Centrally Banked Cryptocurrencies

George Danezis (University College London)
Sarah Meiklejohn (University College London)
who’s interested in ‘blockchain’?

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 lan 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’?

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

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

3. 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.

4. Blockchain may transform banking, says CBA CEO lan 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
   EvenTimes - 1 hour ago
   Explore in depth (2 more articles)

5. 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 wavres 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

ASX Details Blockchain Strategy in Financial Update

Ascribe announces BigChainDB, a scalable blockchain d…

Linux, IBM

South Korea

KB Kookmin Bank to offer blockchain remitt...
who’s interested in ‘blockchain’?
who’s interested in ‘blockchain’?

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

Russian Central Bank Official Warns Banks of Blockchain...
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
Explore in depth (12 more articles)

How Decentralized Applications Could Bring the Blockch...
who’s interested in ‘blockchain’?

Russian Central Bank Official Warns Banks of Blockchain

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...

Ukraine Embraces Ethereum Blockchain For Election Tra...

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...

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 …

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

Explore in depth (12 more articles)
fully decentralized cryptocurrencies
fully decentralized cryptocurrencies
fully decentralized cryptocurrencies

tx

tx(addr_A → addr_B)
fully decentralized cryptocurrencies

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

"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

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

“mining”

(generate transaction ledger)

(generate monetary supply)

append-only

transparent
fully decentralized cryptocurrencies

\[ \text{tx}(\text{addr}_A \rightarrow \text{addr}_B) \]

“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!
monetary supply: decentral | central | central
monetary supply: decentralized
ledger: decentralized
RSCoin: central
distribute: central
monetary supply: decentral, central, central
ledger: decentral, distribute, central
transparent?: y, y (or n), n
<table>
<thead>
<tr>
<th>Feature</th>
<th>RSCoin</th>
<th>Bitcoin</th>
<th>Traditional Bank</th>
</tr>
</thead>
<tbody>
<tr>
<td>Monetary Supply</td>
<td>decentral</td>
<td>central</td>
<td>central</td>
</tr>
<tr>
<td>Ledger</td>
<td>decentral</td>
<td>distribute</td>
<td>central</td>
</tr>
<tr>
<td>Transparent?</td>
<td>y</td>
<td>y (or n)</td>
<td>n</td>
</tr>
<tr>
<td>Pseudonyms?</td>
<td>y</td>
<td>y (or n)</td>
<td>n</td>
</tr>
<tr>
<td>Feature</td>
<td>RSCoin</td>
<td>Bitcoin</td>
<td>Traditional Banking</td>
</tr>
<tr>
<td>-------------------------</td>
<td>--------</td>
<td>---------</td>
<td>---------------------</td>
</tr>
<tr>
<td>Monetary Supply</td>
<td>decentral</td>
<td>central</td>
<td>central</td>
</tr>
<tr>
<td>Ledger</td>
<td>decentral</td>
<td>distribute</td>
<td>central</td>
</tr>
<tr>
<td>Transparency?</td>
<td>y</td>
<td>y (or n)</td>
<td>n</td>
</tr>
<tr>
<td>Pseudonyms?</td>
<td>y</td>
<td>y (or n)</td>
<td>n</td>
</tr>
<tr>
<td>Computation</td>
<td>high!</td>
<td>low</td>
<td>low</td>
</tr>
</tbody>
</table>
bank (generate monetary supply)
(generate transaction ledger)

mintette

mintette

mintette

bank

(generate monetary supply)
(generate transaction ledger)

mintette

mintette

mintette

user

mintette

mintette

bank

(generate monetary supply)
user

(mintette) (generate transaction ledger)

(mintette)

(mintette)

bank (generate monetary supply)
user

mintette

mintette

mintette

mintette

bank

(generate monetary supply)

(generate transaction ledger)
user

mintette

mintette

mintette

consensus?

bank
what gets sent?

mintette

mintette

consensus?

mintette

mintette

user

bank
what gets sent?

how do mintettes collect txs?

user

mintette

mintette

consensus?

mintette

mintette

bank
how do mintettes collect txs?

what gets sent?

mintette

mintette

mintette

consensus?

bank

user

mintette

mintette

mintette
consensus

user

tx: 1 → 2
Each address is **owned** by a set of mintettes.
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)
“bundle of evidence” contains ‘yes’ votes from majority of mintettes in shard
mintettes check validity of bundle by checking for signatures from authorized mintettes…
...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!

\[
T = \text{set of txs generated per second} \\
Q = \# \text{mintettes per shard} \\
M = \# \text{mintettes}
\]

comm. per mintette per sec = \( \frac{\sum_{tx \in T} 2(m_{tx}+1)Q}{M} \)
simple (adaption of Two-Phase Commit)

scalable!

$T = \text{set of txs generated per second}$

$Q = \# \text{ mintettes per shard}$

$M = \# \text{ mintettes}$

$\sum_{tx \in T} 2(m_{tx} + 1)Q$

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

scales infinitely as more mintettes are added!
each new mintette adds ≈ 75 tx/sec
each new mintette adds $\approx 75$ tx/sec

compared to Bitcoin’s 7
what gets sent?

how do mintettes collect txs?

user

mintette

mintette

mintette

(2PC)

consensus?

bank

mintette

mintette

mintette
(contacted based on shard)

what gets sent?

how do mintettes collect txs?

user

mintette

mintette

consensus?

(2PC)

mintette

mintette

bank


(contacted based on shard)

how do mintettes collect txs?

what gets sent?

(2PC)

bank

user

mintette

mintette

mintette

mintette
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)
(cross-hashed chains)

what gets sent?

where do mintettes collect txs?

(contacted based on shard)

(2PC)

mintette

mintette

mintette

consensus?

user

bank
(cross-hashed chains)

what gets sent?

mintette

mintette

how do mintettes collect txs?

user

mintette

mintette

(2PC)

consensus?

mintette

mintette

bank

-collate transactions
(cross-hashed chains)

what gets sent?

mintette

mintette

mintette

(2PC)

consensus?

how do mintettes collect txs?

user

mintette

mintette

mintette

bank

-collate transactions

-allocate fees

-audit mintettes
(cross-hashed chains)

what gets sent?

mintette

mintette

mintette

(2PC)

consensus?

(user)

mintette

mintette

mintette

(called based on shard)

how do mintettes collect txs?

(bank)

-collate transactions

-allocate fees

-audit mintettes

(-add coin generation)

-authorize mintettes

(called based on shard)
<table>
<thead>
<tr>
<th>Feature</th>
<th>RSCoin</th>
<th>central</th>
<th>central</th>
</tr>
</thead>
<tbody>
<tr>
<td>Monetary Supply</td>
<td>decentral</td>
<td>central</td>
<td>central</td>
</tr>
<tr>
<td>Ledger</td>
<td>decentral</td>
<td>distribute</td>
<td>central</td>
</tr>
<tr>
<td>Transparent?</td>
<td>y</td>
<td>y (or n)</td>
<td>n</td>
</tr>
<tr>
<td>Pseudonyms?</td>
<td>y</td>
<td>y (or n)</td>
<td>n</td>
</tr>
<tr>
<td>Computation</td>
<td>high!</td>
<td>low</td>
<td>low</td>
</tr>
</tbody>
</table>
monetary supply: central
ledger: central
transparency: y
pseudonyms: y
computation: high!