Blockgraph: A Scalable Alternative To Blockchain

Zhenbo Sun, Seth C. Goldstein
Tsinghua University & Carnegie Mellon University

Introduction

Blockchain technology

- A digital currency system where different parties can make, receive and verify payment.
- All active nodes maintain a public ledger and participate in the consensus mechanism.

Problems

- Scalability: Bitcoin is limited to low throughput because of the propagation delay and limited block size.(<10TPS)
- Cost: massive energy required for POW.

Method

Locality

A locality can be any group of people who will transact within the group to a greater extent than outside the group. For example, people in the same place, company, organization.

Blockgraph

The Blockgraph splits the blockchain into a global chain and multiple local chains. Every locality has its own chain and all local chains are synchronized to the global chain. If an end user wants to spend money in another locality, she has to transfer her money to that locality first, just like people will exchange money when they go abroad.

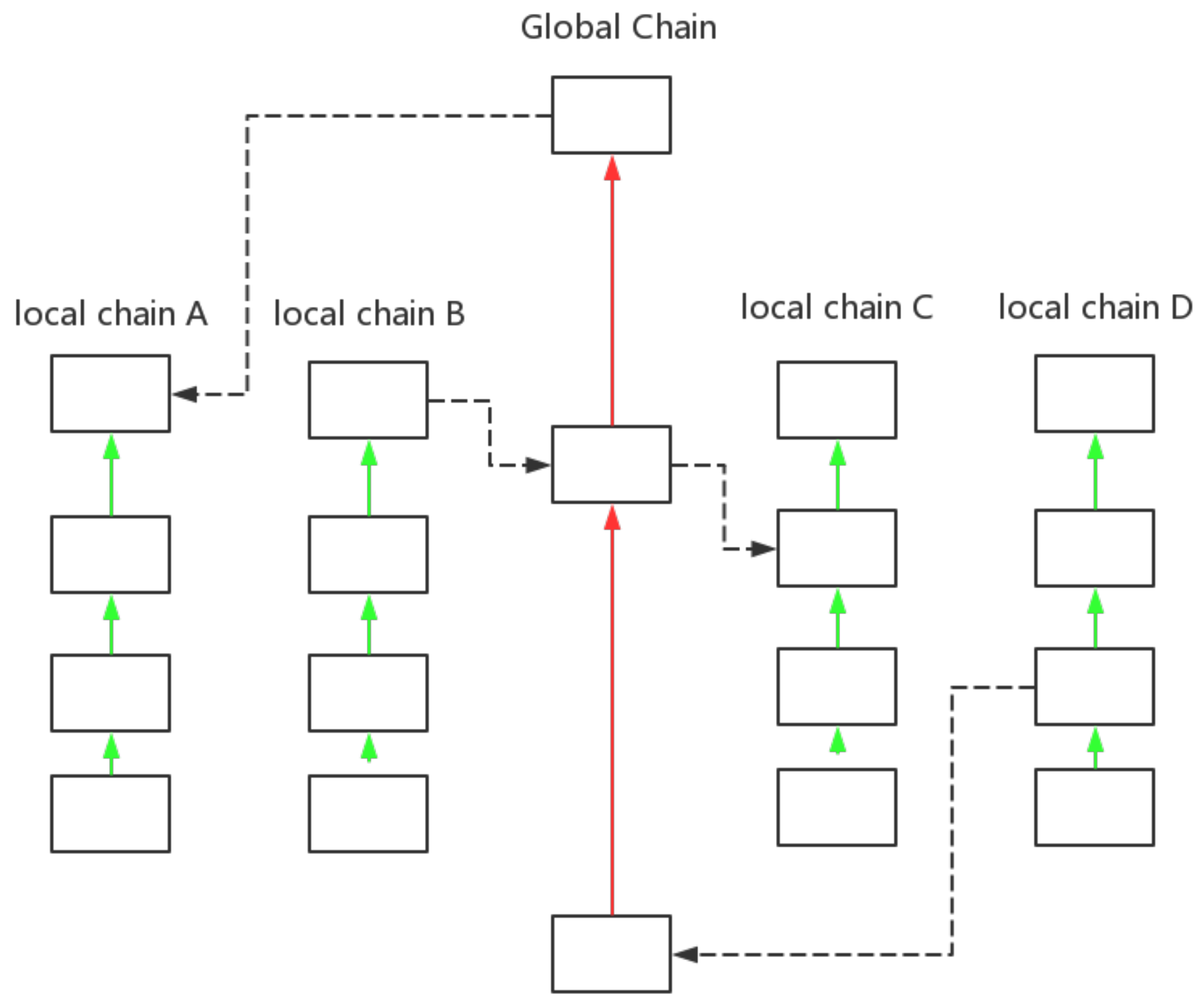

Figure 1: Blockgraph

Advantages

- create parallel local chains which can extend multiple blocks simultaneously.
- reduce propagation latency and inter-block time while retaining stability.

Implement

New Transactions

- ITT: lock one's money in a blockchain when transferring to another chain.
- XDP: receive money from another blockchain.
- BSP: a checkpoint of a local chain.

Example of Inter-local Transaction

Suppose Alice in locality A wants to transfer money to Bob in locality B. First, Alice should transfer money from locality A to locality B through global chain. After the transfer to locality B is complete, Alice send a regular P2PKH as an input to Bob' address.

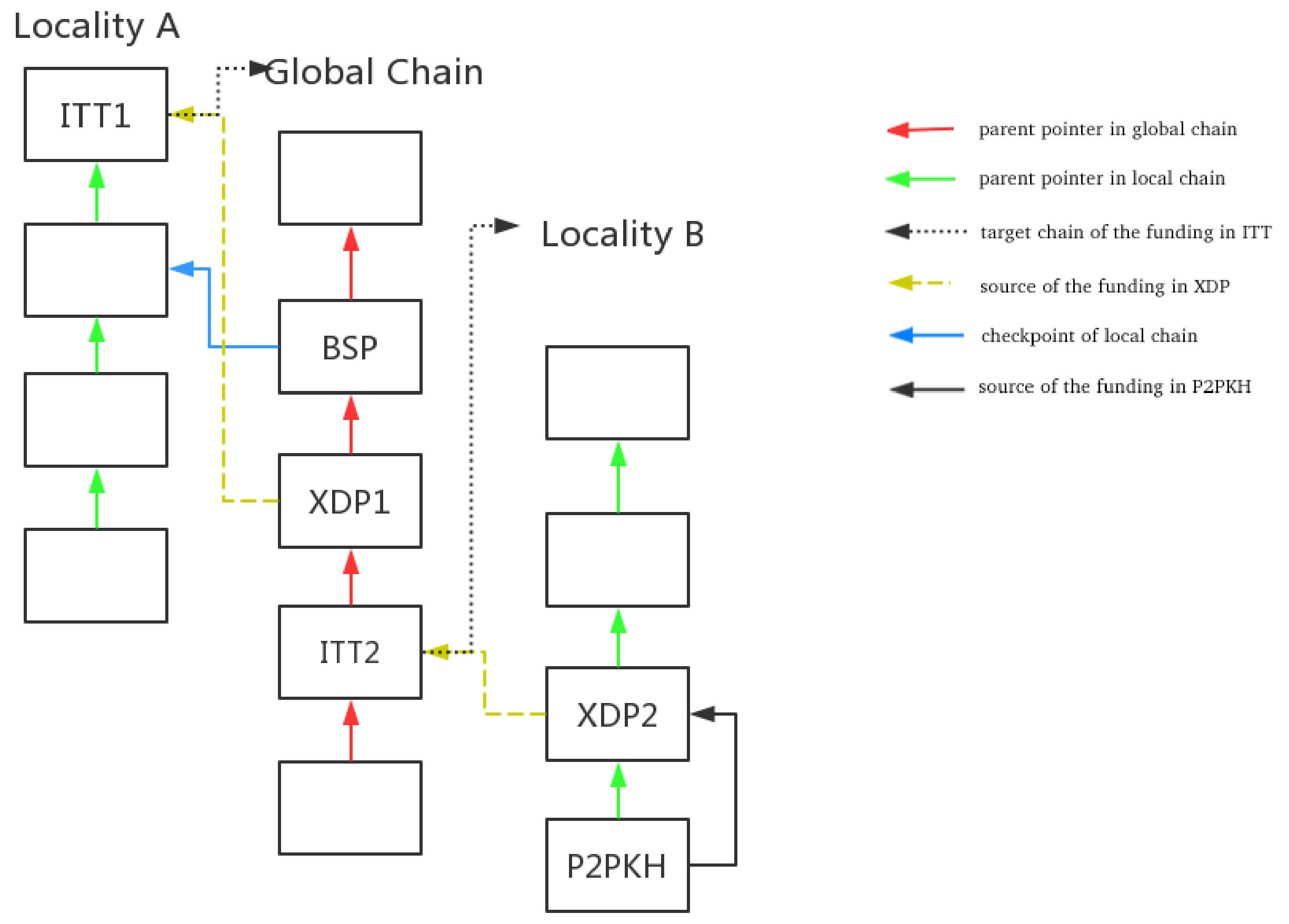
Locality A
Global Chain
Locality B
ITT1
BSP
XDP1
ITT2
XDP2
P2PKH
parent pointer in global chain
parent pointer in local chain
target chain of the funding in ITT
source of the funding in XDP
checkpoint of local chain
source of the funding in P2PKH

Figure 2: Inter-local Example

Miners

Global miners have copies of all local chains in order to verify their transactions. Similarly, local miners need to save a copy of global chain.

Local chain

Local chains are protected by checkpoints on the global chain, which means local blocks before the checkpoint will never be orphaned even though the local chain has potentially little hash power available.

DNS seeds

DNS seeds are DNS servers that return a list of IP addresses of full nodes. In Blockgraph, DNS seeds return IP addresses according to the hash of genesis block of blockchain. We extend the server so miners can register new local chains on DNS seeds for other miners to find them.

Conclusion

Blockgraph Protocol allows a higher transaction rate while maintaining the same security as current Bitcoin protocol does. Compared with pegged sidechains, global chains and local chains in Blockgraph are aware of each other in order to stay consistent and prevent attacks.