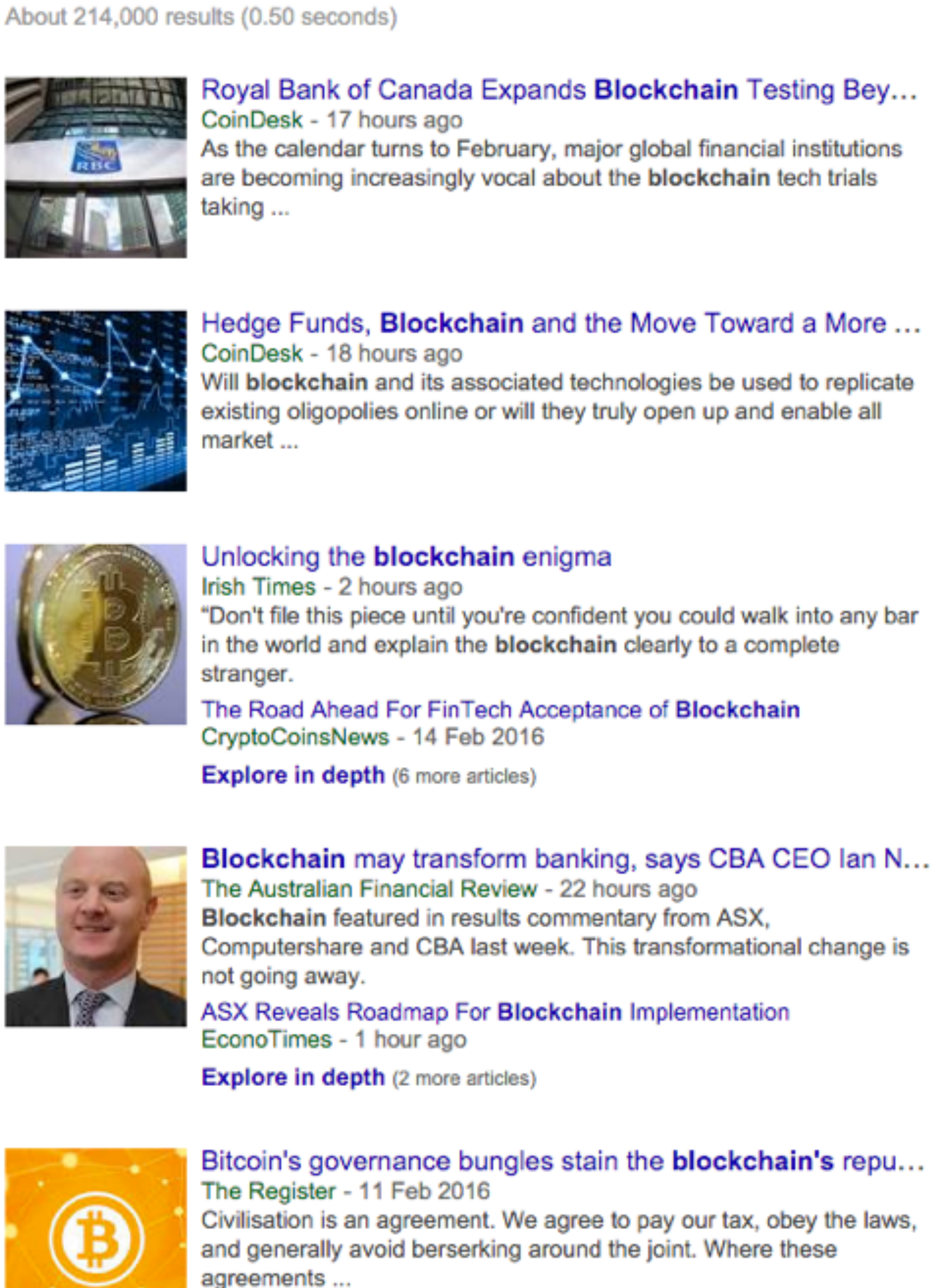
Centrally Banked Cryptocurrencies

George Danezis (University College London)

Sarah Meiklejohn (University College London)

who’s interested in ‘blockchain’?



About 214,000 results (0.50 seconds)

Royal Bank of Canada Expands **Blockchain** Testing Bey...
CoinDesk - 17 hours ago
As the calendar turns to February, major global financial institutions are becoming increasingly vocal about the **blockchain** tech trials taking ...

Hedge Funds, **Blockchain** and the Move Toward a More ...
CoinDesk - 18 hours ago
Will **blockchain** and its associated technologies be used to replicate existing oligopolies online or will they truly open up and enable all market ...

Unlocking the **blockchain** enigma
Irish Times - 2 hours ago
“Don't file this piece until you're confident you could walk into any bar in the world and explain the **blockchain** clearly to a complete stranger.

The Road Ahead For FinTech Acceptance of **Blockchain**
CryptoCoinsNews - 14 Feb 2016

Explore in depth (6 more articles)

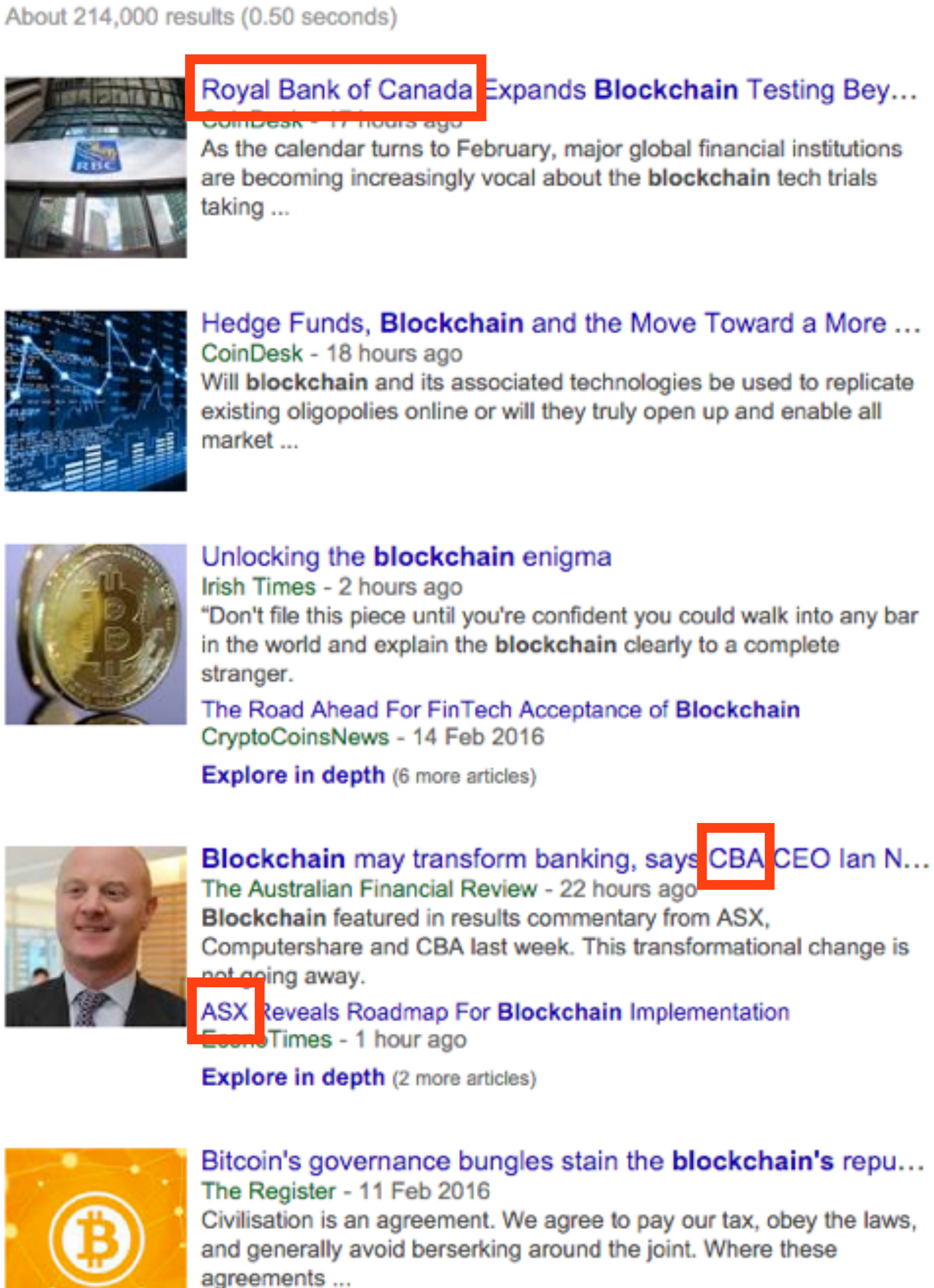
Blockchain may transform banking, says CBA CEO Ian N...
The Australian Financial Review - 22 hours ago
Blockchain featured in results commentary from ASX, Computershare and CBA last week. This transformational change is not going away.

ASX Reveals Roadmap For **Blockchain** Implementation
EconoTimes - 1 hour ago

Explore in depth (2 more articles)

Bitcoin's governance bungles stain the **blockchain's** repu...
The Register - 11 Feb 2016
Civilisation is an agreement. We agree to pay our tax, obey the laws, and generally avoid berserking around the joint. Where these agreements ...

who’s interested in ‘blockchain’?



About 214,000 results (0.50 seconds)

Royal Bank of Canada Expands **Blockchain** Testing Bey...
CoinDesk - 17 hours ago
As the calendar turns to February, major global financial institutions are becoming increasingly vocal about the **blockchain** tech trials taking ...

Hedge Funds, **Blockchain** and the Move Toward a More ...
CoinDesk - 18 hours ago
Will **blockchain** and its associated technologies be used to replicate existing oligopolies online or will they truly open up and enable all market ...

Unlocking the **blockchain** enigma
Irish Times - 2 hours ago
“Don't file this piece until you're confident you could walk into any bar in the world and explain the **blockchain** clearly to a complete stranger.

The Road Ahead For FinTech Acceptance of **Blockchain**
CryptoCoinsNews - 14 Feb 2016

Explore in depth (6 more articles)

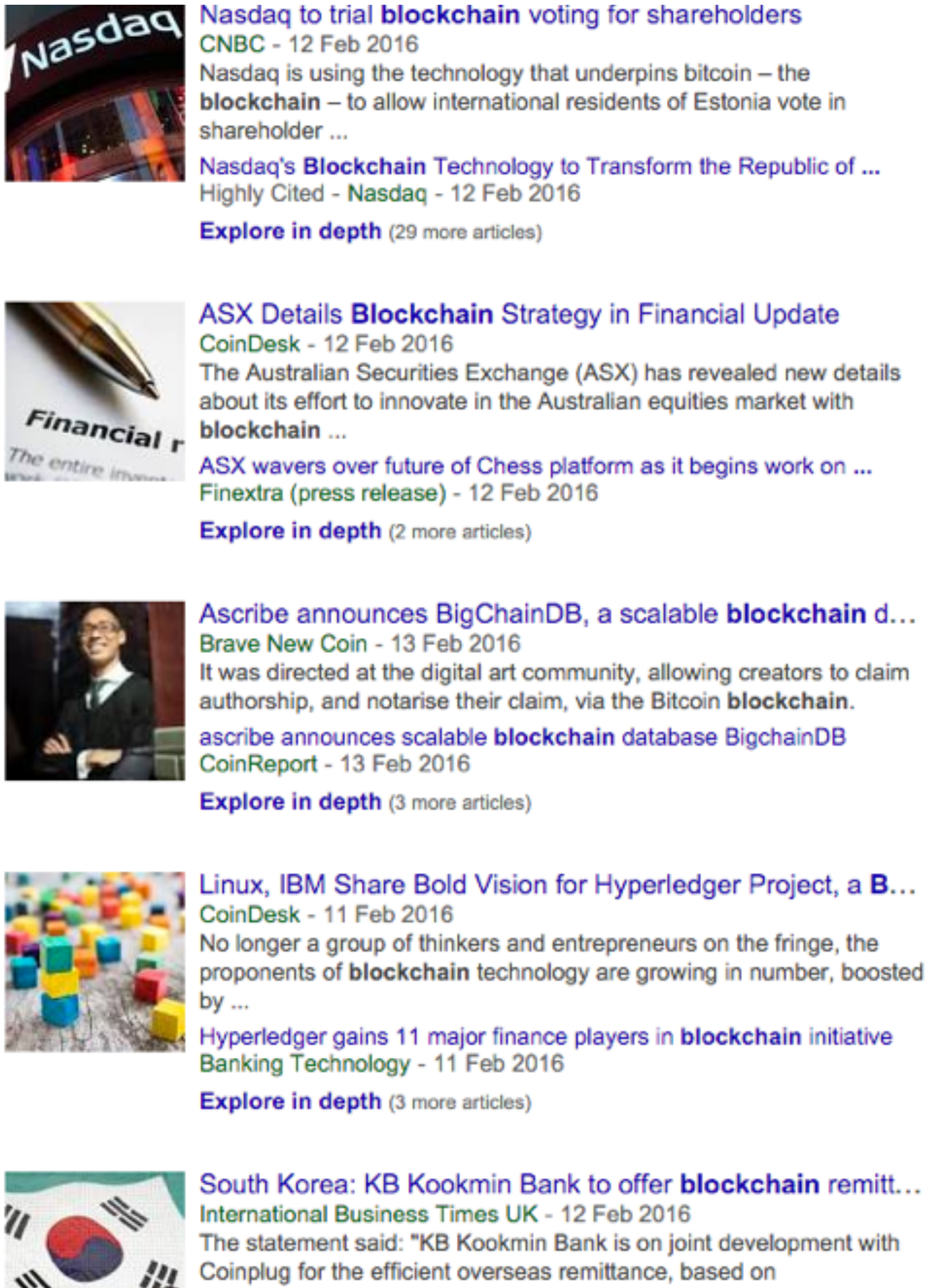
Blockchain may transform banking, says CBA CEO Ian N...
The Australian Financial Review - 22 hours ago
Blockchain featured in results commentary from ASX, Computershare and CBA last week. This transformational change is not going away.

ASX Reveals Roadmap For **Blockchain** Implementation
EconoTimes - 1 hour ago

Explore in depth (2 more articles)

Bitcoin's governance bungles stain the **blockchain's** repu...
The Register - 11 Feb 2016
Civilisation is an agreement. We agree to pay our tax, obey the laws, and generally avoid berserking around the joint. Where these agreements ...

who’s interested in ‘blockchain’?



Nasdaq to trial **blockchain** voting for shareholders
CNBC - 12 Feb 2016
Nasdaq is using the technology that underpins bitcoin – the **blockchain** – to allow international residents of Estonia vote in shareholder ...

Nasdaq's **Blockchain** Technology to Transform the Republic of ...
Highly Cited - Nasdaq - 12 Feb 2016

Explore in depth (29 more articles)

ASX Details **Blockchain** Strategy in Financial Update
CoinDesk - 12 Feb 2016
The Australian Securities Exchange (ASX) has revealed new details about its effort to innovate in the Australian equities market with **blockchain** ...

ASX wavers over future of Chess platform as it begins work on ...
Finextra (press release) - 12 Feb 2016

Explore in depth (2 more articles)

Ascribe announces BigChainDB, a scalable **blockchain** d...
Brave New Coin - 13 Feb 2016
It was directed at the digital art community, allowing creators to claim authorship, and notarise their claim, via the Bitcoin **blockchain**.

ascribe announces scalable **blockchain** database BigchainDB
CoinReport - 13 Feb 2016

Explore in depth (3 more articles)

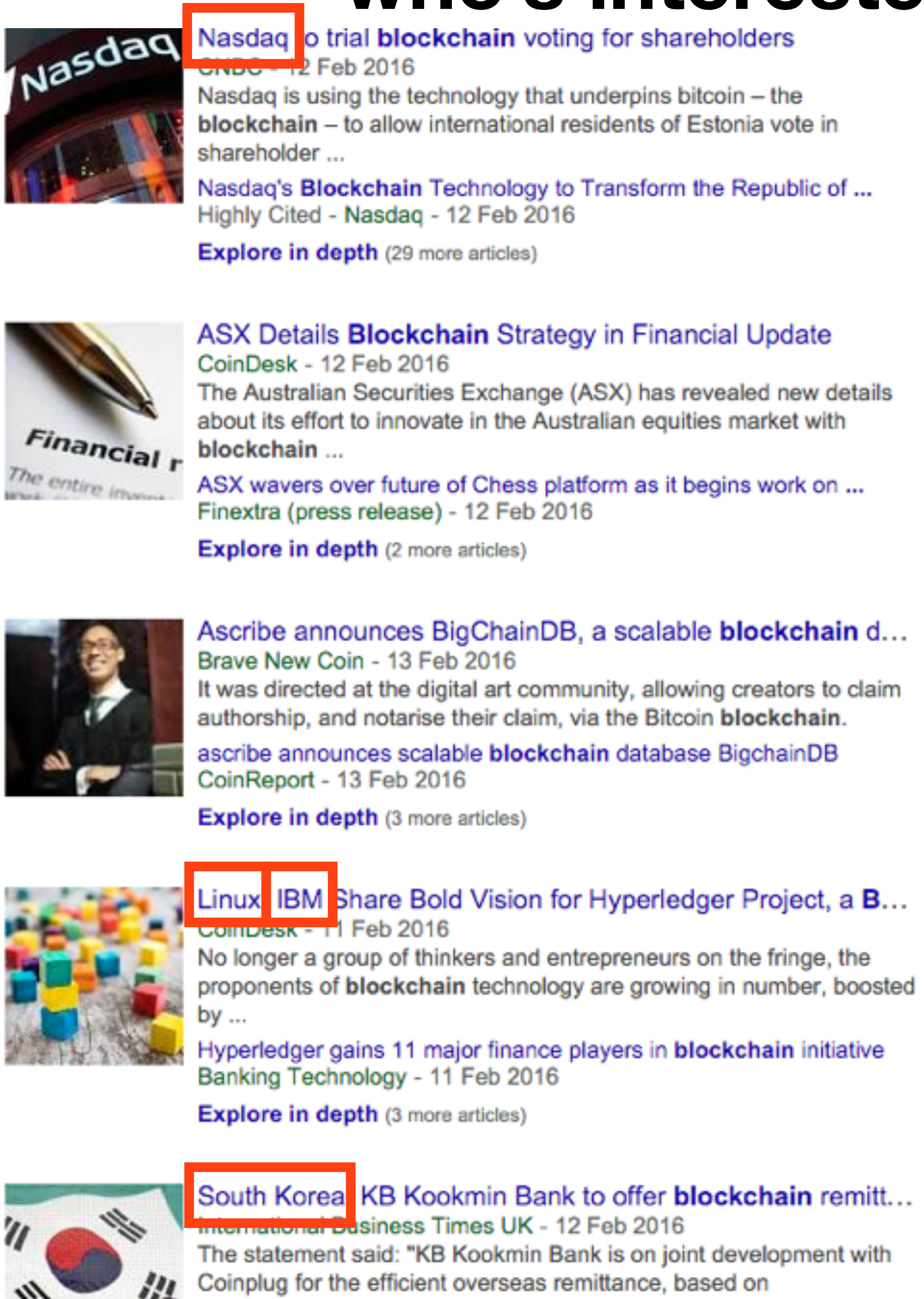
Linux, IBM Share Bold Vision for Hyperledger Project, a **B**...
CoinDesk - 11 Feb 2016
No longer a group of thinkers and entrepreneurs on the fringe, the proponents of **blockchain** technology are growing in number, boosted by ...

Hyperledger gains 11 major finance players in **blockchain** initiative
Banking Technology - 11 Feb 2016

Explore in depth (3 more articles)

South Korea: KB Kookmin Bank to offer **blockchain** remitt...
International Business Times UK - 12 Feb 2016
The statement said: "KB Kookmin Bank is on joint development with Coinplug for the efficient overseas remittance, based on

who’s interested in ‘blockchain’?



Nasdaq to trial **blockchain** voting for shareholders
CNBC - 12 Feb 2016
Nasdaq is using the technology that underpins bitcoin – the **blockchain** – to allow international residents of Estonia vote in shareholder ...

Nasdaq's **Blockchain** Technology to Transform the Republic of ...
Highly Cited - Nasdaq - 12 Feb 2016

Explore in depth (29 more articles)

ASX Details **Blockchain** Strategy in Financial Update
CoinDesk - 12 Feb 2016
The Australian Securities Exchange (ASX) has revealed new details about its effort to innovate in the Australian equities market with **blockchain** ...

ASX wavers over future of Chess platform as it begins work on ...
Finextra (press release) - 12 Feb 2016

Explore in depth (2 more articles)

Ascribe announces BigChainDB, a scalable **blockchain** d...
Brave New Coin - 13 Feb 2016
It was directed at the digital art community, allowing creators to claim authorship, and notarise their claim, via the Bitcoin **blockchain**.

ascribe announces scalable **blockchain** database BigchainDB
CoinReport - 13 Feb 2016

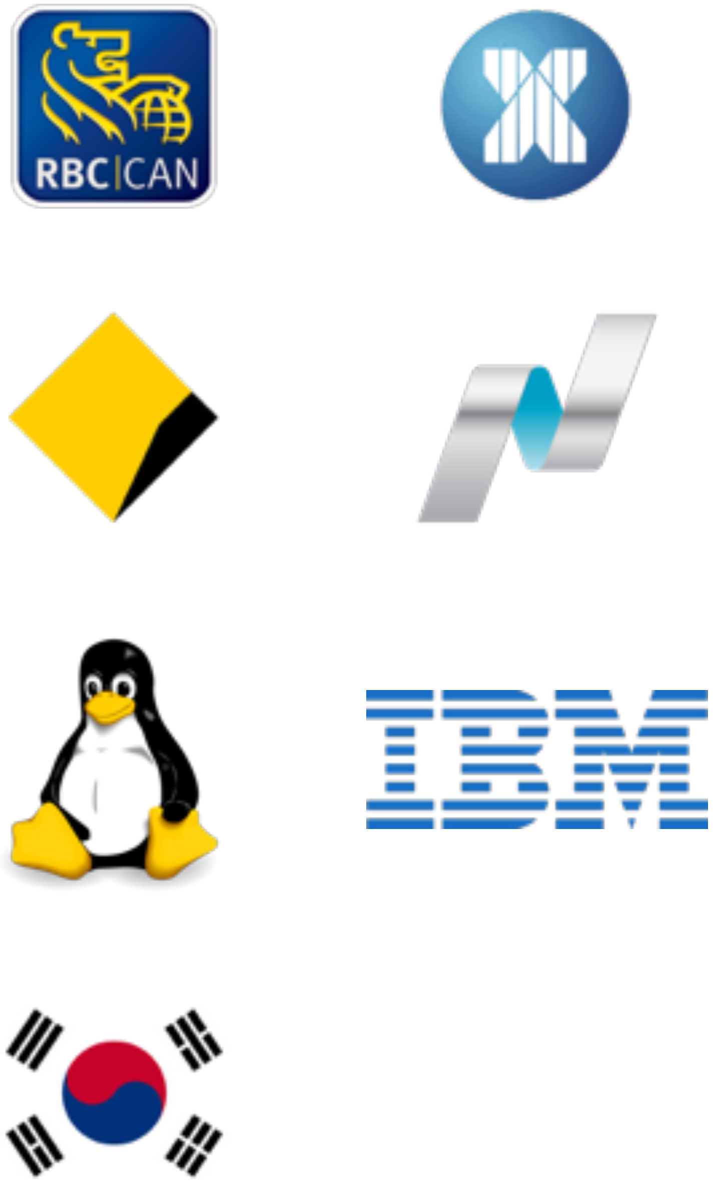
Explore in depth (3 more articles)

Linux, IBM Share Bold Vision for Hyperledger Project, a **B**...
CoinDesk - 11 Feb 2016
No longer a group of thinkers and entrepreneurs on the fringe, the proponents of **blockchain** technology are growing in number, boosted by ...

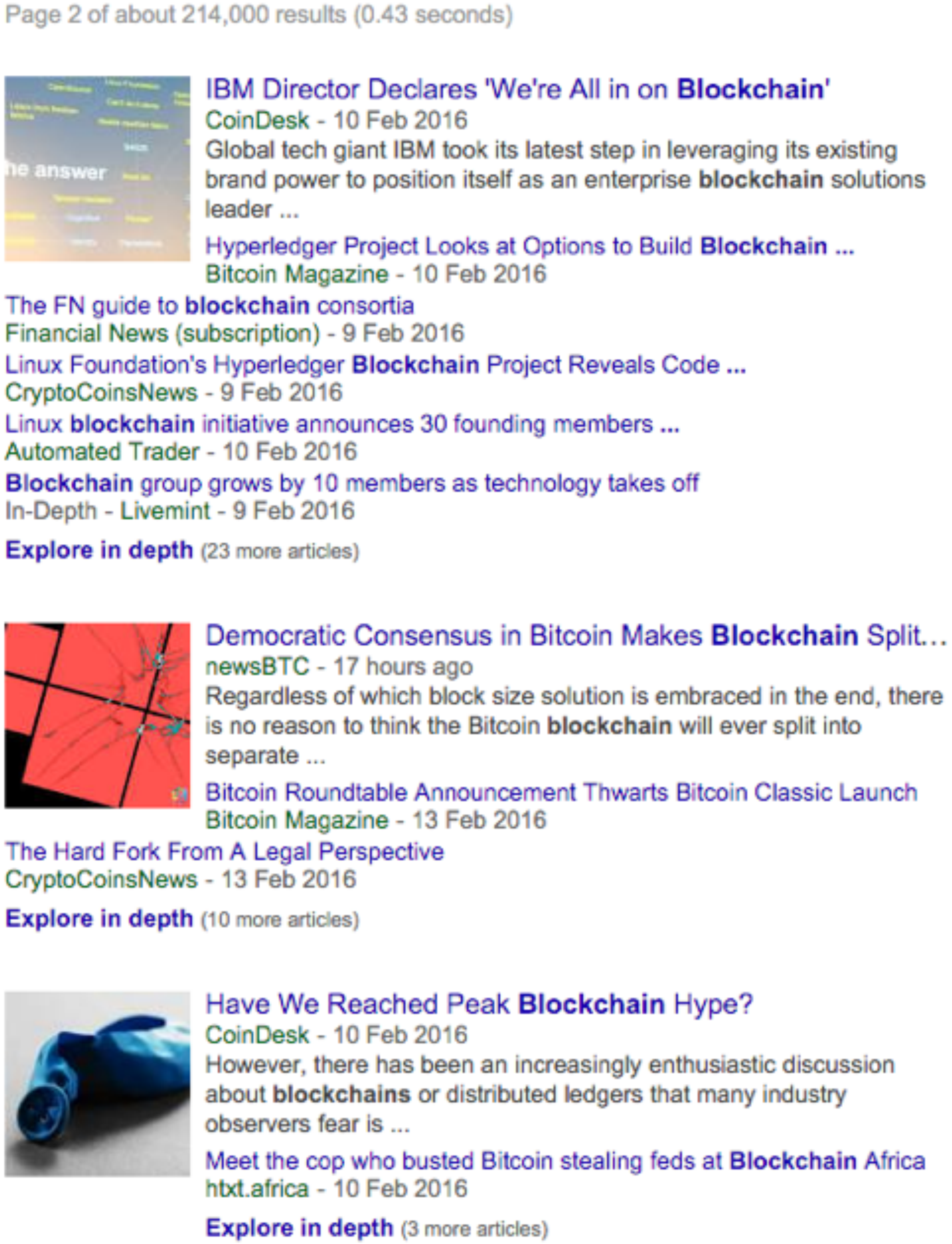
Hyperledger gains 11 major finance players in **blockchain** initiative
Banking Technology - 11 Feb 2016

Explore in depth (3 more articles)

South Korea: KB Kookmin Bank to offer **blockchain** remitt...
International Business Times UK - 12 Feb 2016
The statement said: "KB Kookmin Bank is on joint development with Coinplug for the efficient overseas remittance, based on



who’s interested in ‘blockchain’?



Page 2 of about 214,000 results (0.43 seconds)

IBM Director Declares 'We're All in on **Blockchain**'
CoinDesk - 10 Feb 2016
Global tech giant IBM took its latest step in leveraging its existing brand power to position itself as an enterprise **blockchain** solutions leader ...

Hyperledger Project Looks at Options to Build **Blockchain** ...
Bitcoin Magazine - 10 Feb 2016

The FN guide to **blockchain** consortia
Financial News (subscription) - 9 Feb 2016

Linux Foundation's Hyperledger **Blockchain** Project Reveals Code ...
CryptoCoinsNews - 9 Feb 2016

Linux **blockchain** initiative announces 30 founding members ...
Automated Trader - 10 Feb 2016

Blockchain group grows by 10 members as technology takes off
In-Depth - Livemint - 9 Feb 2016

Explore in depth (23 more articles)

Democratic Consensus in Bitcoin Makes **Blockchain** Split...
newsBTC - 17 hours ago
Regardless of which block size solution is embraced in the end, there is no reason to think the Bitcoin **blockchain** will ever split into separate ...

Bitcoin Roundtable Announcement Thwarts Bitcoin Classic Launch
Bitcoin Magazine - 13 Feb 2016

The Hard Fork From A Legal Perspective
CryptoCoinsNews - 13 Feb 2016

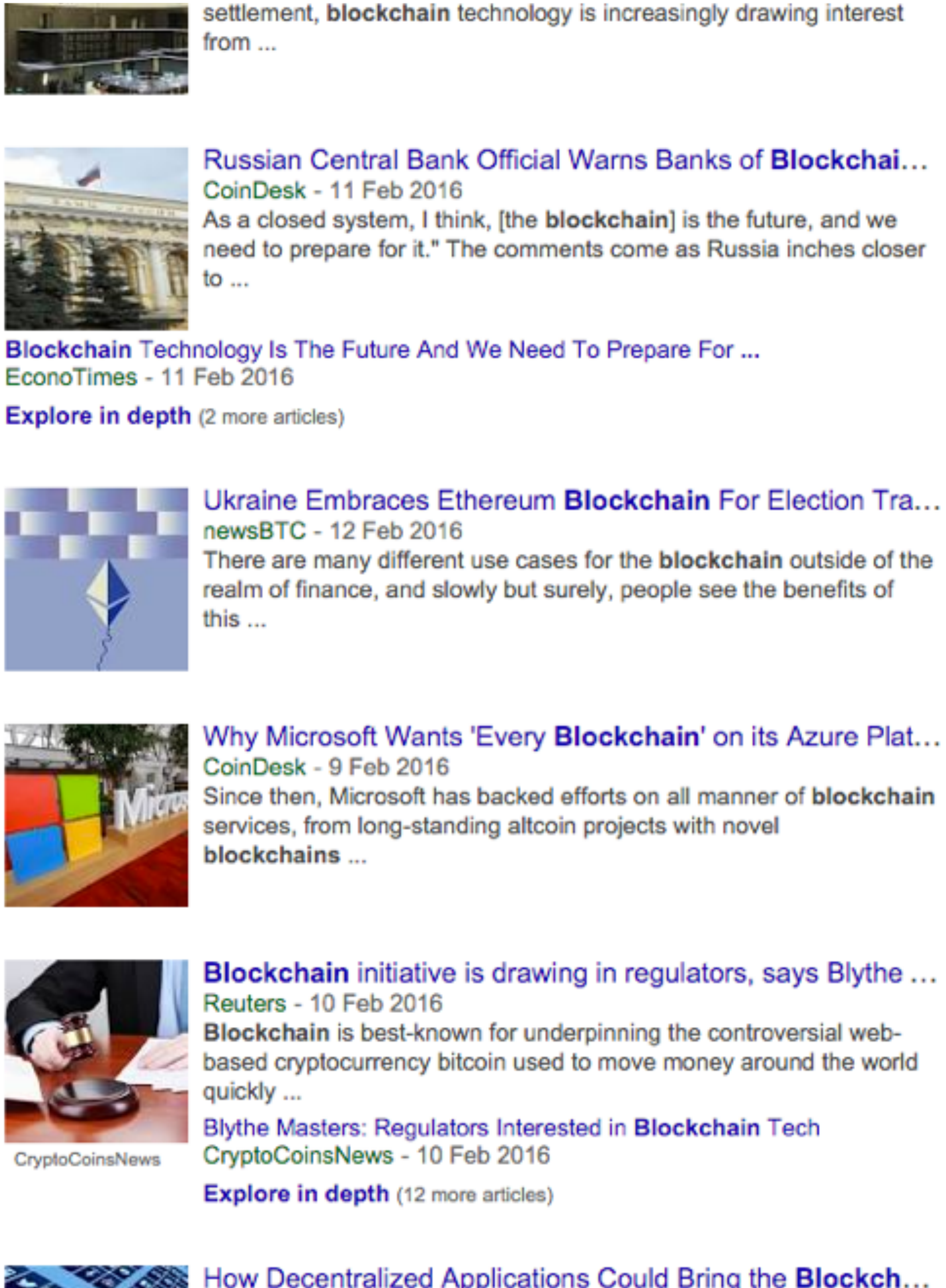
Explore in depth (10 more articles)

Have We Reached Peak **Blockchain** Hype?
CoinDesk - 10 Feb 2016
However, there has been an increasingly enthusiastic discussion about **blockchains** or distributed ledgers that many industry observers fear is ...

Meet the cop who busted Bitcoin stealing feds at **Blockchain** Africa
htxt.africa - 10 Feb 2016

Explore in depth (3 more articles)

who’s interested in ‘blockchain’?



settlement, **blockchain** technology is increasingly drawing interest from ...

Russian Central Bank Official Warns Banks of **Blockchai**...
CoinDesk - 11 Feb 2016
As a closed system, I think, [the **blockchain**] is the future, and we need to prepare for it." The comments come as Russia inches closer to ...

Blockchain Technology Is The Future And We Need To Prepare For ...
EconoTimes - 11 Feb 2016
Explore in depth (2 more articles)

Ukraine Embraces Ethereum **Blockchain** For Election Tra...
newsBTC - 12 Feb 2016
There are many different use cases for the **blockchain** outside of the realm of finance, and slowly but surely, people see the benefits of this ...

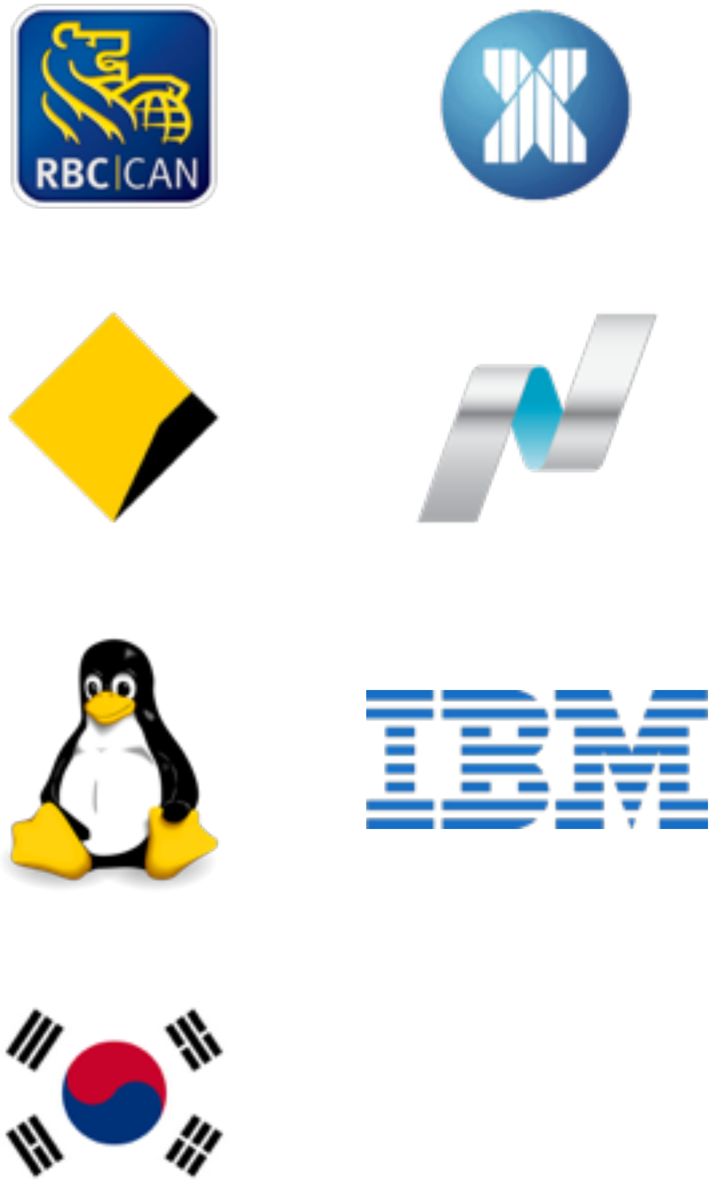
Why Microsoft Wants 'Every **Blockchain**' on its Azure Plat...
CoinDesk - 9 Feb 2016
Since then, Microsoft has backed efforts on all manner of **blockchain** services, from long-standing altcoin projects with novel **blockchains** ...

Blockchain initiative is drawing in regulators, says Blythe ...
Reuters - 10 Feb 2016
Blockchain is best-known for underpinning the controversial web-based cryptocurrency bitcoin used to move money around the world quickly ...

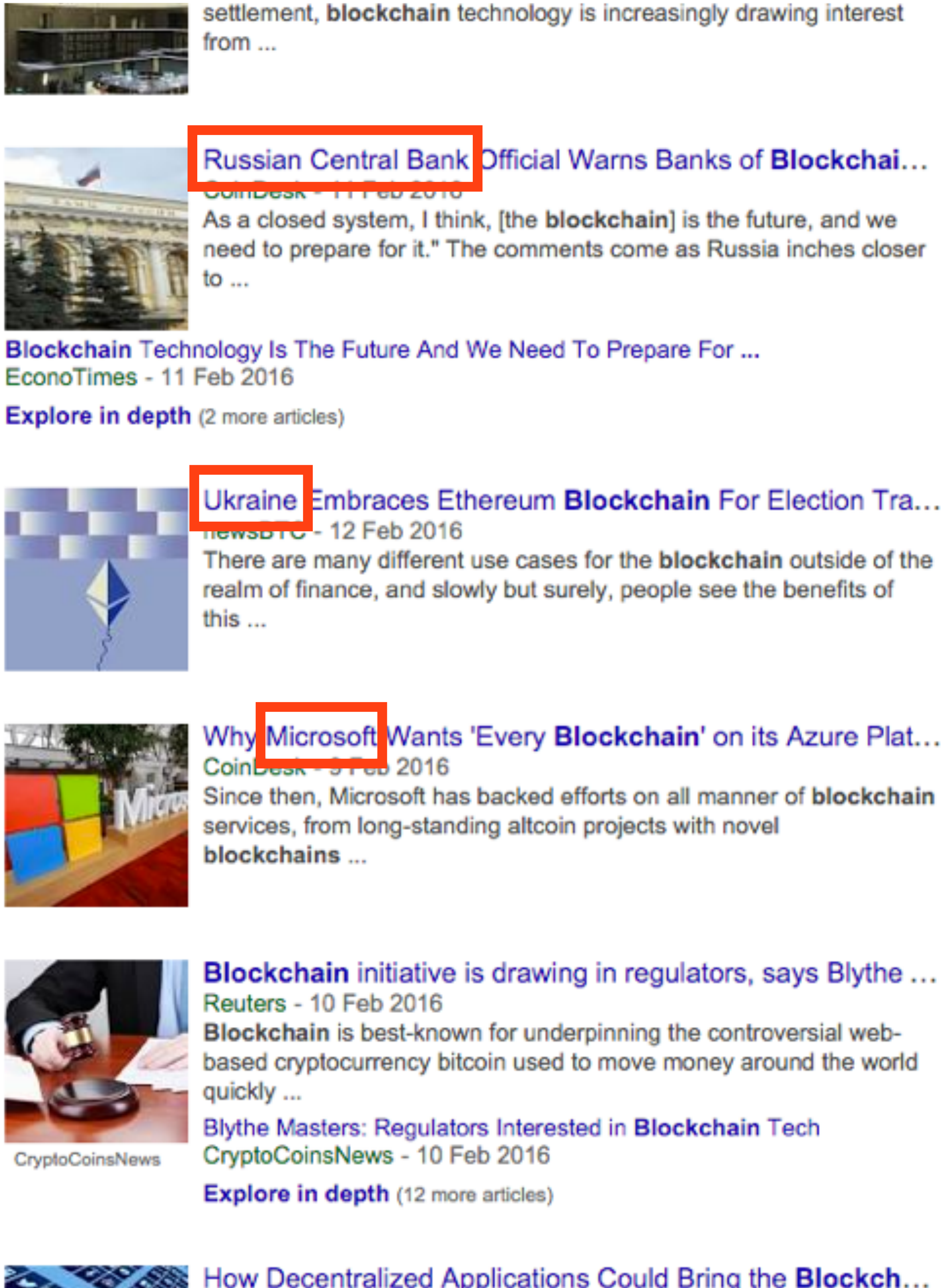
CryptoCoinsNews

Blythe Masters: Regulators Interested in **Blockchain** Tech
CryptoCoinsNews - 10 Feb 2016
Explore in depth (12 more articles)

How Decentralized Applications Could Bring the **Blockch**...



who’s interested in ‘blockchain’?



settlement, **blockchain** technology is increasingly drawing interest from ...

Russian Central Bank Official Warns Banks of **Blockchai**...
CoinDesk - 11 Feb 2016
As a closed system, I think, [the **blockchain**] is the future, and we need to prepare for it." The comments come as Russia inches closer to ...

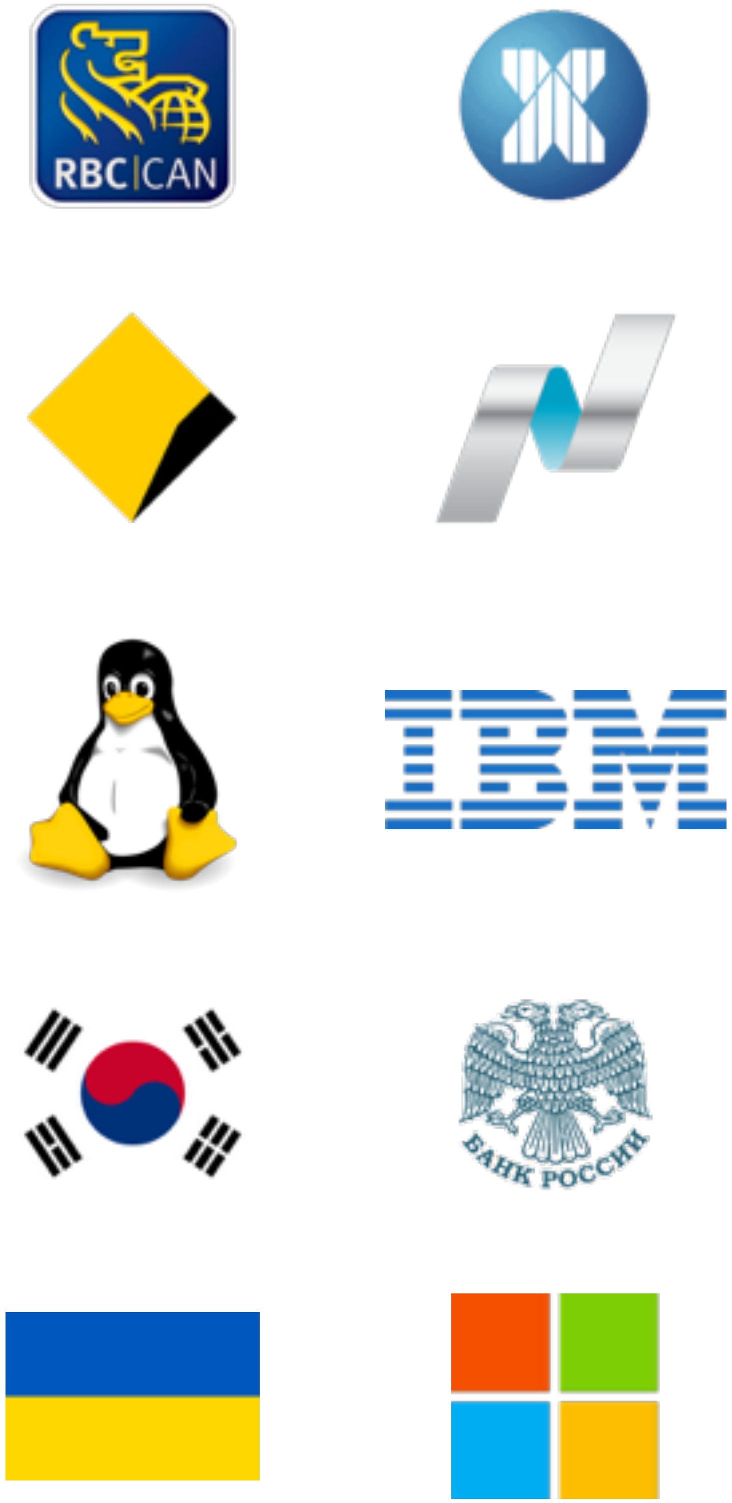
Blockchain Technology Is The Future And We Need To Prepare For ...
EconoTimes - 11 Feb 2016
Explore in depth (2 more articles)

Ukraine Embraces Ethereum **Blockchain** For Election Tra...
newsBTC - 12 Feb 2016
There are many different use cases for the **blockchain** outside of the realm of finance, and slowly but surely, people see the benefits of this ...

Why Microsoft Wants 'Every **Blockchain**' on its Azure Plat...
CoinDesk - 9 Feb 2016
Since then, Microsoft has backed efforts on all manner of **blockchain** services, from long-standing altcoin projects with novel **blockchains** ...

Blockchain initiative is drawing in regulators, says Blythe ...
Reuters - 10 Feb 2016
Blockchain is best-known for underpinning the controversial web-based cryptocurrency bitcoin used to move money around the world quickly ...
Blythe Masters: Regulators Interested in **Blockchain** Tech
CryptoCoinsNews - 10 Feb 2016
CryptoCoinsNews
Explore in depth (12 more articles)

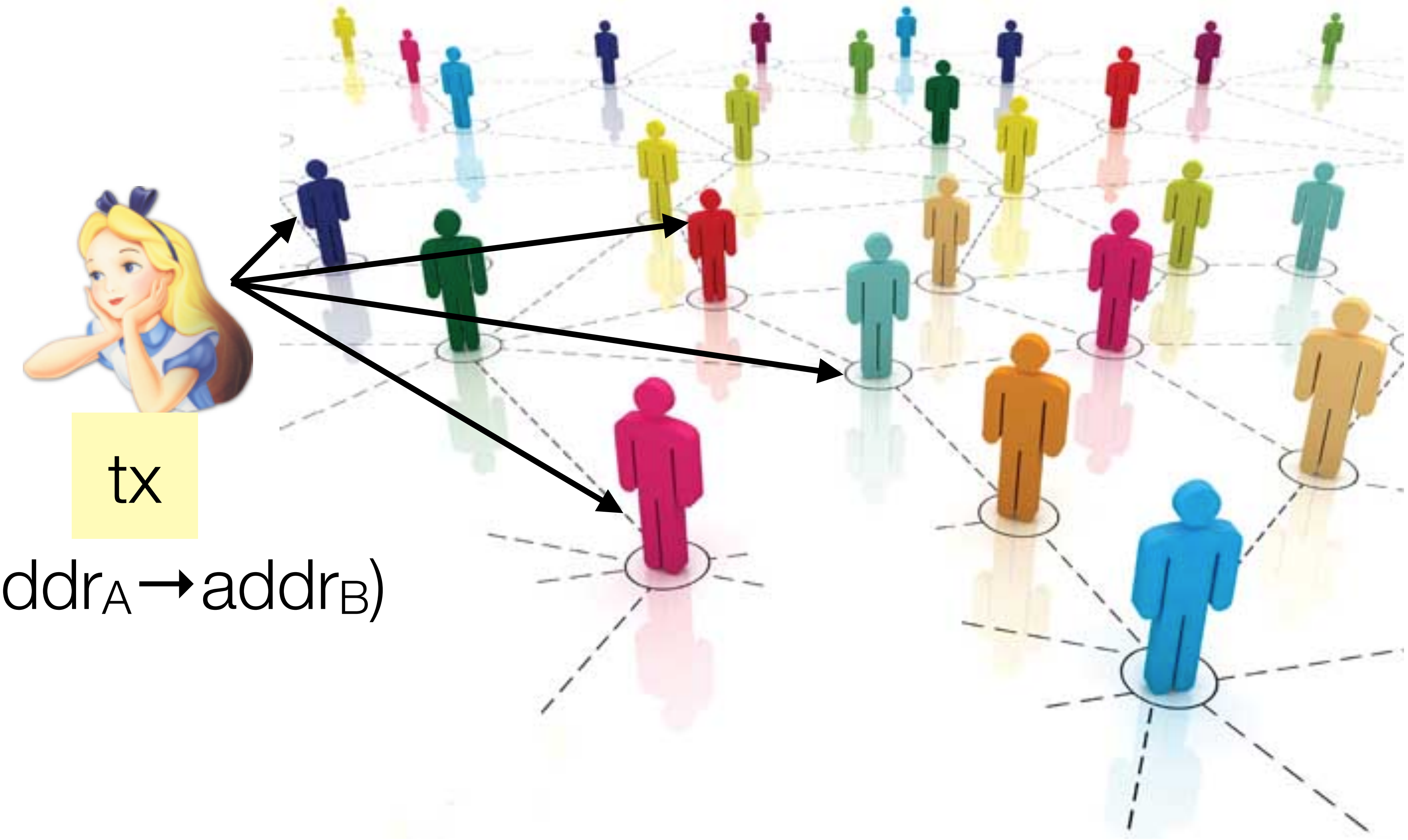
How Decentralized Applications Could Bring the **Blockch**...



fully decentralized cryptocurrencies

fully decentralized cryptocurrencies

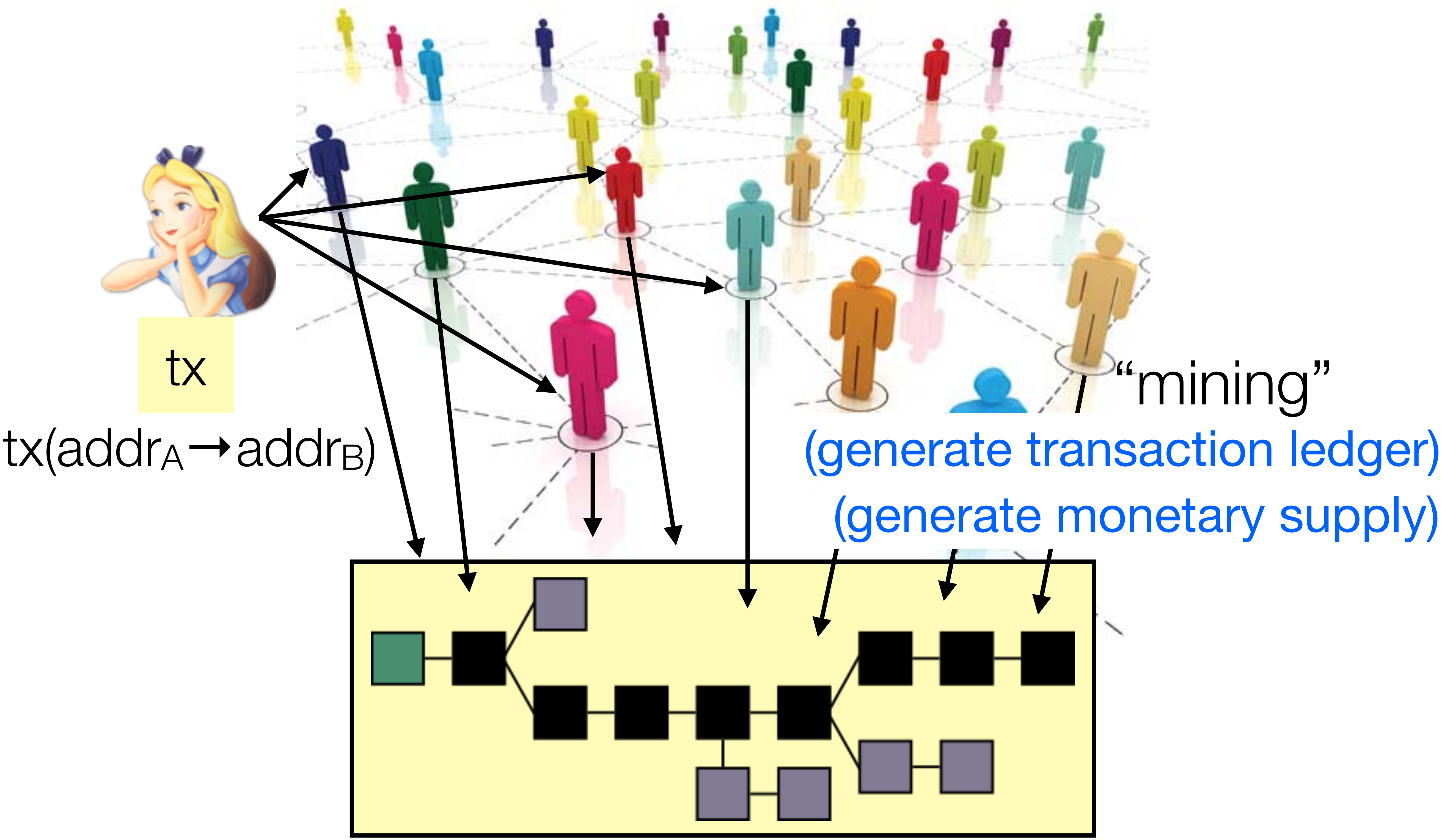
fully decentralized cryptocurrencies



tx

$\text{tx}(\text{addr}_A \rightarrow \text{addr}_B)$

fully decentralized cryptocurrencies



tx

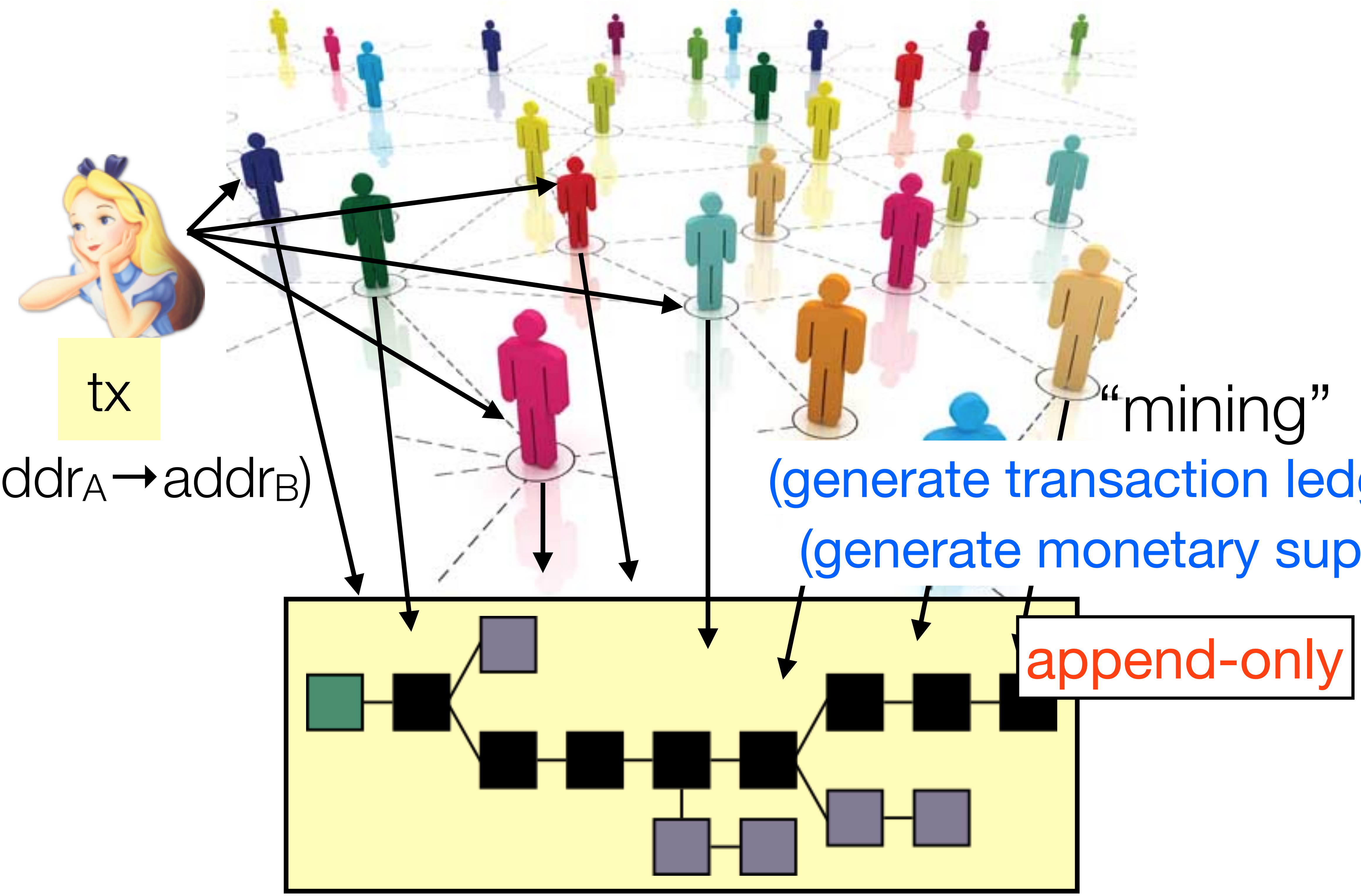
tx($addr_A$→$addr_B$)

“mining”

(generate transaction ledger)

(generate monetary supply)

fully decentralized cryptocurrencies



tx

tx($addr_A$ → $addr_B$)

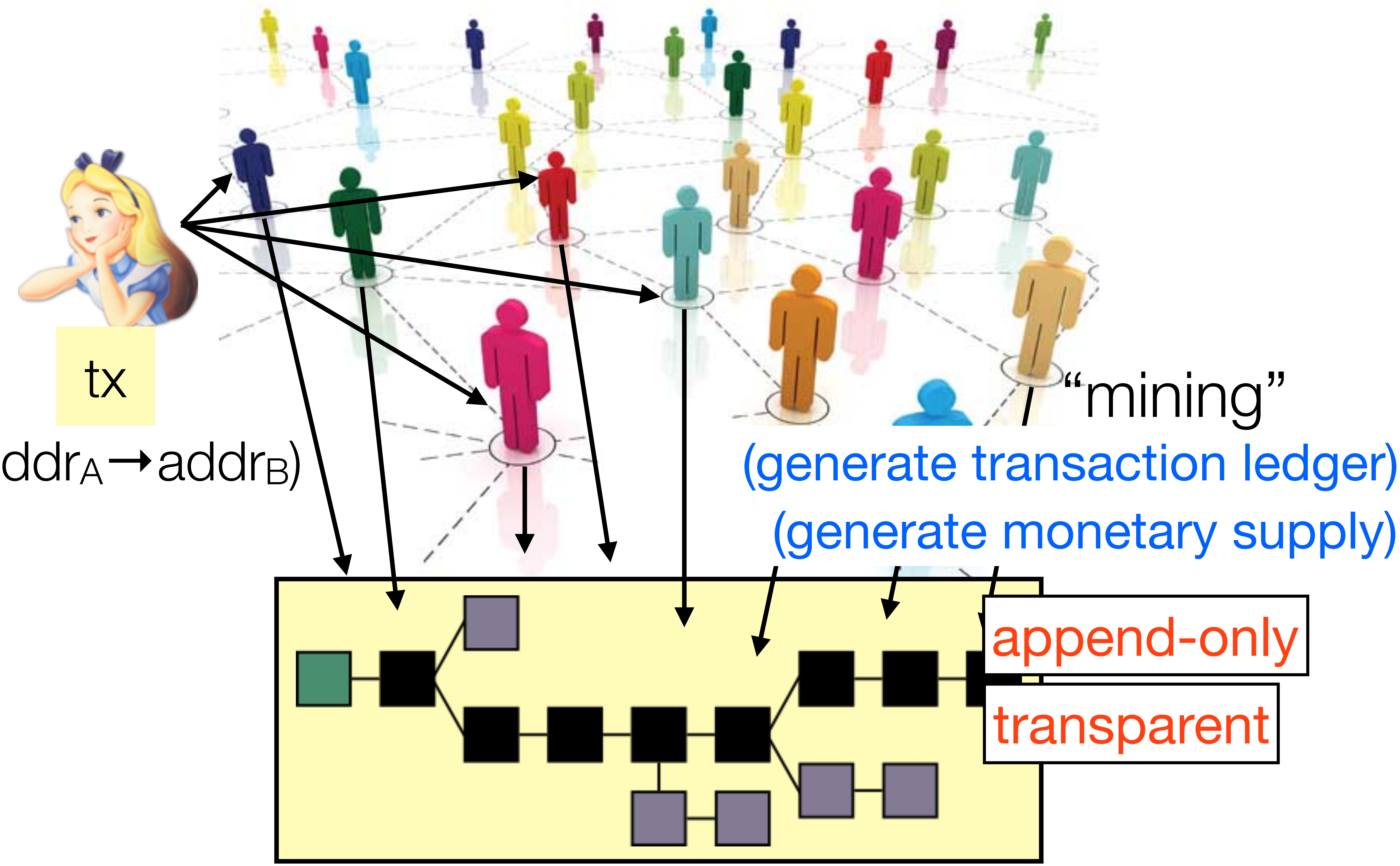
“mining”

(generate transaction ledger)

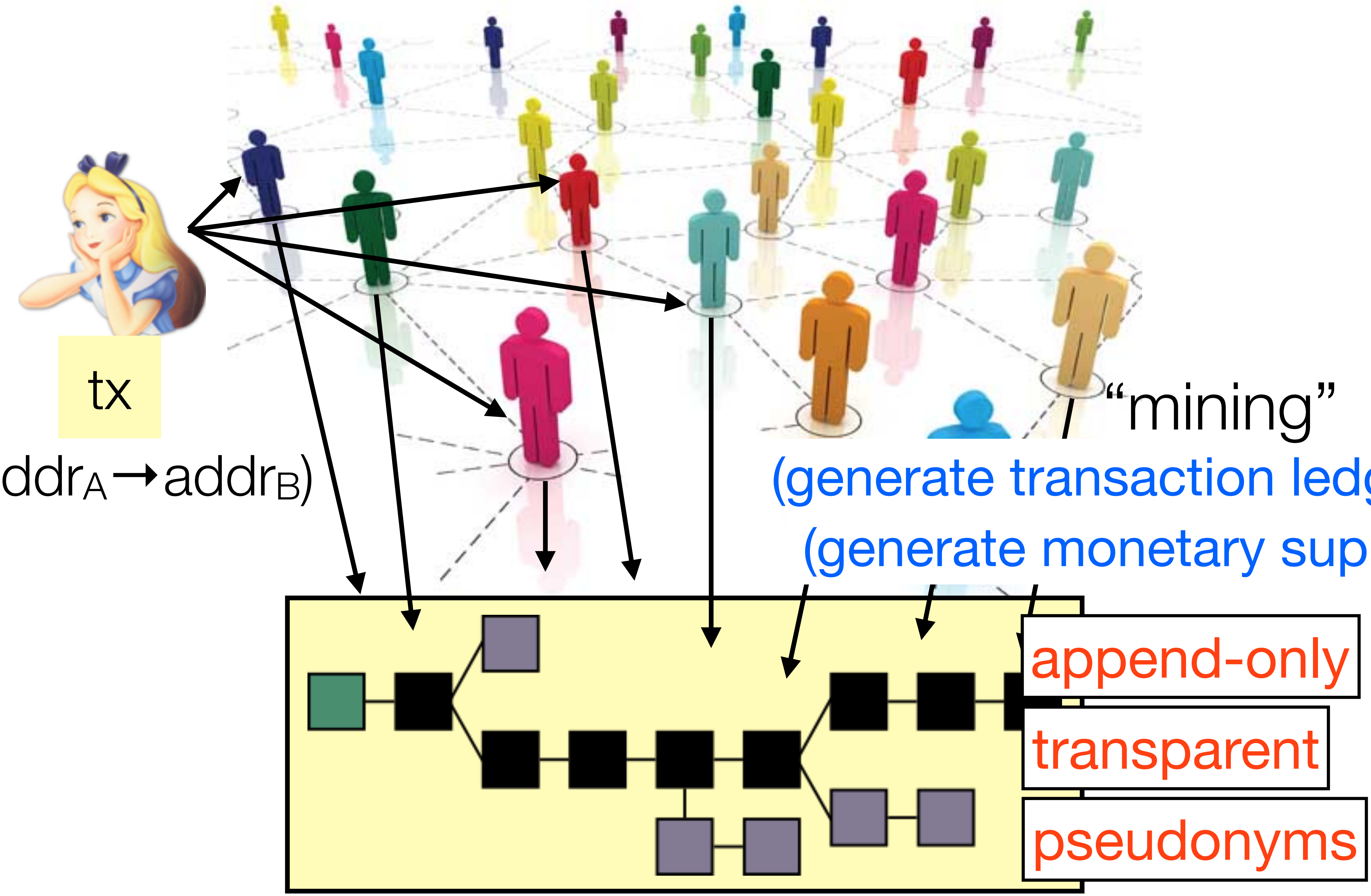
(generate monetary supply)

append-only

fully decentralized cryptocurrencies



fully decentralized cryptocurrencies



tx

$\text{tx}(\text{addr}_A \rightarrow \text{addr}_B)$

“mining”

(generate transaction ledger)

(generate monetary supply)

append-only

transparent

pseudonyms

issues with Bitcoin

no control over monetary policy

hashing rates are out of control

incentive structure is messed up

attacks on mining

issues with Bitcoin

no control over monetary policy

hashing rates are out of control

incentive structure is messed up

attacks on mining

not suitable for most applications!

RSCoin

		RSCoin	
monetary supply	decentral	central	central

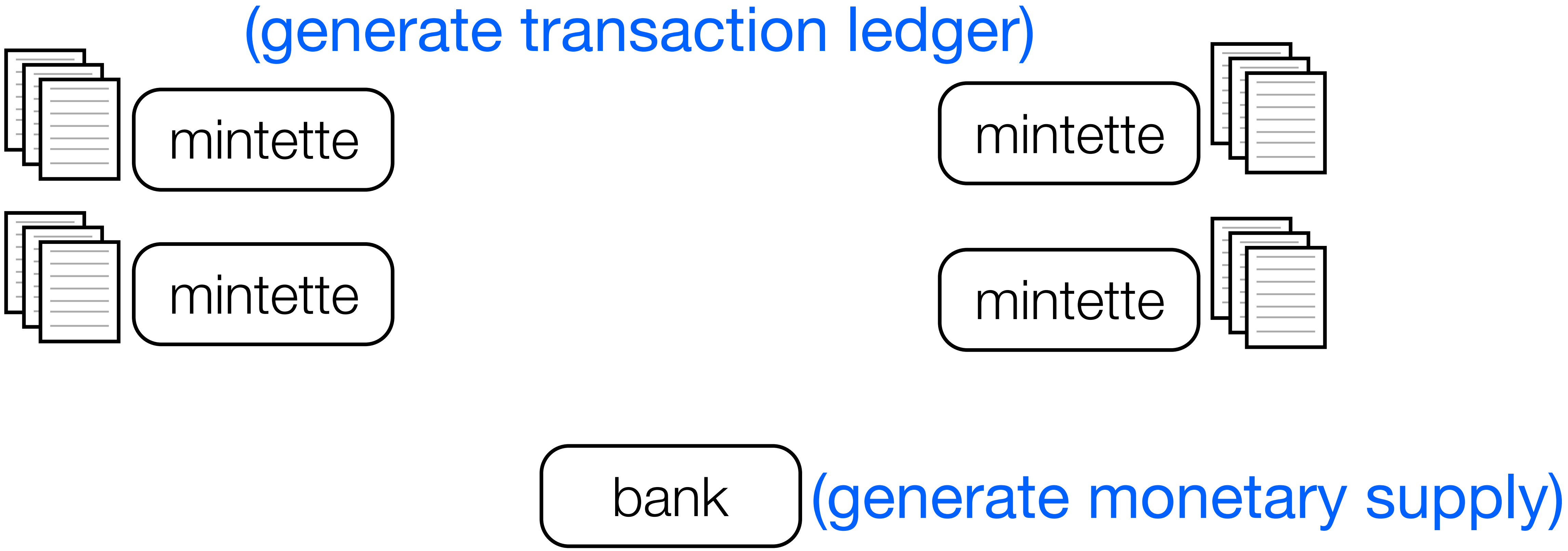
		RSCoin	
monetary supply	decentral	central	central
ledger	decentral	distribute	central

		RSCoin	
monetary supply	decentral	central	central
ledger	decentral	distribute	central
transparent?	y	y (or n)	n

		RSCoin	
monetary supply	decentral	central	central
ledger	decentral	distribute	central
transparent?	y	y (or n)	n
pseudonyms?	y	y (or n)	n

		RSCoin	
monetary supply	decentral	central	central
ledger	decentral	distribute	central
transparent?	y	y (or n)	n
pseudonyms?	y	y (or n)	n
computation	high!	low	low

bank (generate monetary supply)



(generate transaction ledger)

mintette

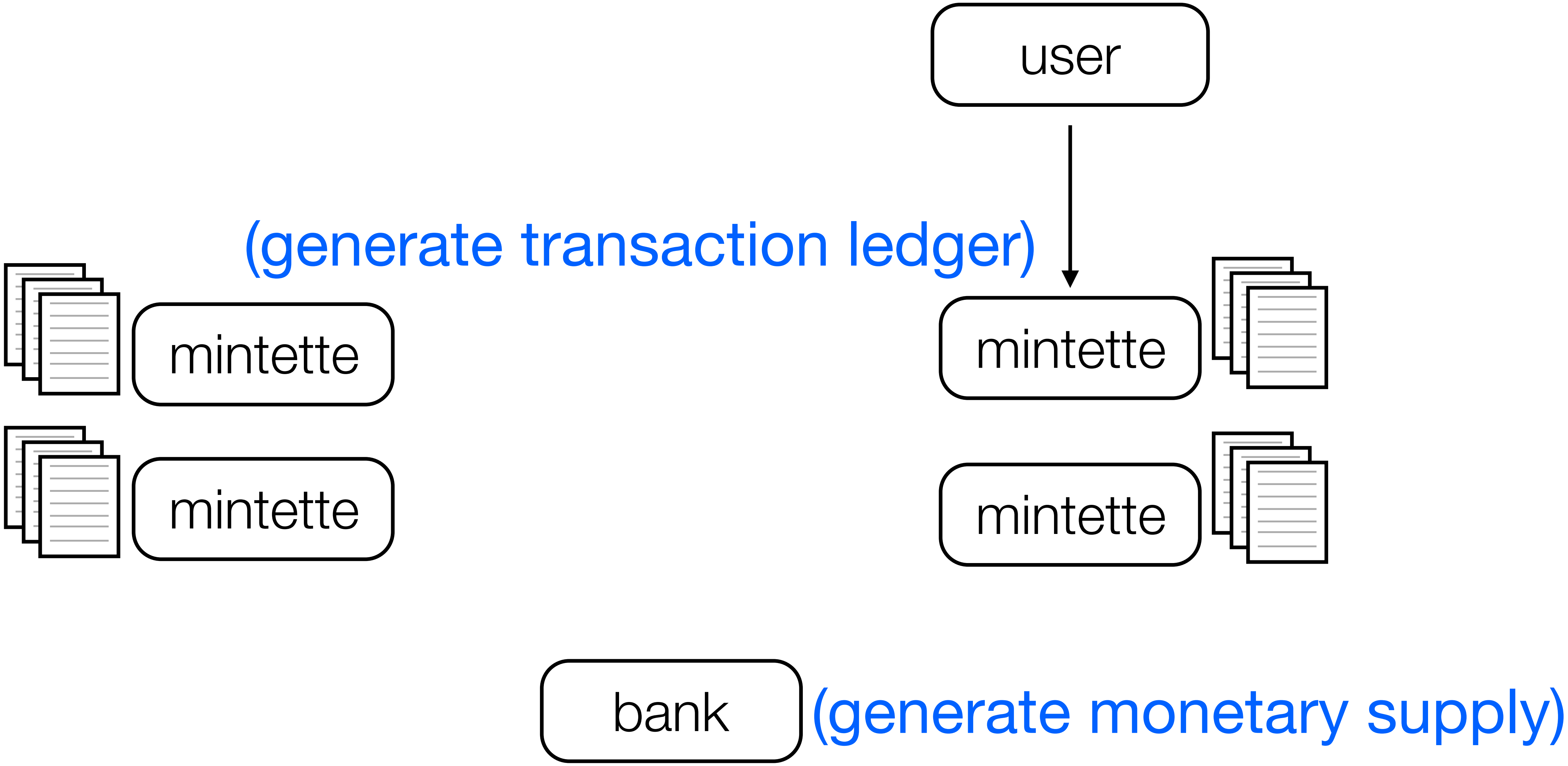
mintette

mintette

mintette

bank

(generate monetary supply)



user

(generate transaction ledger)

mintette

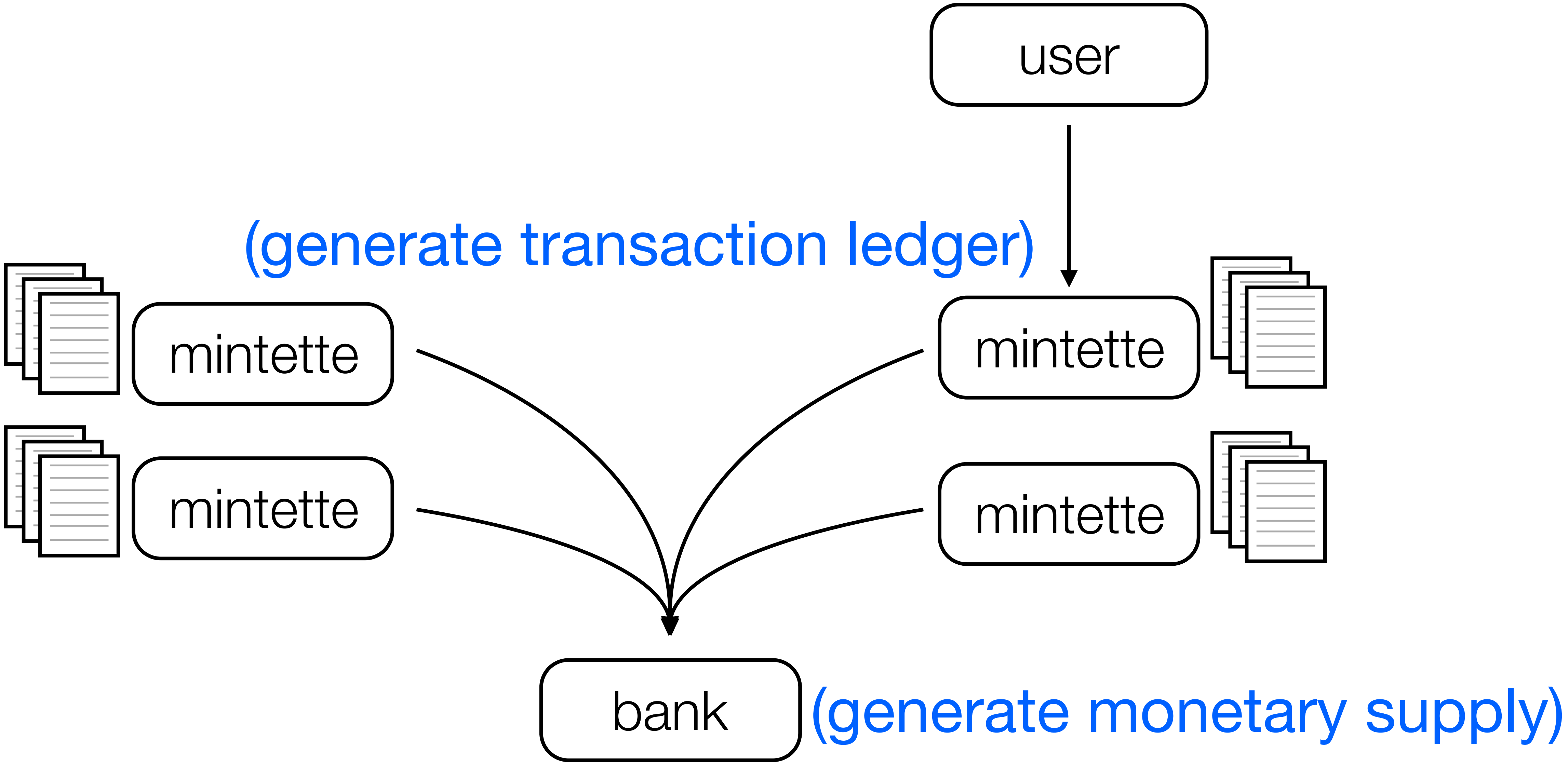
mintette

mintette

mintette

bank

(generate monetary supply)



user

(generate transaction ledger)

mintette

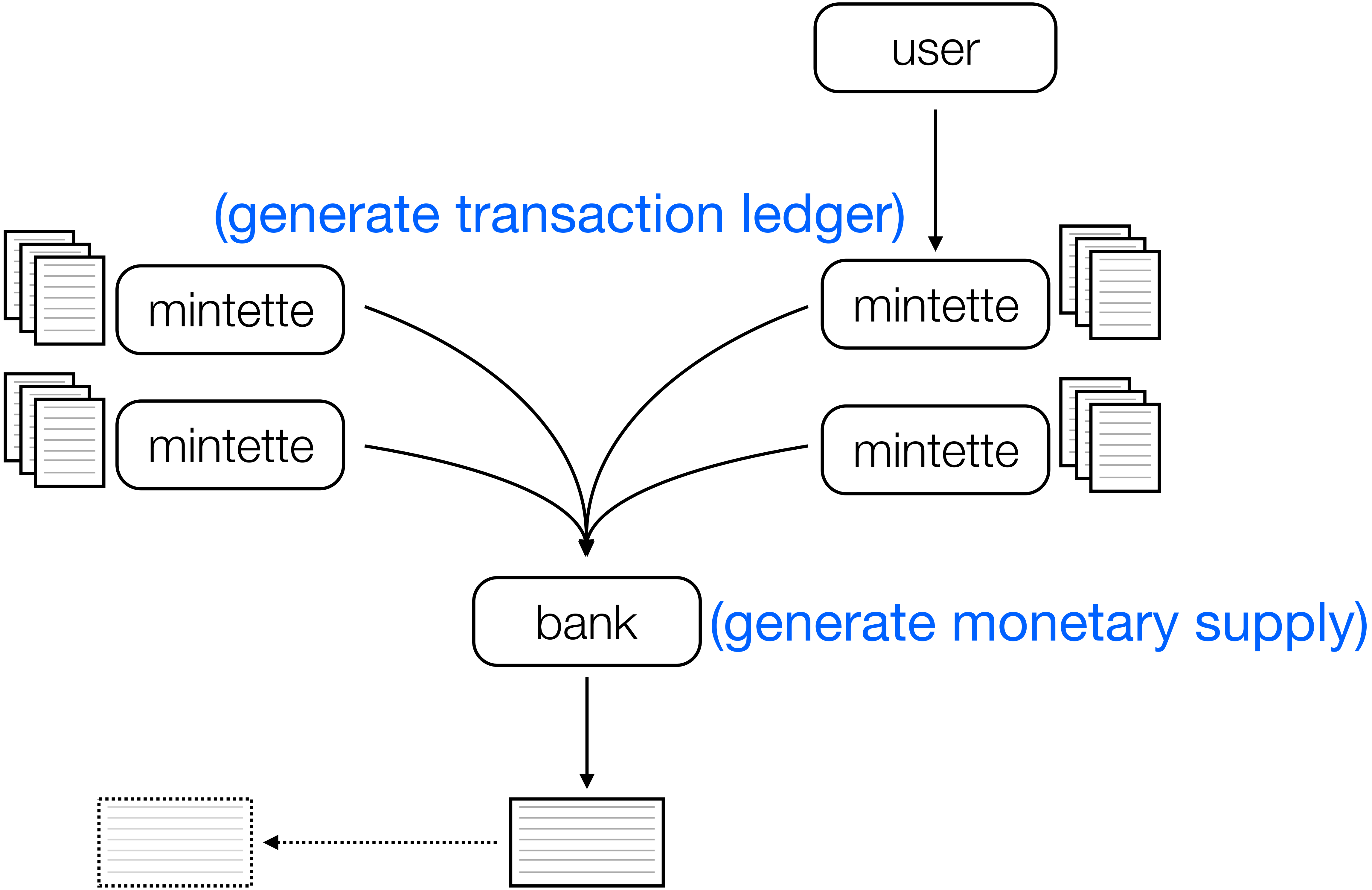
mintette

mintette

mintette

bank

(generate monetary supply)



user

(generate transaction ledger)

mintette

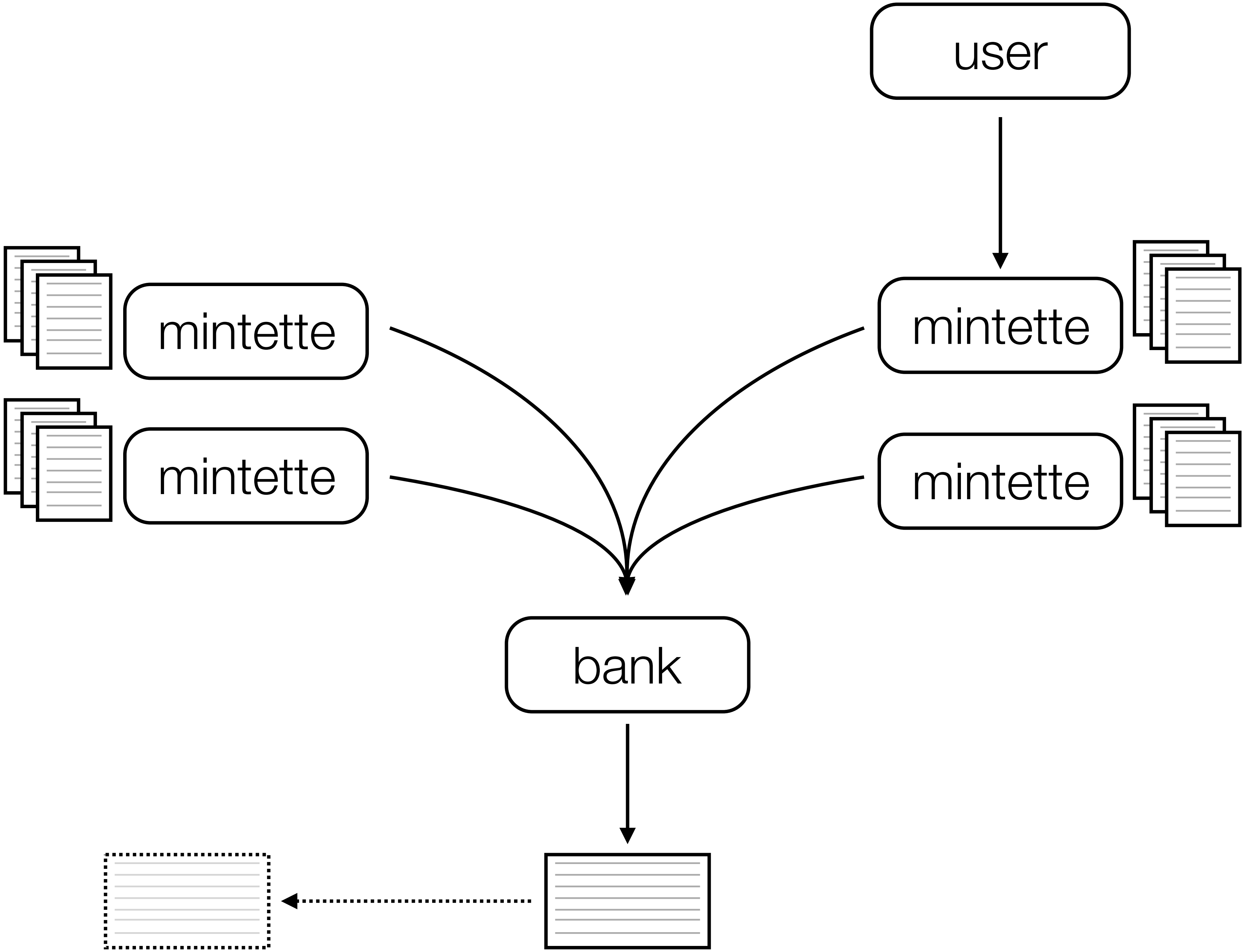
mintette

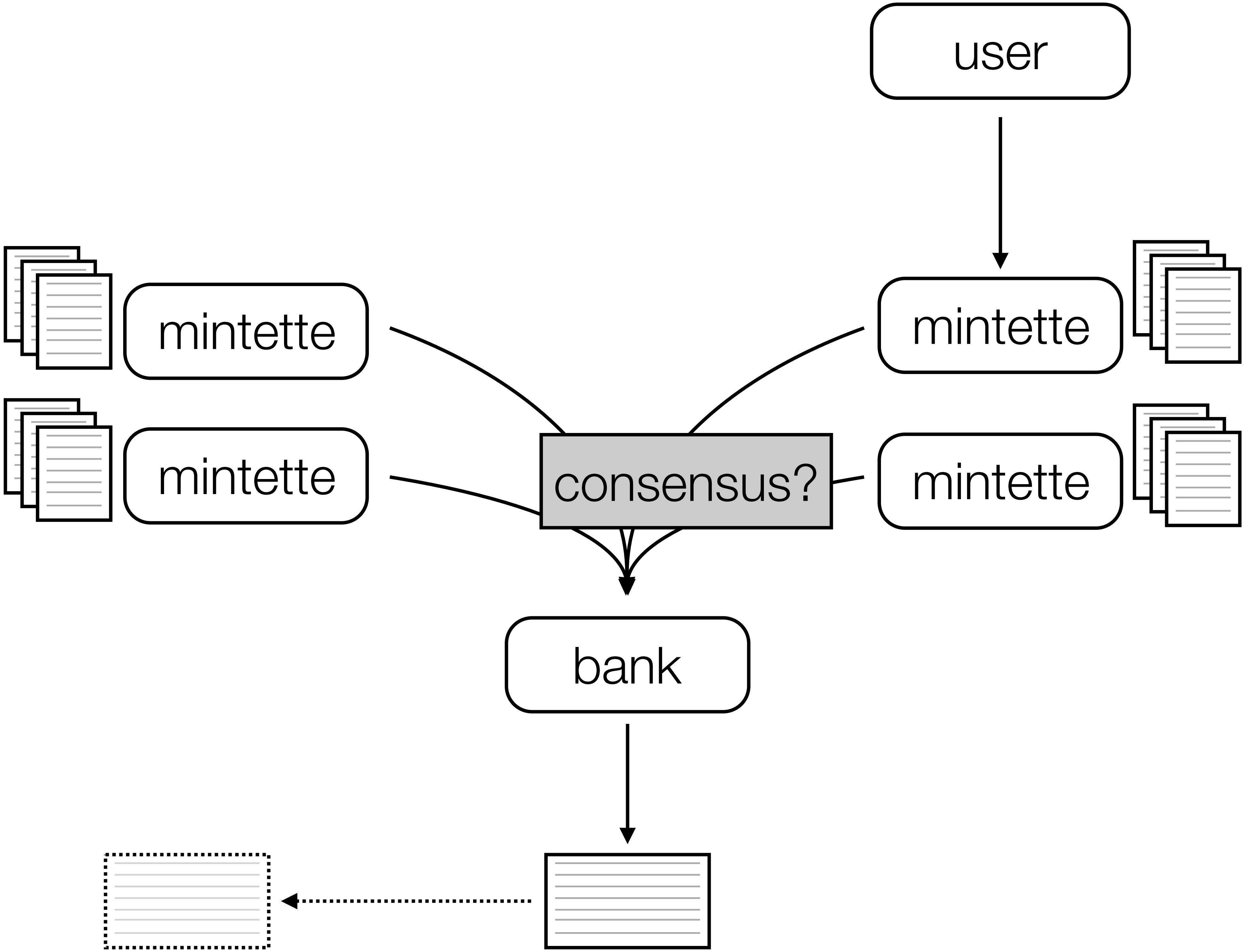
mintette

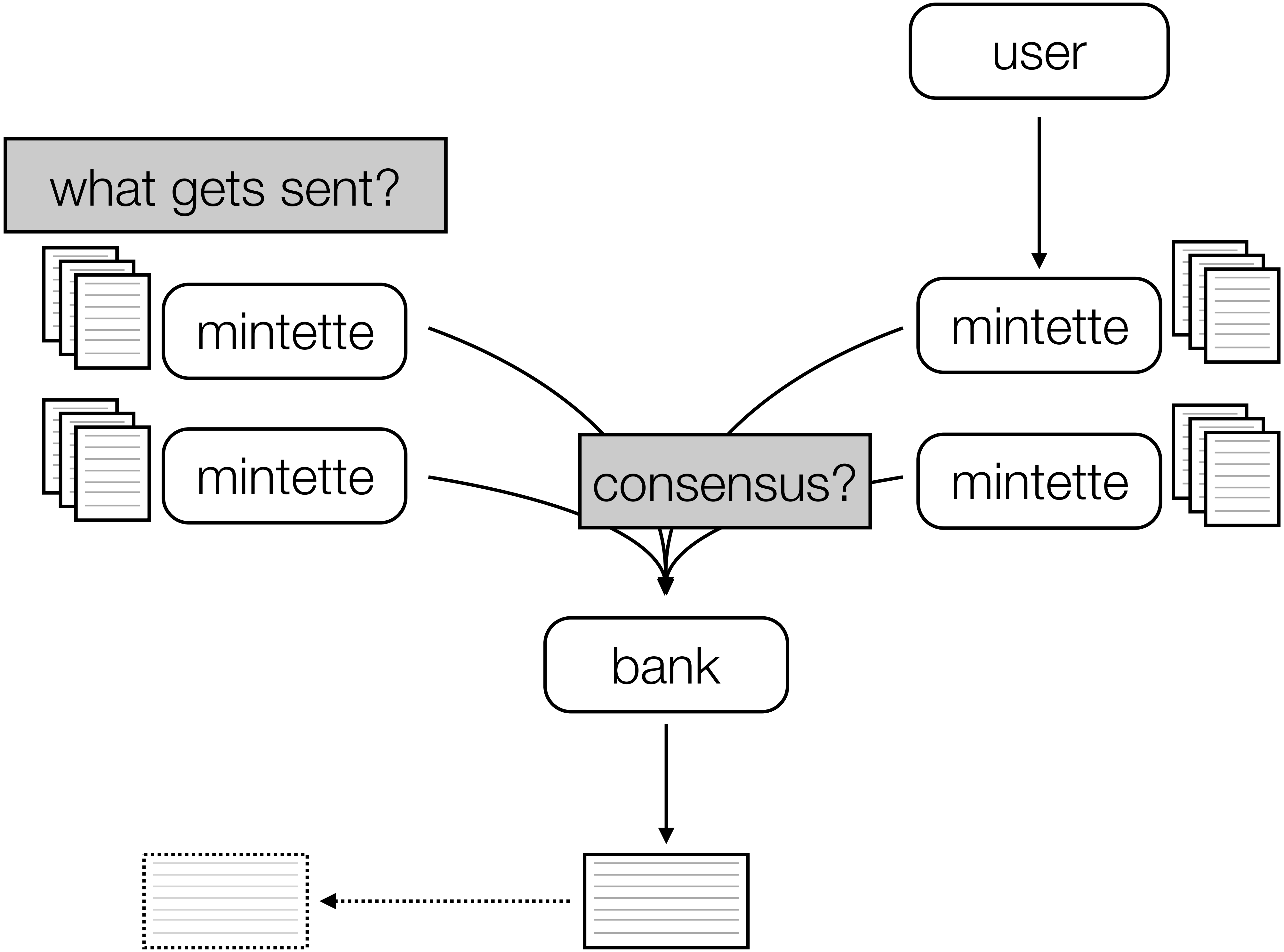
mintette

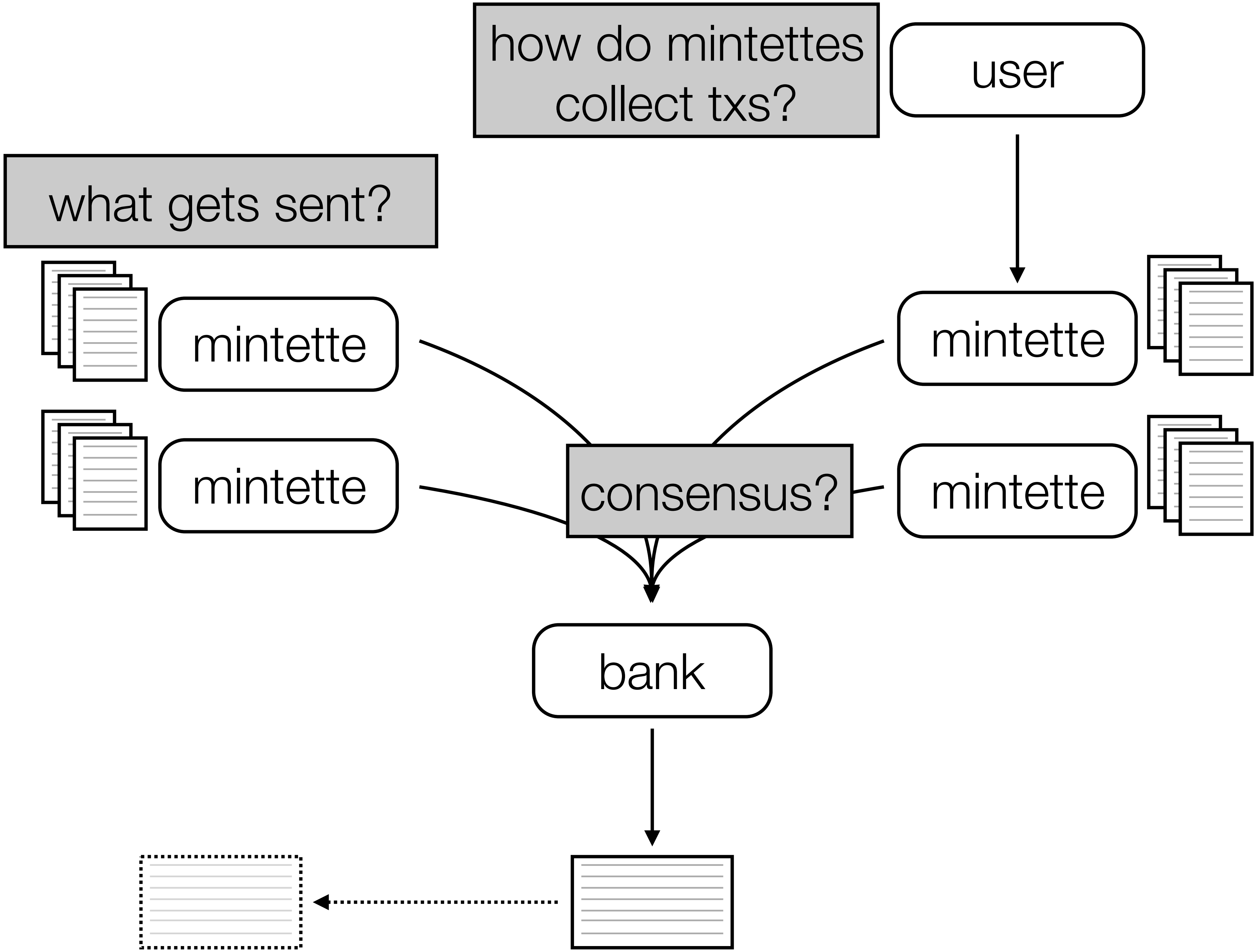
bank

(generate monetary supply)


user
mintette
mintette
mintette
mintette
bank


user
mintette
mintette
mintette
mintette
consensus?
bank


user
what gets sent?
mintette
mintette
mintette
mintette
consensus?
bank



how do mintettes collect txs?

user

what gets sent?

mintette

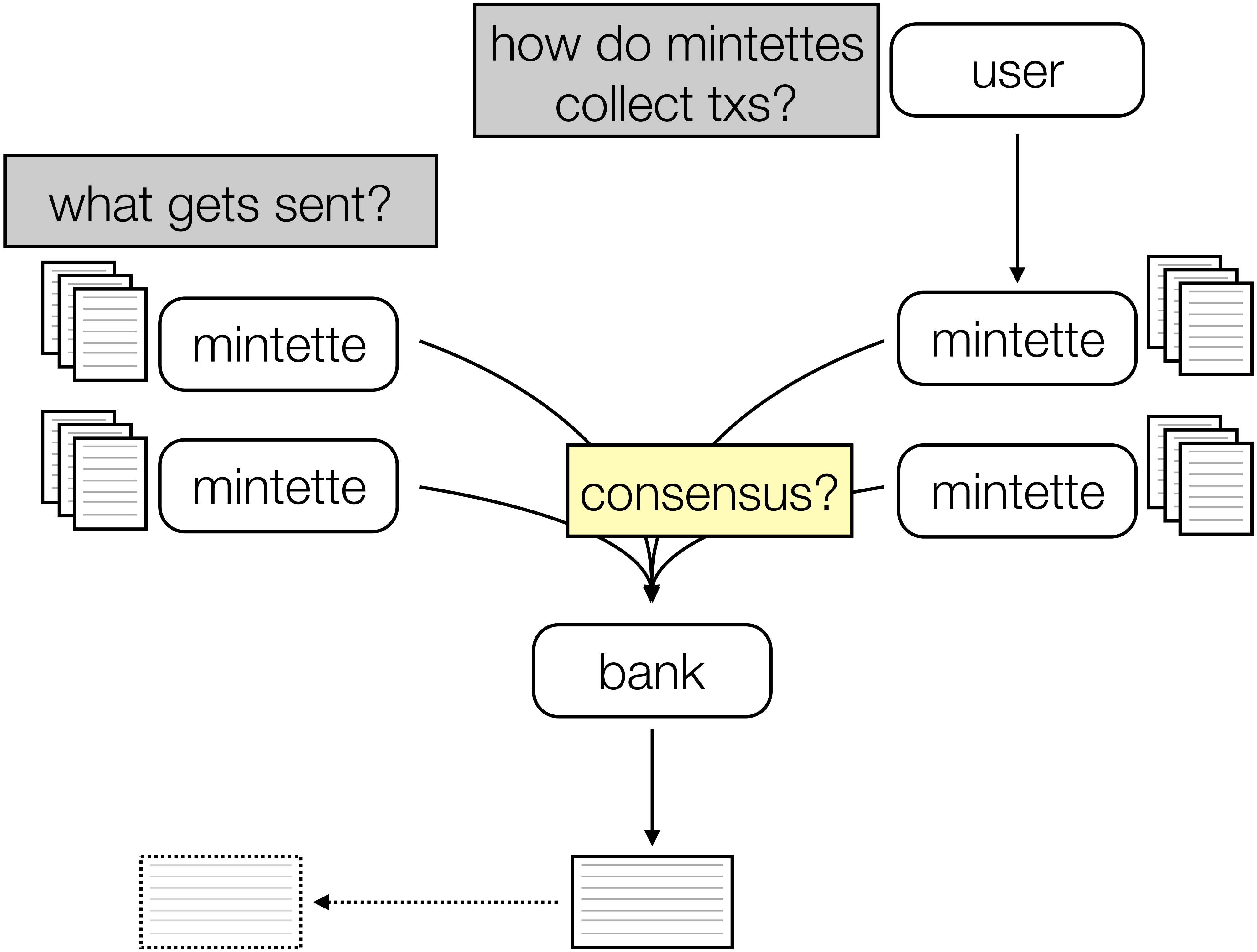
mintette

mintette

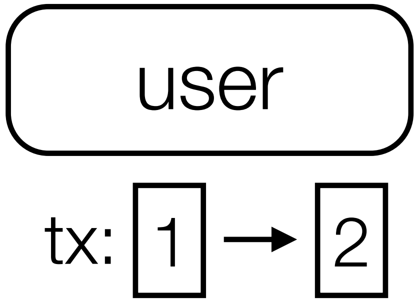
mintette

consensus?

bank

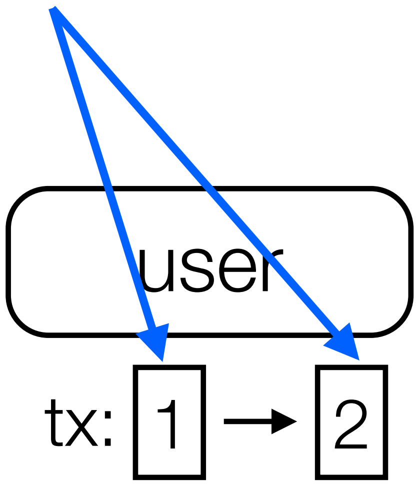

how do mintettes collect txs?
user
what gets sent?
mintette
mintette
mintette
mintette
consensus?
bank

consensus



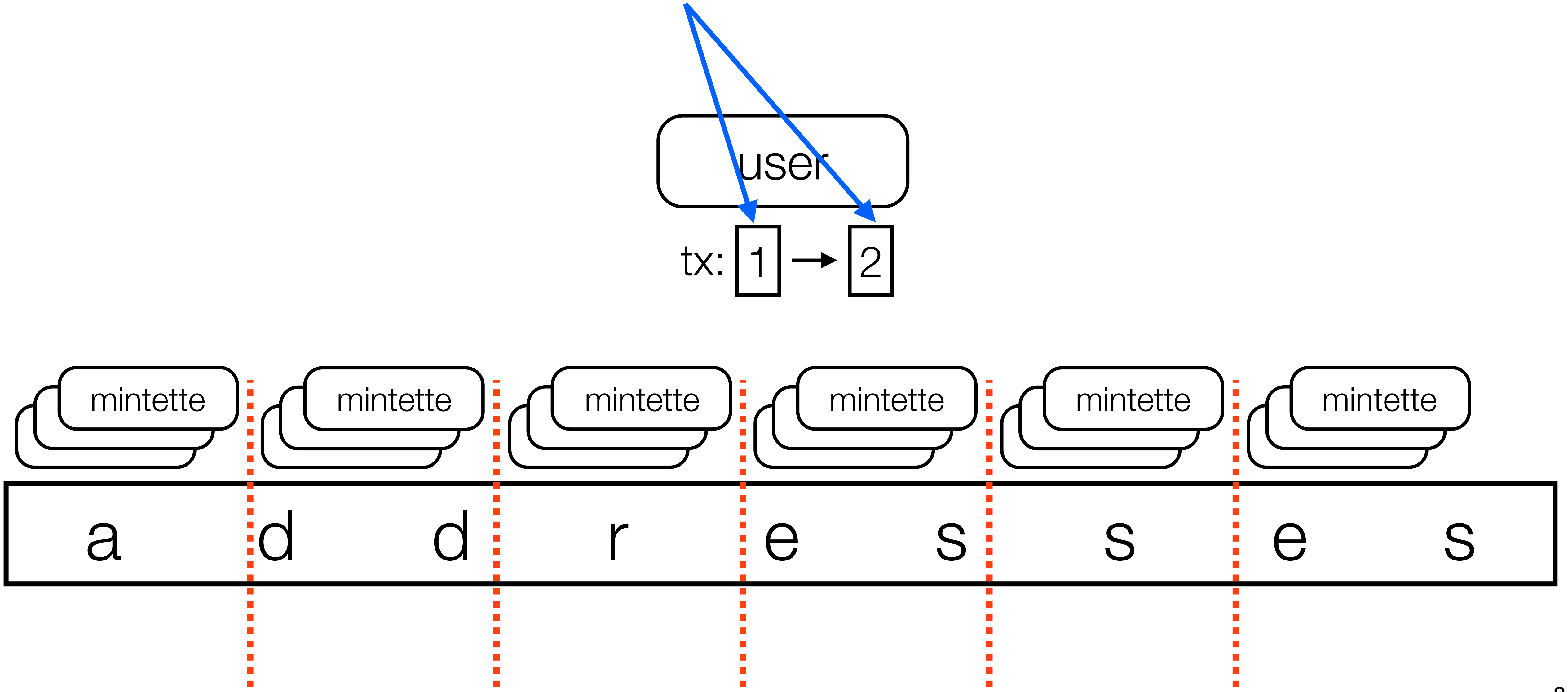
consensus

each address is **owned** by a set of mintettes

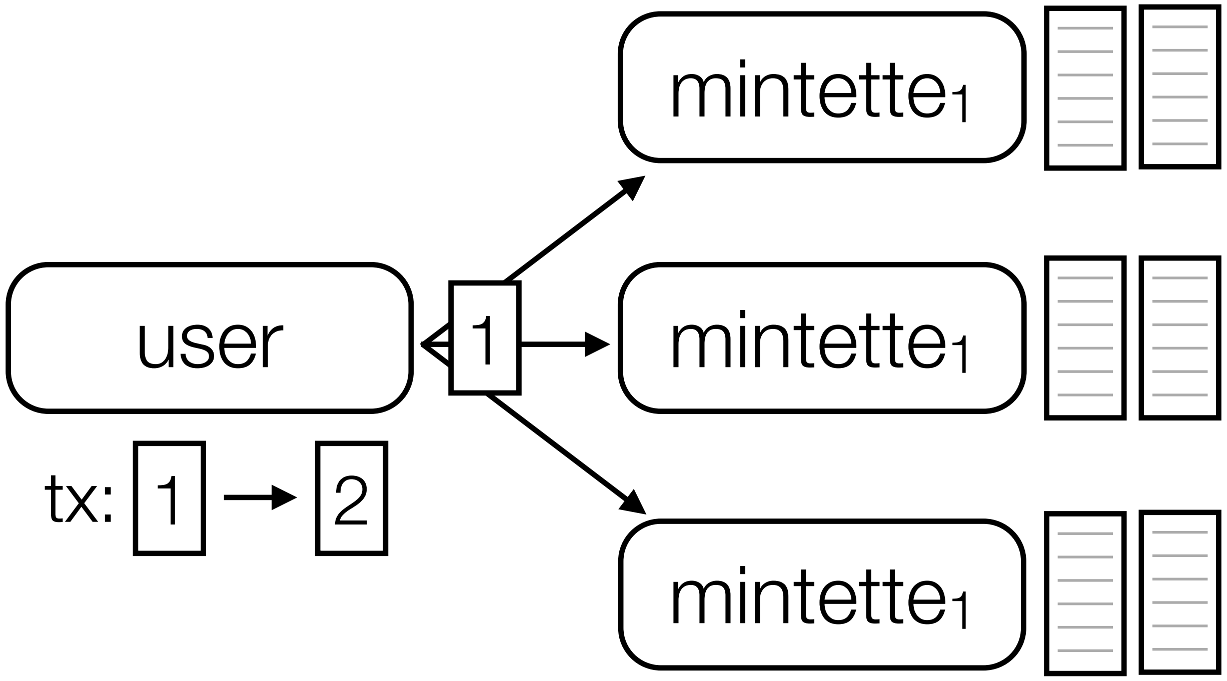


consensus

each address is **owned** by a set of mintettes

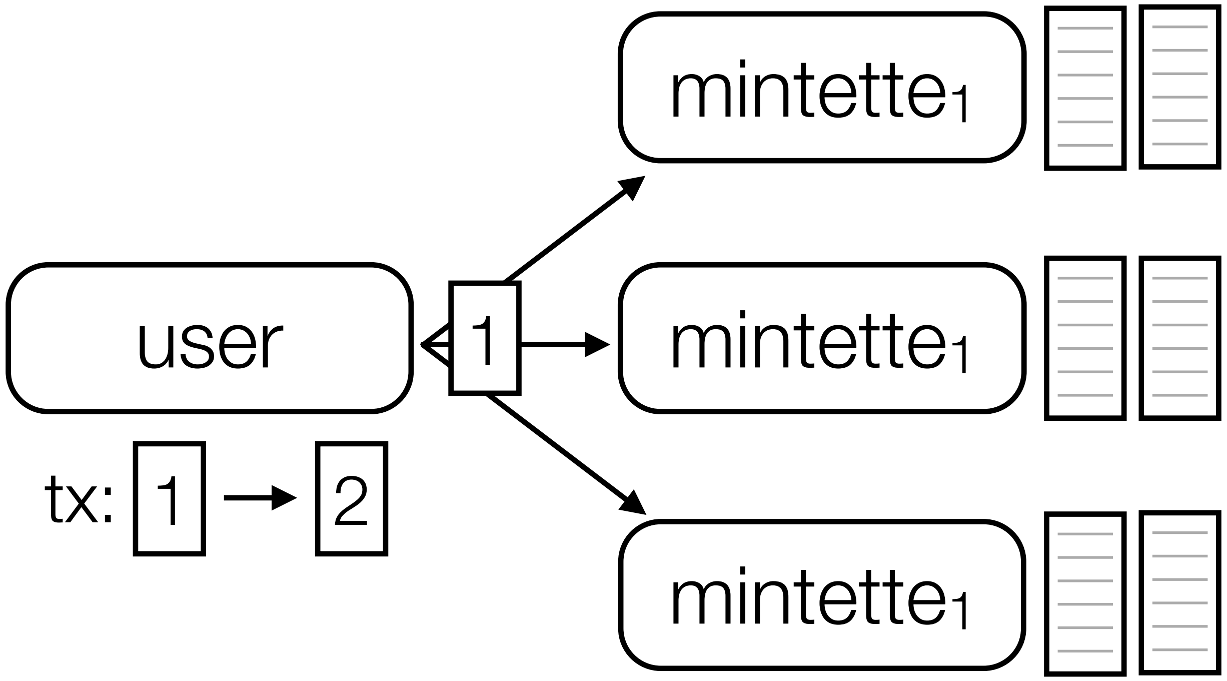


consensus



consensus

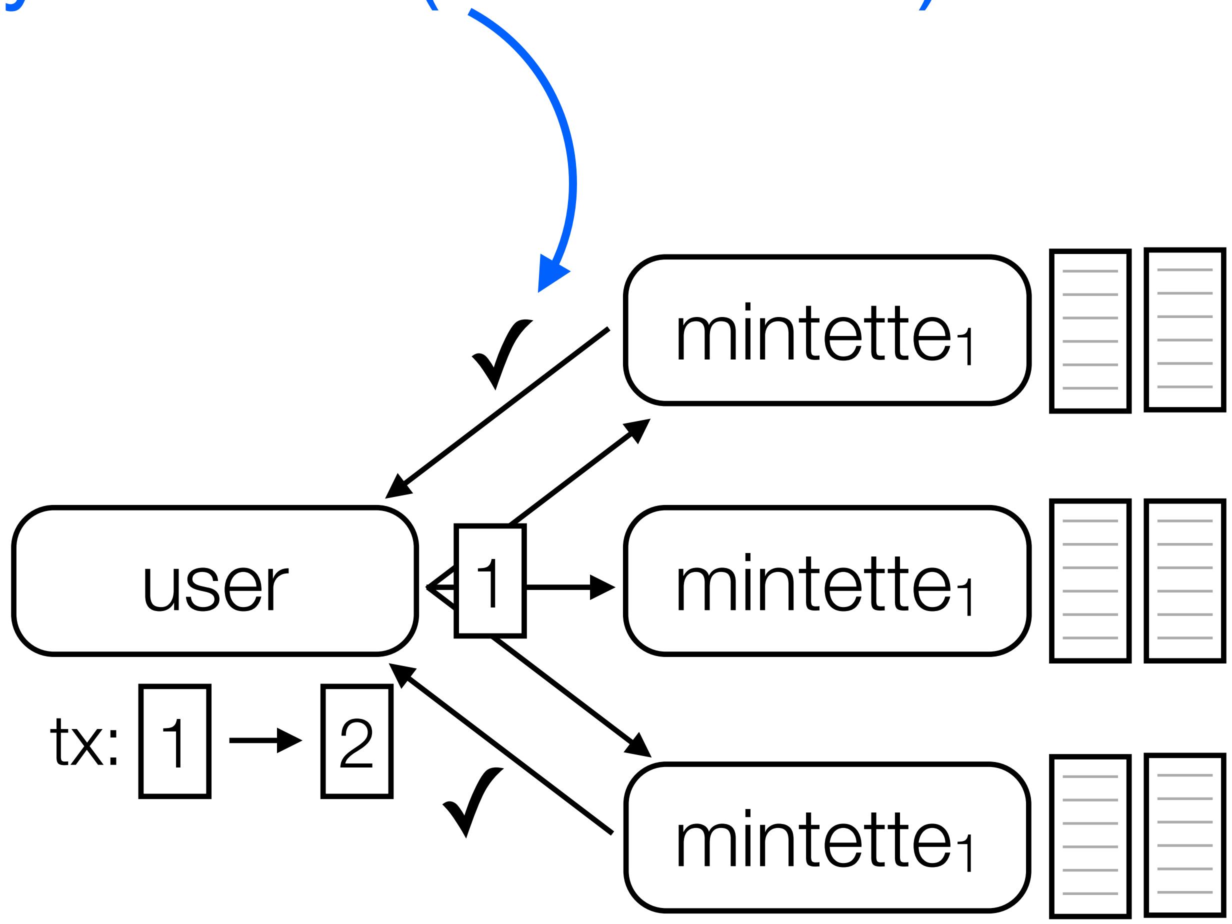
mintettes check for **double spending**…



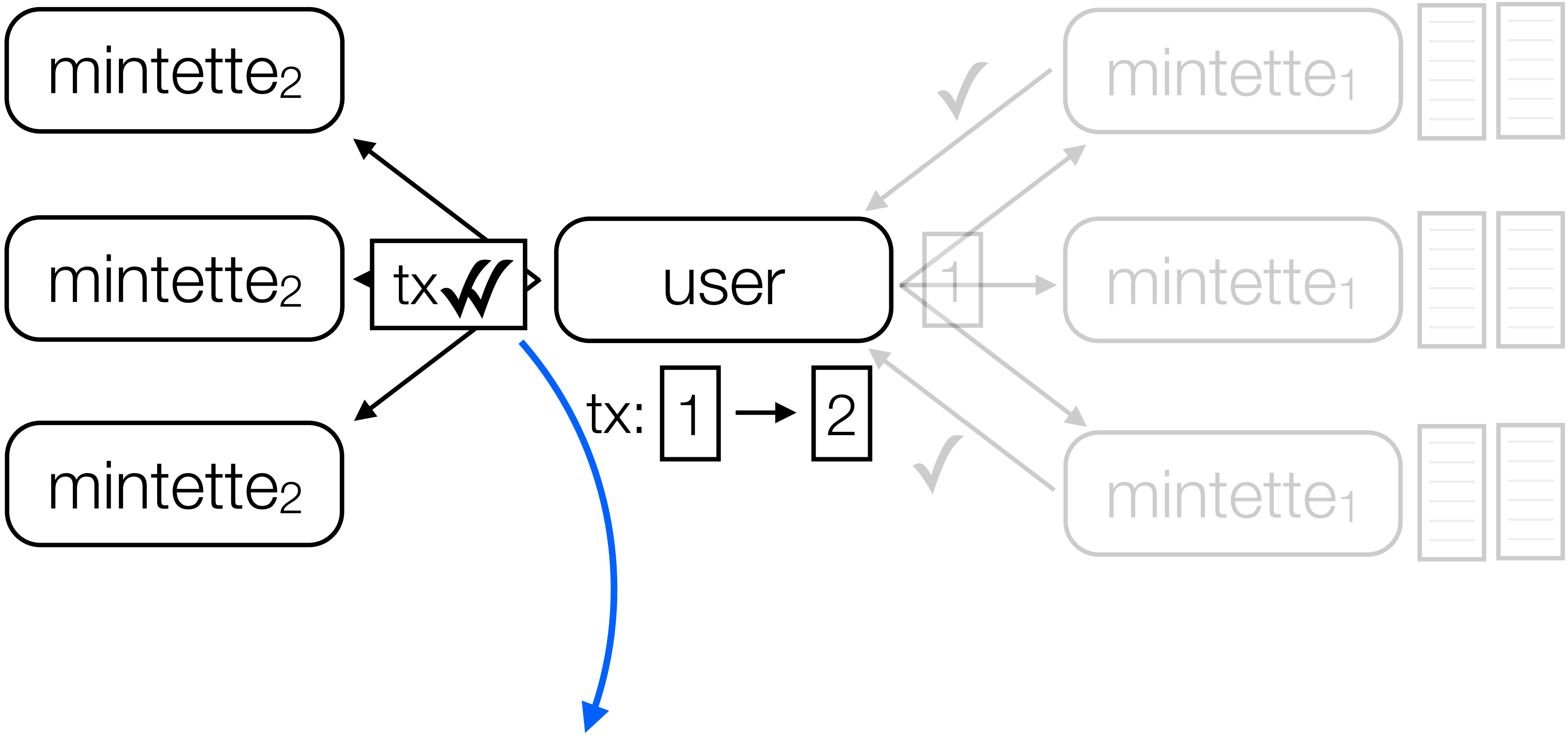
…using lists of **unspent transaction outputs** (utxo)

consensus

signed ‘yes’ vote (and head h)



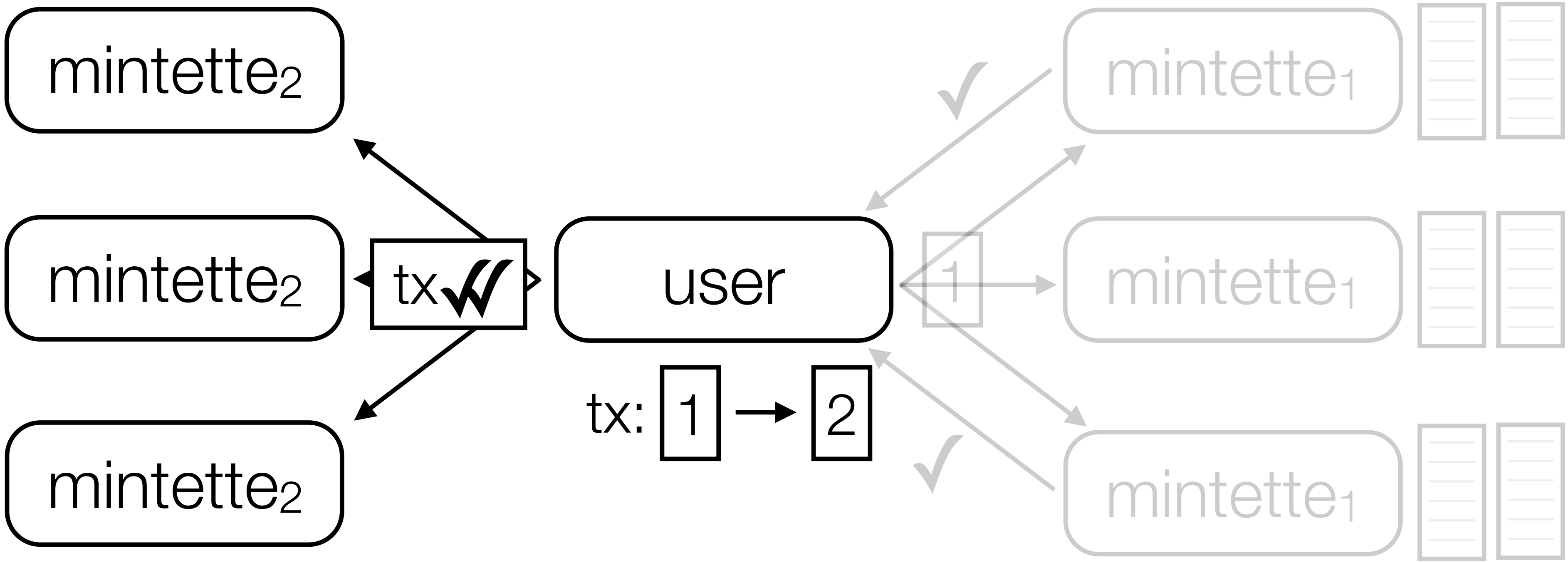
consensus



“bundle of evidence” contains ‘yes’ votes from **majority** of mintettes in shard

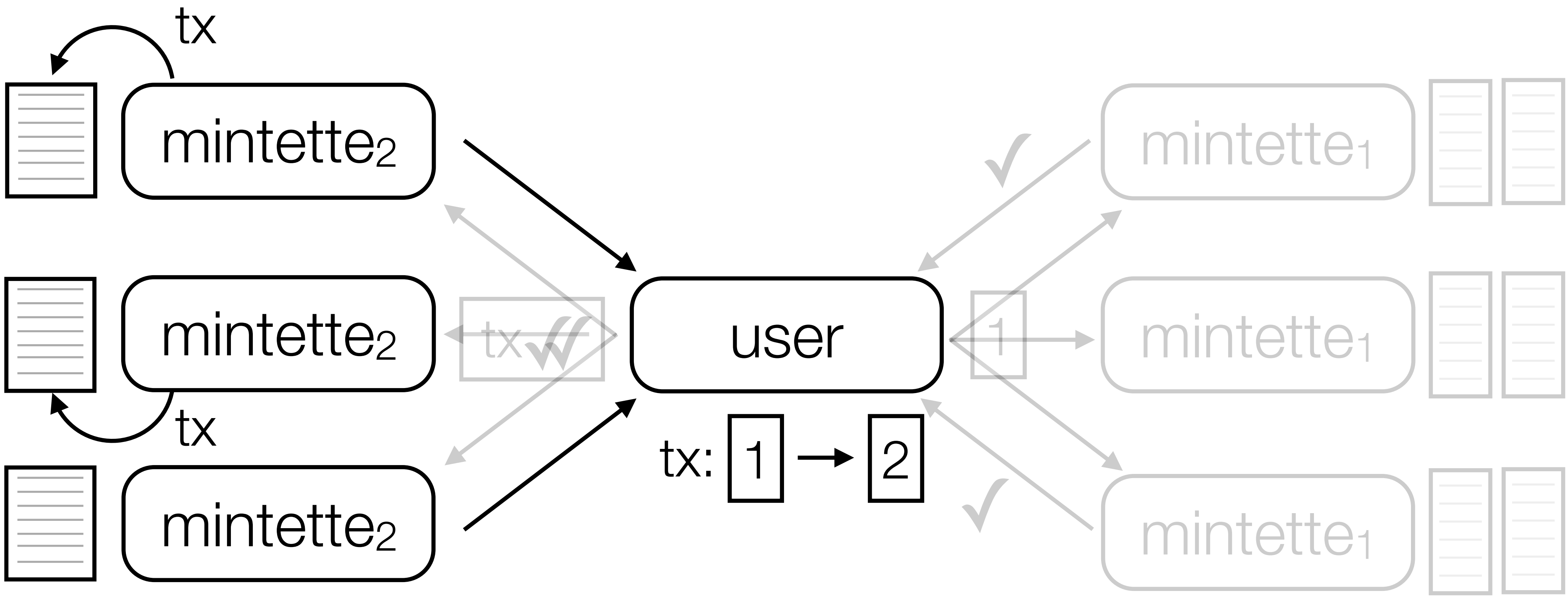
consensus

mintettes check validity of bundle by checking for signatures from authorized mintettes…



consensus

…and if satisfied they add transaction to be **committed** and send back **receipt**



consensus features

consensus features

simple (adaption of Two-Phase Commit)

consensus features

simple (adaption of Two-Phase Commit)

scalable!

consensus features

simple (adaption of Two-Phase Commit)

scalable!

T = set of txs generated per second

Q = # mintettes per shard

M = # mintettes

consensus features

simple (adaption of Two-Phase Commit)

scalable!

T = set of txs generated per second

Q = # mintettes per shard

M = # mintettes

$$\text{comm. per mintette per sec} = \frac{\sum_{tx \in T} 2(m_{tx}+1)Q}{M}$$

consensus features

simple (adaption of Two-Phase Commit)

scalable!

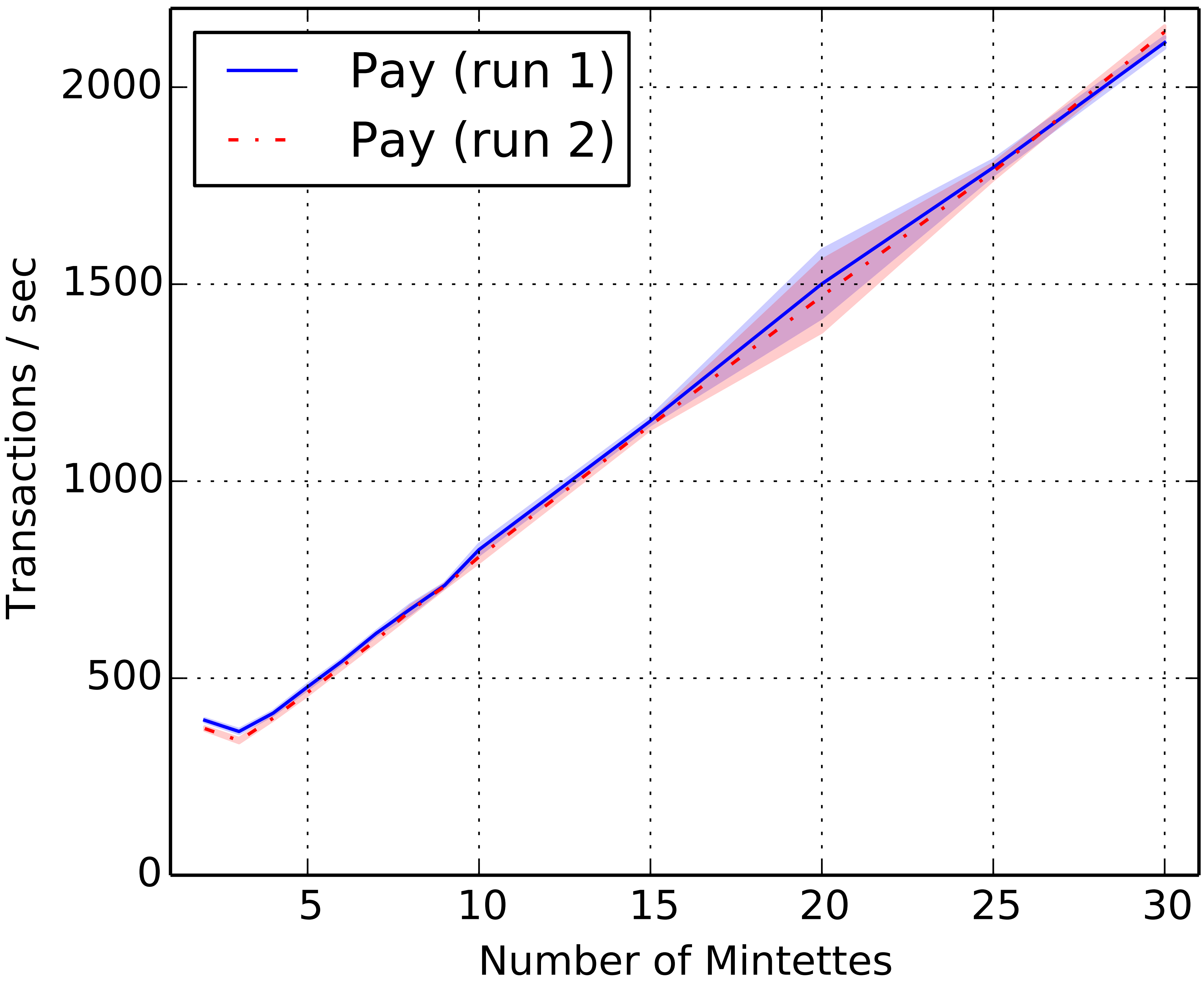
T = set of txs generated per second

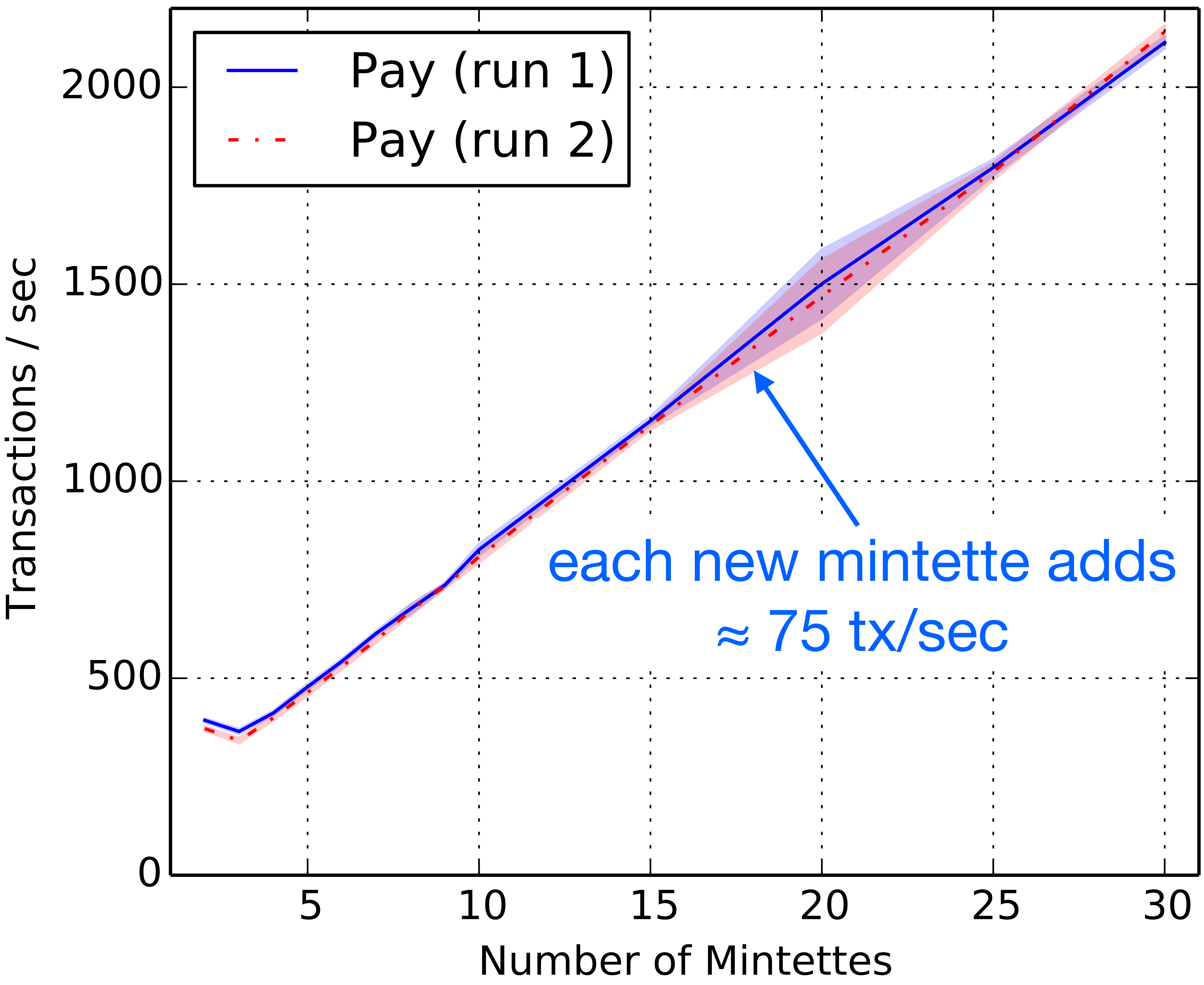
Q = # mintettes per shard

M = # mintettes

$$\text{comm. per mintette per sec} = \frac{\sum_{tx \in T} 2(m_{tx}+1)Q}{\boxed{M}}$$

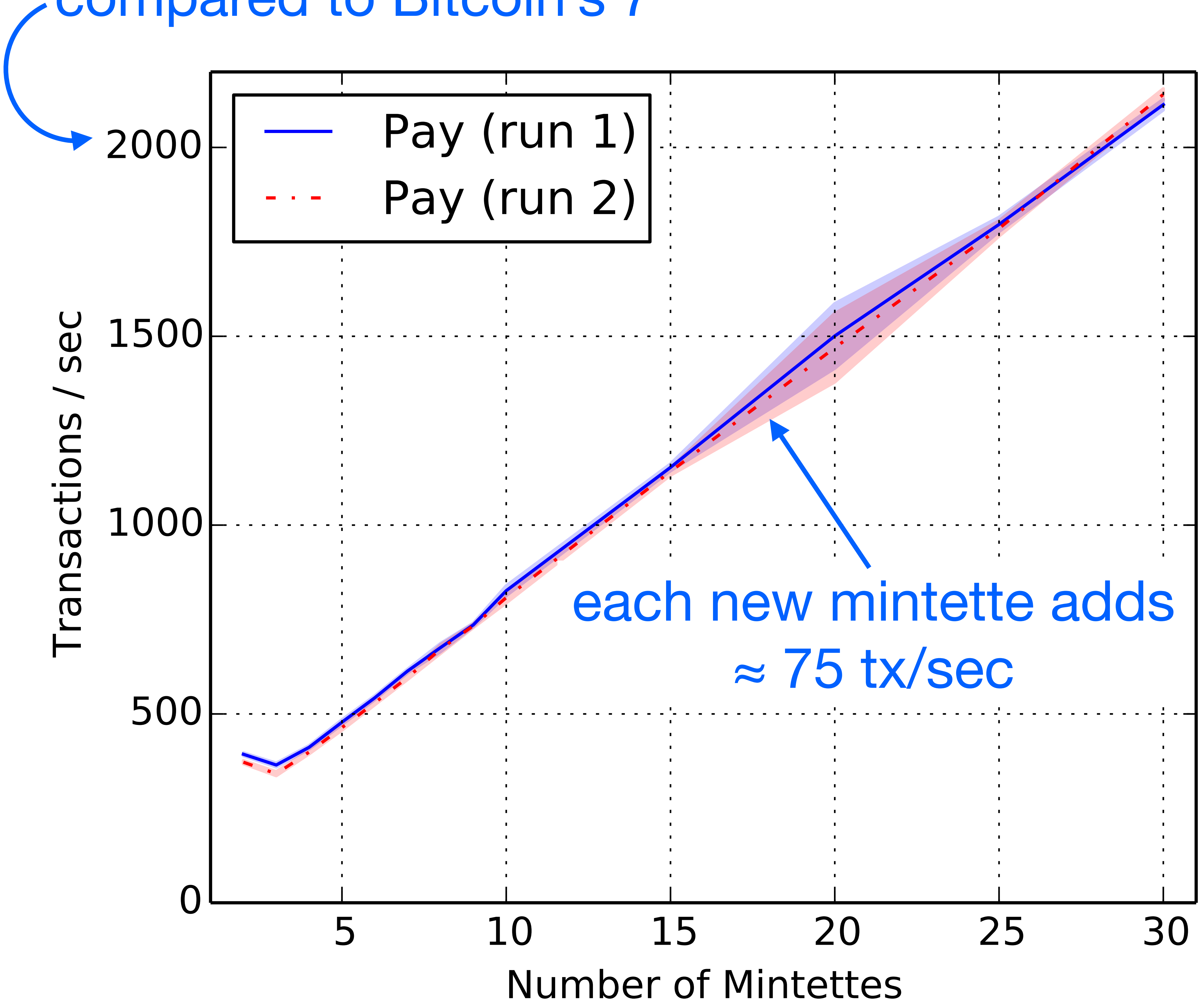
scales infinitely as more mintettes are added!


Pay (run 1)
Pay (run 2)
Transactions / sec
0
500
1000
1500
2000
Number of Mintettes
5
10
15
20
25
30

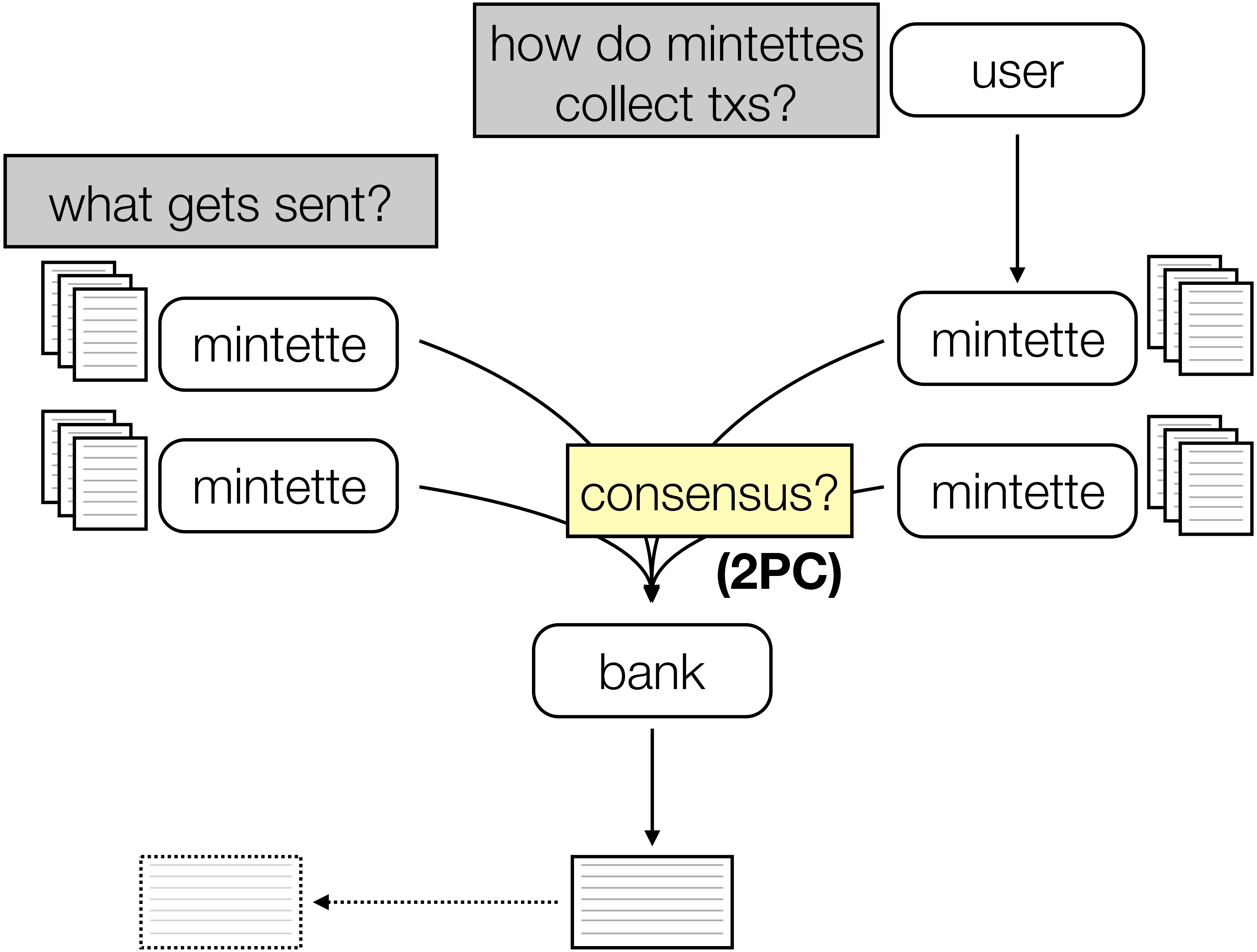


each new mintette adds ≈ 75 tx/sec

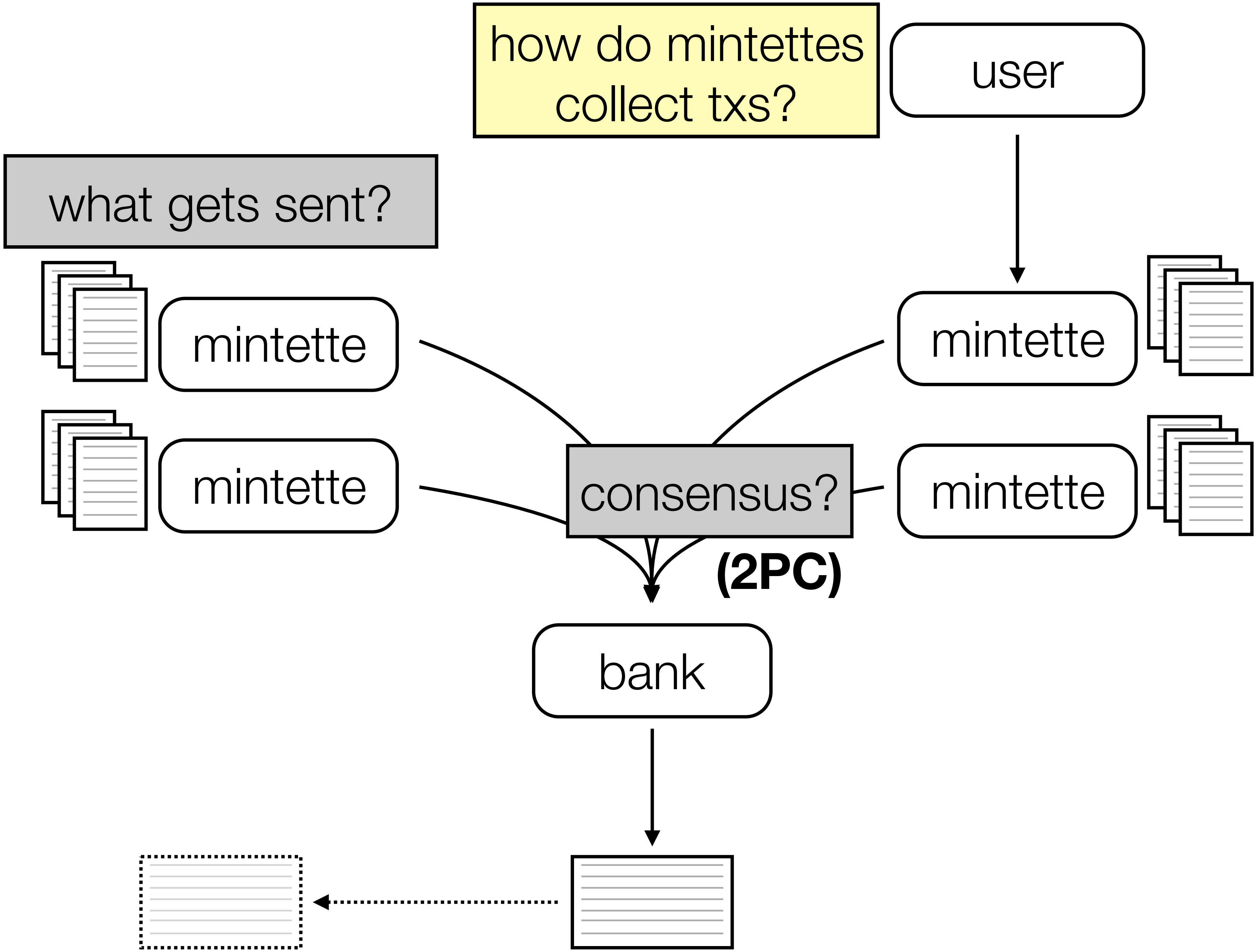
compared to Bitcoin's 7



each new mintette adds ≈ 75 tx/sec


how do mintettes collect txs?
user
what gets sent?
mintette
mintette
mintette
mintette
consensus?
(2PC)
bank

(contacted based on shard)

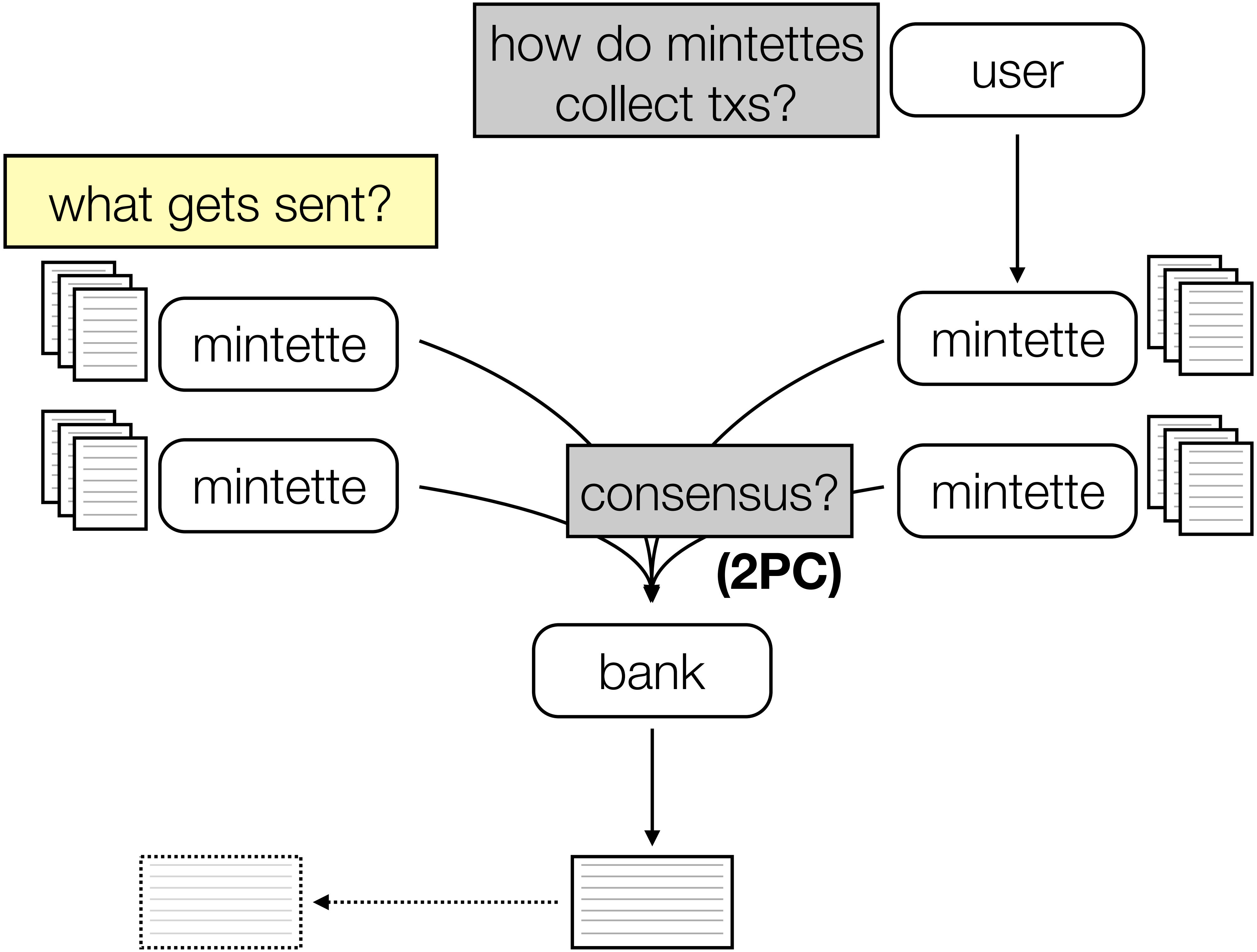

how do mintettes collect txs?

what gets sent?

consensus?

(2PC)

(contacted based on shard)



how do mintettes collect txs?

what gets sent?

consensus?

(2PC)

security properties

no double spending (only “good” transactions get included)

security properties

✓ no double spending (only “good” transactions get included)

(if honest majority)

security properties

✓ no double spending (only “good” transactions get included)

non-repudiation (mintettes are held to their promises)

security properties

✓ no double spending (only “good” transactions get included)

✓ non-repudiation (mintettes are held to their promises)

(because mintettes provide receipt upon committing transaction)

security properties

✓ no double spending (only “good” transactions get included)

✓ non-repudiation (mintettes are held to their promises)

auditability (mintettes can’t cheat without detection)

mintette logs

borrow ideas from Certificate Transparency to log actions

mintette logs

borrow ideas from Certificate Transparency to log actions

mintettes create log entry every time they:

-act as mintette in first phase (Query)

-act as mintette in second phase (Commit)

-publish head of hash chain (CloseEpoch)

rolling hash chain of log acts as commitment to actions

mintette logs

borrow ideas from Certificate Transparency to log actions

mintettes create log entry every time they:

- -act as mintette in first phase (Query)
- -act as mintette in second phase (Commit)
- -publish head of hash chain (CloseEpoch)

rolling hash chain of log acts as commitment to actions

mintettes cross-hash chains to provide evidence of activity

mintette logs

borrow ideas from Certificate Transparency to log actions

mintettes create log entry every time they:

- -act as mintette in first phase (Query)
- -act as mintette in second phase (Commit)
- -publish head of hash chain (CloseEpoch)

rolling hash chain of log acts as commitment to actions

mintettes cross-hash chains to provide evidence of activity

send logs to bank at end of every period

security properties

✓ no double spending (only “good” transactions get included)

✓ non-repudiation (mintettes are held to their promises)

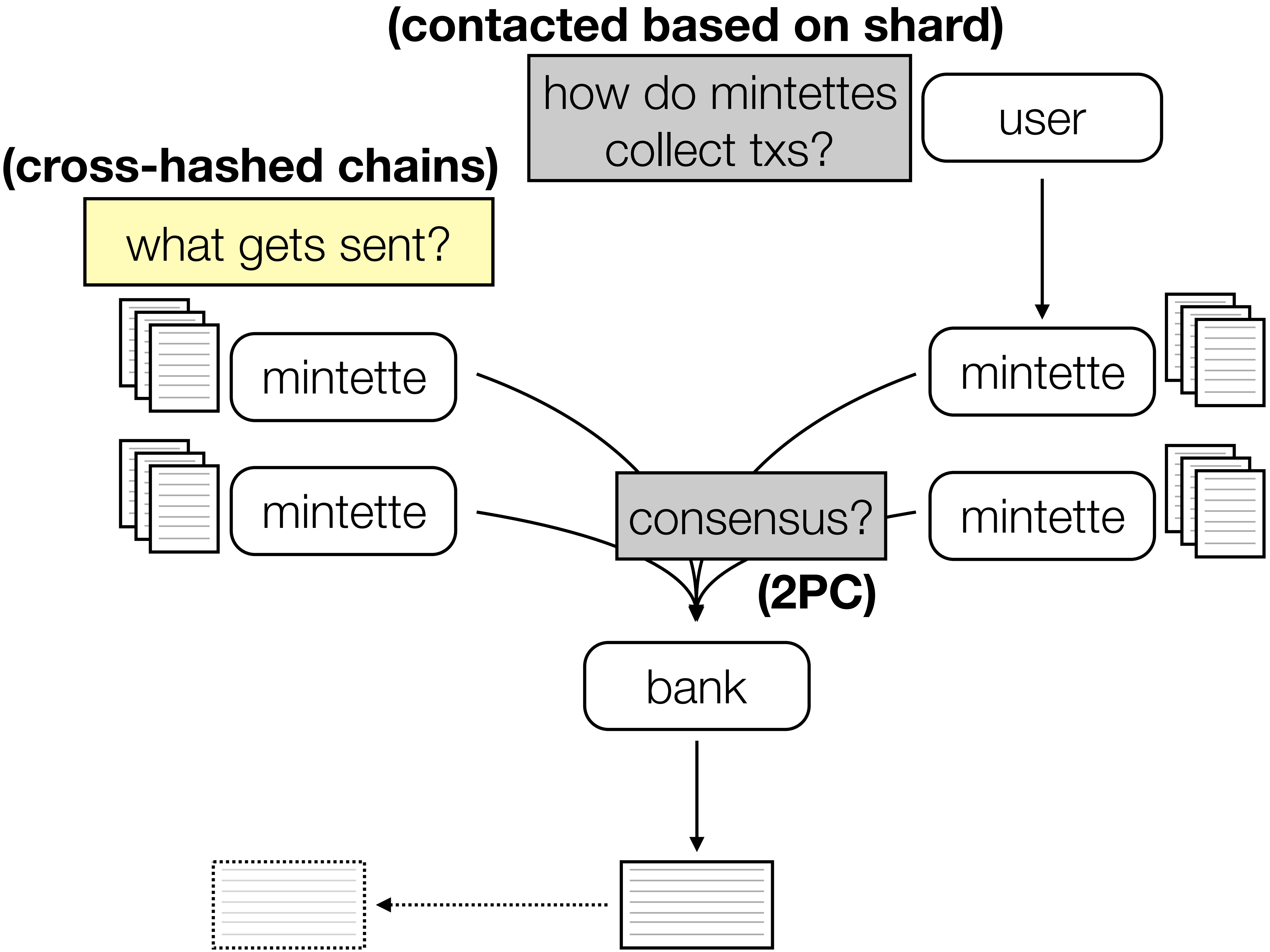
auditability (mintettes can’t cheat without detection)

security properties

✓ no double spending (only “good” transactions get included)

✓ non-repudiation (mintettes are held to their promises)

✓ auditability (mintettes can’t cheat without detection)



(contacted based on shard)

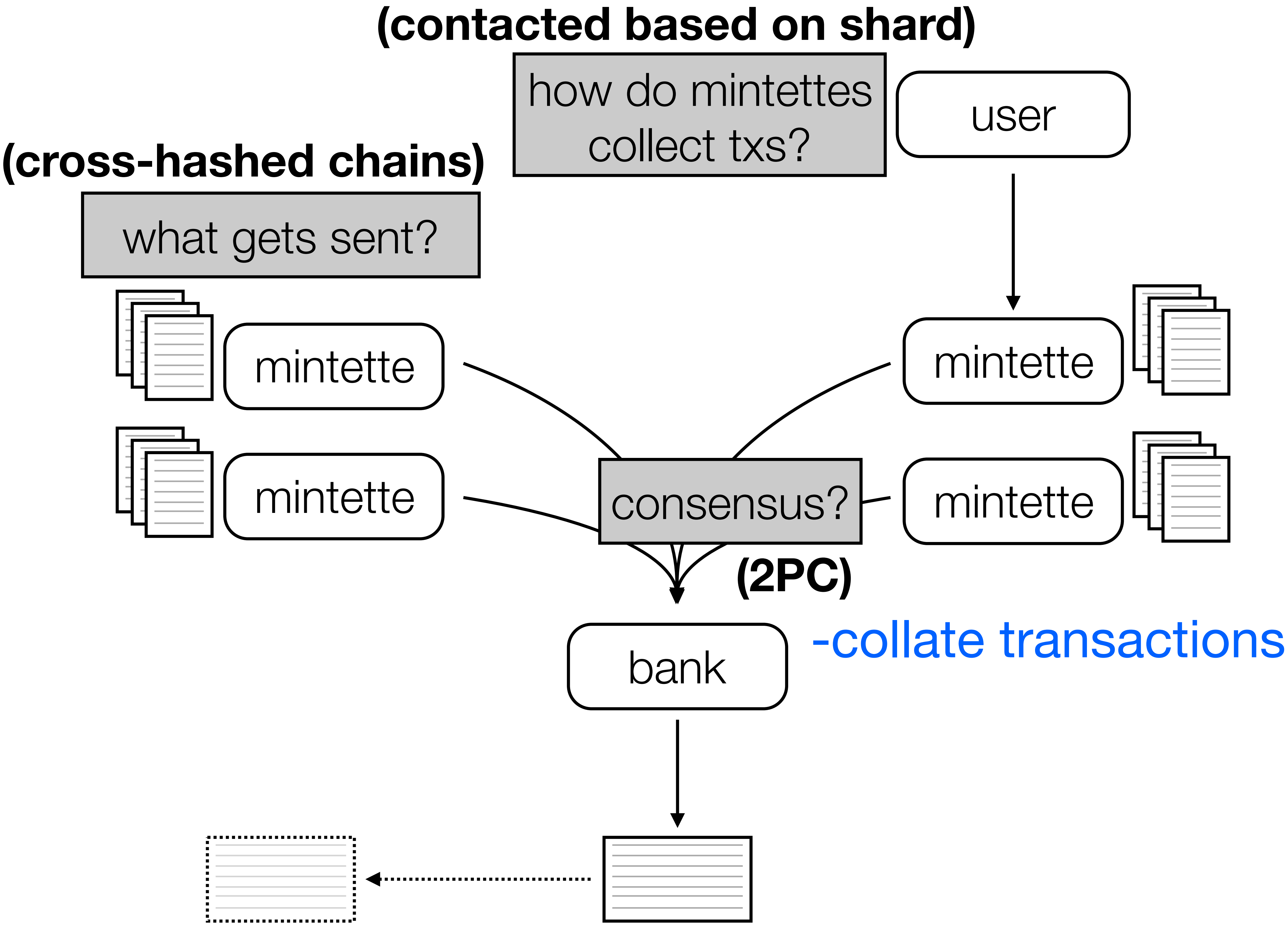
how do mintettes collect txs?

(cross-hashed chains)

what gets sent?

consensus?

(2PC)



(contacted based on shard)

how do mintettes collect txs?

user

(cross-hashed chains)

what gets sent?

mintette

mintette

mintette

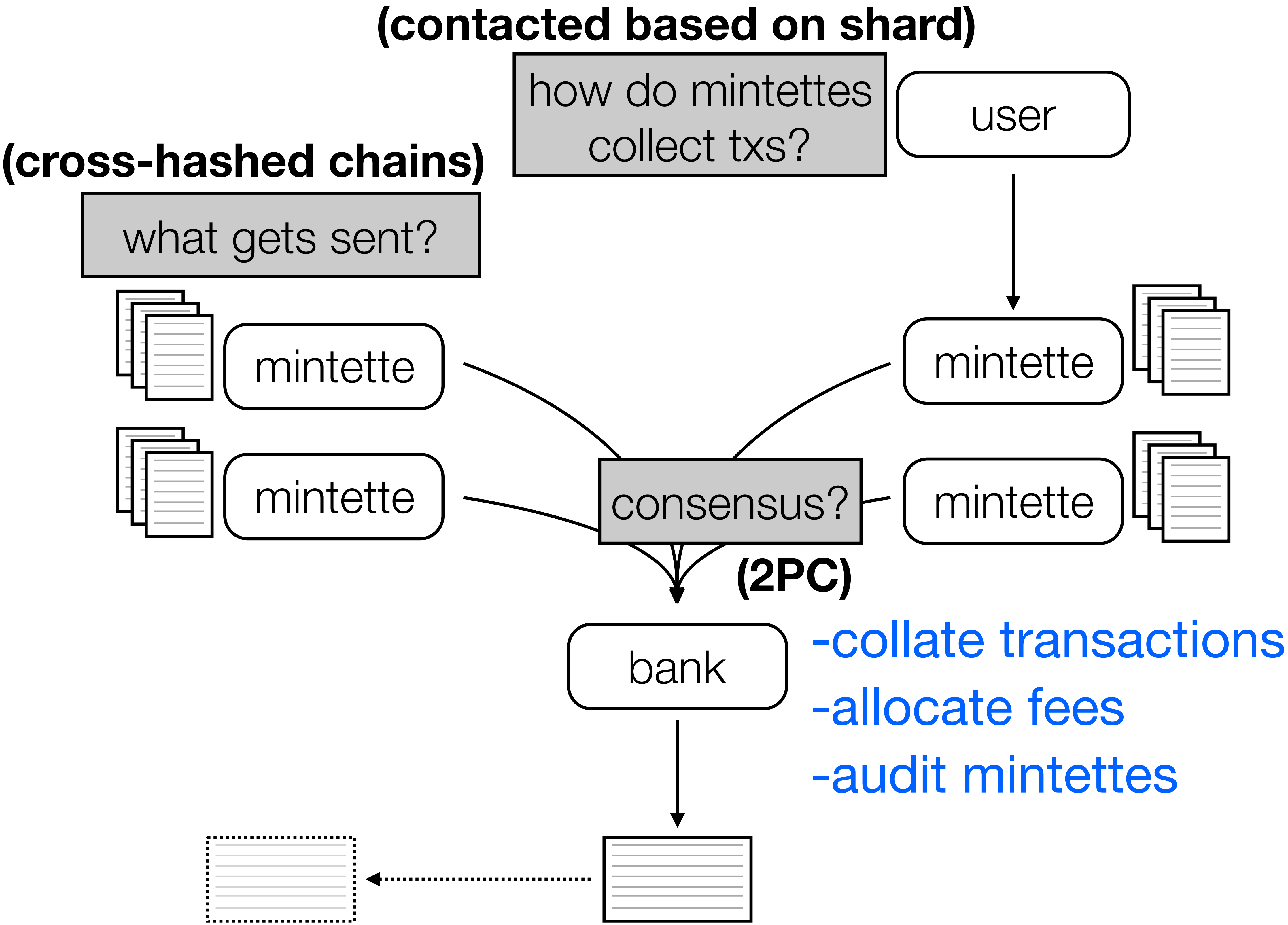
mintette

consensus?

(2PC)

bank

-collate transactions



(contacted based on shard)

how do mintettes collect txs?

user

(cross-hashed chains)

what gets sent?

mintette

mintette

mintette

mintette

consensus?

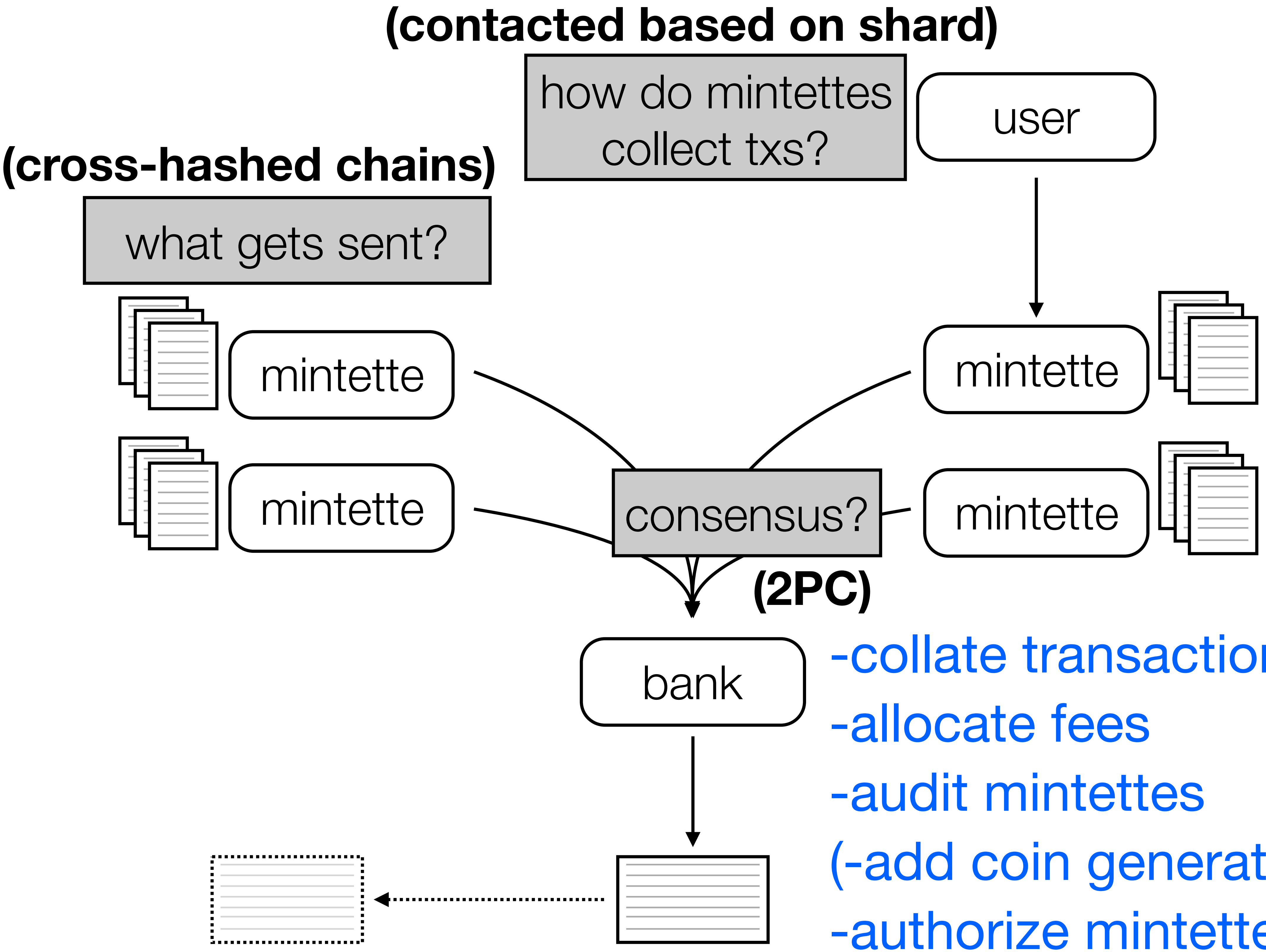
(2PC)

bank

-collate transactions

-allocate fees

-audit mintettes



(contacted based on shard)

how do mintettes collect txs?

user

(cross-hashed chains)

what gets sent?

mintette

mintette

mintette

mintette

consensus?

(2PC)

bank

-collate transactions

-allocate fees

-audit mintettes

(-add coin generation)

-authorize mintettes

		RSCoin	
monetary supply	decentral	central	central
ledger	decentral	distribute	central
transparent?	y	y (or n)	n
pseudonyms?	y	y (or n)	n
computation	high!	low	low

Thanks! Any questions?

		RSCoin	
monetary s			central
ledge			central
transparent?	y	y (or n)	n
pseudonyms?	y	y (or n)	n
computation	high!	low	low