Presentation Title

Optional Subtitle

K. Cong

Faculty of Electrical Engineering, Mathematics and Computer Science
Delft University of Technology

2017

Outline

Outline

TrustChain

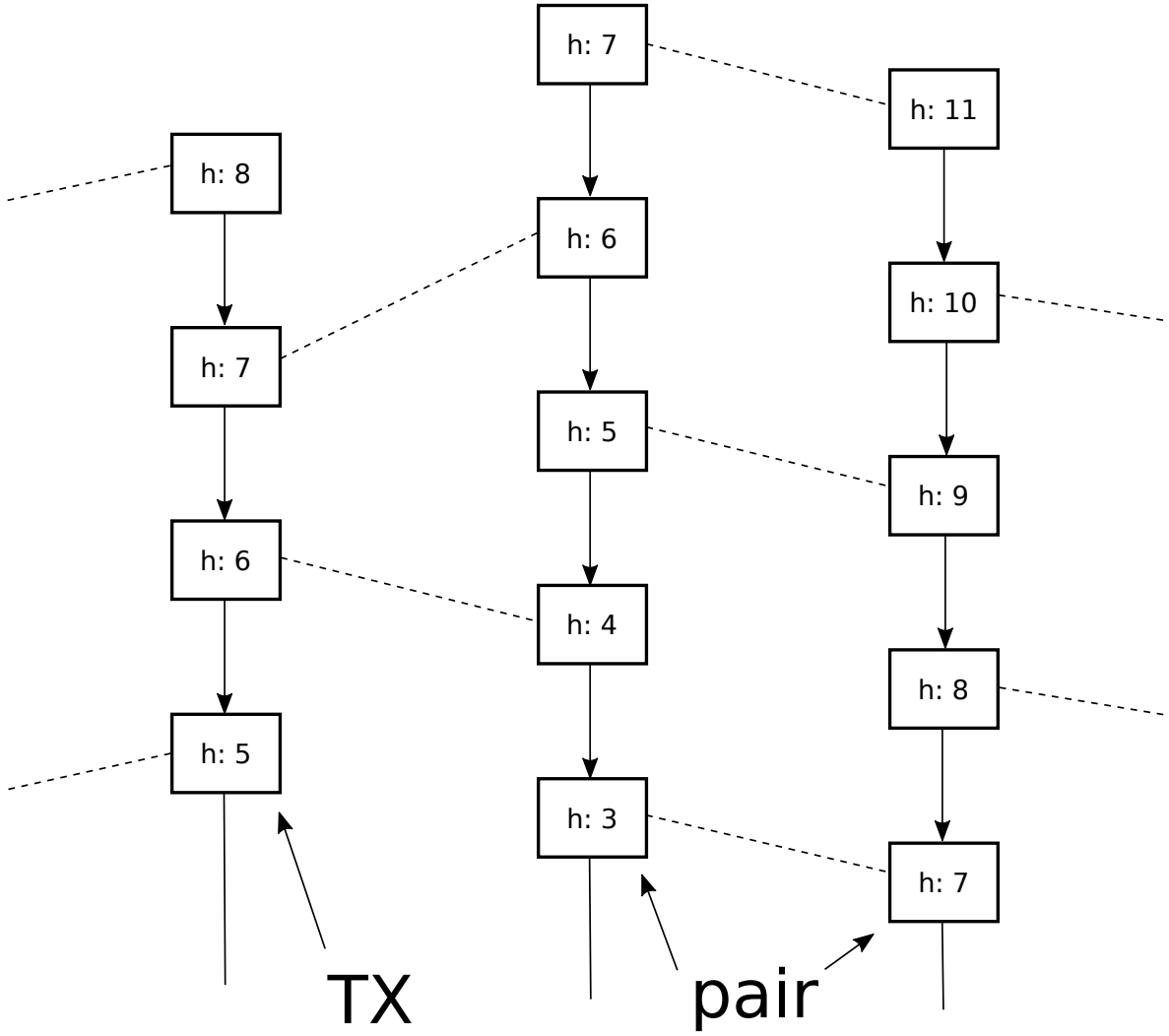

Figure: *TX block* is a six-tuple: $t_{i,j} = (\mathtt{h}(b_{i,j-1}), h_s, h_r, s_s, s_r, m)$, one transaction results in two TX blocks—*a pair*.

TrustChain

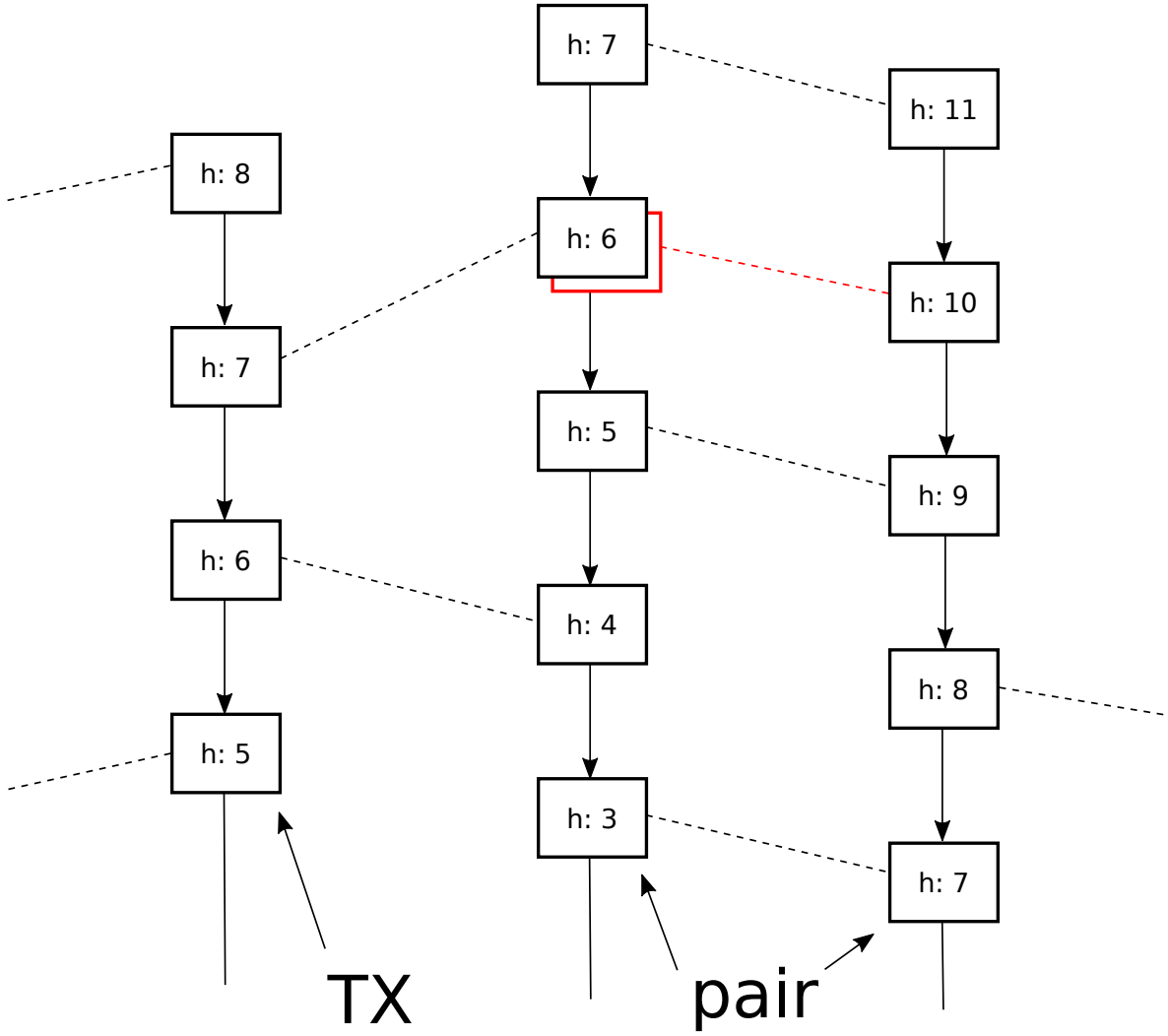

Figure: Fork is two correctly signed TX blocks that has the same h_s but involve different receivers. Only one TX block may be in consensus.

TrustChain

- Everyone has their own chain
- Transactions are on arbitrary data m
- Transactions make the chains intertwined
- No consensus (my thesis)

Outline

TrustChain with Checkpoints

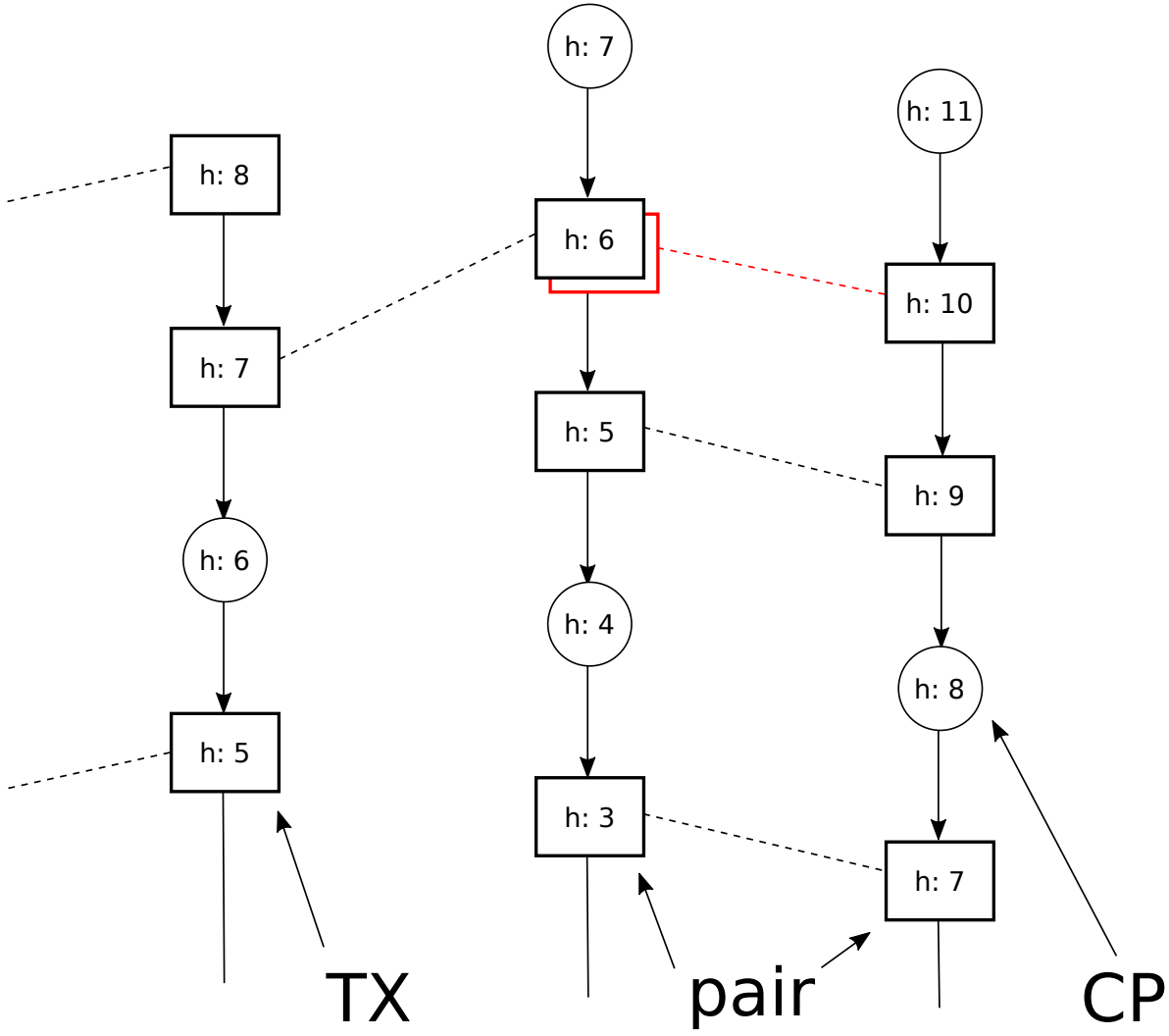

Figure: CP block is a five-tuple: $c_{i,j} = (\mathrm{h}(b_{i,j-1}), \mathrm{h}(\mathcal{C}_r), r, p, s)$, $\mathcal{C}_r$ is the consensus result at round r, p = promoter indicator, s = signature.

Outline

Consensus Protocol Overview

1. N lucky nodes are selected at random to act as promoters.
2. Every node sends CP blocks to promoters.
3. Promoters run a BFT (Byzantine Fault Tolerant) consensus algorithm to agree on a set of CP blocks—$\mathcal{C}_r$.
4. Disseminate $\mathcal{C}_r$.
5. Any node can verify that their transaction is in consensus.
6. Repeat for next round.

Outline

Promoter Registration

Blocks

Block Title

You can also highlight sections of your presentation in a block, with it's own title

Theorem

There are separate environments for theorems, examples, definitions and proofs.

Example

Here is an example of an example block.

Summary

- The first main message of your talk in one or two lines.
- The second main message of your talk in one or two lines.
- Perhaps a third message, but not more than that.

- Outlook
  - Something you haven't solved.
  - Something else you haven't solved.

For Further Reading I

A. Author.
Handbook of Everything.
Some Press, 1990.

S. Someone.
On this and that.
Journal of This and That, 2(1):50–100, 2000.