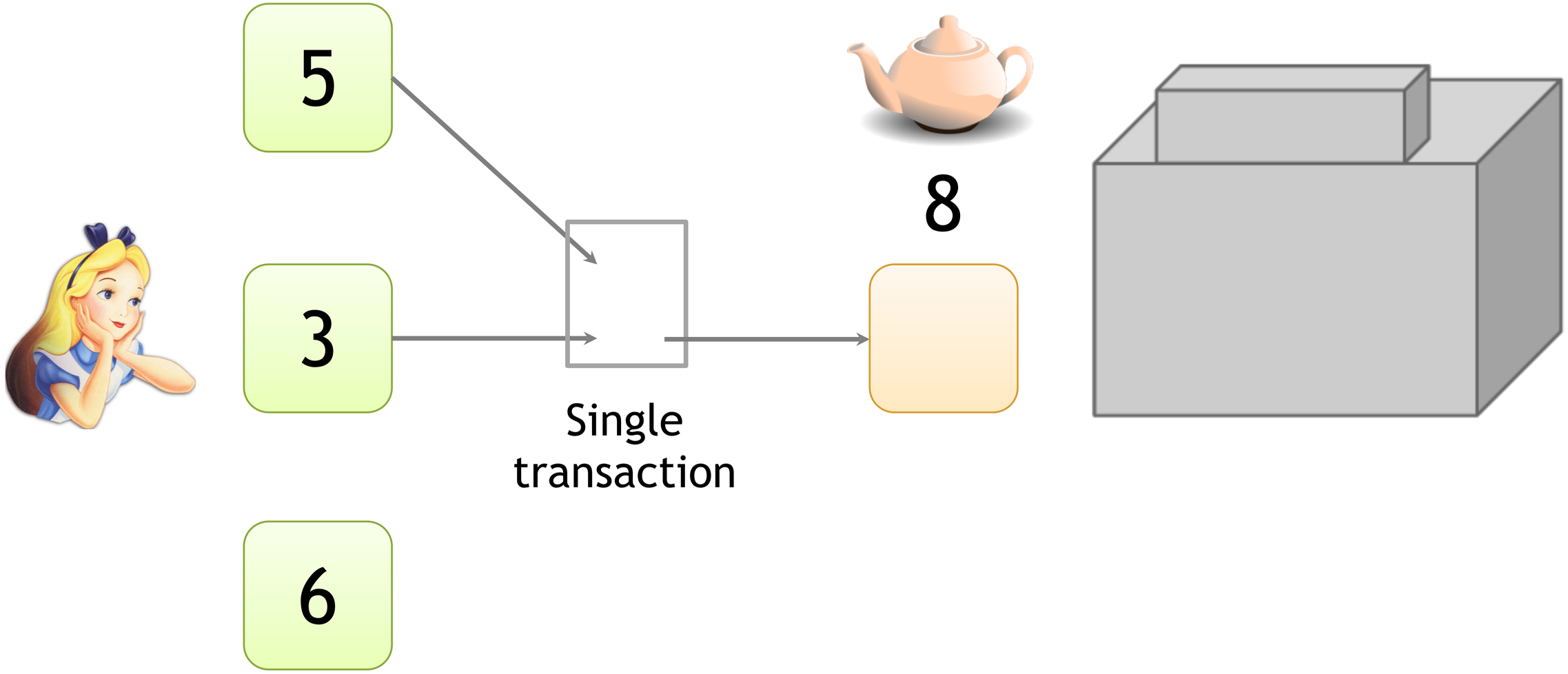
How to de-anonymize Bitcoin

Trivial to create new addresses in Bitcoin

Best practice: always receive at fresh address

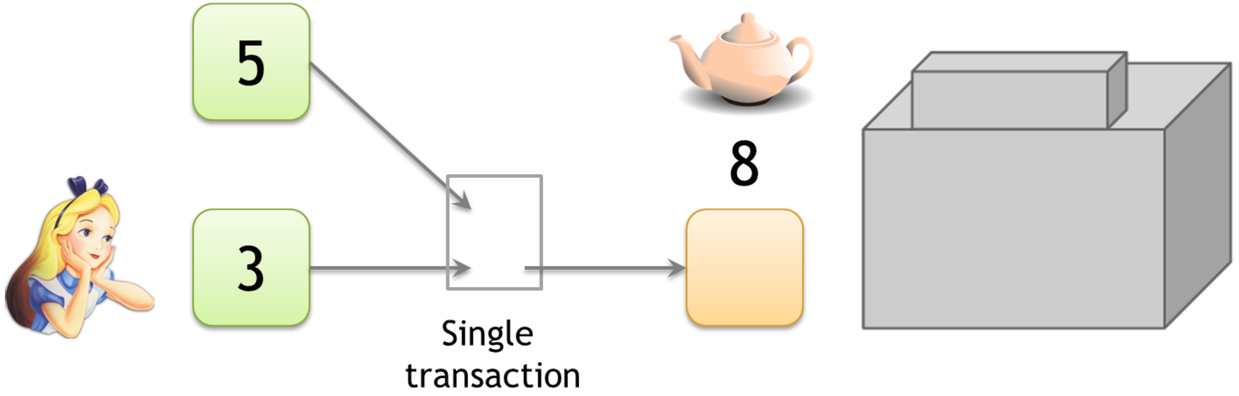
So, unlinkable?

Alice buys a teapot at Big box store



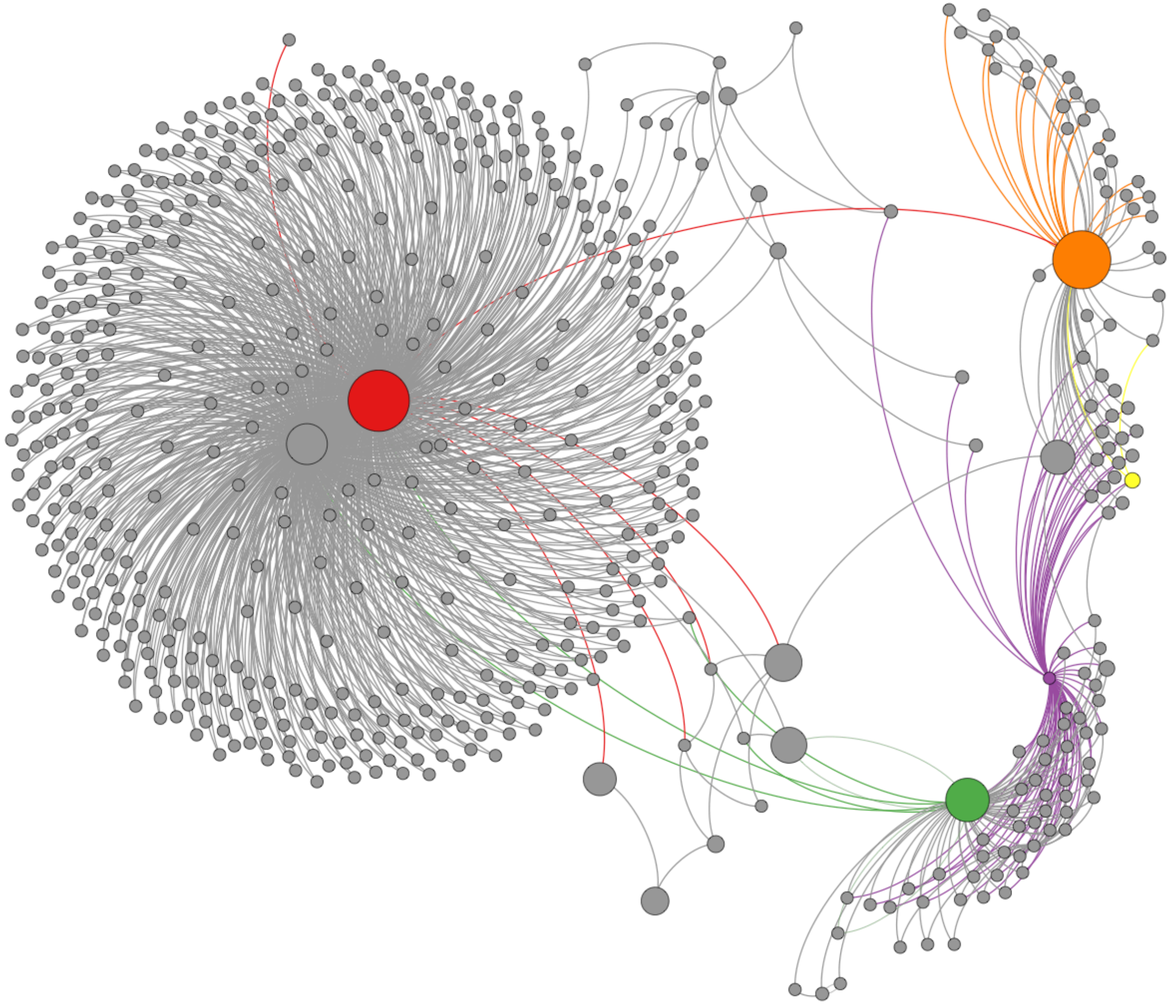
Linking addresses

Shared spending is evidence of joint control



Addresses can be linked transitively

Clustering of addresses



An Analysis of Anonymity in the Bitcoin System

F. Reid and M. Harrigan
PASSAT 2011

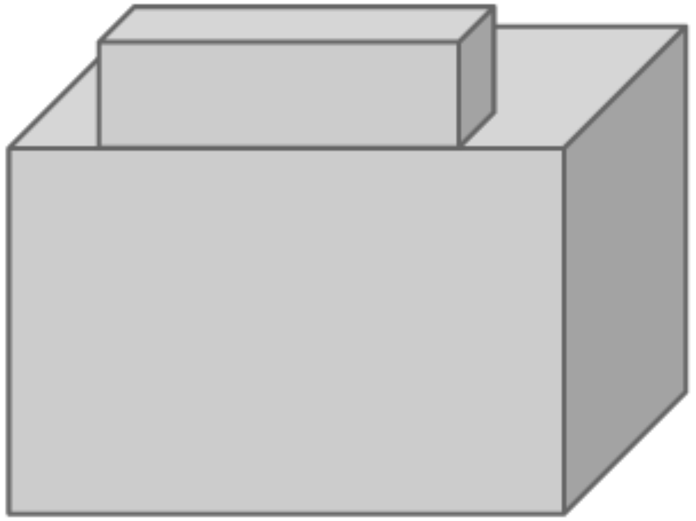
Change addresses

5

3

6

8.5



.5

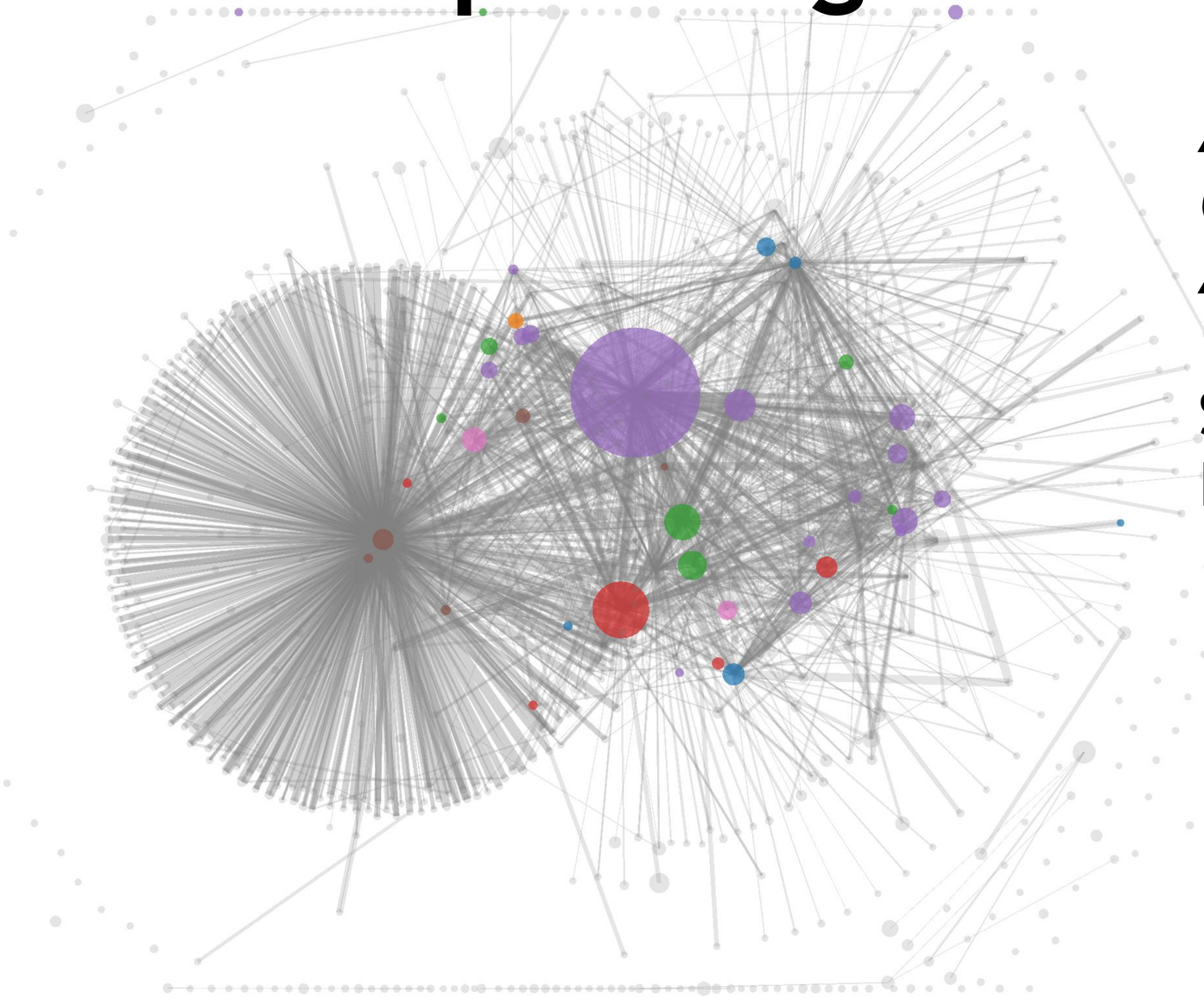
Which address is change?

“Idioms of use”

Idiosyncratic features of wallet software

e.g., each address used only once as change

Shared spending + idioms of use



A Fistful of Bitcoins: Characterizing Payments Among Men with No Names

S. Meiklejohn et al.
IMC 2013

To tag service providers: transact!

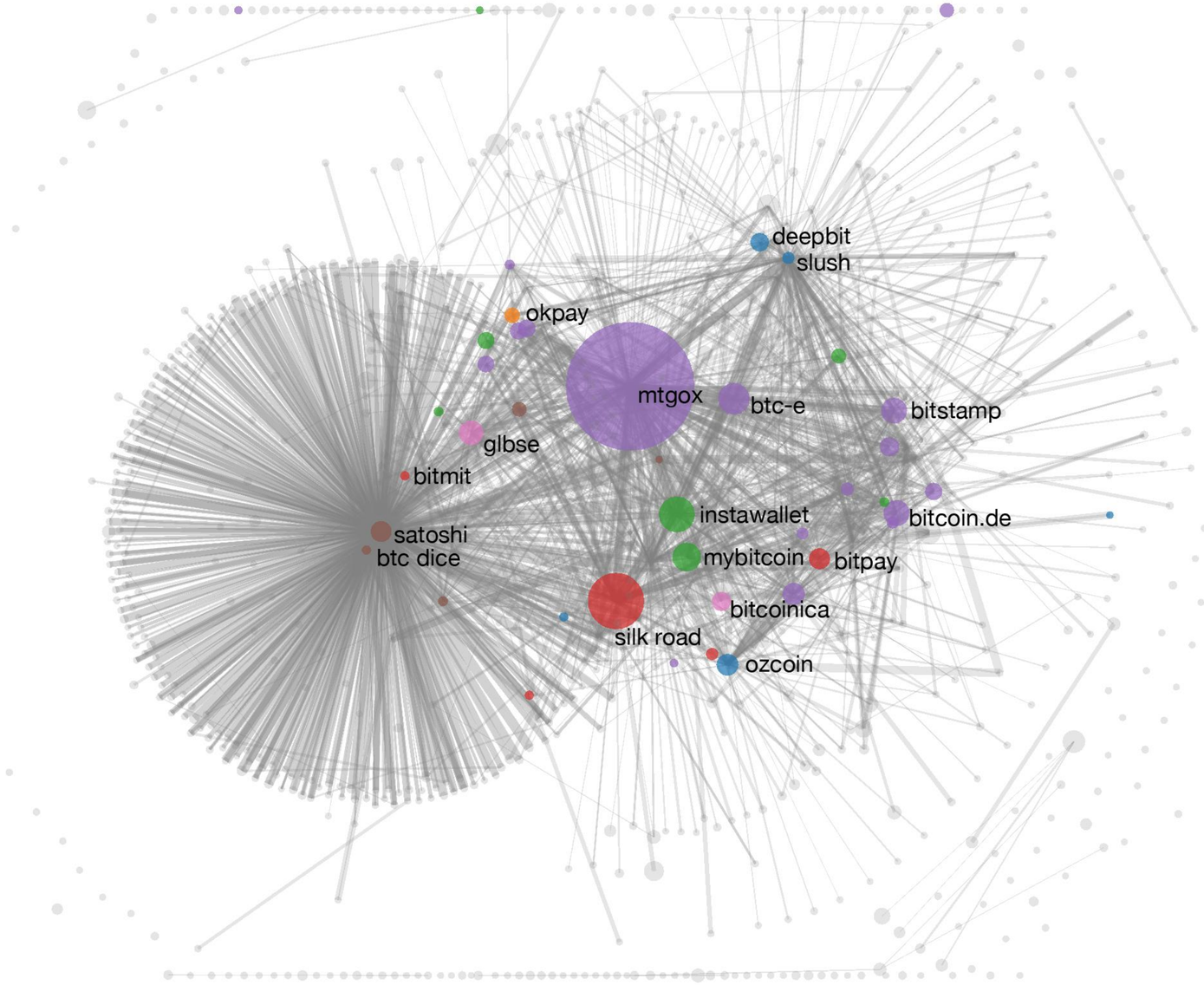
A Fistful of Bitcoins: Characterizing Payments Among Men with No Names

S. Meiklejohn et al.

344 transactions

- Mining pools
- Wallet services
- Exchanges
- Vendors
- Gambling sites

Shared spending + idioms of use



A Fistful of Bitcoins: Characterizing Payments Among Men with No Names

S. Meiklejohn et al.
IMC 2013

From services to users

1. High centralization in service providers

   Most flows pass through one of these — in a traceable way

2. Address — identity links in forums

Achieving Anonymity

Approaches

- **Mixing**: Pool in multiple transactions (ideally same value), and then create new transactions
  - Centralized: E.g., online wallets
  - Decentralized: E.g., CoinJoin
  - Untrusted intermediary using crypto: Tumblebit
- **New cryptocurrencies:**
  - Using Zero-knowledge proofs: Zerocoin and Zerocash
  - Using Ring signatures: Monero

Approaches

- **Mixing**: Pool in multiple transactions (ideally same value), and then create new transactions
  - Centralized: E.g., online wallets
  - Decentralized: E.g., CoinJoin (e.g., implementation: Dash)
  - Untrusted intermediary using crypto: Tumblebit
- **New cryptocurrencies:**
  - Using Zero-knowledge proofs: Zerocoin and Zerocash
  - Using Ring signatures: Cryptonote (e.g., implementation: Monero)