Blockchain Pros, Cons and Tradeoffs

Introductory Lecture Series

Rhys Bidder
rhys.m.bidder@kcl.ac.uk

KBS, QCGBF

September 2023

Disclaimer: Any opinions expressed, errors or omissions should be regarded as those of the author and not necessarily those of KCL, KBS, QCGBF, QCB or BoE.

Outline

Cryptoasset transactions are illegal in many jurisdictions. Do not violate these or any other laws. I am not promoting the use of crypto in countries where it is illegal in any form and these slides are not a promotion of crypto or an invitation to participate in crypto-related activities in such countries. They are purely for educational purposes.

Introduction

Introduction

- So far, we have simply stated what a blockchain is - generally, and with some examples
- The ambition of these platforms can be intoxicating
- **Possibly transformational for society (some might say)**

Introduction

But they are not flawless - there are many drawbacks

- Some may be transitory, some may be deeper

We will discuss some of the challenges blockchain faces, and how they *might* be overcome

The blockchain trilemma

The blockchain trilemma

'The Blochcain Trilemma' $\Rightarrow$ a blockchain system can have only two of the following three properties (or, at least, they have to be traded off against eachother)

1. **Decentralization:** No or limited reliance on a coordinating, dominant, central authority (remember our server-client vs P2P)
2. **Security:** Protocol is robust to malevolent actors or individual units' failures, and reaches appropriate consensus on the evolution of the state
3. **Scalability:** Speed, size, and throughput can expand without prohibitive expense - thus maintain user interest and find wide application

The blockchain trilemma

Quick side note: It's not completely certain that the trilemma actually *is* a trilemma

- We might be able to find a way (lots of people are currently trying) to relax it
- But in recent years it **does** seem to have been a binding constraint

Also, some people (e.g. regulators, policymakers, industry participants?) may prefer centralization

- *Incumbents* might benefit from centralization
- So there is a bigger 'social choice'/debate needed

The blockchain trilemma

We are familiar with a *very* centralized world

- Especially in finance, central banks, regulators - this is how we have done business for a long time!

Many companies/institutions we interact with are hubs for activities, services, storage, permissions...

- **Central Banks:** In reserves / RTGS systems, everything settles through the central bank
- **Web2.0 systems:** Companies control our data, set access policies (recall client-server structure)
- **Banks/custodians:** Protect our information and assets (almost nobody self-custodies)
- **Governments/regulators:** Set laws and rules that (some would argue) infringe upon individual rights

The blockchain trilemma

We rely on **trusted** third parties to behave well

- Disincentives for bad behavior exist
- **But they are costly to implement**
- Sometimes involve other centralized parties anyway

Even honest central parties may be 'single points of failure'

- Their systems might fail (see the recent RTGS failure in the UK - and in 2014)
- They also provide a juicy target for attackers!

The blockchain trilemma

How benevolent or competent are the central authorities varies by country!

- But broadly speaking, decentralizing is a key aspect of the origin of the wave of blockchains

Tellingly, in the first mined Bitcoin block, Satoshi Nakamoto included the following lines in the metadata:

> *The Times 03/Jan/2009 Chancellor on brink of second bailout for banks.*

Hard to overstate how deep the desire for decentralization runs in the blockchain community - certainly in its early years

The blockchain trilemma

Beyond an ideological desire for de-centralization there also are (important) resilience benefits:

- Ledger recorded by multiple parties

$\Rightarrow$ Even if one node goes offline, information on offline node is not ‘trapped’

- Can be reliably sourced from elsewhere, enabling continuity for active nodes
- Also allows rapid recovery for the failed node when reconnects

The blockchain trilemma

Some of us are lucky enough to live in a world that is both **secure** and has **scalable** systems - take the UK for example

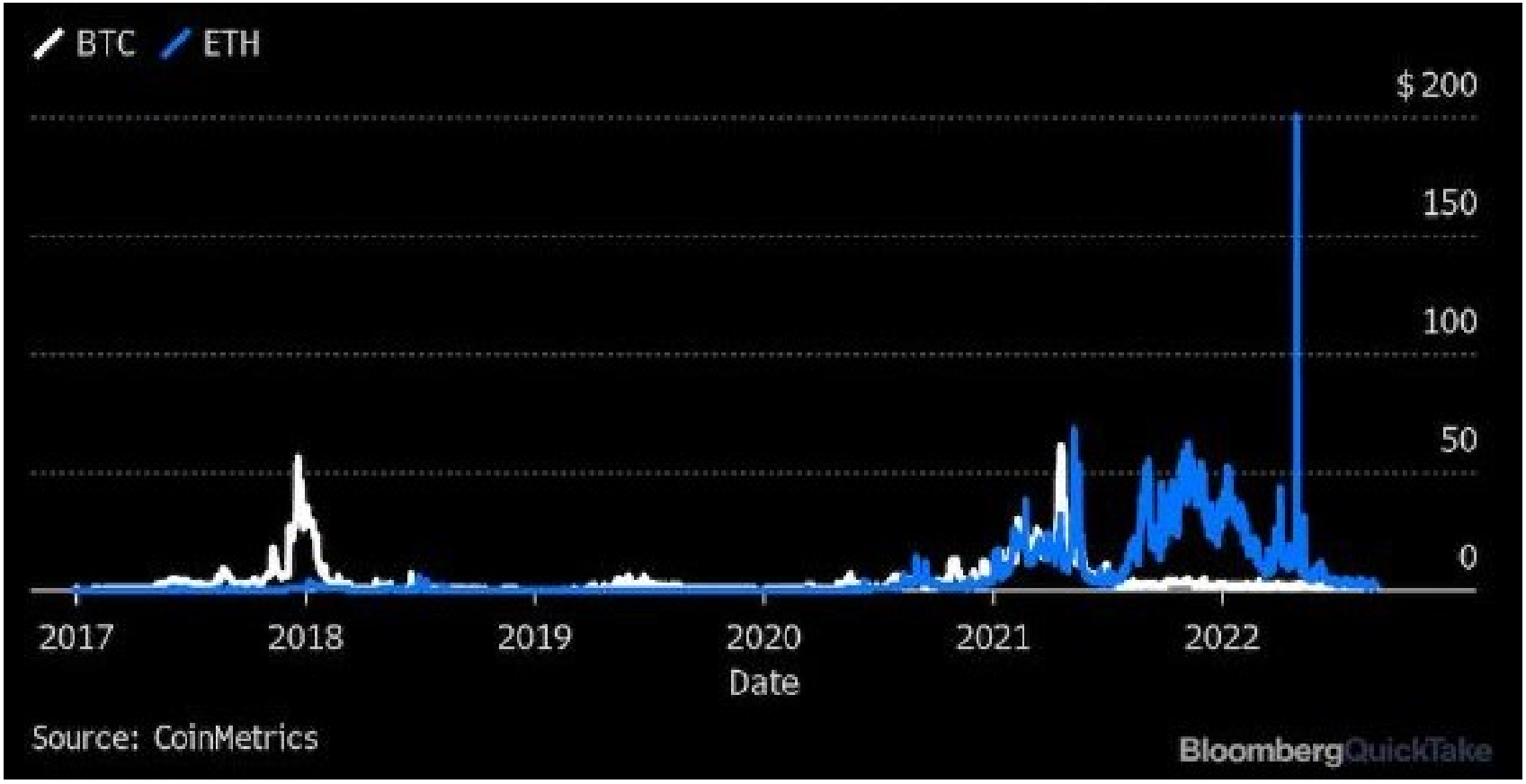
- For all its (many) flaws, the centralized systems I interact with generally run very fast/efficiently
  - Compare Blockchain's 10 minute blocks and 5-7 transactions per second (TPS) with Visa's 24k TPS
- By and large they are very secure
  - Fishing attacks and other attacks aimed at bank *customers* - rather than attacking banks directly
  - Banks' systems are very secure and heavily battle tested

The blockchain trilemma

Simplifying - it is perhaps fair to say that **we currently have security and scalability, but not decentralization**

- Trilemma $\Rightarrow$ need to give up (at least some) security or scalability to decentralize
- Currently, blockchain $\Rightarrow$ severe hit to scalability
- At times Ethereum gas fees have become absurdly high
  - When demand pushes Ethereum to scale - it doesn't
  - Instead, the 'price' rations access
  - Not just the level is a problem, but also volatility

The blockchain trilemma



Bitcoin and Ethereum transaction fees. Source: Washington Post

The blockchain trilemma

Transactions per Second. Note: 2020 numbers. Source: crypto.com

Enhancing scalability

Various approaches have been taken to enhancing scalability

- 'On-chain' changes (layer-1 solutions)
  - 'The merge' moved Ethereum to PoS consensus
  - Not yet enormous benefits seen in TPS **but** is though likely to allow 'sharding' more easily
  - Sharding allows for parallel processing of different bits (shards) of the overall blockchain
  - Nodes will only handle a fraction of transactions
  - Hoped that this and other planned upgrades $\Rightarrow$ 100,000 TPS

Enhancing scalability

Various approaches have been taken to enhancing scalability

- 'Off-chain' changes (layer-2 solutions)
  - State channels
  - Side chains
  - Rollups

Enhancing scalability

State channels are one way of taking computation and multiple transactions off chain

- Off chain, counterparties track transactions back and forth
- Then they only record final net position on the blockchain
- In terms of implementation:
  - Channel is managed by a multisig smart contract on Ethereum.
  - Participants deploy the channel contract and deposit in it
  - They sign a state update to initialize the channel's state
  - Then they can transact **off-chain**
  - To close the channel, participants submit the last agreed-upon state of the channel on-chain
  - Locked funds are distributed based on channel's final state
  - SC also handles disputes
- Especially useful for repeated counterparties, are private, and fast since no decentralized consensus
  - Example: Raiden

Enhancing scalability

Side chains are themselves blockchains (unlike state channels)

- The sidechain is interoperable with a 'main' blockchain
  - Tokens on the sidechain are obtained when tokens on the main chain are locked up
  - Transactions can then be processed on the side chain
  - Ultimately, the tokens can be sent back, in exchange for (now unlocked) original tokens
- Remember, there are various elements of a blockchain that affect throughput
  - Sidechains basically are tuned for speed (and also used for broader interoperability)
- Note, they are (typically) public - unlike state channels
  - Example: Polygon

Enhancing scalability

Rollups are methods by which transaction data are 'rolled up' and taken off chain to be executed/processed

- Recall in 'normal' operation, all nodes in the chain would process the transactions
- Then information is compressed and returned to the main chain

There are two common types:

1. Optimistic rollups
2. ZK-Rollups

Enhancing scalability

Optimistic rollups:

- After executing and compressing transactions, all the information is returned to the chain (in compressed form)
- On return **all the transactions are assumed valid** - hence 'optimistic'
- There is, however, a 'challenge period', during which time a challenge (using a 'fraud proof') can be launched
  - Challenge period adds to latency
- If the proof is correct, the transaction is re-executed
  - There is also a penalty for the 'sequencer' who made the rollup
- After the challenge period, the set of transactions are treated as approved
  - May still be reverted if later found invalid
- Example: Arbitrum

Enhancing scalability

ZK rollups:

- After executing transactions, only a compressed summary of transactions is returned to the chain, accompanied by a zero knowledge 'validity proof'
  - Far less information is sent to the main chain (than implied by the original transactions - i.e. what optimistic rollup sends)
  - This speeds up its operation - and additionally, there is no latency from any 'challenge periods'
- More complex to implement than optimistic rollups
- Example: Polygon zkEVM (beta)

Enhancing scalability

Are these layer-2 - and other - solutions working?

Enhancing scalability

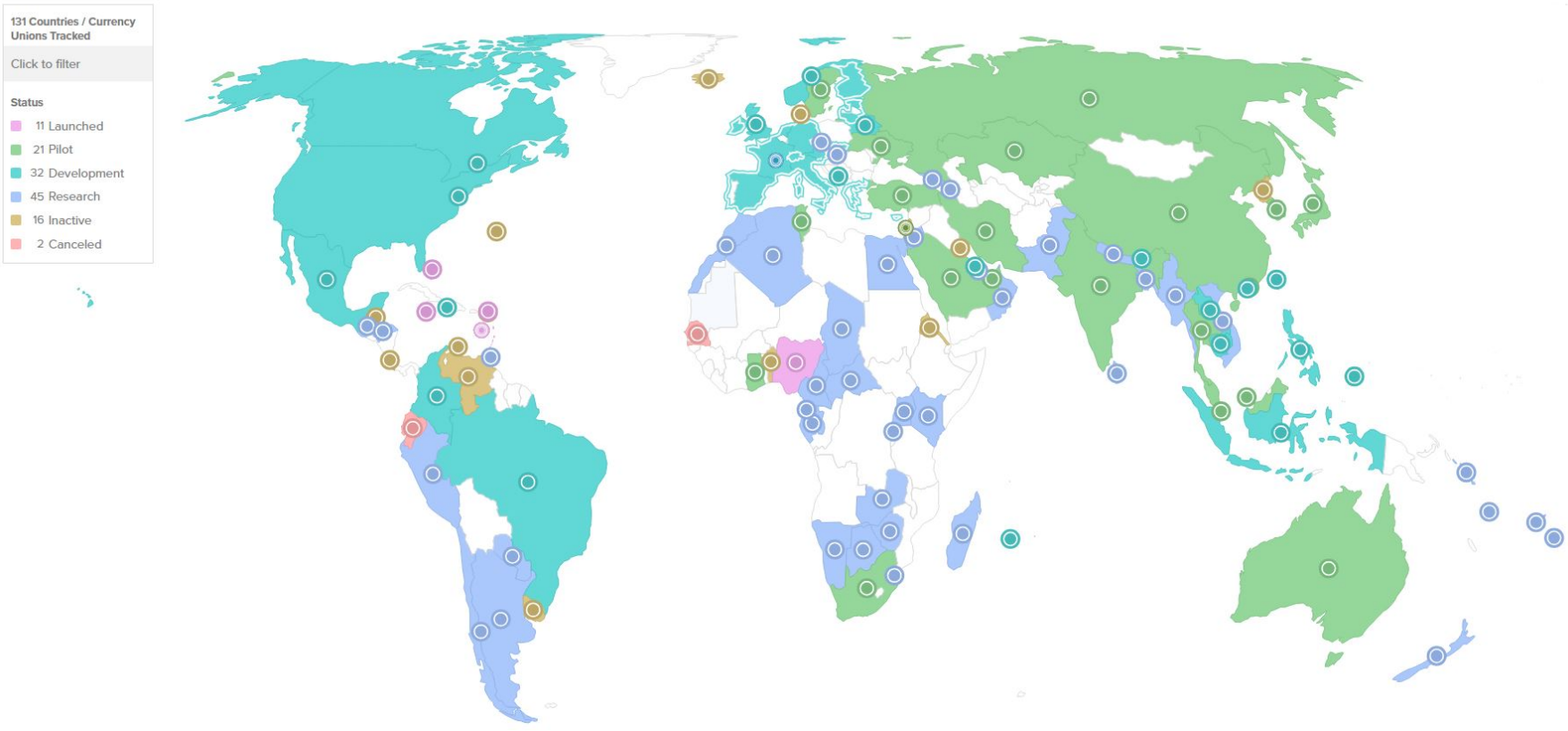
Are these layer-2 - and other - solutions working?

Maybe. . . see here and here

- Gas fees are now very low and didn't recently spike enormously around the launch of Friend.tech (a new 'crypto' social app)

Insights from CBDC

Insights from CBDC



CBDC Tracker. Source: Atlantic Council

Insights from CBDC

- I am going to focus on **wholesale** CBDC
  - No time to cover retail (and the picture there is much more ambiguous)
- wCBDC relates to money used by commerical banks and perhaps other important financial institutions
  - *In a sense*, most countries already have a digital currency of this type - **reserves**
  - But many central banks have been exploring blockchains as possible complements/replacements
- Key applications:
  - Large value payments
  - Systemically important financial market infrastructure (FMI)

Insights from CBDC

Topics to mention briefly, building on CBDC research/pilots:

- Tweaking the blockchain structure
- Where do benefits outweigh costs?
- Privacy/confidentiality and oversight

Tweaking the blockchain structure

Some key desiderata for wCBDC:

- High throughput with immediate finality
- Confidentiality
- Resilience (including CB downtime)

Tweaking the blockchain structure

Some key desiderata for wCBDC:

- **High throughput with immediate finality**
- **Confidentiality**
- Resilience (including CB downtime)

Tweaking the blockchain structure

Some benefits of blockchain come almost for free

- Clearing and settlement in many financial markets is a huge mess, difficult, expensive, manual, inconsistent, slow. . . or all of the above

Blockchains promise enormous savings in important areas

- Automatic reconciliation/compatibility
- Avoiding failed/reverted trades
- Reduced average security spend per node

Tweaking the blockchain structure

High throughput (fast and large volumes) with immediate finality

- Demand consensus protocols such as PoA, pBFT, iBFT
- Less bullet-proof than PoW, PoS - but they are far too slow
- Also, much higher 'trust' within wCBDC networks, compared to the *trustless* assumptions of Bitcoin etc.
  - Relatively small # of institutions with reputations to protect
  - Heavily regulated
  - Bound to need PKI, given systemic importance

Higher trust can perhaps relax the security vs scalability trade-off

Tweaking the blockchain structure

Solutions also often featured node specialization

- Specific roles for (possibly small) groups of nodes
- Helps divide up computation and enhance parallelism
- May further centralize the system - create dependence on a small number of nodes

Unsurprisingly, big banks are not horrified by centralized systems!

- Very different crowd from public blockchain innovators

Tweaking the blockchain structure

The upshot is that wCBDC pilots adopted **permissioned** blockchains

- There are various important companies specializing in such systems (Corda, Consensys, Digital Asset,. . .)
- We will consider one of them - Hyperledger Fabric (HLF)
  - Platforms change rapidly so I base the analysis on this relatively recent text

Tweaking the blockchain structure

HLF is flexible: ‘pluggable’ consensus and ‘identity management’

- Can use a variety of rapid consensus approaches
- Unlike Bitcoin (and even Eth.) finality reached ‘immediately’
- Trials found that wCBDC systems could handle comparable loads to incumbent systems

Tweaking the blockchain structure

HLF is broad in the smart contract languages it supports

- Promotes interoperability (which may be important as other elements of financial system adopt other blockchain implementations)
- Also allows more flexibiliy in the design of its transaction flow and network structure

Tweaking the blockchain structure

HLF's *'execute-order-validate'* workflow reflects specialized roles for nodes

- Too detailed to discuss here but...
  - Proposed transactions are initially sent to an **'endorser'** peer
  - Endorser checks it for technical correctness, evaluates (runs) the transaction, checks it against **'endorsement policy'**
  - If endorsed, sends the transaction to an **'orderer'** (possibly one or several nodes operating under some consensus protocol)
  - Orderer orders the transactions and combines into a **'block'**
  - Sends block to peers who check transactions again, **'commit'** to the chain if legitimate, and broadcast

Tweaking the blockchain structure

Various aspects of this design enhance speed:

- Only small set of endorsers ever execute the transaction
  - Frees up computational resources elsewhere)
- Endorsers can operate in parallel
  - Ordering (at that stage) is not yet considered
- Separation of ordering from execution
  - Allows endorsers to start on new transactions while ordering is occurring
- Agreement among orderers (consensus mechanism) or endorsers (endorsement policies) can be handled differently
  - Depending on where trust is greater
- Economization on communication and data transfer
  - Relative to P2P transmission of 'everything' in main public blockchains

Where do benefits outweigh costs?

CBDC trials continue apace

- Some at an advanced stage

Net benefits from implementing wCBDC *domestically* may be difficult to evaluate

- Many systems are extremely efficient already
- Benefits of blockchains likely depend on network effects
  - Gains larger if there is a private blockchain ecosystem to interact with (but still in infancy)
  - Hard to capture in a pilot or trial (lack of scale)
  - *'Chicken and egg' problem:* Private sector might not invest without a clear signal on CBDC/crypto regulation

Where do benefits outweigh costs?

Net benefits from implementing **international** CBDC systems / interaction seem much clearer:

- Here the technology isn't the question
- International payment (correspondent banking etc.) are horribly inefficient and costly
- The difficulty here will be political / technocratic (harmonizing approaches etc.)
- Several important pilots have been run / are running (such as Inthanon-Lionrock / mBridge)
  - A recent BIS study on various pilots is here

Where do benefits outweigh costs?

		Inthanon LionRock2	Jura	Dunbar	mBridge
Experiment design	BIS Innovation Hub Centre	Hong Kong	Switzerland	Singapore	Hong Kong
	Central banks	HKMA, BoT	BdF, SNB	MAS, SARB, RBA, BNM	HKMA, BoT, PBoC, CBUAE
	Output	PoC	Prototype	Prototype	Prototype
	Type of wCBDC	Intraday	Intraday	Overnight w/o interest	Intraday and overnight
	Currencies	HKD, THB	EUR, CHF	AUD, MYR, SGD, SAR	HKD, CNY, THB, AED
	Transaction type	Simulated	Real value	Simulated	Real value
	Interoperability model	Common platform	Common plat. w. subnetworks	Common platform	Common platform
	DLT	Hyperledger Besu	Corda	Corda, Quorum	mBridge Ledger (MBL)
	Non-resident banks can ... wCBDC	Hold and transfer	Hold and transfer	Hold and transfer (ok from sponsor)	Hold and transfer
	Platform operator	Central banks	Private	Central banks	Central banks
Use cases	Domestic payments	(✓)	(✓)	(✓)	(✓)
	Cross-border payments	✓	✓	✓	✓
	Offshore payments	✓	✓	✓	✓
	Domestic payment in foreign currency	×	✓	✓	×
	PvP[1]	✓	✓	✓	✓
	DvP[2]	×	✓	×	×

✓ = Tested; (✓) = possible but not tested/out of scope; × = not possible;

Recent international CBDC pilots. Source: BIS

Where do benefits outweigh costs?

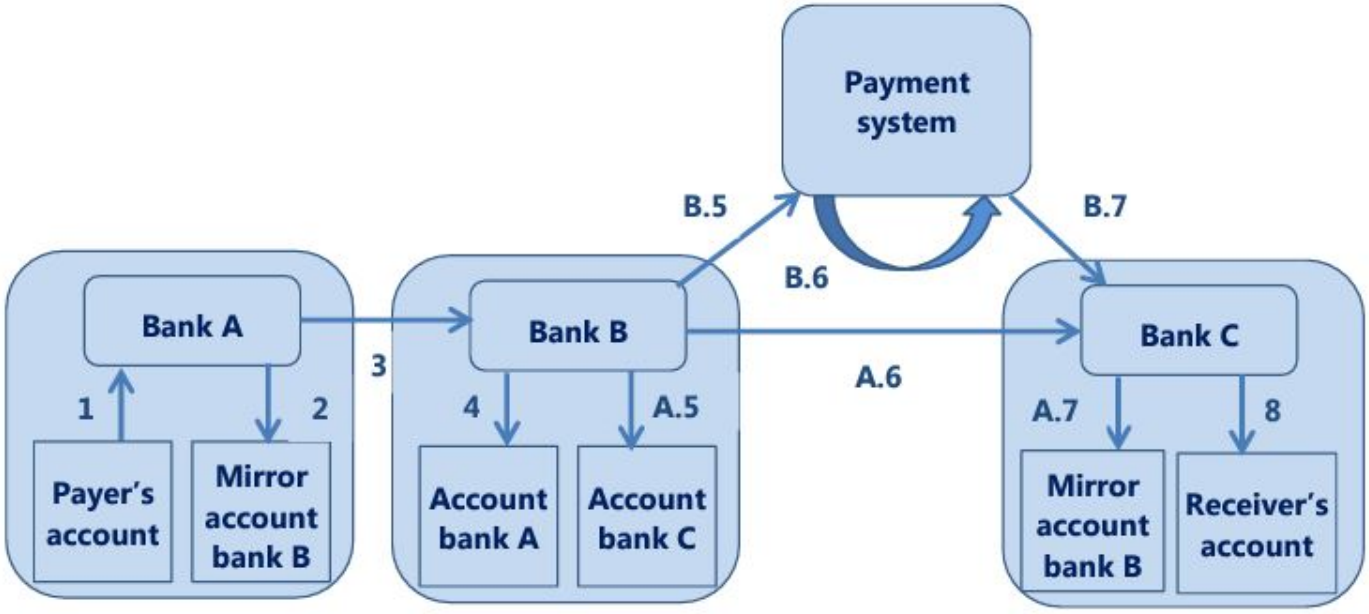
Correspondent banking:

> *correspondent banking requires the opening of accounts by respondent banks in the correspondent banks' books and the exchange of messages to settle transactions by crediting and debiting those accounts*
>
> *a respondent bank enters into an agreement with the correspondent bank in order to execute payments on behalf of the respondent bank and its customers. The respondent bank's customers do not have direct access to the correspondent account, but they transact business indirectly.*

Where do benefits outweigh costs?

- We can consider a payment from bank A to bank C
- Assume in different 'jurisdictions' and thus who do not hold accounts with eachother, or with a common Central Bank
- Assume B is in the same jurisdiction as C and acts as a correspondent bank for A
  - There could be longer chains of banks/jurisdictions than this
  - With each step there would be more manual checking, fees, delays and errors in maintaining consistent ledgers
  - Compliance and various other business logic would not be automated

Where do benefits outweigh costs?



1. Debiting of payer's account with bank A
2. Crediting of bank B's mirror account with bank A, which is kept for accounting purposes
3. Payment message from bank A to bank B via telecommunication network
4. Debiting of bank A's account with bank B (loro account)

A. Use correspondent bank only

5. Crediting of bank C's account with bank B
6. Payment message from bank B to bank C via telecommunication network
7. Debiting of bank's B mirror account with bank C, which is kept for accounting purposes
8. Crediting of receiver's account with bank C

B. Involvement of payment system

5. Payment message from bank B to payment system
6. Settlement via payment system
7. Payment message from payment system to bank C
8. Crediting of receiver's account with bank C

Correspondent banking example. Source: SWIFT Institute

Where do benefits outweigh costs?

Correspondent banking involves extraordinarily costly processes

- See this note from JP Morgan / OliverWyman
- Attempt to calculate possible cost reduction by replacing with international CBDC-based transactions
- Headline number of savings for global corporates is $\$120bn$

Privacy/confidentiality and oversight

- CBDC raises some of the same issues on privacy (or confidentiality) as public blockchains
  - In private blockchains - particularly in finance - confidentiality is paramount
  - In public blockchains, despite pseudonymity, AI/ML can analyse transaction data - maybe combined with external data - to track particular users and possibly identify them
- At the same time, regulators, police and other authorities require oversight and monitoring ability
  - CBDC pilots have tried to balance these concerns
  - Public blockchains also have seen advancements in privacy protection - bordering on complete anonymity

Privacy/confidentiality and oversight

We have seen that public blockchains are typically pseudonymous

- **Naive attitude:** It doesn't matter that the transactions are completely public (we can see them on block explorers) because no one knows who I am

Privacy/confidentiality and oversight

Transactions contain a lot of data that narrows down quite precisely who the user may be

- Times of typical transactions may indicate user's location
  - May also be detected based on location of nodes that receive messages first (in the P2P broadcasts)
- 'Taint analysis' connects addresses based on how correlated their balances are (possibly revealing multiple addresses of the same owner, or business relationships)
  - 'Transaction graph analysis' can also make use of UTXO consolidations to connect addresses
- Transaction *amounts* (directly visible on Bitcoin) may also reveal what is being bought

Even more precise if blended with off-chain data

Privacy/confidentiality and oversight

Many companies have been set up, specifically to sell chain analytics of this sort

- And of course criminals and security services can use these techniques too

Given the fact that the blockchain stores long chains of transactions, identification of the party in a single transaction could expose enormous amounts of information

Privacy/confidentiality and oversight

There are several possible responses:

- Use different addresses for each transaction and multiple wallets for different purposes
  - Some wallet software may help with this
- Use CoinJoin (or some other 'mixer')
  - These pool transactions with other users so that payments come out of the pool, disguising who specifically is paying for what
- There are also cryptocurrencies designed to be 'privacy coins', such as Monero and Zcash
  - As default (part of the basic protocol) transaction amounts, addresses, and transaction histories are hidden
  - Zero knowledge proofs feature prominently in such coins
  - Essentially the only information that needs to be verifiable on the blockchain is the validity of the transaction

Privacy/confidentiality and oversight

Turning to CBDC pilots:

- Zero Knowledge Proofs have featured in some pilots - often connected with Quorum blockchain
  - Quroum is essentially an extended version of Ethereum with enhanced privacy elements

- ZKPs take the place of the underlying sensitive data and can be operated on, verified and shared on-chain
  - They may replace identities with simply proof that the user's identity was valid
  - They may prove that a transaction was made by someone with an adequate balance, without revealing balance or transaction amount to unauthroized parties

Privacy/confidentiality and oversight

CBDC pilots suggest ZKPs may have performance costs / delays

- ZKPs are being heavily researched and are starting to appear in production frameworks
- Likely their efficiency will improve, going forward

Alternative methods that are also causing excitement are:

- **Homomorphic encryption:** Protocols that can operate upon encrypted data without decrypting it
  - Seems like *magic*
- **Trusted execution environments:** Located in special processors, such as Intel's SGX technology
  - Send encrypted information to a counterparty in a way that the counterparty will be unable to decrypt the information, **even if their hardware has**
  - See also R3's Conclave product

Privacy/confidentiality and oversight

There are also network structure responses that permissioned chains have tried:

- HLF's 'private channels' create subnetworks for groups of counterparties
  - A private 'sub' blockchain is associated with the channel
  - Within channels off chain 'private data collections' can also be used to further enhance confidentiality
  - Somewhat similarly, Corda operates using a 'need-to-know' communication model whereby only counterparties to a transactions (and a 'notary') are aware

Privacy/confidentiality and oversight

- Both HLF and R3's corda have implemented some form of single use identities, to allow anonymity and unlinkability of transactions
  - In addition, since it uses UTXOs, Corda also has methods to limit how far back transaction chains can go
  - Ameliorates 'walking the chain' problems where parties to a transaction today, can observe prior transactions between *other parties* that are present in the UTXO chain
- Downsides of these approaches are:
  - Complexity of (especially HLF's) network structure has been commented on in the pilots
  - There is not a single shared ledger, stored by all, in the case of private channels and need-to-know communication
  - Possibly reduces robustness of the system

Privacy/confidentiality and oversight

Many of the privacy enhancing techniques in CBDC trials were designed to nevertheless allow regulatory oversight:

- Often through CB running a notary or monitoring node
- Privacy enhancing techniques could be used to control what aspects of the transaction were visible to them
  - In **Helvetia 1 (2020)** the notary node would not see or validate the *business content* of a transaction
  - In **Inthanon 1 (2019)** the CB could check if a transaction was a double spend, without knowing much else
  - Partial decryption has also be used in **Khokha 1 (2018)** - only elements of the transaction relevant to KYC/AML were revealed

Of course, privacy enhancing techniques in public block chains are not so accommodating of regulators and oversight!