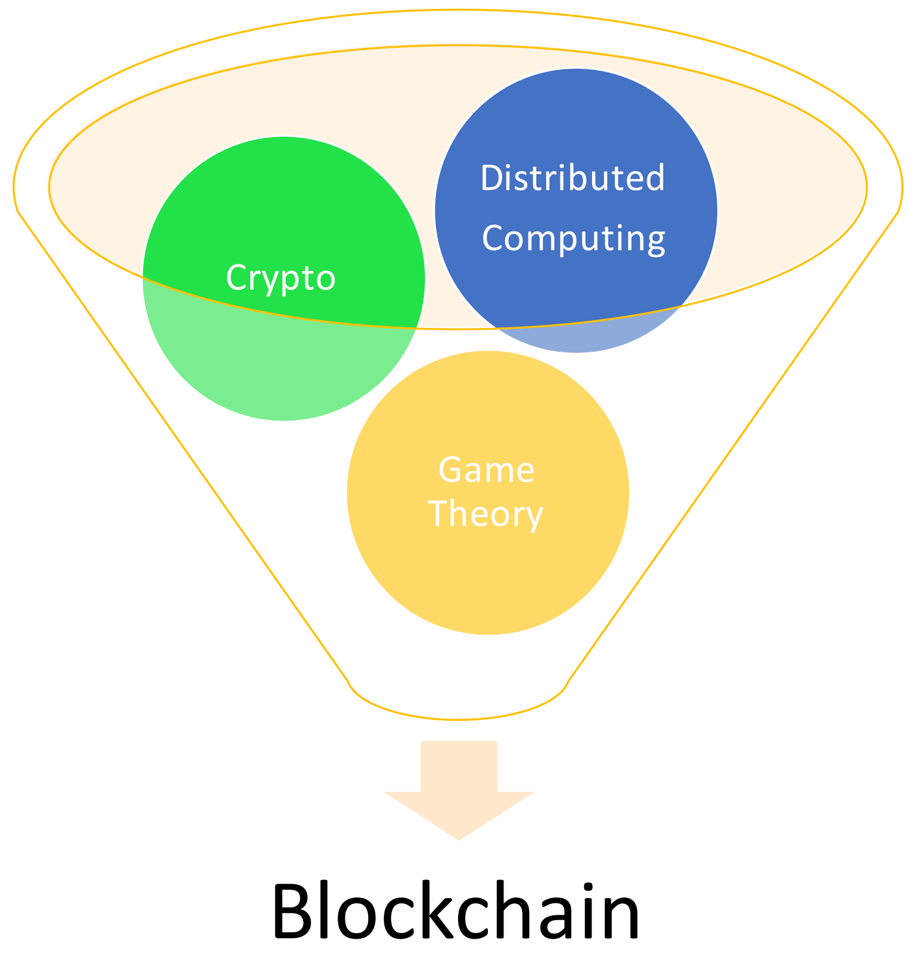
INTERNATIONAL INSTITUTE OF INFORMATION TECHNOLOGY
HYDERABAD

R&D SHOWCASE 2020

Distributed Trust via Blockchains

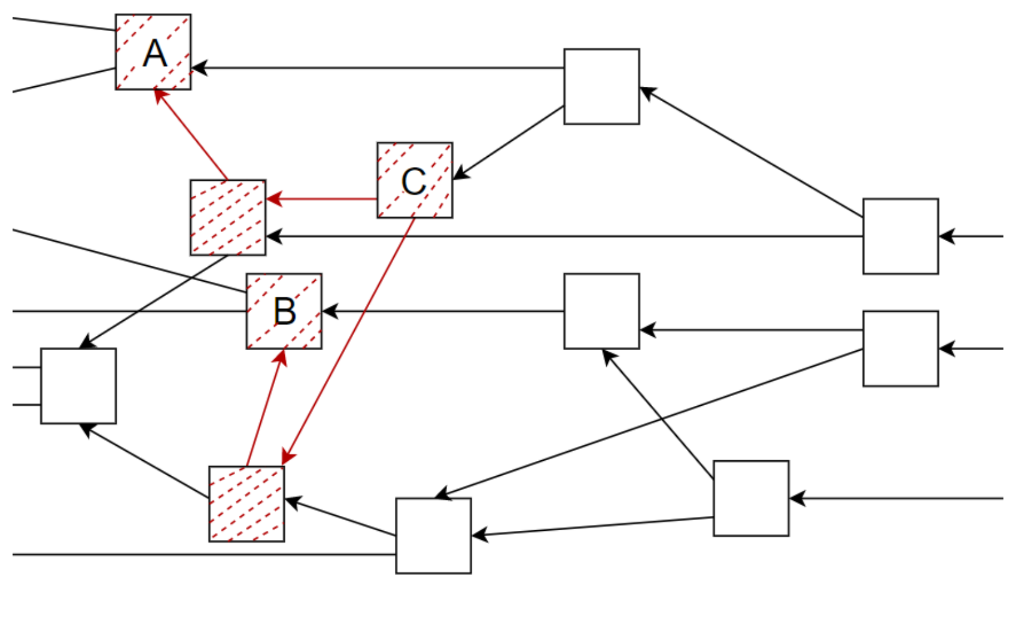
What is a Blockchain?

- Append Only Distributed Ledger
- Uses Cryptographic Primitives: hash functions and digital signatures
- Achieves persistence, liveness, enables distributed trust and supports pseudo-anonymity
- Requires bounded network delay and honest majority enabled by reward schemes
- Applications: Cryptocurrency, Smart contracts, Record keeping

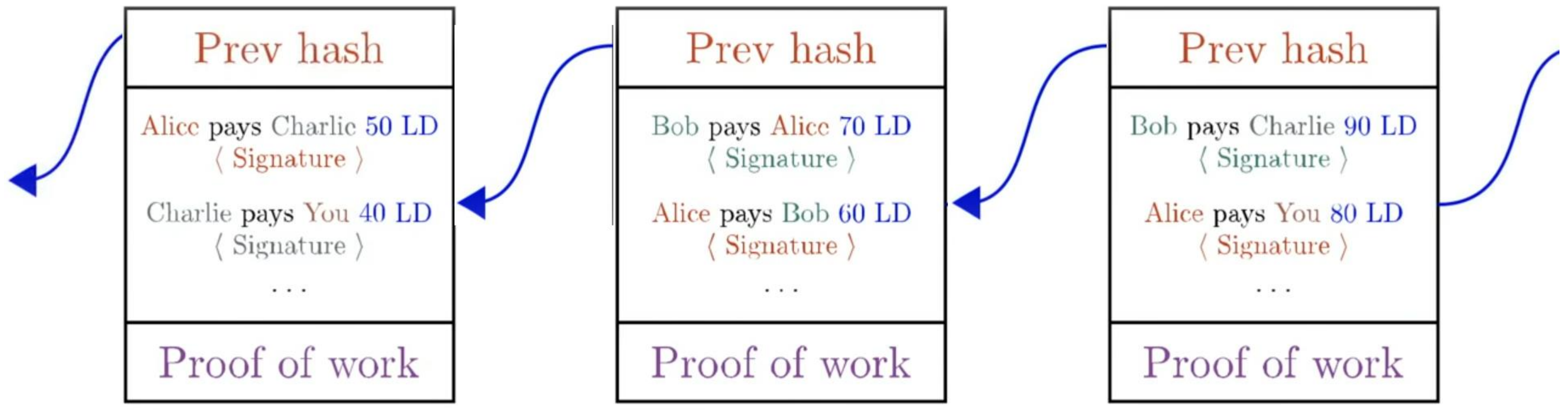


DAGs

- Directed Acyclic Graph
- Not a single chain
- A block can extend multiple blocks
- Can achieve high transactions per second



DAG based blockchains



Prev hash
Alice pays Charlie 50 LD
⟨ Signature ⟩
Charlie pays You 40 LD
⟨ Signature ⟩
. . .
Proof of work

Prev hash
Bob pays Alice 70 LD
⟨ Signature ⟩
Alice pays Bob 60 LD
⟨ Signature ⟩
. . .
Proof of work

Prev hash
Bob pays Charlie 90 LD
⟨ Signature ⟩
Alice pays You 80 LD
⟨ Signature ⟩
. . .
Proof of work

Blocks contain "hashes" of the previous block to form a chain

Mode of Publisher Selection

- Only one block accepted as extension
- Stochastically selection, popular modes:
- Proof of Work: Solve a cryptographic puzzle by brute force computations
- Proof of Stake: Chosen with probability proportional to their stake
- Proof of Location:
- LocalCoin: Trusted nodes validate and process local transactions. Geographically distributed nodes avoid double spend
- Mneme: DAG-based. Proof-of-Context establishes locality. Proof-of-Equivalence summarizes data using regenesis

Liveness and Persistence

- Requirements for any robust ledger
- Liveness: Any transaction broadcast is eventually confirmed
- Persistence: An honest node will agree with a transaction's placement in the ledger if it was confirmed by any honest node
- Blockchain ledgers achieve these by ensuring common prefix, chain quality and chain growth

Publications

- Dimitrios Chatzopoulos, Sujit Gujar, Boi Faltings and Pan Hui, "LocalCoin: An Ad-hoc payment scheme for areas with high connectivity". MobiHoc'16
- Dimitrios Chatzopoulos, Sujit Gujar, Boi Faltings and Pan Hui, "Mneme: A Mobile Distributed Ledger". INFOCOM'20
- Shoeb Siddiqui, Ganesh Vanahalli, Sujit Gujar, "BitcoinF: Achieving Fairness For Bitcoin In Transaction Fee Only Model". AAMAS'20

Recent Work

BitcoinF

- Game theoretic modelling and analysis
- Achieves fairness for miners and users, in transaction fee only model
- Simple modification to Bitcoin

Quick Sync

- Proof-of-Stake protocol
- Differentiates between published blocks
- Common knowledge which block to extend
- Avoids forking amongst honest nodes
- Uses metric derived from Sybil resistant function

Authors: Dr Sujit P Gujar; Shoeb S, Sankarshan Damle, Moin H Moti, Anurag Jain *Research Center Name: Machine Learning Lab*