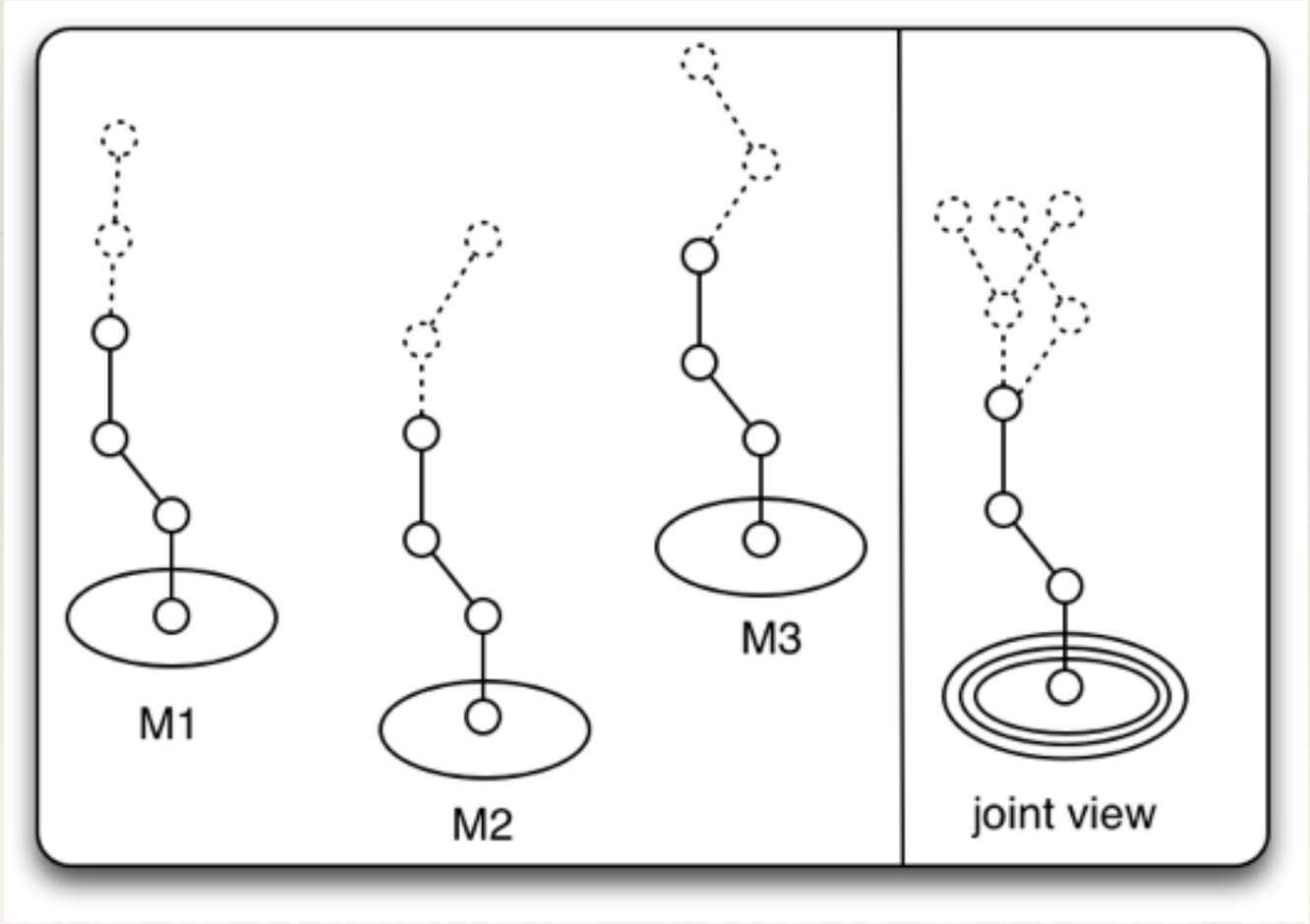
The Bitcoin Backbone: Analysis & Applications

Juan Garay (Yahoo Labs)
Aggelos Kiayias (U. Athens)
Nikos Leonardos (U. Athens)

Bitcoin's blockchains

- Parties (called miners) maintain a distributed data structure in the form of a blockchain.



- blocks contain transactions that are inserted by miners.
- each block requires solving a "proof of work."

Our work : the Bitcoin backbone

- We
  - extract
  - formally describe
  - and analyze
  the “core” of the bitcoin protocol.
- we call this, the bitcoin *backbone* protocol.

Our Results, 1

- We prove two fundamental properties of the bitcoin backbone for an unauthenticated network:
  - the common prefix property. (the honest players' chains share a large prefix).
  - the chain quality property (lower bounding the nr. of entries the honest players plug into the chain)
- both properties require suitable assumptions and impose bounds on the hashing power of the adversary.

Our Results, 2

- common prefix : can be proven assuming *honest majority* under the assumption that the ***network synchronizes much faster than doing proof of work***.
- In case the network desynchronizes and gets closer to the proof of work solution rate, the honest majority bound drops from $1/2$ to $\frac{1}{1+\phi} \approx 38\%$

Our Results, 3

- Regarding bitcoin operation, we prove that
  - the common prefix property implies *the persistence of transactions in the bitcoin ledger.*
  - the chain quality property implies *the liveness of the bitcoin transaction ledger.*

Does bitcoin solve consensus?

- Nakamoto (13.Nov.08) suggested (and sketched a protocol) stating that Bitcoin mining solves the "Byzantine generals" problem.
- This is highly relevant : Byzantine agreement is at the heart of bitcoin system.

Our Results, 4

- We review Nakamoto's suggested solution and even though might thought to do so, it does not solve consensus.
  - it solves a weaker version of the problem where only *agreement* is satisfied but *validity* cannot be guaranteed with overwhelming probability

Our Results, 5

- We prove that a **consensus protocol** can be built over the bitcoin backbone, and
  - common prefix + chain quality protocol imply *agreement* and *validity* with overwhelming probability assuming an honest majority of players

The Bitcoin Backbone: Analysis & Applications

Juan Garay (Yahoo Labs)
Aggelos Kiayias (U. Athens)
Nikos Leonardos (U. Athens)