



# Decentralisation in digital finance: possibilities and limits

Hyun Song Shin\*

Economic Adviser and Head of Research, Bank for International Settlements  
London Business School, AQR Asset Management Institute, Insight Summit

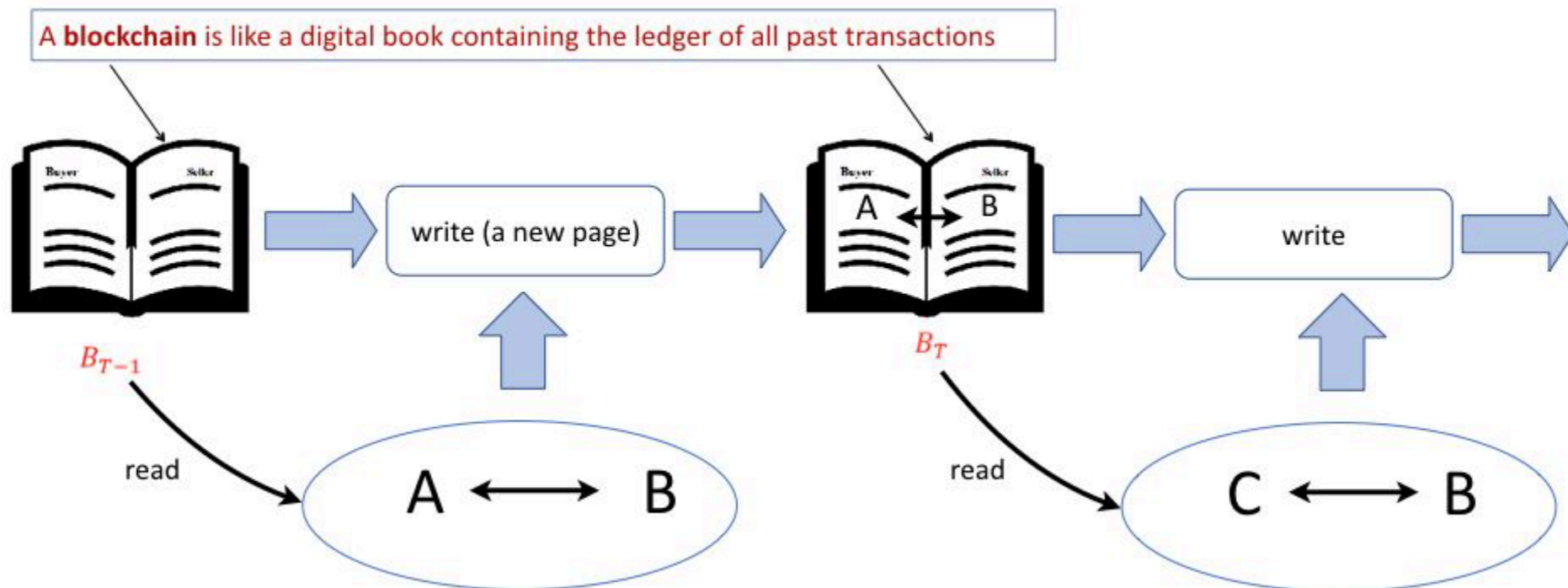
Virtual, 17 November 2021

\*The views expressed here are mine and not necessarily those of the Bank for International Settlements

## Setting the stage: distributed ledgers and the governance of money

- Money is a record of goods sold and of services rendered
  - Alternative to a ledger that records the complete history of all transactions
  - Kocherlakota (JET 1998): “Money is memory”
- Lugging around a universal ledger was a fanciful notion; a theoretical construct, more than a practical one
- But have advances in computing and cryptography brought such a ledger closer to reality?

A universal ledger as a vision for “money as memory” begs the questions of who should update the ledger and how



Source: R Auer, C Monnet and HS Shin (2021), “Distributed ledger and the governance of money”, *BIS Working Papers*, no 924, January.

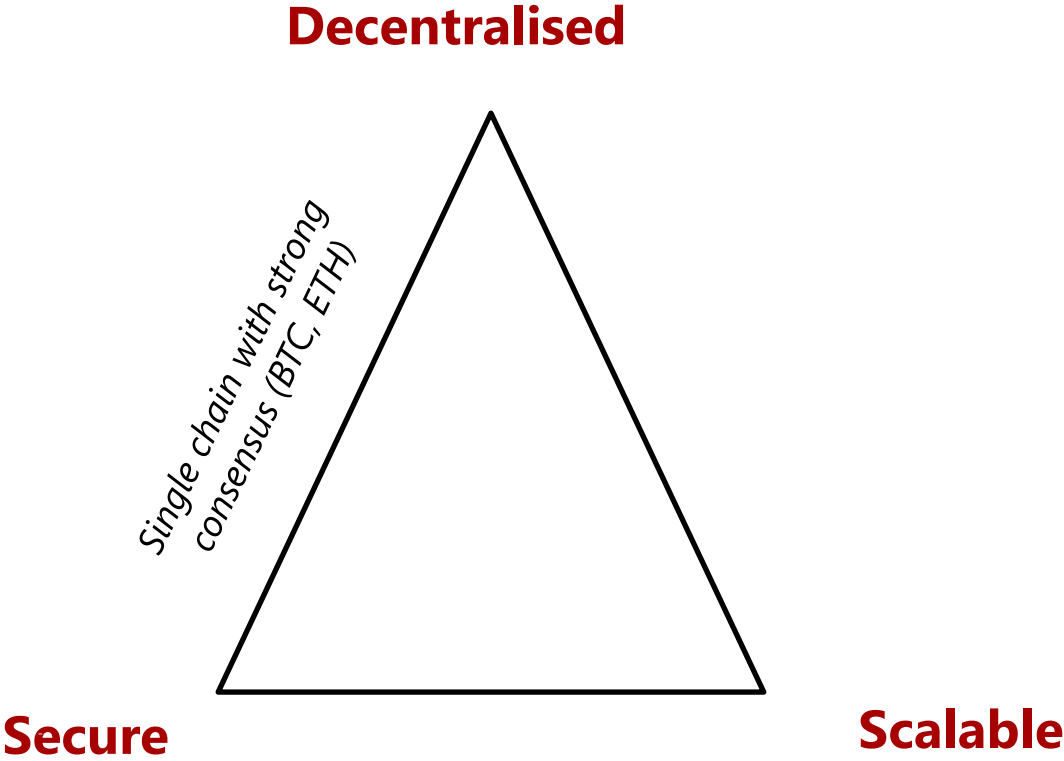
A universal ledger as a vision for “money as memory” begs the questions of who should update the ledger and how

- Rationale for blockchain appeals to governance benefits
  - Checks and balances on the integrity of the system by necessitating consensus
  - No need for trusted entity like the central bank
  - No need for intermediaries like commercial banks or broker-dealers
- What are the costs going in this direction? What are the tradeoffs?

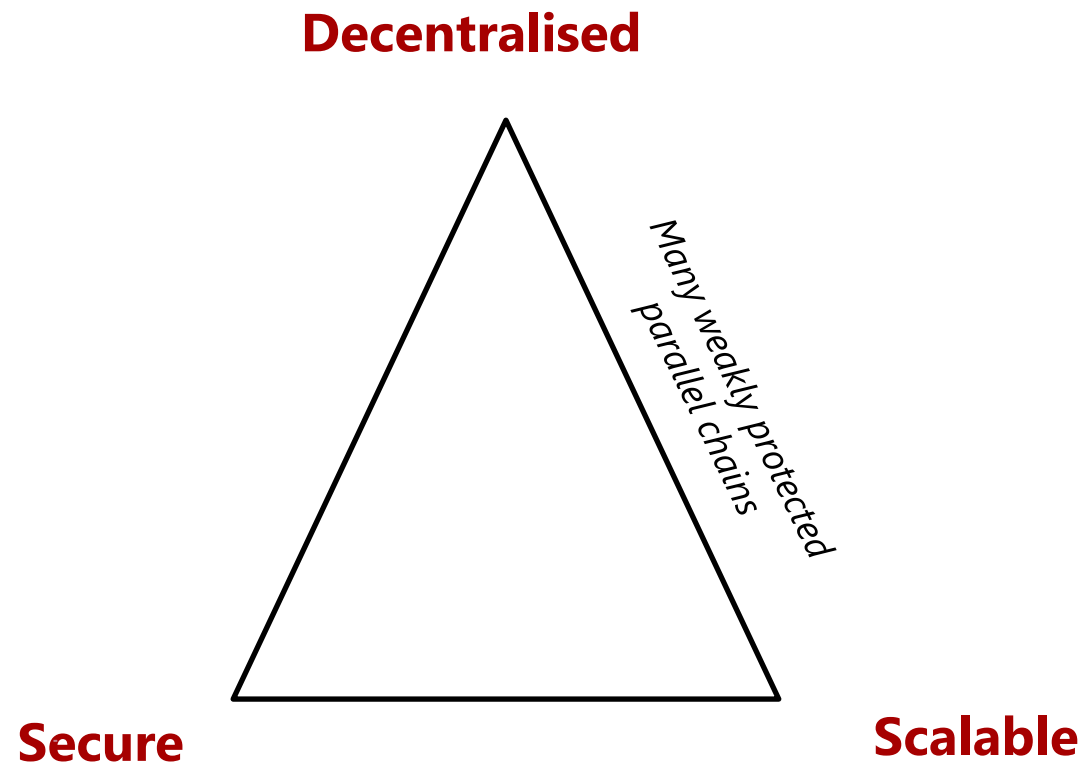
Auer, Monnet and Shin (2021) “Distributed ledgers and the governance of money”  
BIS Working Paper 924 <https://www.bis.org/publ/work924.htm>



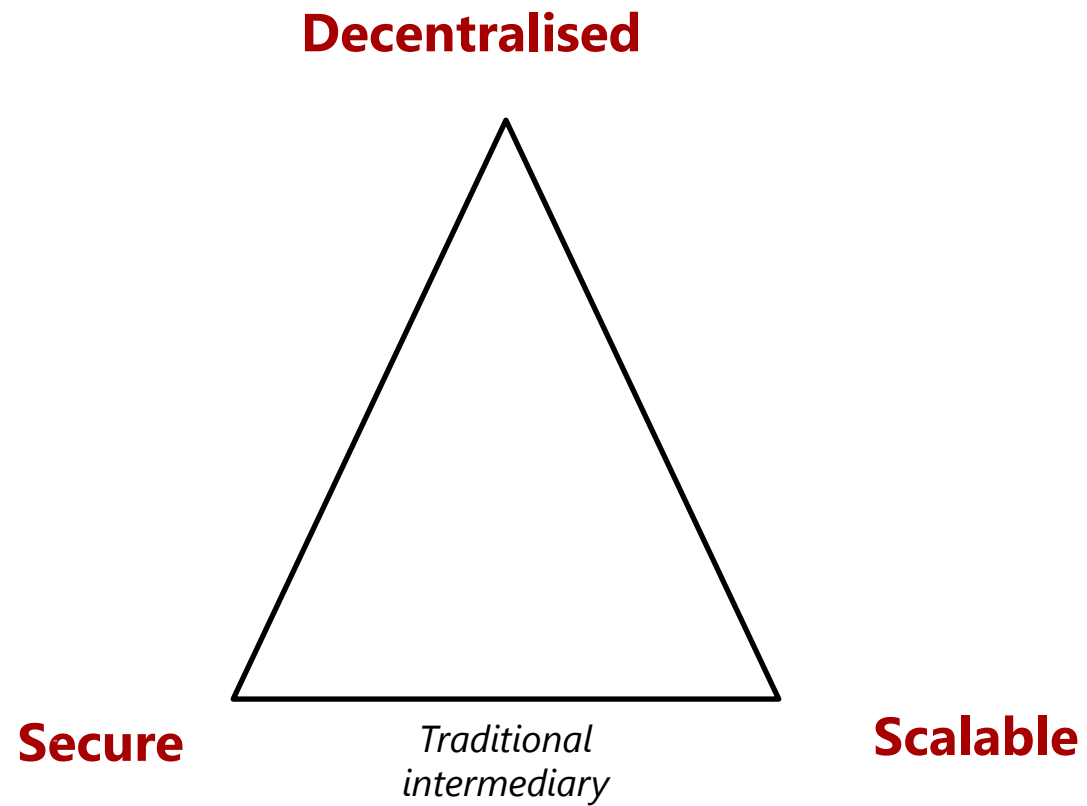
# Buterin's trilemma



## Buterin's trilemma



## Buterin's trilemma



## Key tradeoffs

- Decentralisation is motivated by governance benefits
  - Checks and balances of the community as a whole
  - Avoid capture one or a few powerful entities
- But the price to be paid for this better governance is the lack of scalability
  - Buterin's trilemma

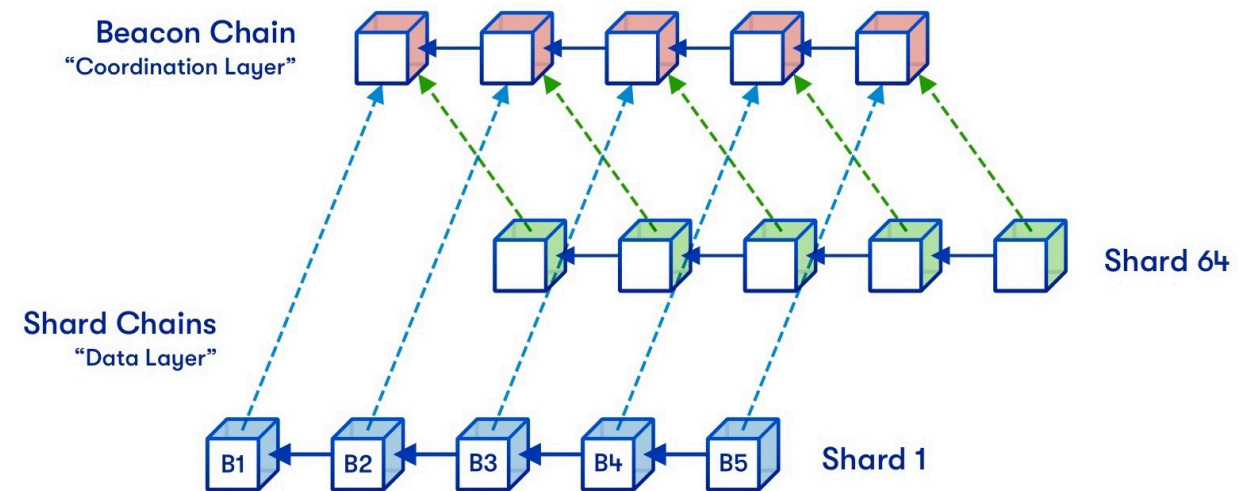


## Two notions of scalability

1. Time needed to reach consensus on every decision due to technological limits.
  - This is about the laws of physics
2. Incentive structure to maintain the protocol as an equilibrium of a game
  - This is about the laws of economics
  - Incentive compatibility and self-sustaining nature of decentralised arrangements

## Sharding may address physical limits but economic limits need to be examined, too

- Sharding is akin to parallel computing and may resolve technical scale limitations
- However, **impact on incentive limits are unclear**
  - Auer et al. model a DLT without scale limitations, but still find the volume of trade to be limited as a higher volume of trade requires higher rents for the validators

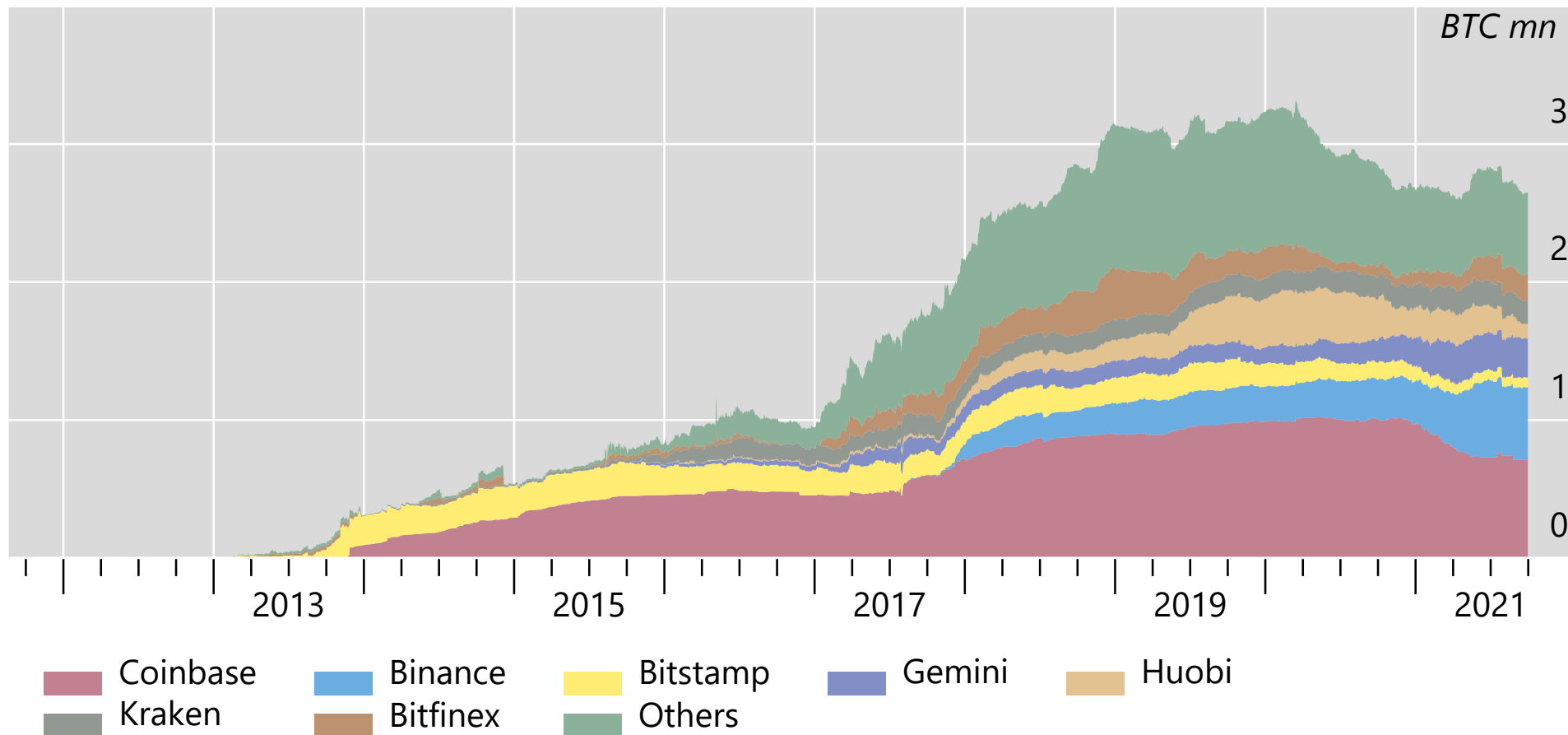


Source: V Buterin (2021), "Why sharding is great: demystifying the technical properties", April.

## Example 1: Makarov and Schoar (2021) "Blockchain analysis of the Bitcoin market"

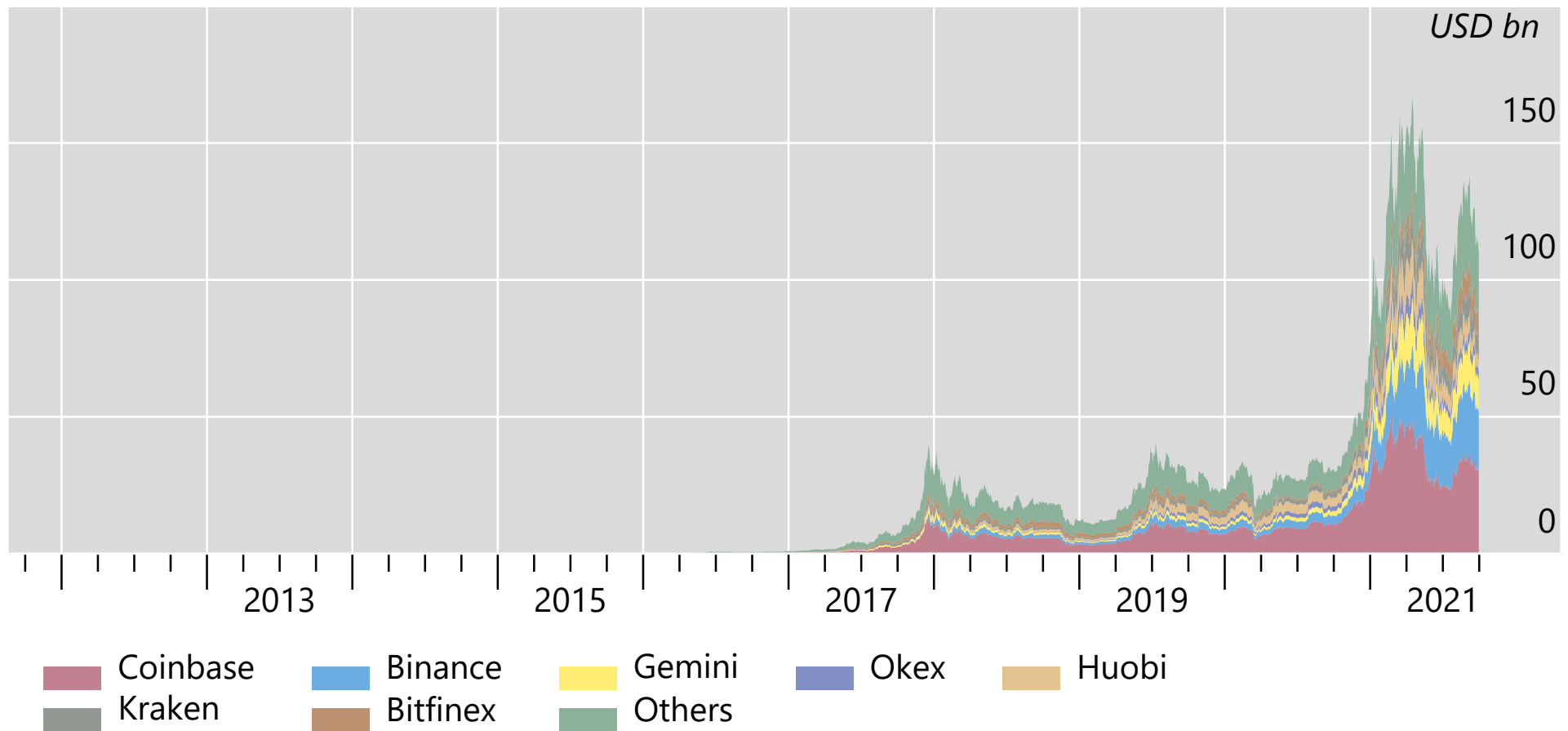
- Bitcoin transactions are mostly tied to investments, not monetary exchange
  - 90% of transactions are noise designed to mask user identity; among "real" transactions, 75% are linked to exchanges, on-line wallets, etc.
  - Consistent with survey-based findings in Auer and Lucas-Tercero (2021); bitcoin holders tend to be young, male, well-educated and do not distrust traditional financial institutions
- Exchanges are the new intermediaries
  - Exchanges are the focal nodes, act as investment vehicles holding customer assets in cold wallets
  - Large fraction of transactions are between exchanges; high concentration in ownership and mining (top 1000 investors control  $\simeq$  3 million BTC; top 10,000 control  $\simeq$  5 million BTC; top 10% of miners control 90% of mining capacity, top 0.1% (around 50 miners) control 50% of mining capacity)

## Total number of bitcoin held in custody by main exchanges



Sources: Auer et al, forthcoming; Glassnode.com.

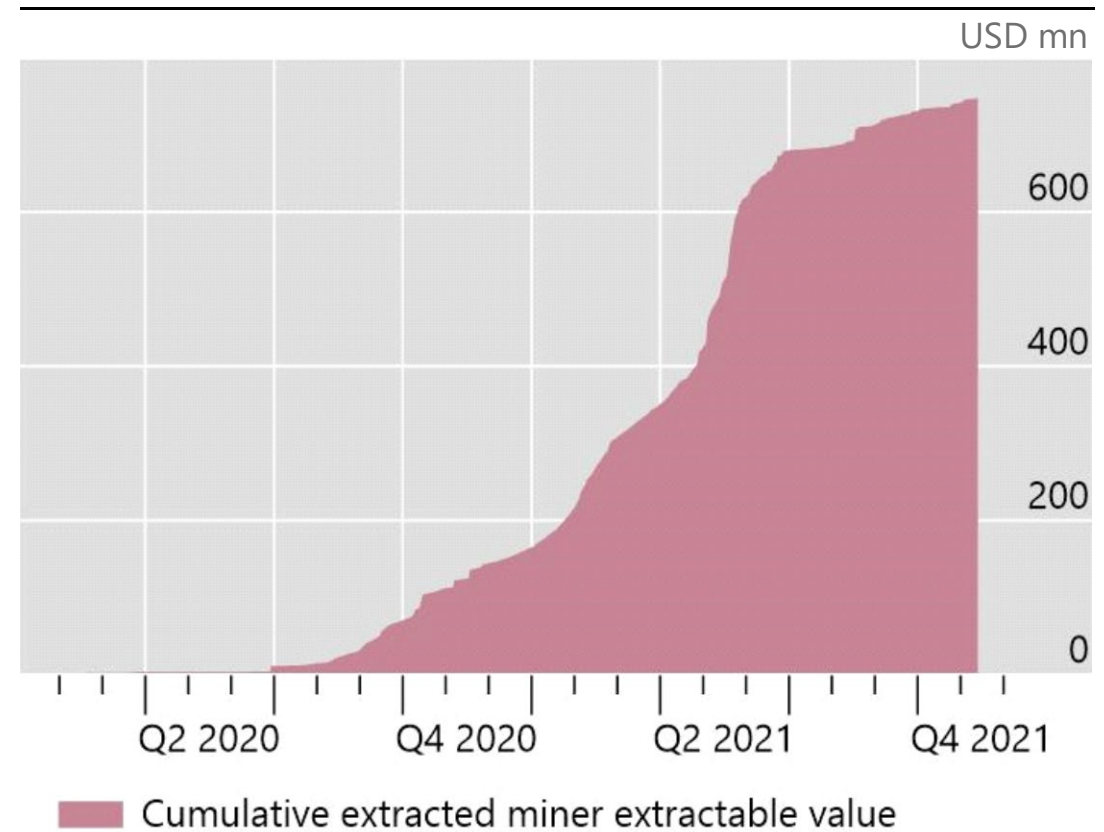
## Total amount of bitcoin held in custody by main exchanges, denominated in USD



Sources: Auer et al, forthcoming; Glassnode.com.

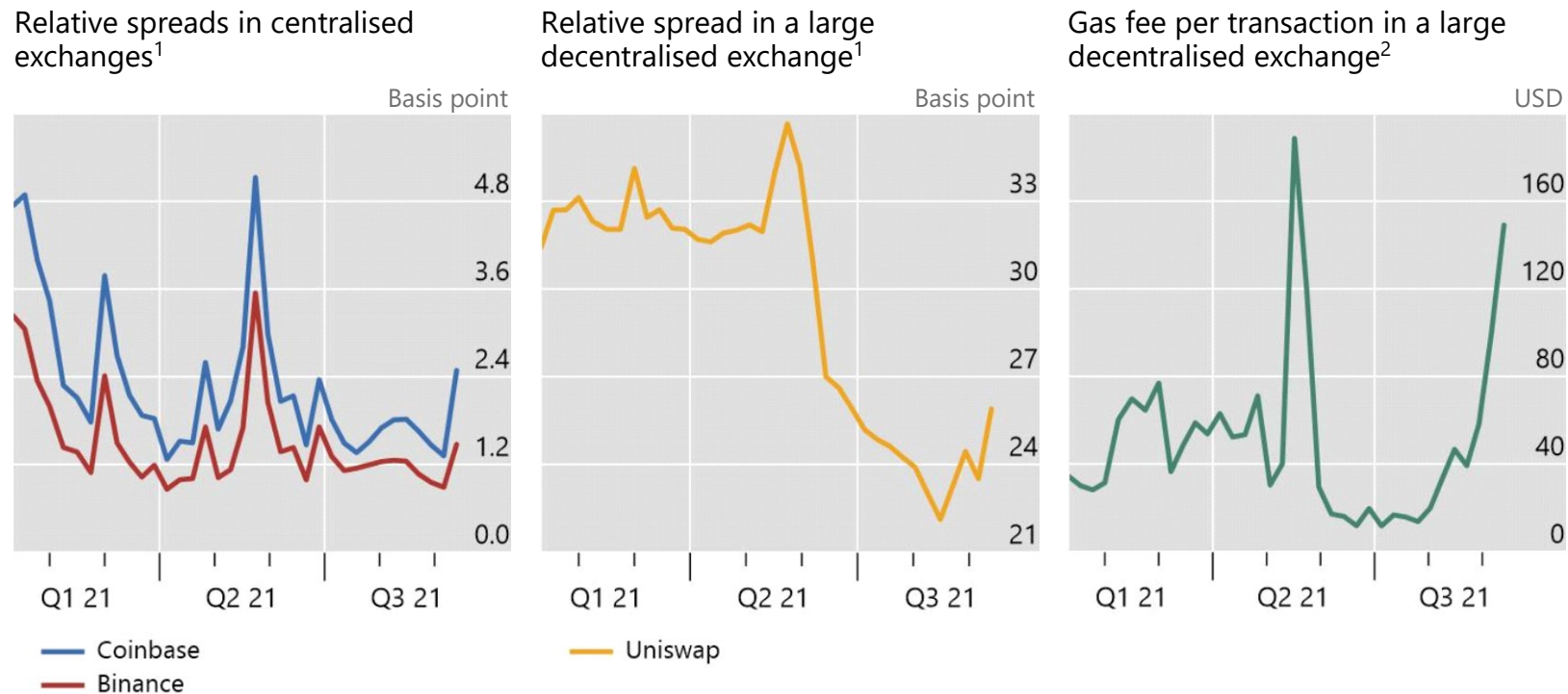
## Example 2: Miner Extractable Value (MEV)

- **MEV is a measure of the profit a miner/validator can make through their ability to include, exclude, or re-order transactions within the blocks they add to the blockchain.**
- **Example:** a validator spots an arbitrage opportunity on a DeFi exchange and submits a transaction to capture this opportunity; instead of processing the transaction, the validator front runs the trade by including his own trade in the block



Source: [MEV-Explore v0](#).

## Example 3: trading costs in decentralised exchanges



<sup>1</sup> Relative spread is defined as  $2 \times (\text{ask price} - \text{bid price}) / (\text{ask price} + \text{bid price})$ . This is calculated for USDT-ETH in Coinbase, Binance and Uniswap. <sup>2</sup> Gas fees are payments made by users to compensate miners for the computing energy required to process and validate transactions on the Ethereum blockchain. The time series is calculated for USDT-ETH in Uniswap.

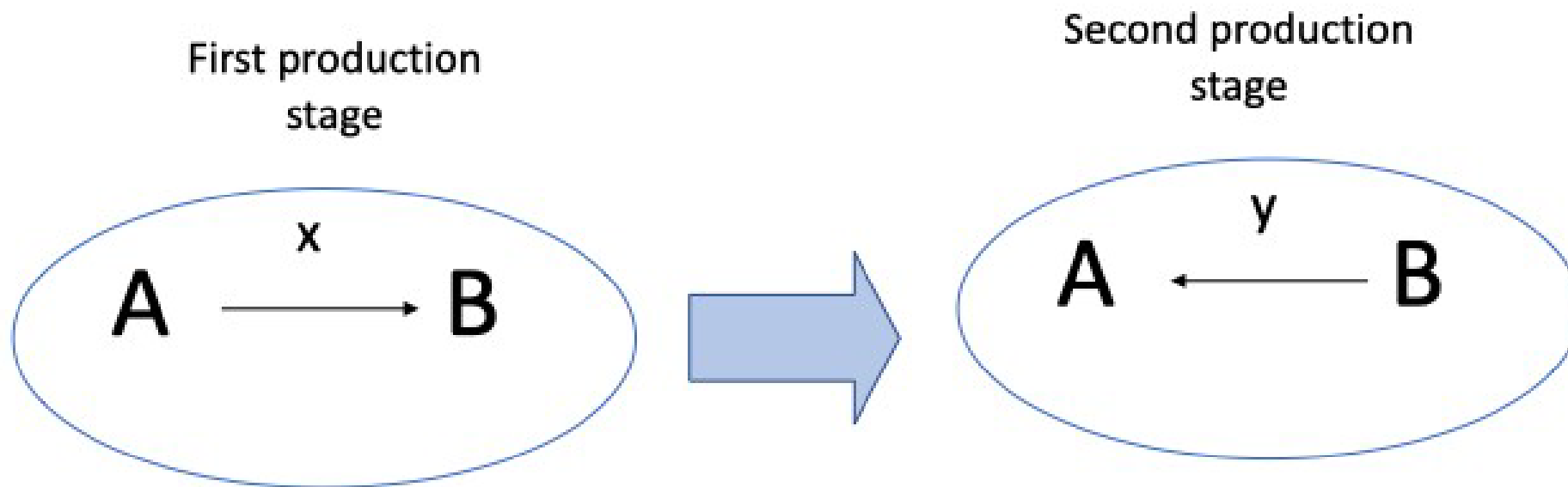
Sources: Binance; Coinbase pro; Bitquery; authors' calculations.

## Auer, Monnet and Shin (2021)

- Optimal design of distributed ledger balancing scalability, security, and decentralisation
- To keep system self-sustaining, the validators need to be rewarded:
  - The payoffs need to be such that following the protocol is an equilibrium of the game.
- Coordination can be enforced in equilibrium provided that the rewards to validators are high enough, but we know from the global games literature that coordination is fragile
  - Rationale for decentralisation is for its governance benefits but it entails rents to validators

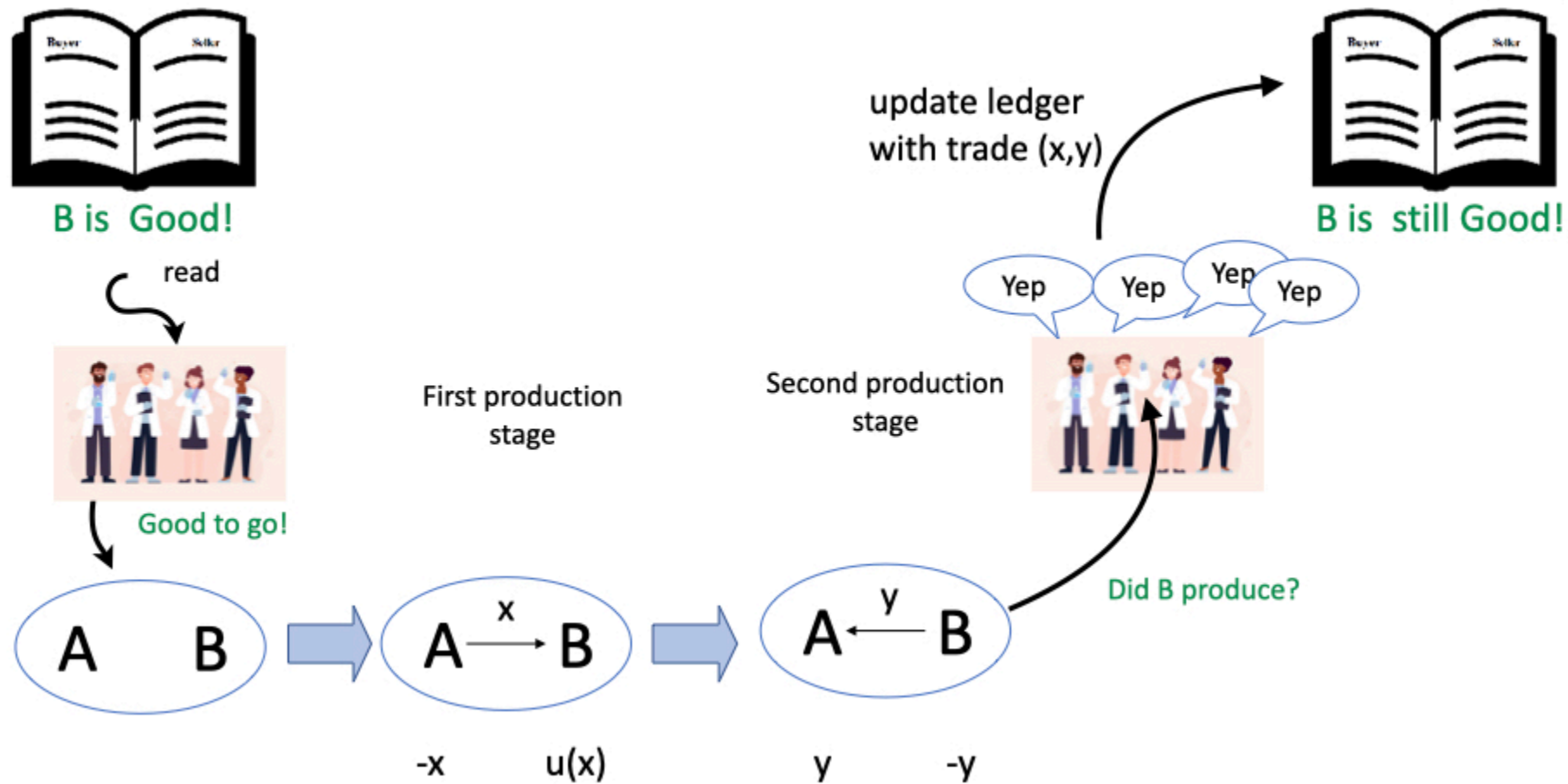


## Economic exchange involves overcoming trust problems



Source: R Auer, C Monnet and HS Shin (2021), "Distributed ledger and the governance of money", *BIS Working Papers*, no 924, January.

## What incentives do validators need to update the ledger?



Source: R Auer, C Monnet and HS Shin (2021), "Distributed ledger and the governance of money", *BIS Working Papers*, no 924, January.

## Key takeaways

- **Technology will only take us so far** along the route to decentralisation
  - The incentives of participants in DLT and DeFi are key
- Specifically, we find that:
  - Centralised ledger is superior, unless **weaknesses in the rule of law and contract enforcement necessitate a decentralised ledger**
  - If there is a case for decentralisation, **market design and ensuring incentives of the validators matter**
    - Supermajority role strictly below 1 facilitates consensus
    - “Participation economy” – the users of the system should act as validators
    - Optimal number of validators, their fees, and voting rule depend on how forward looking agents are



## Conclusion

- DeFi and distributed ledger technology are part of the move toward decentralisation.
  - They bring **benefits in terms of governance, with checks and balances** that maintain the integrity of the system as a whole; but the price to be paid has been **lack of scalability**
- There are proposed solutions to the lack of scalability, but they have been various ways to **bring back intermediaries in some way, and to skip on-chain activity**.
  - Can we really have our cake and eat it too?
- For decentralisation to work, the validators need to be rewarded; how much are the high rewards just a reflection of the **inflows of new users**?
- Can we maintain **strong governance when the systems mature and rents dissipate**?