CHAINWEB

HARSH VARDHAN IIT2015045 (21)

ABHISHEK NEGI IIT2015126 (46)

CONTENT

- INTRODUCTION
  - DEFINITION
  - NEED
- ARCHITECTURE
  - SPV
  - INTER CHAIN TRANSFERS
- PROTOCOL
  - HEADERS
  - BASE GRAPH
  - PEER REFERENCE PROTOCOL REQUIREMENT
- CONCLUSION

INTRODUCTION

DEFINITION

- A Proof of work parallel chain architecture for massive throughput i.e. it's a parallel chain Proof of Work architecture that combines hundreds or thousands of individually mined peer chains into a single network, capable of achieving throughput in excess of 10,000 transactions per second.

- Peer chains incorporate each other's Merkle roots to enforce a single super chain that offers an effective hash power that is the sum of the hash rate of each individual chain.

- Each chain in the network mines the same cryptocurrency which can be transferred cross-chain via a trustless, two-step Simple Payment Verification (SPV).

NEED

- CONS of POW
  - SLOW
  - CONSUMPTION OF LARGE AMOUNT OF ENERGY
  - LOW THROUGHPUT
  - CONGESTION PRICING IN FORM OF HIGH TRANSACTION FEES.
- ALTERNATIVE APPROACHES
  - PROOF OF STAKE
  - LIGHTNING NETWORK

- PROOF OF STAKE (DISADVANTAGES)
  - Different participants in a transaction need to stake funds in order to validate can be subjected to different regulatory controls in financial markets.
  - Requires central authorities to erase transaction.
  - It's bounded by the causally consistent execution speed of the application layer, which creates a hard upper bound on throughput.

- LIGHTNING NETWORK
  - The idea of Payment Channels protocols is to break down a transaction into a series of smaller payments executed through a channel.
  - funds are sequestered from the main network and are used in a series of smaller payments (or commitments) between a specified set of actors, with the ability to net out the payments on the main network at any time.
- CONS
  - Do not fundamentally change the overall throughput of the system, as side-chain commitments are fundamentally not equivalent to transfers on the main network.
  - Funds must be pre-allocated.

ARCHITECTURE

ARCHITECTURAL FEATURES

- The novel architecture of Chainweb is predicated upon two separate, yet related features that operate at distinct layers of the Chain web stack.

1) Cross-chain cryptocurrency transfers via on chain SPV.

2) Parallel-chain binding at hashing level via peer chain Merkle root inclusion.

- The former, which occurs in the application (smart contract) layer, leverages the latter to create valid Merkle proofs of currency transfer.

SIMPLE PAYMENT VERIFICATION (SPV)

- It allows light client to verify that a transaction is included in blockchain without downloading entire blockchain.
- It only downloads block headers which are much smaller than full blocks. For verification , SPV client request proof of inclusion in form of Merkle branch.
- Transaction is accomplished by obtaining the Merkle branch linking the transaction to the block it's timestamped in, and linking it to a Merkle root obtained from the block header stream of the longest chain.

INTERCHAIN TRANSFERS

- **Moves coin by deleting it in an account on one chain and creating it in an account on other.**

1.Chain 1 - Delete: User signs and publishes transaction, calling cx − delete with arguments A (delete account on 1), Y (create chain), B (create account on 2), Q (transfer quantity). cx − delete performs the following:

(a) Enforce A keyset against signature.

(b) Enforce sufficient funds to delete Q in A.

(c) Delete Q from A.

(d) Receipt records X, Y, B, Q, T (transaction ID) in protocol-reserved fields.

2. Chain Y - Create: Anybody publishes transaction, calling cx − create with SPV proof and receipt of deletion transaction on chain 1. cx − create performs the following:

(a) Validate SPV proof of deletion transaction, recovering X, Y, B, Q, T from receipt.

(b) Enforce unique usage of (T, X).

(c) Enforce Y identifies to this chain, and B is a valid account on chain.

(d) Create Q in B.

PROTOCOL

- The Chain web network is comprised of multiple independent peer blockchains minting distinct coins of the same currency.

- Each chain incorporates subset of other peer Merkle roots in its own block hashes.

- The capture of foreign roots serves two purposes:-

  - It allows a given chain to validate that its peer chains are maintaining a consistent fork by locating its own previous Merkle roots in those obtained from its peer chains.

  - It provides a trustless oracle of peer Merkle roots, which is necessary to allow application layer transfer code to validate provided Merkle proofs to guarantee cross-chain transfers of funds.

HEADERS

- In a traditional blockchain, where there is only one chain, each new block must only reference the header of its previous block.
- In Chain web, each parallel blockchain must additionally reference the headers of other chains (peers) at the same block height as its previous block.
- The peer headers found in that block's header are committed to a storage location available to the application layer.
- Users can construct a Merkle proof between any two chains that covers, at most, a one less than diameter number of cross-chain hops, as the last hop is available via query in the application layer.

BASE GRAPH

- The base graph is used to structure the interaction of chains in the web, and can be thought of as the instructions for how to braid the chains together.

- Parameters :-
  - Order
  - Degree
  - Edges
  - Diameter

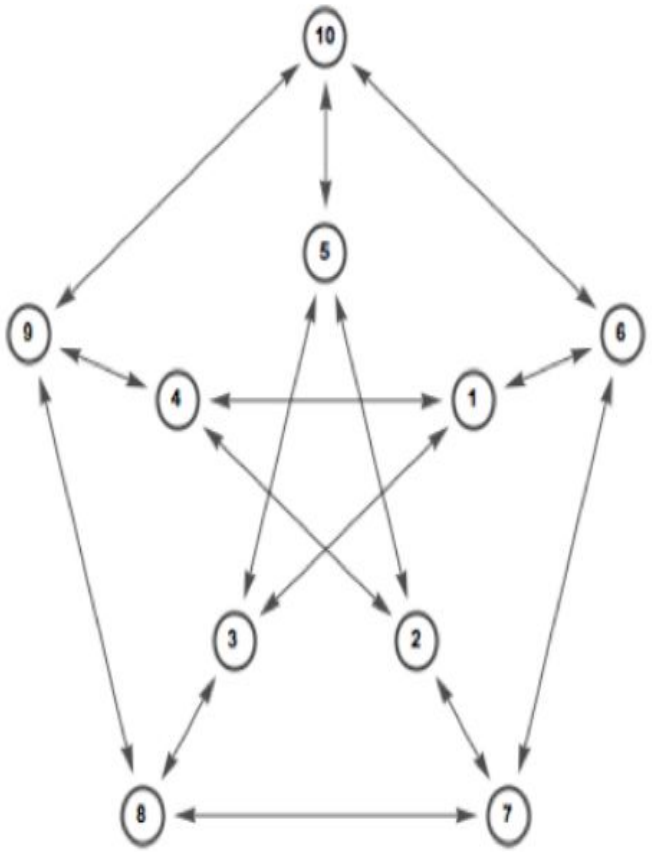
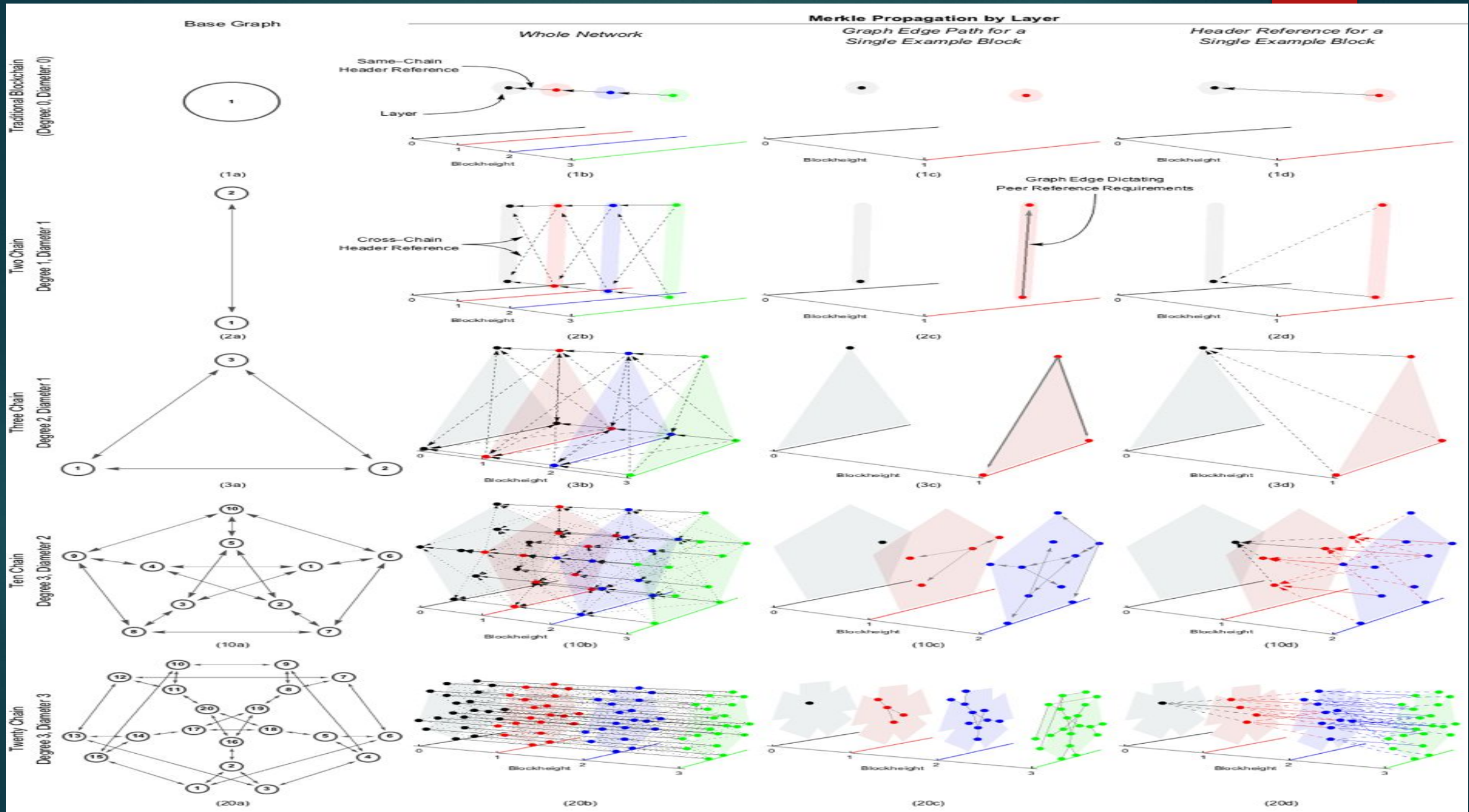


Figure 1: Petersen Graph (Order 10, Degree 3, Diameter 2)

$$Header_{Chain=1,Layer=N} \rightarrow \begin{cases} Header_{1,N-1} \rightarrow \begin{cases} Header_{1,N-2} \\ Peers \begin{cases} Header_{3,N-2} \\ Header_{4,N-2} \\ Header_{6,N-2} \end{cases} \end{cases} \\ Peers \begin{cases} Header_{3,N-1} \rightarrow \begin{cases} Header_{3,N-2} \\ Peers \begin{cases} Header_{1,N-2} \\ Header_{5,N-2} \\ Header_{8,N-2} \end{cases} \end{cases} \\ Header_{4,N-1} \rightarrow \begin{cases} Header_{4,N-2} \\ Peers \begin{cases} Header_{1,N-2} \\ Header_{2,N-2} \\ Header_{9,N-2} \end{cases} \end{cases} \\ Header_{6,N-1} \rightarrow \begin{cases} Header_{6,N-2} \\ Peers \begin{cases} Header_{1,N-2} \\ Header_{7,N-2} \\ Header_{10,N-2} \end{cases} \end{cases} \end{cases} \end{cases}$$

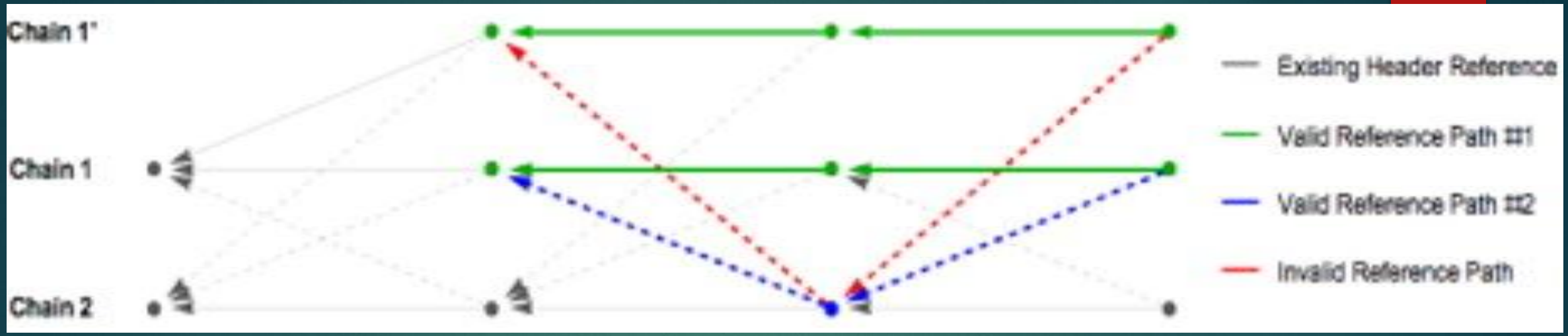
Figure 2: Propagation of header references

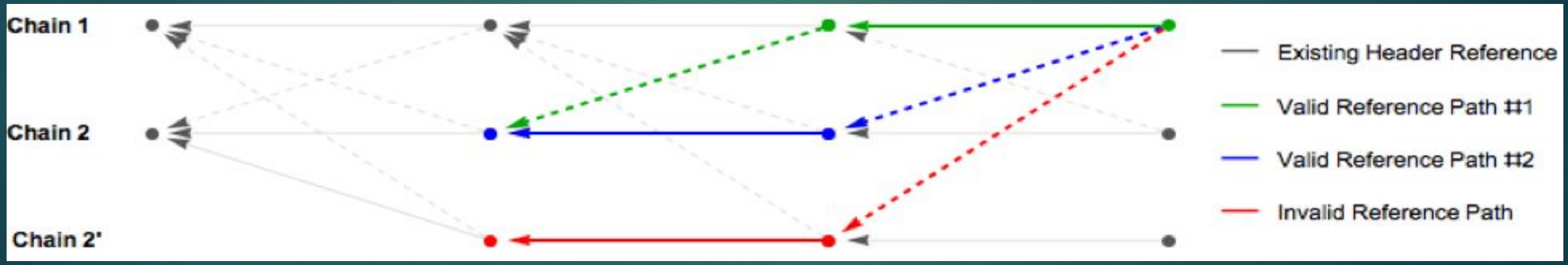

Merkle Propagation by Layer
Base Graph
Whole Network
Graph Edge Path for a Single Example Block
Header Reference for a Single Example Block
Traditional Blockchain
(Degree: 0, Diameter: 0)
Same–Chain Header Reference
Layer
Blockheight
(1a)
(1b)
(1c)
(1d)
Two Chain
Degree 1, Diameter 1
Cross–Chain Header Reference
Graph Edge Dictating Peer Reference Requirements
(2a)
(2b)
(2c)
(2d)
Three Chain
Degree 2, Diameter 1
(3a)
(3b)
(3c)
(3d)
Ten Chain
Degree 3, Diameter 2
(10a)
(10b)
(10c)
(10d)
Twenty Chain
Degree 3, Diameter 3
(20a)
(20b)
(20c)
(20d)

- **PEER REFERENCE PROTOCOL REQUIREMENT**

To replace any given block in the network, all blocks that currently exist within the future Merkle cone of that block must be replaced. This feature is required to ensure that Chain-web network cross-chain transfers conserve cryptocurrency mass.

- **Same Chain Rule**
  - The header of a chain and the headers of referenced peers agree on the ancestry of the header of the chain.
- **Same Peer rule**
  - The header and the headers of referenced peers agree on the ancestry of the referenced peer.


Chain 1'
Chain 1
Chain 2
Existing Header Reference
Valid Reference Path #1
Valid Reference Path #2
Invalid Reference Path


Chain 1
Chain 2
Chain 2'
Existing Header Reference
Valid Reference Path #1
Valid Reference Path #2
Invalid Reference Path

CONCLUSION

- **Significant advances over existing approaches in scalable public blockchain.**
  - Chain web operates within the MTA exception under which miners currently operate and avoids the security and liquidity tradeoffs of payment channels or side-chains.
- **Unparalleled increases in Proof of Work throughput while keeping the global hash rate, and thus energy required, constant.**
  - serves to mitigate the worrisome energy footprint of current mining operations by distributing competition across many chains and reducing spurious competitive mining.
  - The increase in attack-resistance offered by the multiple chain architecture also significantly lowers the required per-chain hash rate, while the use of hash rate to support additional chains serves to increase throughput and utilization, not just security.
  - Layers are formed by the mining of individual chains wherein each chain, being a peer, has the same difficulty level. On average each chain receives the same fraction of total network hash rate, as this allocation is the equilibrium of individual miners selfishly attempting to minimize mining duplicates (both personal and network) and thus waste.
- **Confirmation latency is decreased**
  - Mining a chain depends on the progress of its peers and thus, from time to time, the production of the next block in a given chain will stall. In such an instant, the global hash rate naturally pools toward that chain, increasing its speed of advancement and allowing it to catch up. It is in the best interests of any miner to allocate mining resources at a per-chain level in a manner that keeps the rate of new block production for every chain as even as possible.
- **Trustless (decentralized)**

REFERENCES

1. http://kadena.io/docs/chainweb-v15.pdf
2. https://medium.com/datadriveninvestor/chainweb-and-the-art-of-scalable-blockchains-ed0c9ff03ab3