Deutsche Bank
Research

Scalability of cryptocurrencies

Jochen Möbert
jochen.moebert@db.com
+49 69 910 31727

April 2018

Why do I talk about scalability?
Definition of scalability?

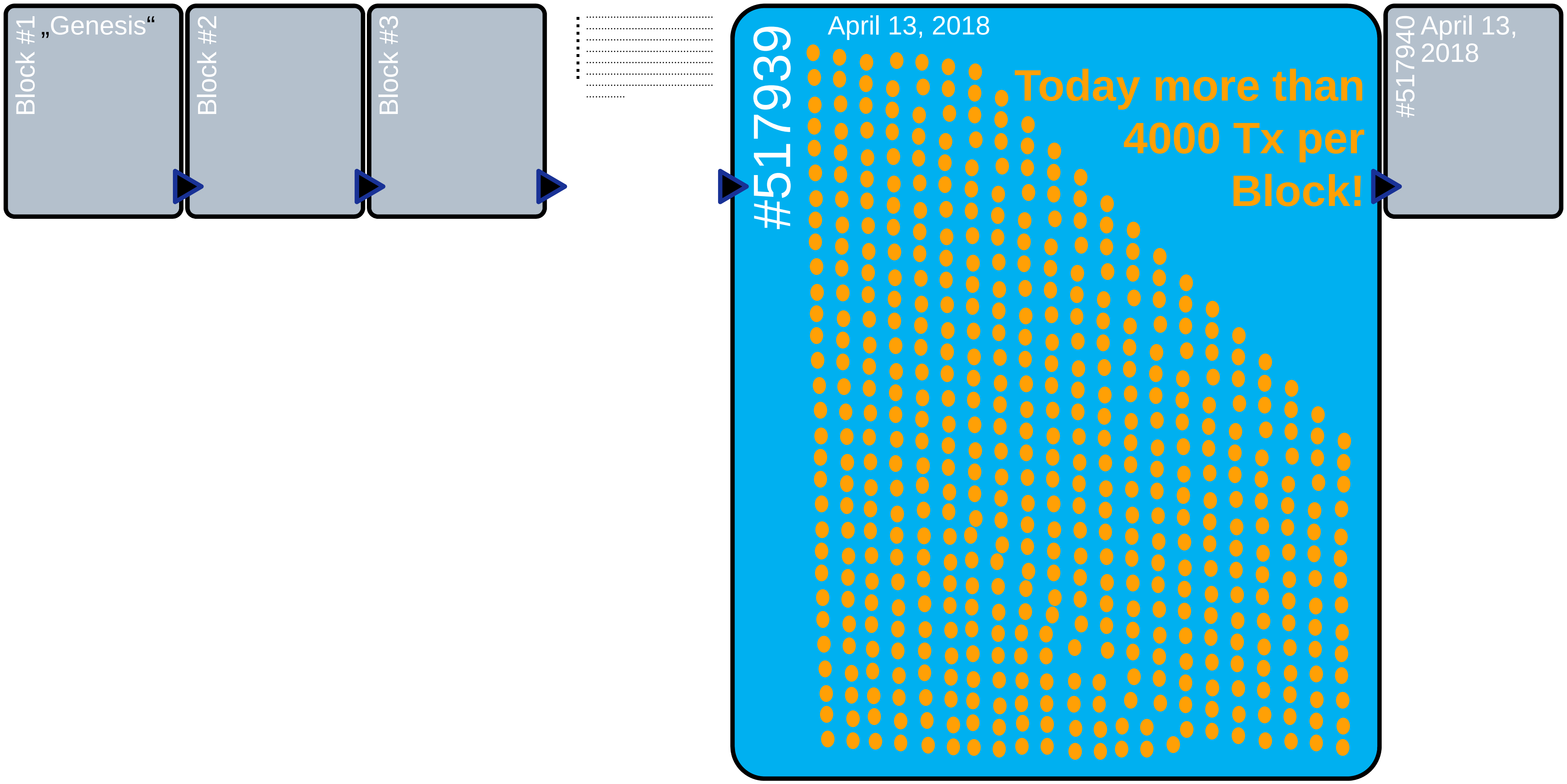
There are two future developments which could really challenge traditional industries and institutions?

- ❑ A completely decentralized crypto infrastructure
- ❑ Cryptocurrencies solve the scalability issue

Scalability has two dimensions

- ❑ Throughput of transactions
- ❑ Latency in the distributed network

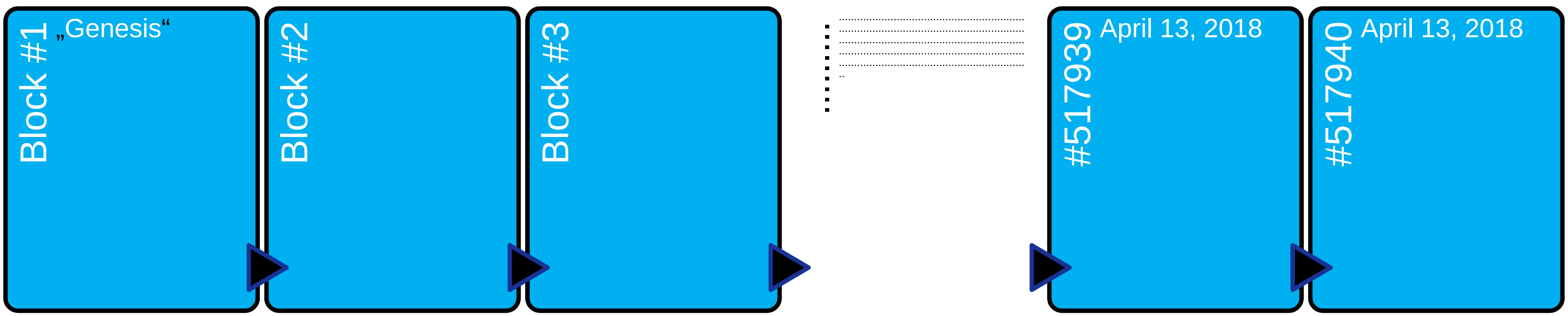
What does scalability of cryptocurrencies mean? Example: Bitcoin



- ❑ **Every 10 min (=600sec) a block is printed**
- ❑ **4200 TPBlock / 600 sec ~ 7 TPS**

TPBlock = Tx per block, TPS = Tx per second

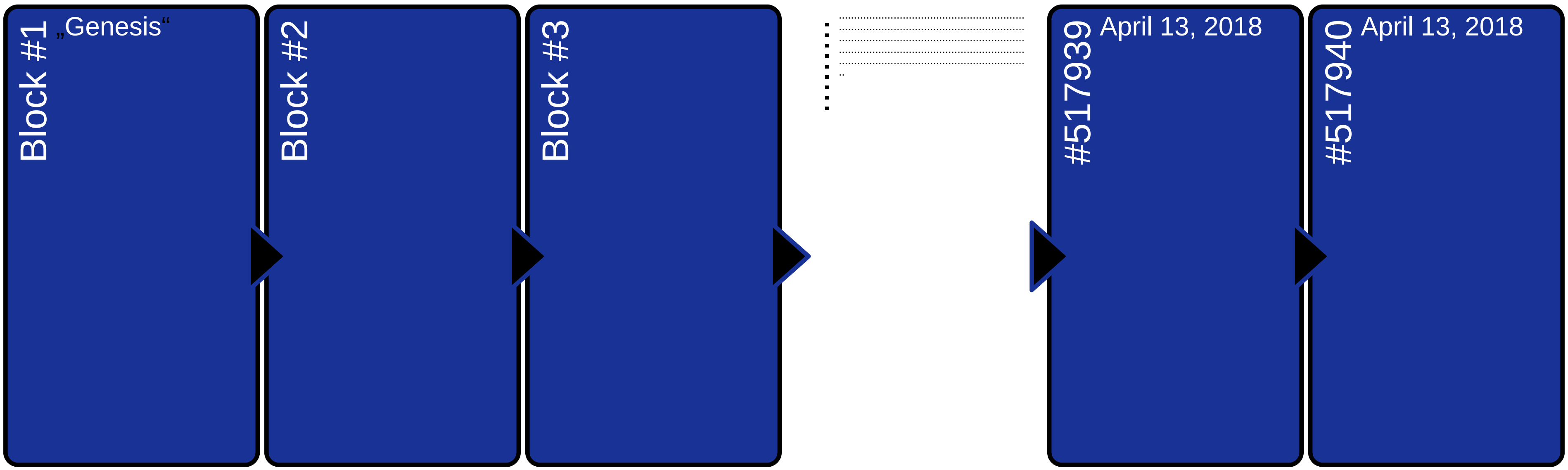
Scalability of cryptocurrencies:
How many transactions can Bitcoin (BTC) handle?



~ max. 7 TPS

Bitcoin does not scale!

Scalability of cryptocurrencies: Increase block size
Is Bitcoin Cash (BCH) different?



~ Max. 60 TPS

Moreover, larger blocks imply
Tradeoff between scalability
and de-/centrality

Bitcoin Cash does not scale!

Interim conclusion

Today, neither Bitcoin nor Bitcoin Cash nor any other decentraliced cryptocurrency scales.

Moreover, no. of Tx handled clearly below technological limits.

Centraliced/traditional payment systems are much more efficient

- ❑ VISA allows for several 1,000 TPS
- ❑ VISAs technological limit could be above 20,000 TPS

Will cryptocurrencies scale in the future?

Key debate in 2017

(1) Bitcoin scaling debate: Increase the blocksize

Will cryptocurrencies scale in the future?

(2) Lightning network

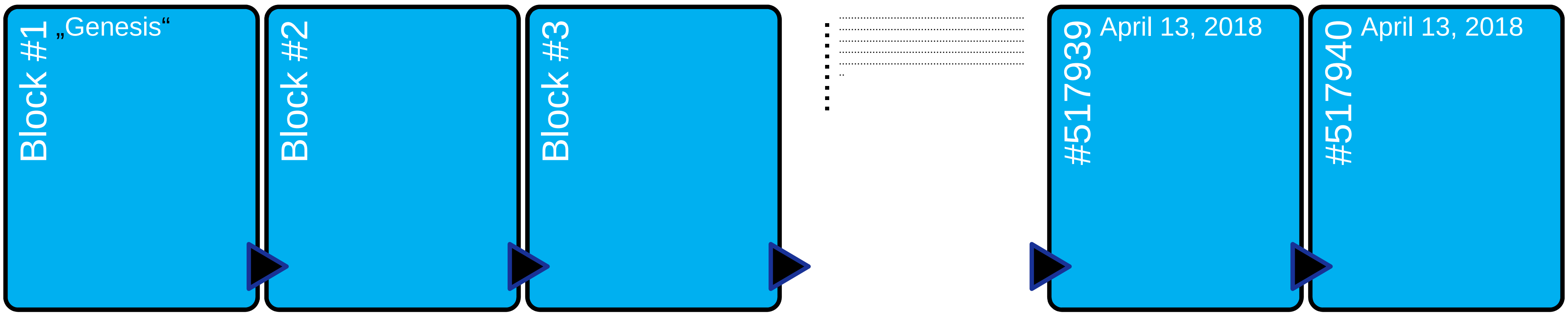
(3) From Blockchains to Blocktrees

Further proposals

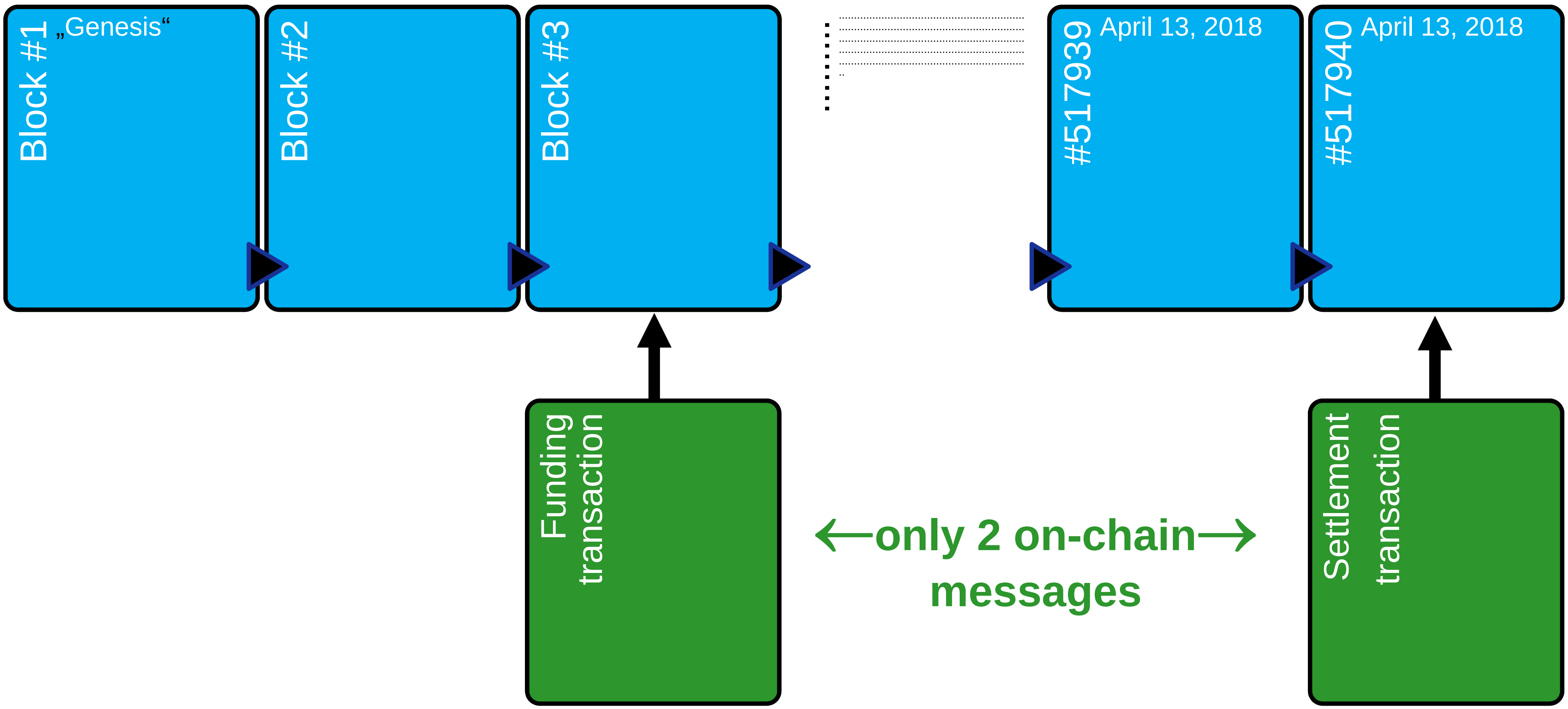
- Switch of Ethereum from Proof of Work to Proof of Stake
- Other payment channel solutions in bitcoin
- Cardano approach „Connecting multiple blockchains“
- Byzcoin
- …..

Jochen Möbert | jochen.moebert@db.com | +49 69 910 31727

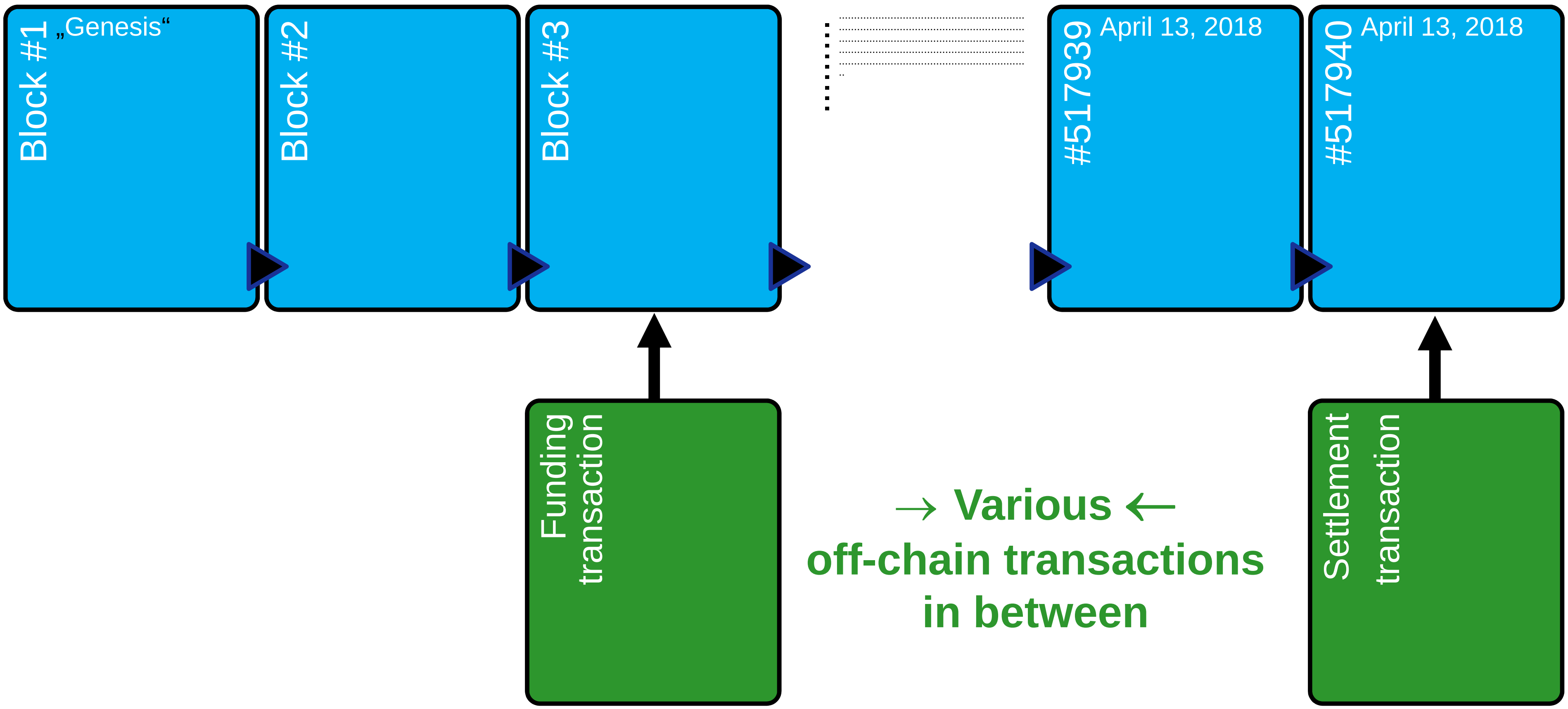
One proposed solution in the Bitcoin system to scale the number of Transactions: Lightning network



Theoretically, the Lightning Network allows for various number of Tx off-chain



Theoretically, the Lightning Network allows for various number of Tx off-chain



How does the Lightning Network work?

Setup a payment channel for Adam & Eve

1) Initial/funding transaction is visible for the Bitcoin nodes: Each person pays bitcoins into a “2x2 multi signature wallet” (= joint account)
2) Then Adam & Eve can perform many potential transactions off-chain, i.e. without announcing it to the Bitcoin network
3) If everyone cooperates transactions are settled on-chain.

Problems and solutions

How to avoid cheating? Simultaneous cross-swap of private keys & semi-signed transactions allows to punish cheaters

How to avoid non-responses? Transactions are automatically terminated in an expected future date → Timeouts

How does the Lightning Network work? Does it scale?

- **Individual scalablility through direct connections:** Enables microtransactions, e.g. daily coffee, newspapers, video streaming, etc. between individuals and could also be used to pay for services per second or even sub-second periods.
- **Network scalability through indirect connections:** Permanent payment channels between important hubs, e.g. cryptoexchanges, could boost no. of Tx and could open up indirect off-chain channels which could scale.
- **Scalability across networks:** Implementing Lightning Network in Bitcoin offsprings, e.g. Litecoin, Bitcoin Cash, allows to transfer funds across blockchains.

However, problems and questions remain

- Nonsimultaneous cross-swap of keys & semi-signed Tx could be abused
- Indirect connections between networks have the potential for multiple failures $\Rightarrow$ multiple timeouts poise a risk of losing funds for a very long time span
- How to handle Tera/Peta/Etabyte of data if crypto scales?

Bottom-line: Lightning Network scales, at least to some extent.

Will cryptocurrencies scale in the future?

Key debate in 2017

(1) Bitcoin scaling debate: Increase the blocksize

Will cryptocurrencies scale in the future?

(2) Lightning network

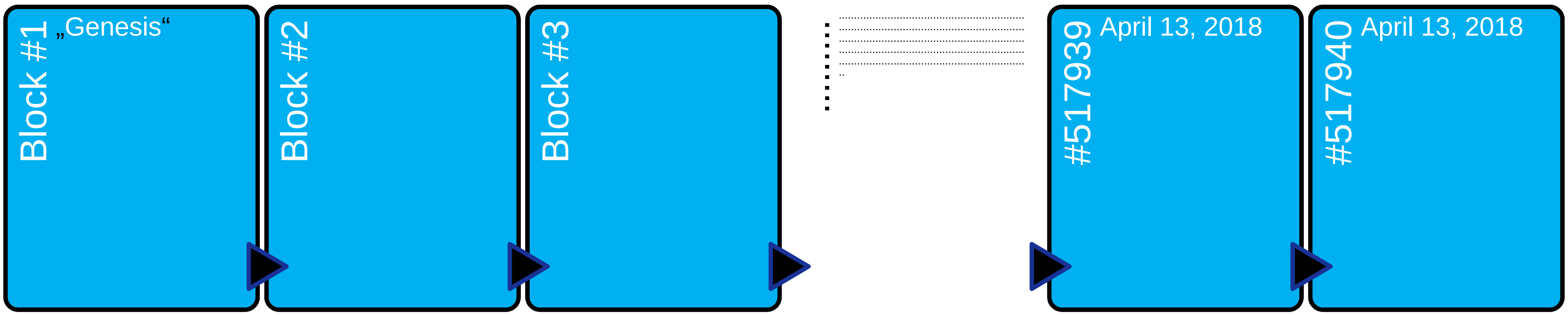
(3) From Blockchains to Blocktrees

Further proposals

- Switch of Ethereum from Proof of Work to Proof of Stake
- Other payment channel solutions in bitcoin
- Cardano approach „Connecting multiple blockchains“
- Byzcoin
- …..

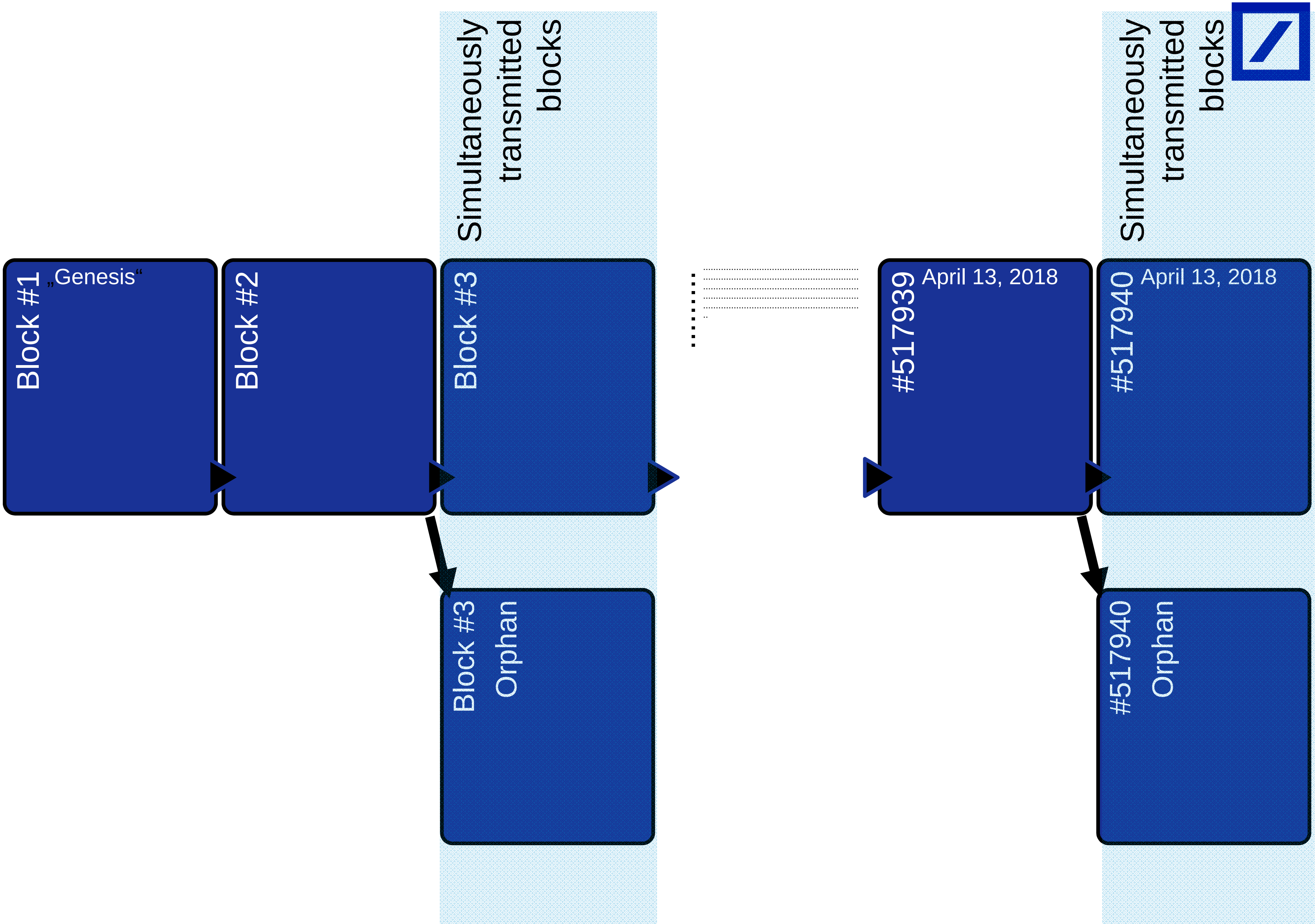
One proposed solution to scale the number of Tx for any blockchain based crypto system: Blocktrees

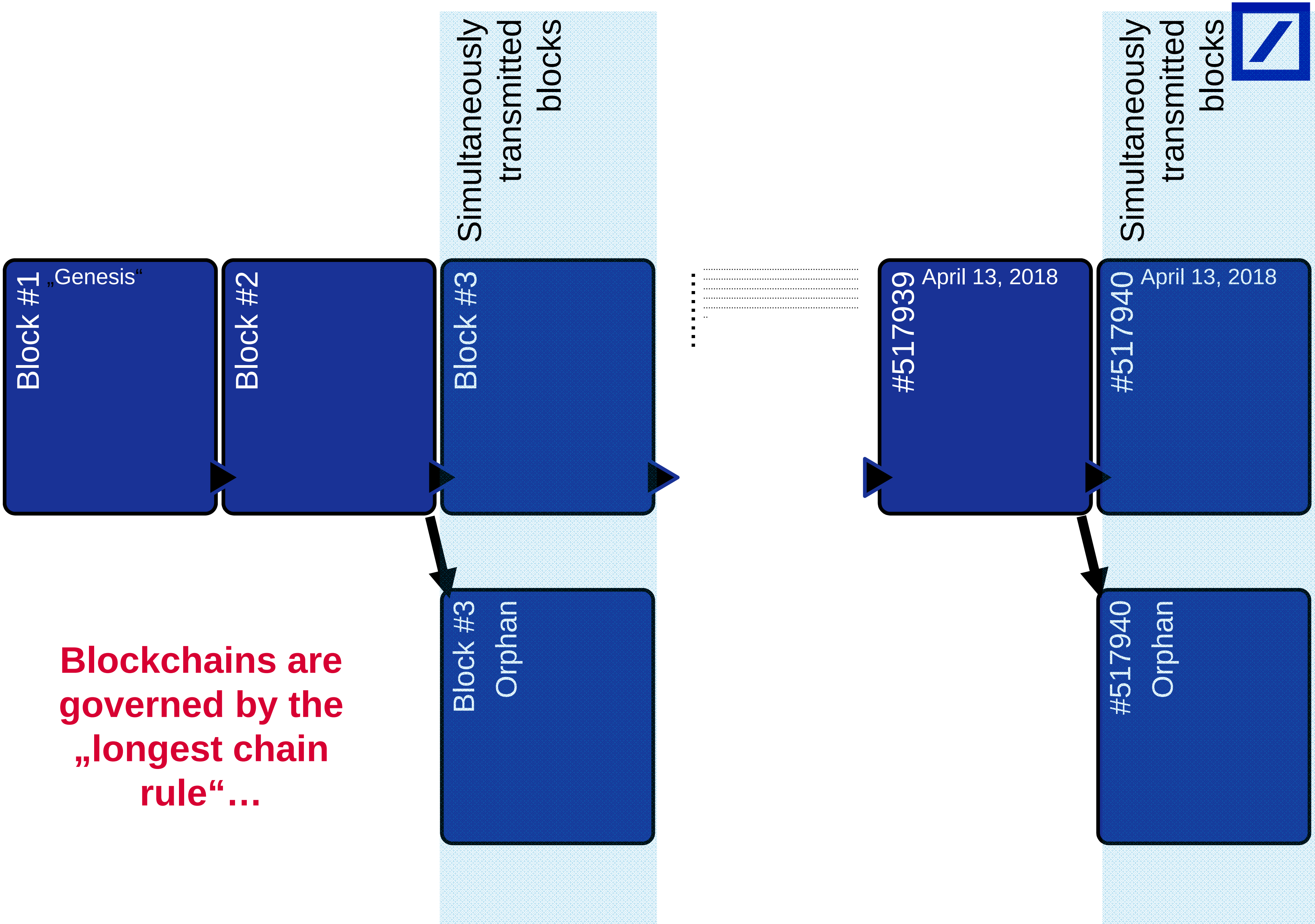
Technical term for Blocktrees = Directed acyclic graphs (DAG)



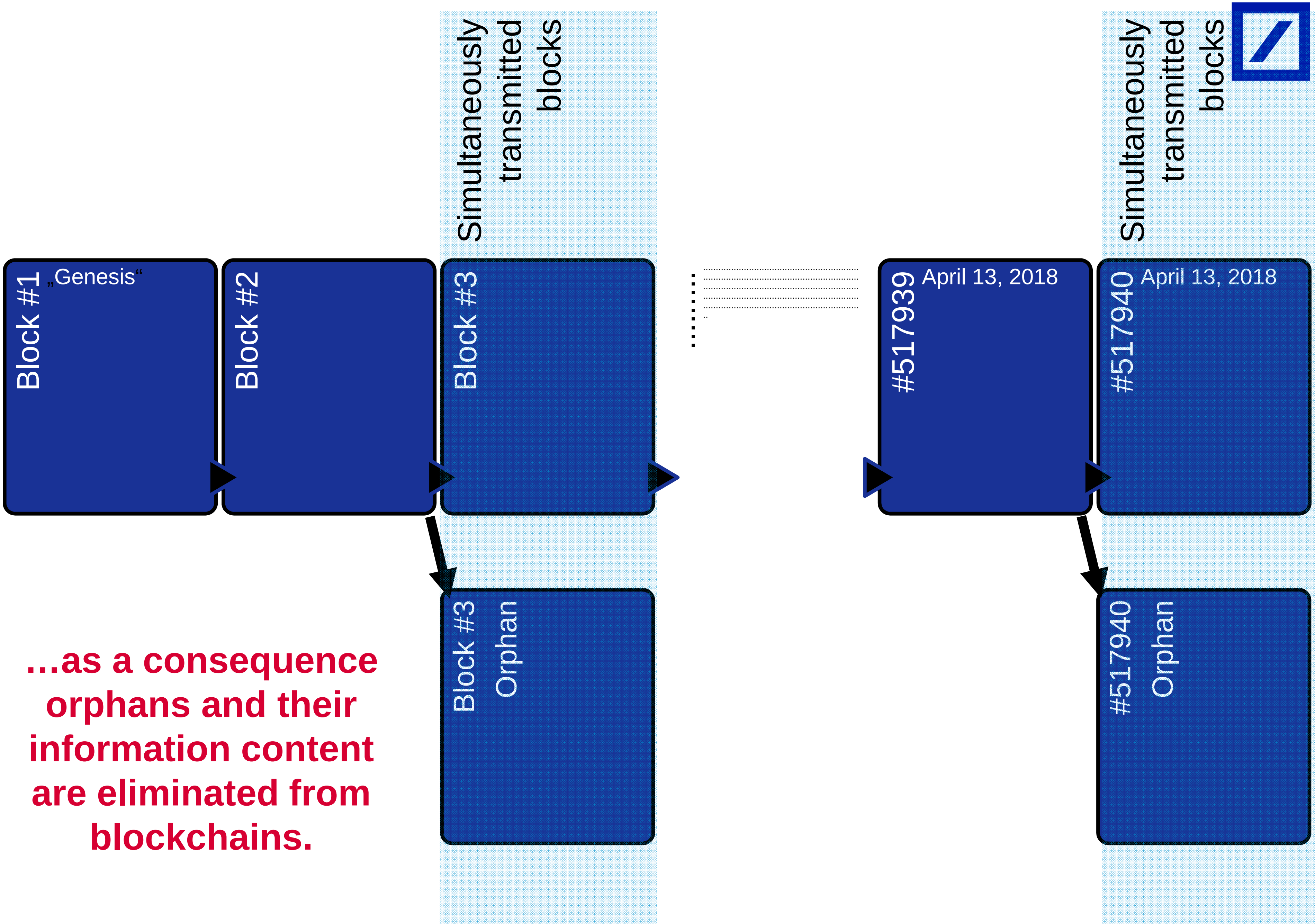
Yonatan Sompolinsky, Yoad Lewenberg & Aviv Zohar
"SPECTRE: Serialization of Proof-of-work Events: Confirming Transactions via Recursive Elections"

See also daglabs.com


Simultaneously transmitted blocks
Block #1
„Genesis“
Block #2
Block #3
Block #3
Orphan
#517939
April 13, 2018
#517940
April 13, 2018
#517940
Orphan
Simultaneously transmitted blocks

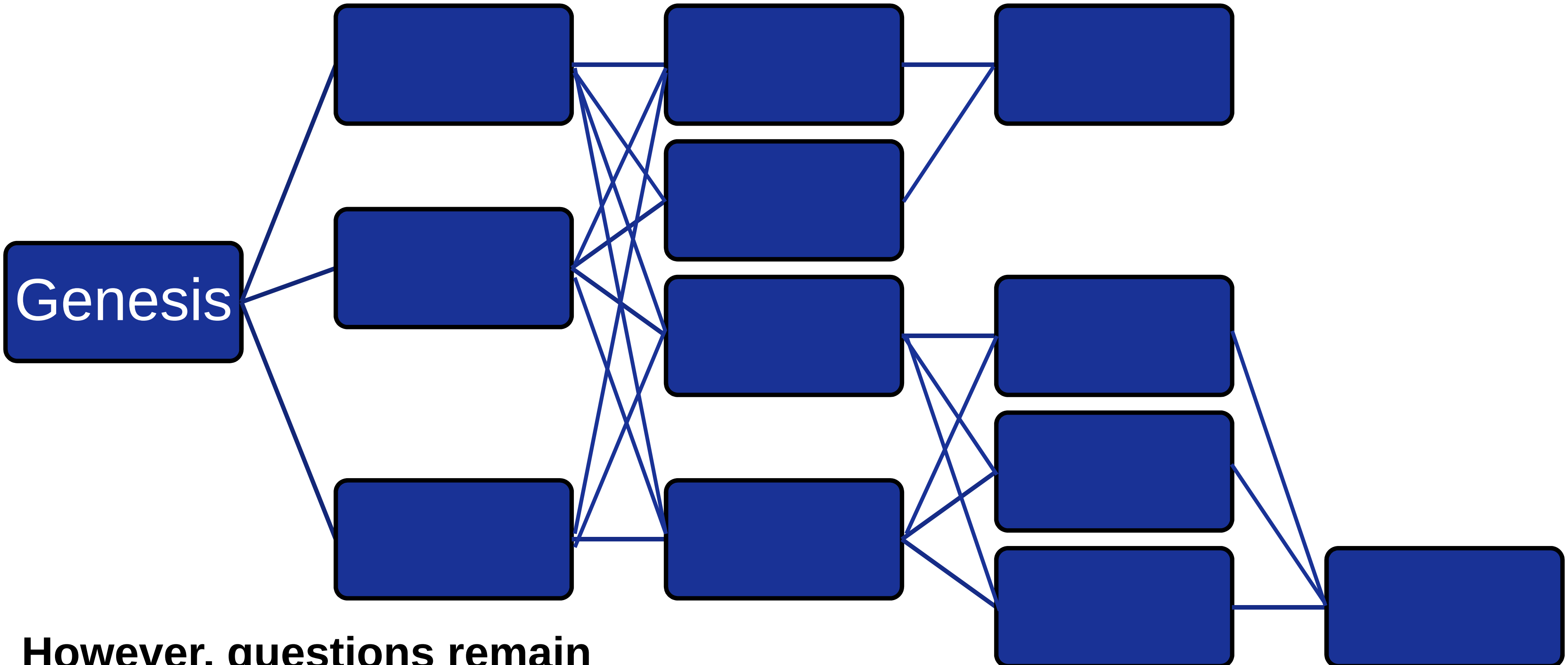


Blockchains are governed by the „longest chain rule“…



…as a consequence orphans and their information content are eliminated from blockchains.

Goal of SPECTRE: 1 m blocks per day (BTC 144) **ZenCash & IOHK** already work **on implementation**.



However, questions remain

- How to handle Tera/Peta/Eta/…byte of data if crypto scales?
- What are the pitfalls in implementing the game-theoretical approach?
- Would SPECTRE result in a less decentralized network node?

Bottom-line on scalability

- ❑ Many projects are in the offing
- ❑ Scalability seems only a matter of time.
  - ❑ Lightning Network and
  - ❑ Blocktrees/DAGs
  - ❑ plus many further proposals

- ❑ However, problems remain. It seems likely that cryptocurrencies scale gradually over the coming years.

  ⇒ very similar to the development of the internet

- ❑ Key problems of scalability are

…adoptability of cryptocurrencies. Many users do not understand either the traditional/centralized nor the new/decentralized payment systems.

…regulatory uncertainty.

Disclaimer

The above information does not constitute the provision of investment, legal or tax advice. Any views expressed reflect the current views of the author, which do not necessarily correspond to the opinions of Deutsche Bank AG or its affiliates. Opinions expressed may change without notice. Opinions expressed may differ from views set out in other documents, including research, published by Deutsche Bank. The above information is provided for informational purposes only and without any obligation, whether contractual or otherwise. No warranty or representation is made as to the correctness, completeness and accuracy of the information given or the assessments made.

In Germany this information is approved and/or communicated by Deutsche Bank AG Frankfurt, licensed to carry on banking business and to provide financial services under the supervision of the European Central Bank (ECB) and the German Federal Financial Supervisory Authority (BaFin). In the United Kingdom this information is approved and/or communicated by Deutsche Bank AG, London Branch, a member of the London Stock Exchange, authorized by UK's Prudential Regulation Authority (PRA) and subject to limited regulation by the UK's Financial Conduct Authority (FCA) (under number 150018) and by the PRA. This information is distributed in Hong Kong by Deutsche Bank AG, Hong Kong Branch, in Korea by Deutsche Securities Korea Co. and in Singapore by Deutsche Bank AG, Singapore Branch. In Japan this information is approved and/or distributed by Deutsche Securities Inc. In Australia, retail clients should obtain a copy of a Product Disclosure Statement (PDS) relating to any financial product referred to in this report and consider the PDS before making any decision about whether to acquire the product.