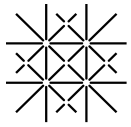


University of Basel

Center for Innovative Finance

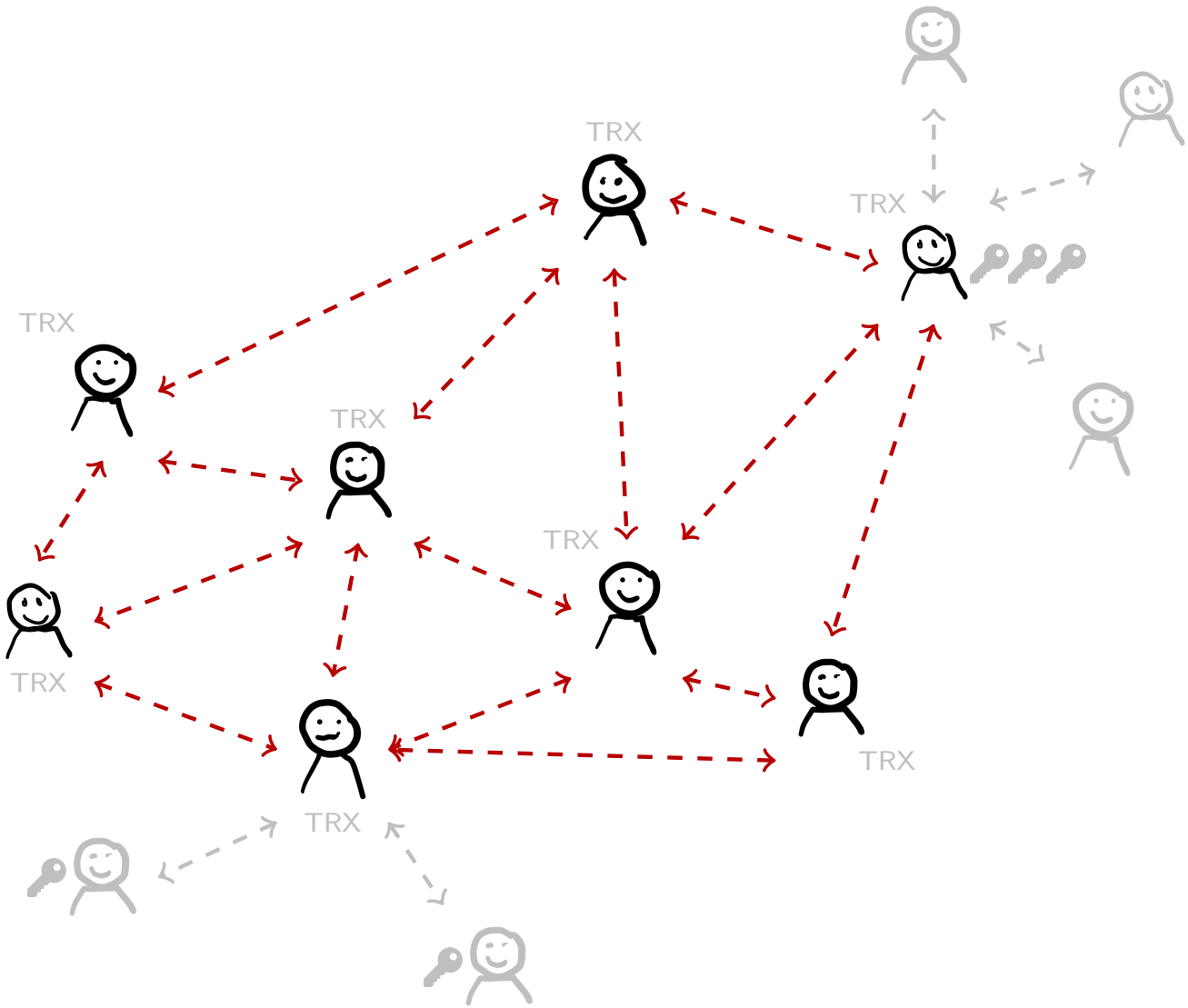
Bitcoin, Blockchain and Cryptoassets

Block Assembly and Chain Structure

Prof. Dr. Fabian Schär
University of Basel

Release Ver.: (Local Release)
Version Hash: (None)
Version Date: (None)

Transaction Distribution



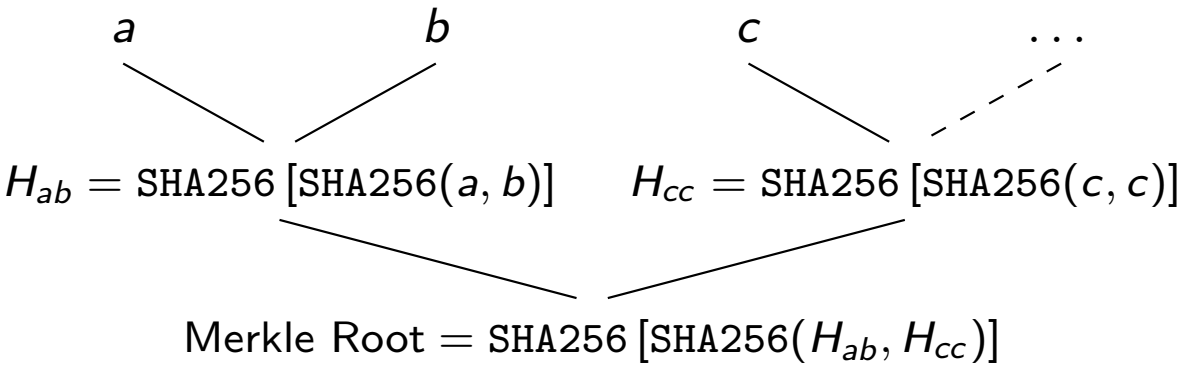
From Transactions to Blocks

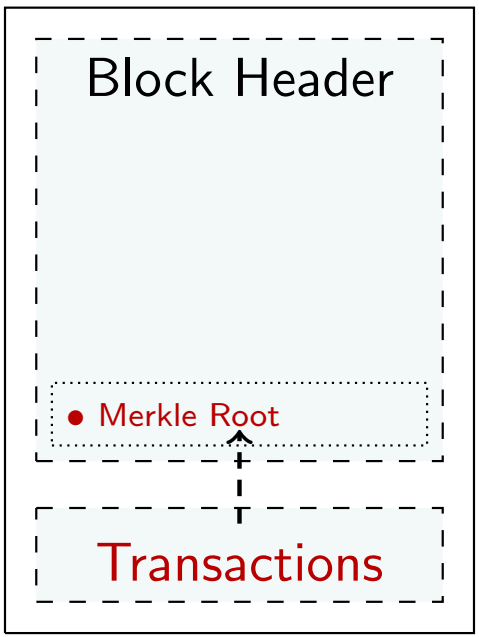
1. Nodes send their transactions to their peers.
2. Each node verifies the received transaction
   - Inputs, Outputs, `ScriptSig`
3. If the transaction is valid, it is . . .
   - . . . forwarded to respective peers.
   - . . . stored in own transaction mempool

Miners will pick a subset of the transactions in their queue (mempool). They usually prefer the transactions with the highest fees/byte.

$\rightarrow$ Let us look at how this works.

Merkle Root

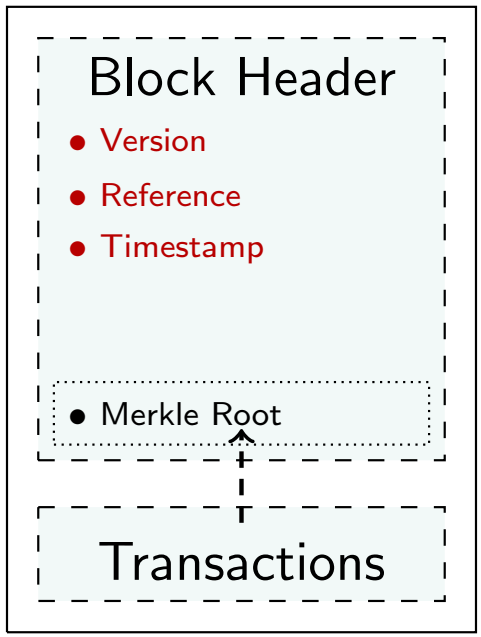




- Represents all transactions of the block in the form of a compact 256-bit entry.
- Guarantees that the transaction data of a block cannot be modified unnoticed.

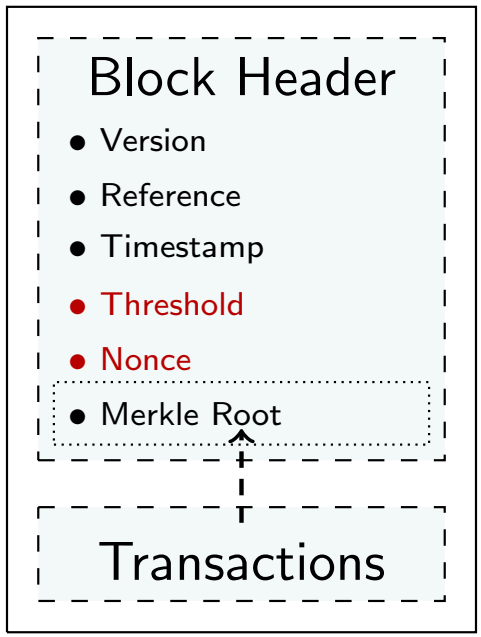
Version, Reference & Timestamp

- **Version:** Followed ruleset of block creation, implicates validation rules.
- **Reference:** Hash value of predecessor block header $\rightarrow$ Foundation of chain structure.
- **Timestamp:** At least median timestamp of the previous eleven blocks; No more than two hours in the future at the time of confirmation.

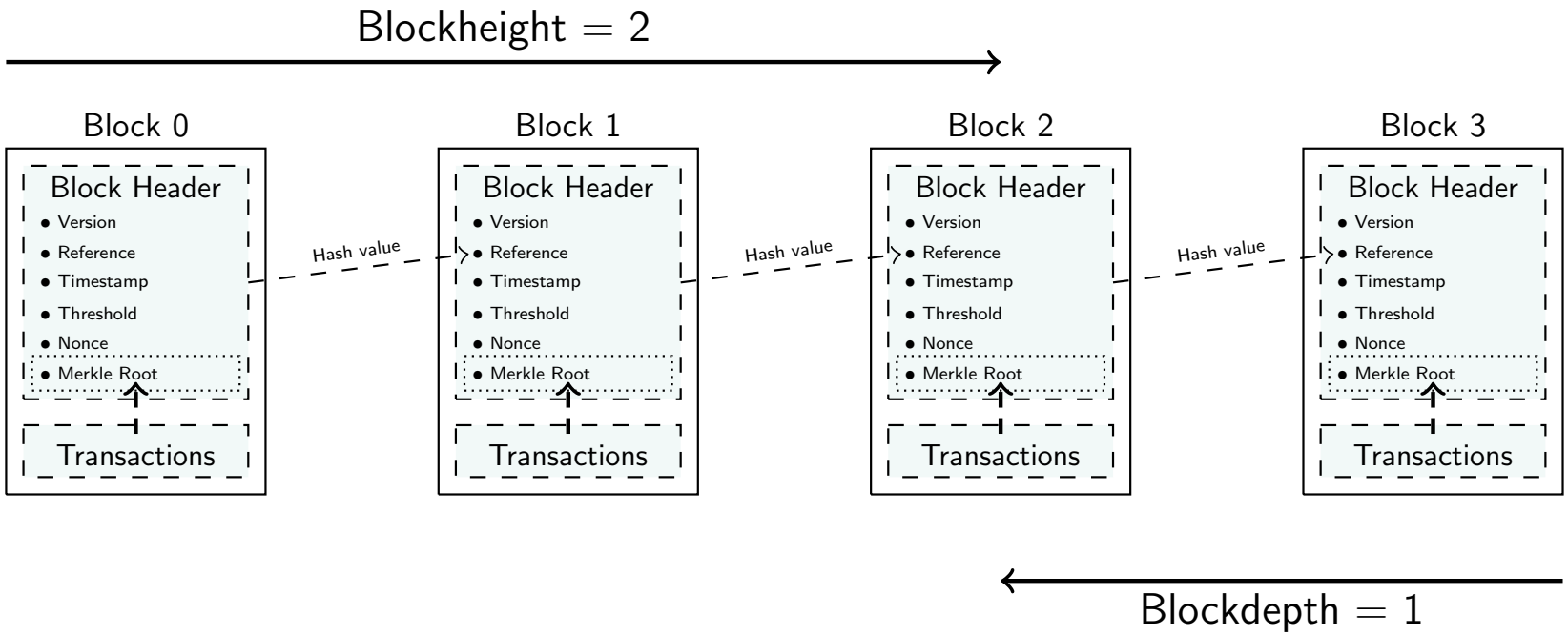


Threshold and Nonce

- **Threshold:** Specifies the maximum hash value a block header may have to be considered valid.
- **Nonce:** Primary source of variation in block creation. Ensures that blocks with otherwise equivalent contents may have different hash values.



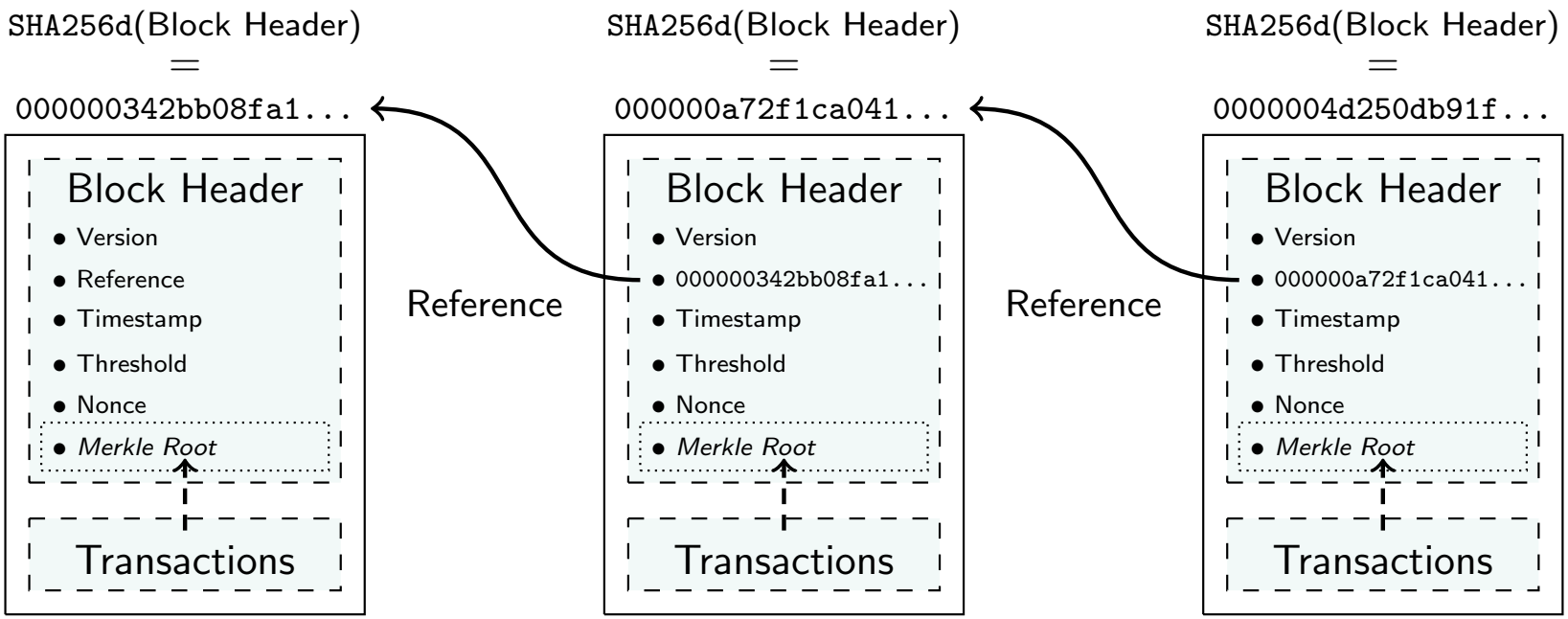
Chain Structure, Block Height and Block Depth



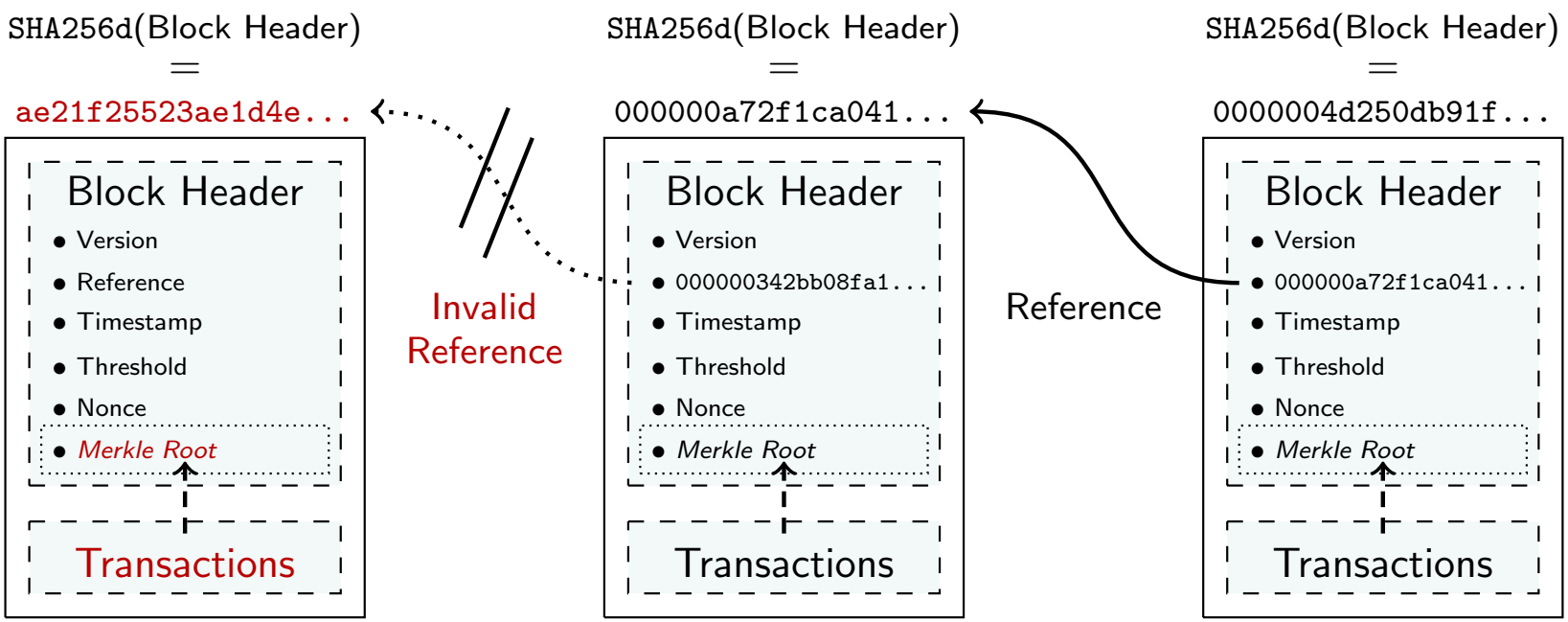
Block Identification:

- Block Height (static, not unique in case of fork)
- Block Depth (dynamic, not unique in case of fork)
- Block Header hash value / Block ID (static)

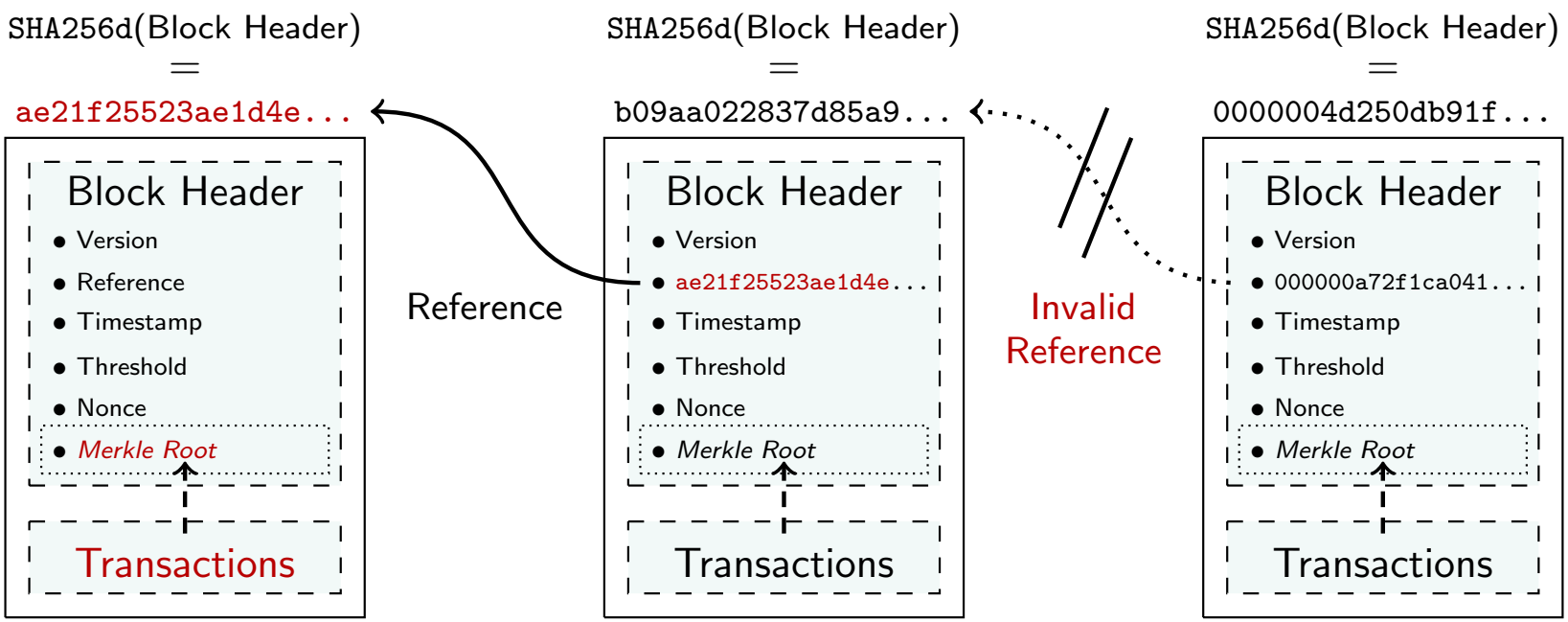
The Domino Effect 1



The Domino Effect 2



The Domino Effect 3



Extending the Chain