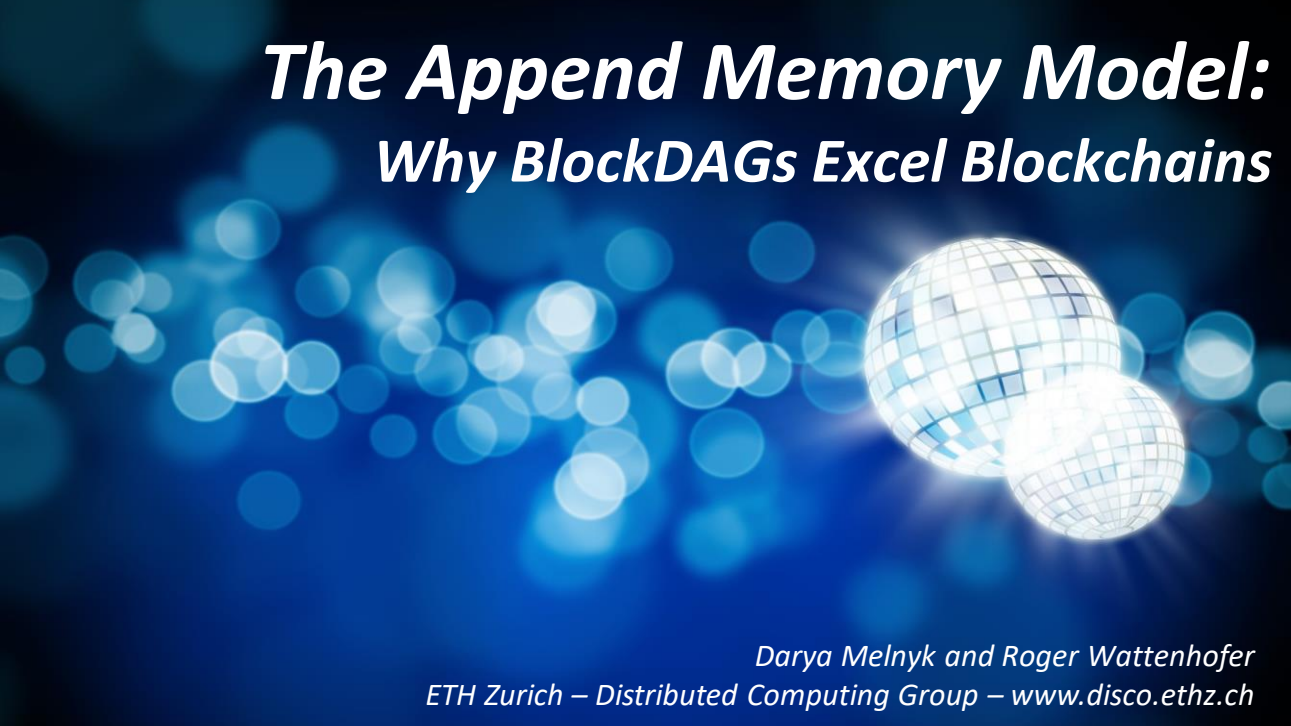
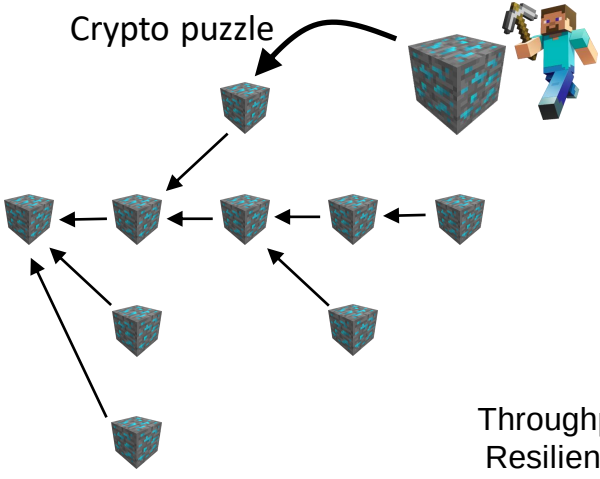
The Append Memory Model:
Why BlockDAGs Excel Blockchains

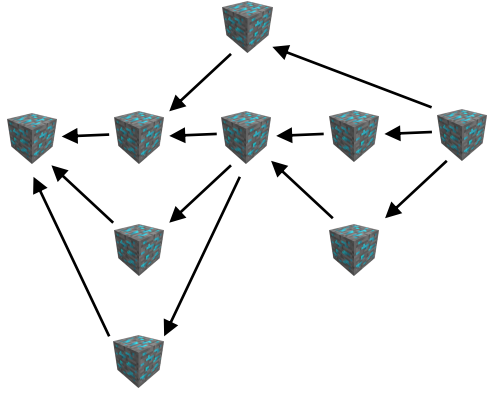


Darya Melnyk and Roger Wattenhofer
ETH Zurich – Distributed Computing Group – www.disco.ethz.ch

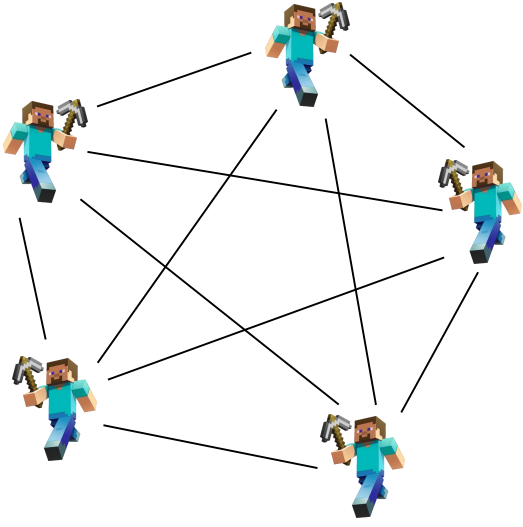
BlockChain vs. BlockDAG



Throughput?
Resilience?



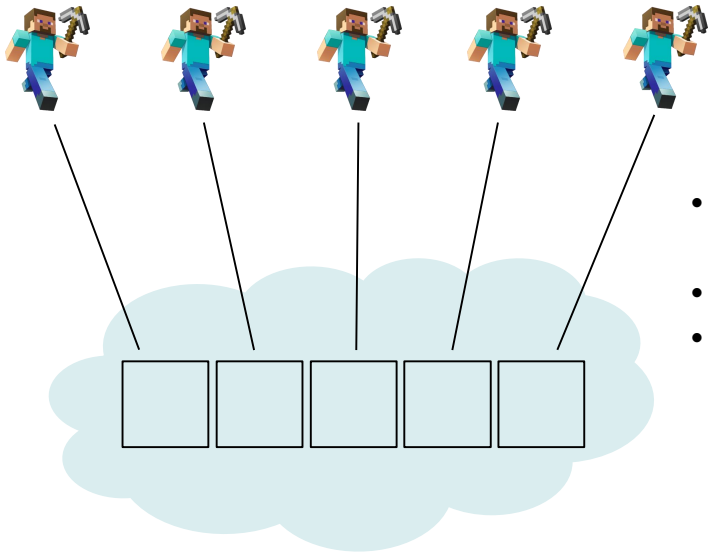
Message Passing Model



- Peer-to-peer communication
- Message delays
- Need to maintain the chain analysis on top

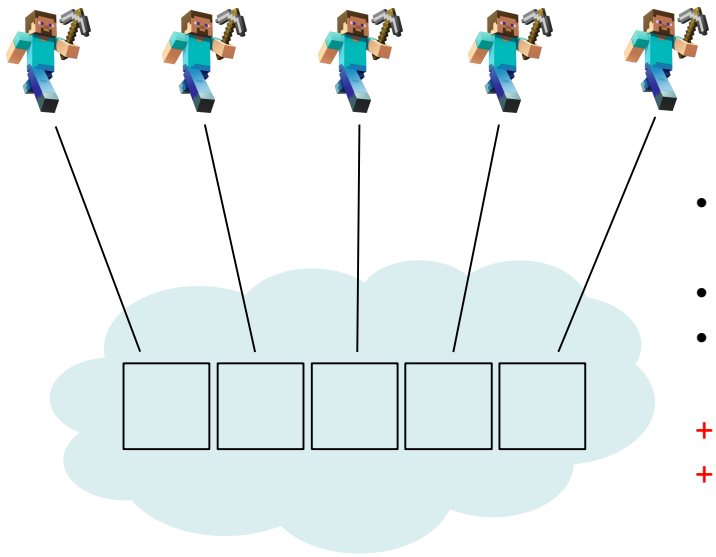
[Ren, 2019]

Shared Memory Model



- Communication with the memory
- Message delays
- Unified view of the chain

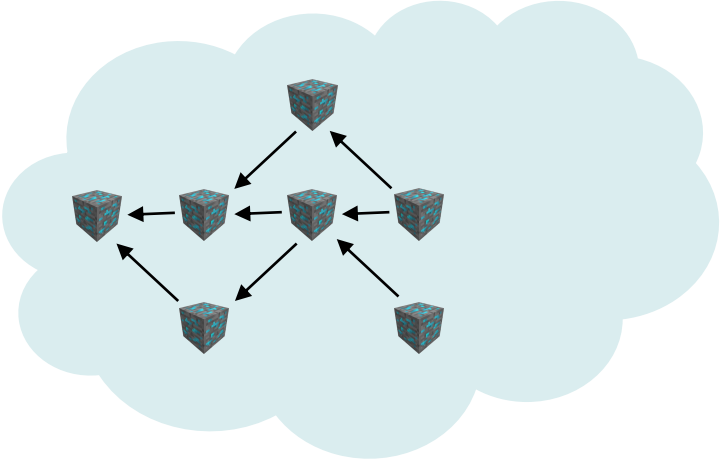
Append Memory Model

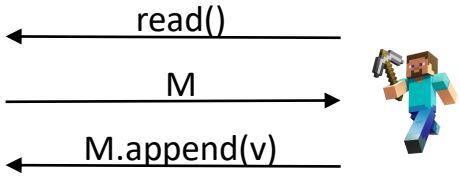


- Communication with the memory
- Message delays
- Unified view of the chain

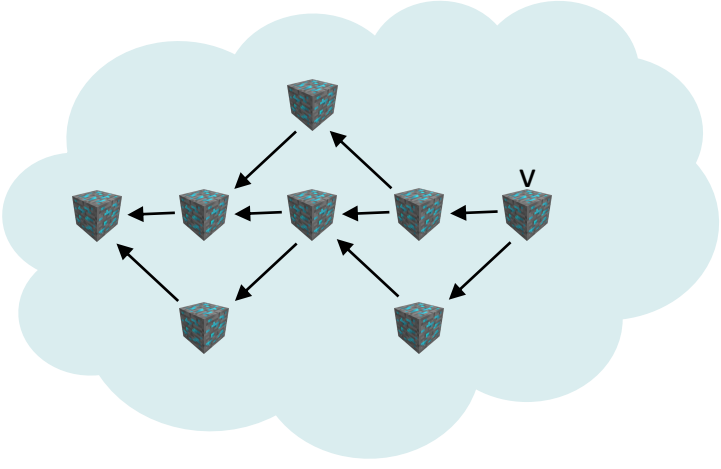
\+ unbounded memory
\+ snapshot of the whole memory

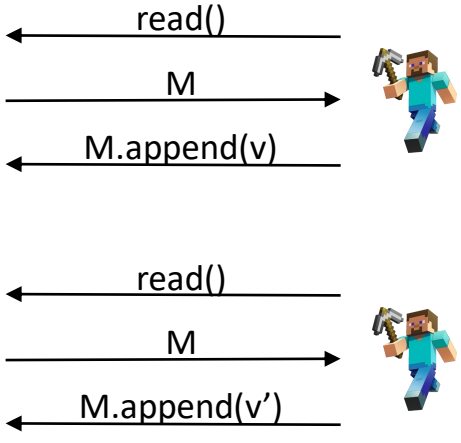
Append Memory Model



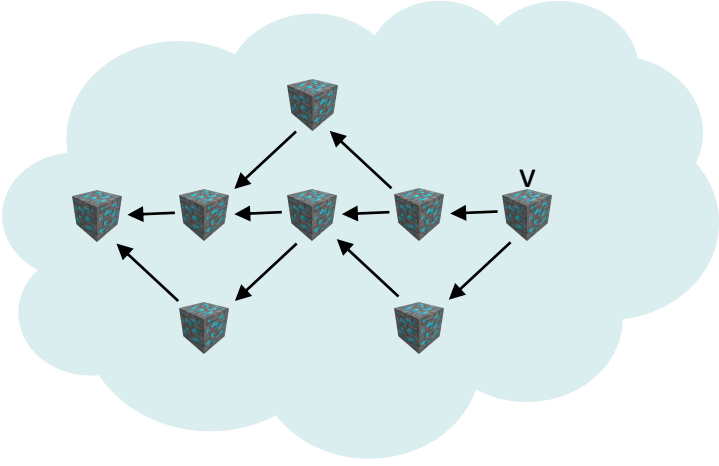


Append Memory Model



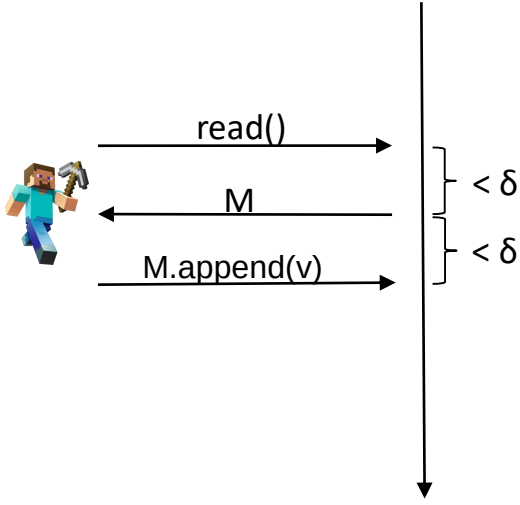


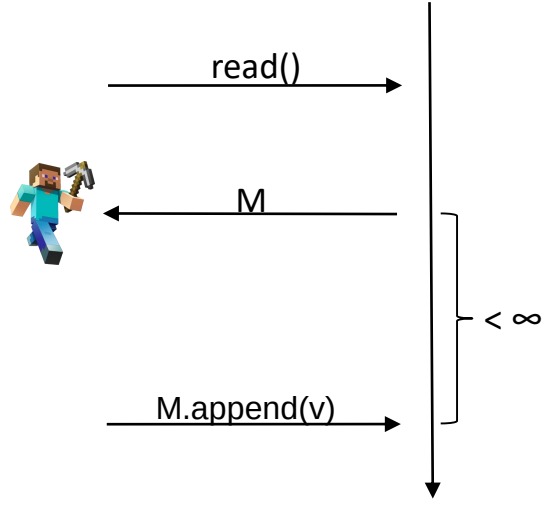
Append Memory Model



M.append(v)

Synchronous vs. Asynchronous





Byzantine Agreement

Binary value:

- either -1 or +1

Correct Party:

- always follows the protocol

+

Termination,
Agreement,
Validity

Byzantine party:

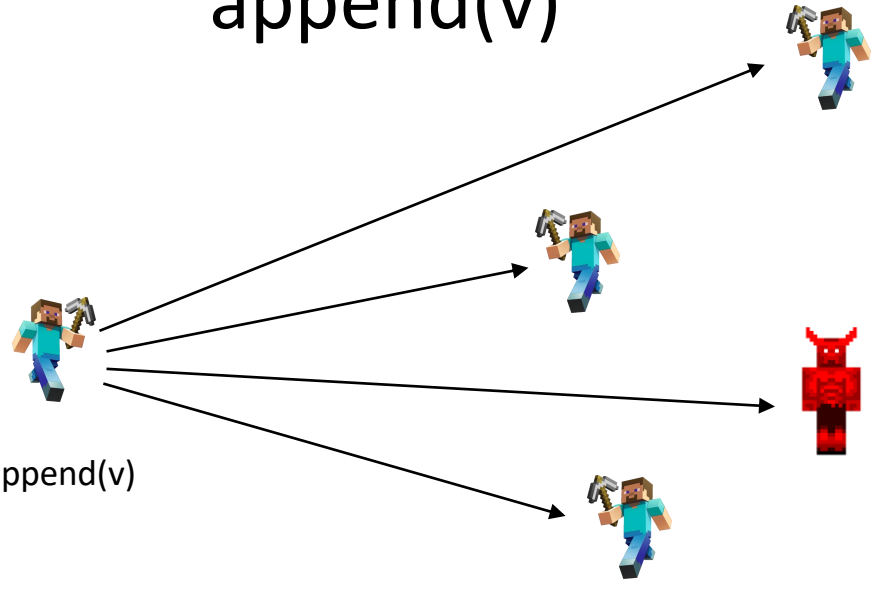
- knows the memory
- controls all byzantine nodes

Append Memory Model - Properties

Synchronous Byzantine agreement	At least t+1 rounds
Asynchronous Byzantine agreement	impossible

Simulation through Message Passing

append(v)



M.append(v)

append(v)

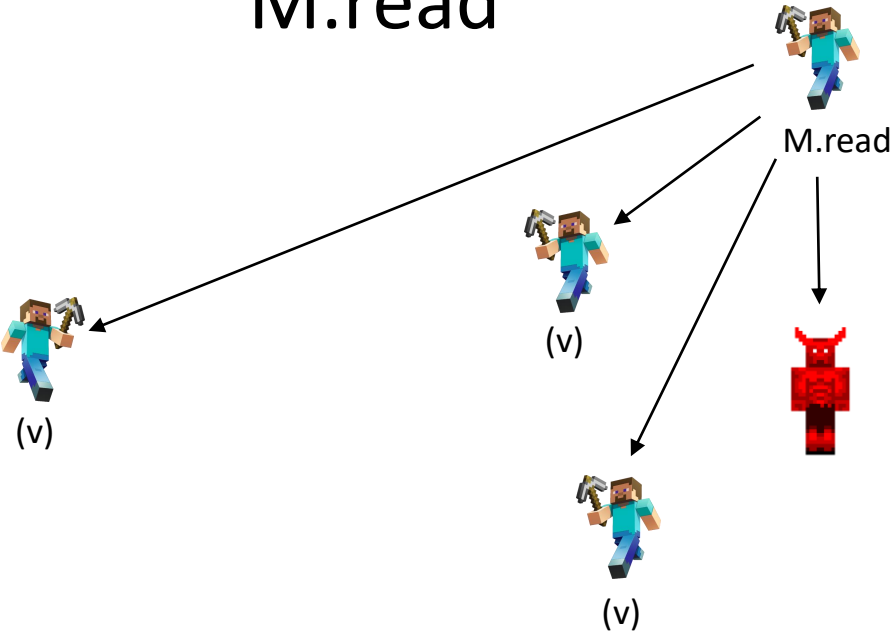
ack(M.append(v))

ack(M.append(v))

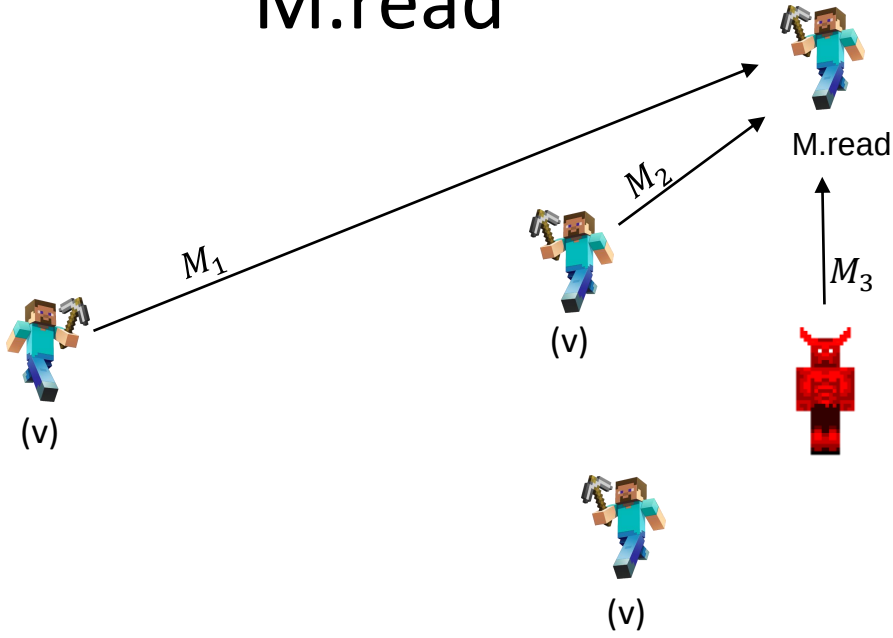
ack(M.append(v))

M.append(v)

M.read



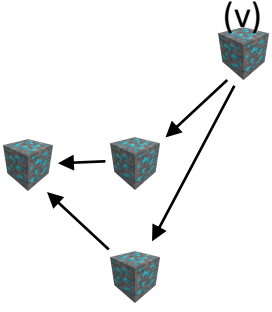
M.read



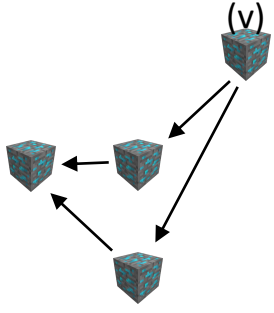
M.read

Accept blocks that are in the snapshots of the majority of all nodes

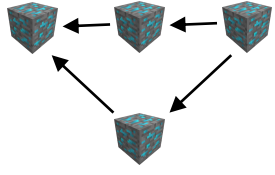
M.read



M_1



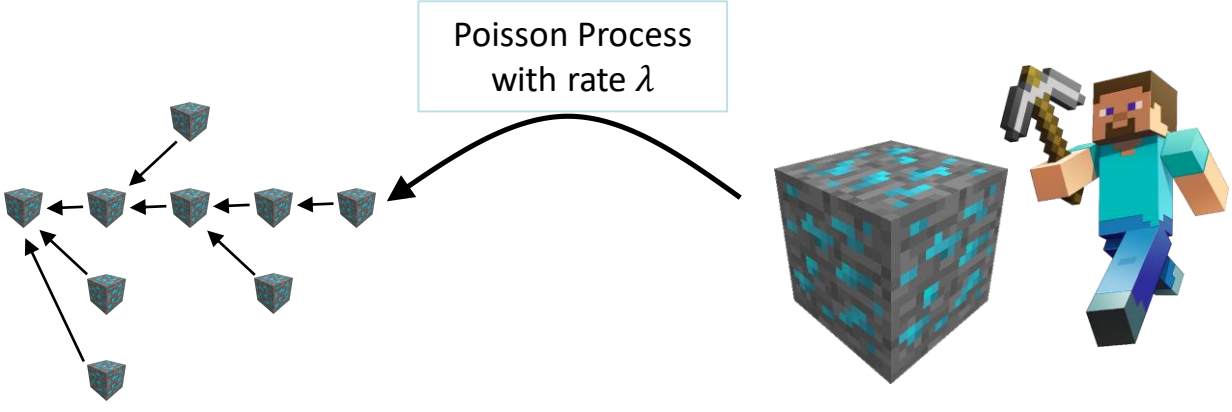
M_2



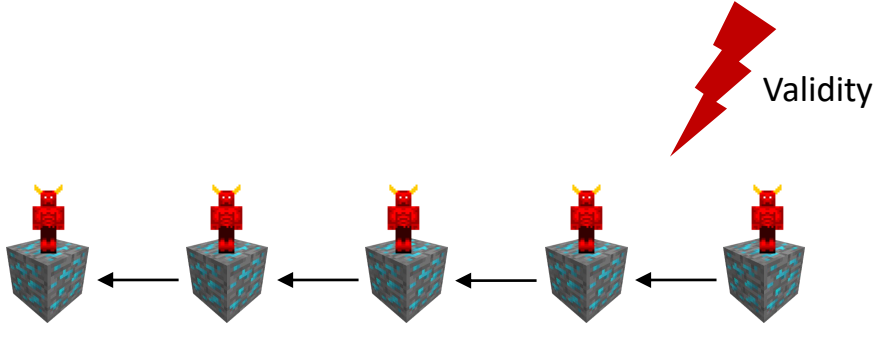
M_3

Resilience Analysis of BlockChain and BlockDAG

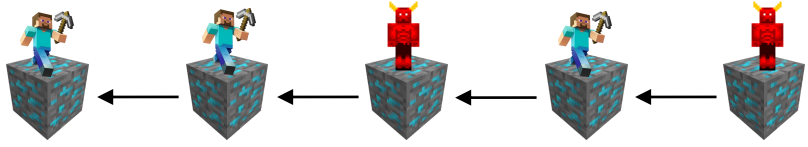
Memory Access



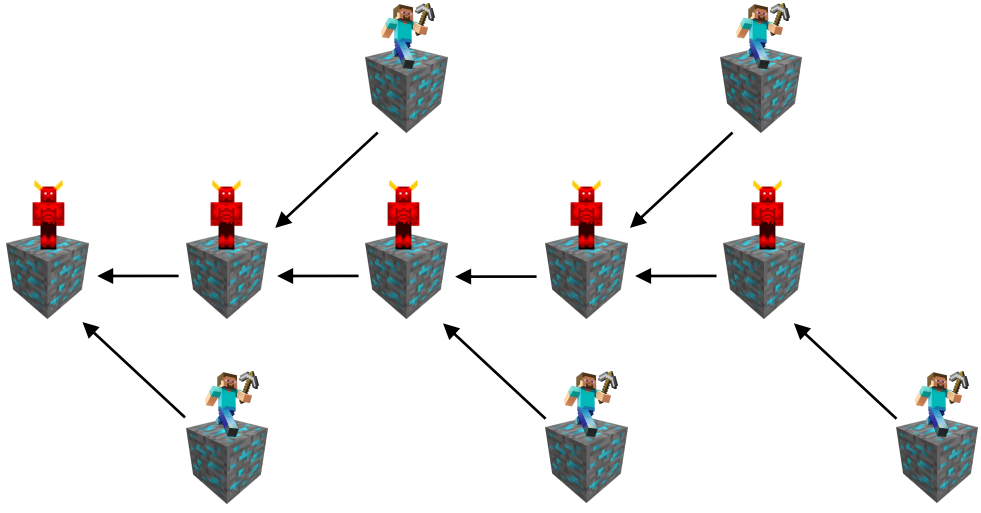
Resilience of the Chain



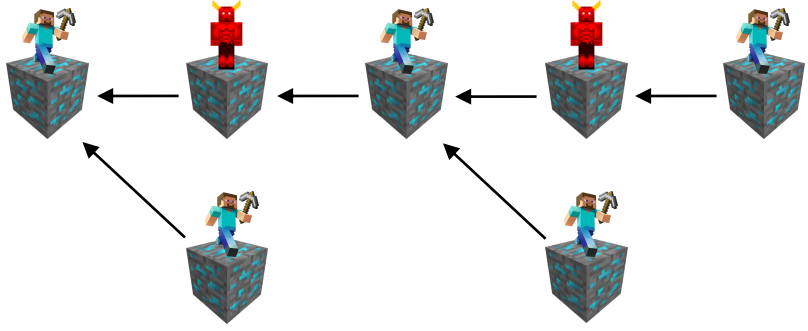
Resilience of the Chain



t=n/2



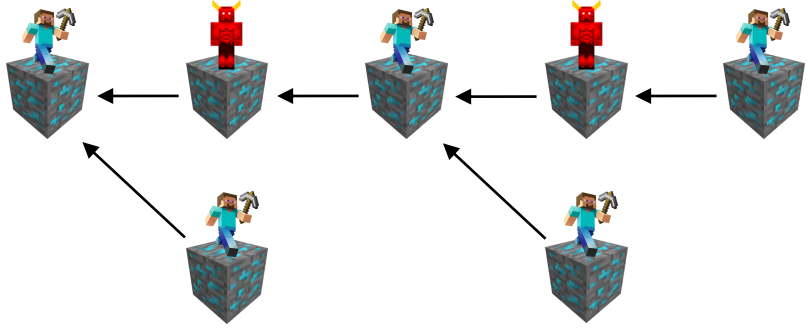
$t<n/3$, $\lambda = 1$



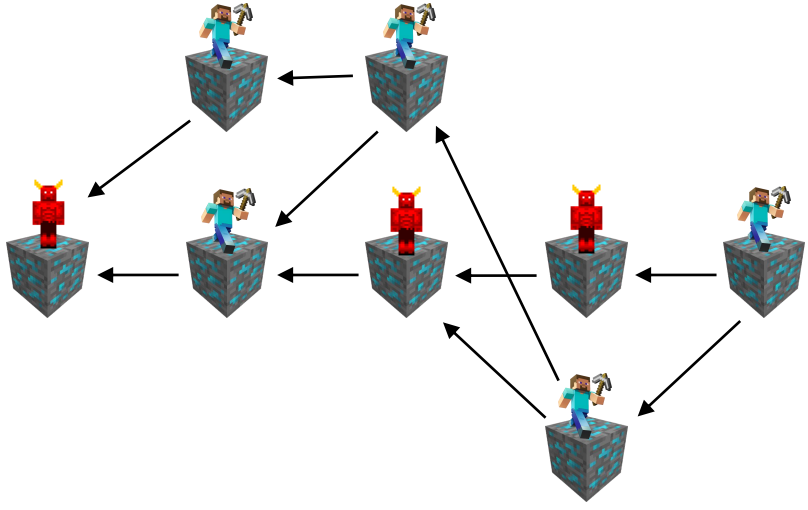
[Sompolinsky, 2015]

Resilience of the Chain

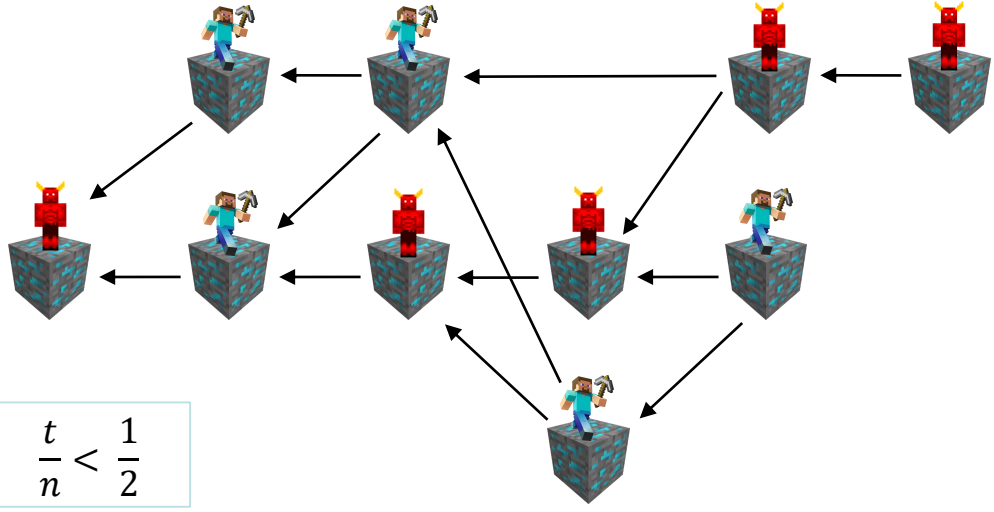
$$\frac{t}{n} < \frac{1}{1 + \lambda(n - t)}$$



Resilience of the DAG



Resilience of the DAG

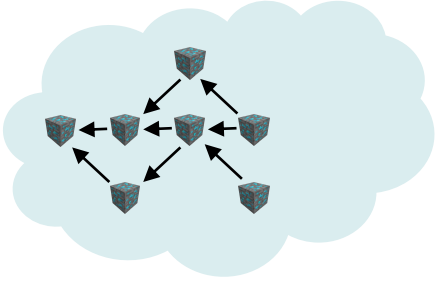


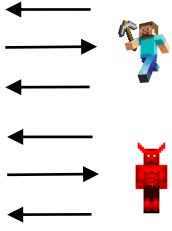
$$\frac{t}{n} < \frac{1}{2}$$

Termination with Validity for DAGs

#  − # 	# 
Ω(1)	$\lambda n \log(n)$
Ω(n)	$\lambda \log(n)$

Summary





- Append Memory Model
- BlockDAG can tolerate up to ½ Byzantine nodes
- resilience than BlockChain depends on the rate λ

Thank You!

Please join the discussion:

Virtual Session 3
July 15, 2020
2:10 pm (EDT)