CryptoContracts

THE FUTURE OF CONTRACTING

organisation

- recap
  - What we already told you…
- creating a block
  - With and without the GUI
- publishing a block
  - Showing it to the network
- verifying a block
  - How to spot cheaters
- harmonizing the network
  - Why we are better than bitcoin
- summary
  - What we‘ve done and why

recap

- Idea

Storing hashes of contracts in a blockchain

Signing the document by cryptographically signing the hash

Storing the public keys in a court based registry

- Hashes

Create document hashes using three hash functions

SHA 3 – WHIRLPOOL – BLAKE

- Storage and registry

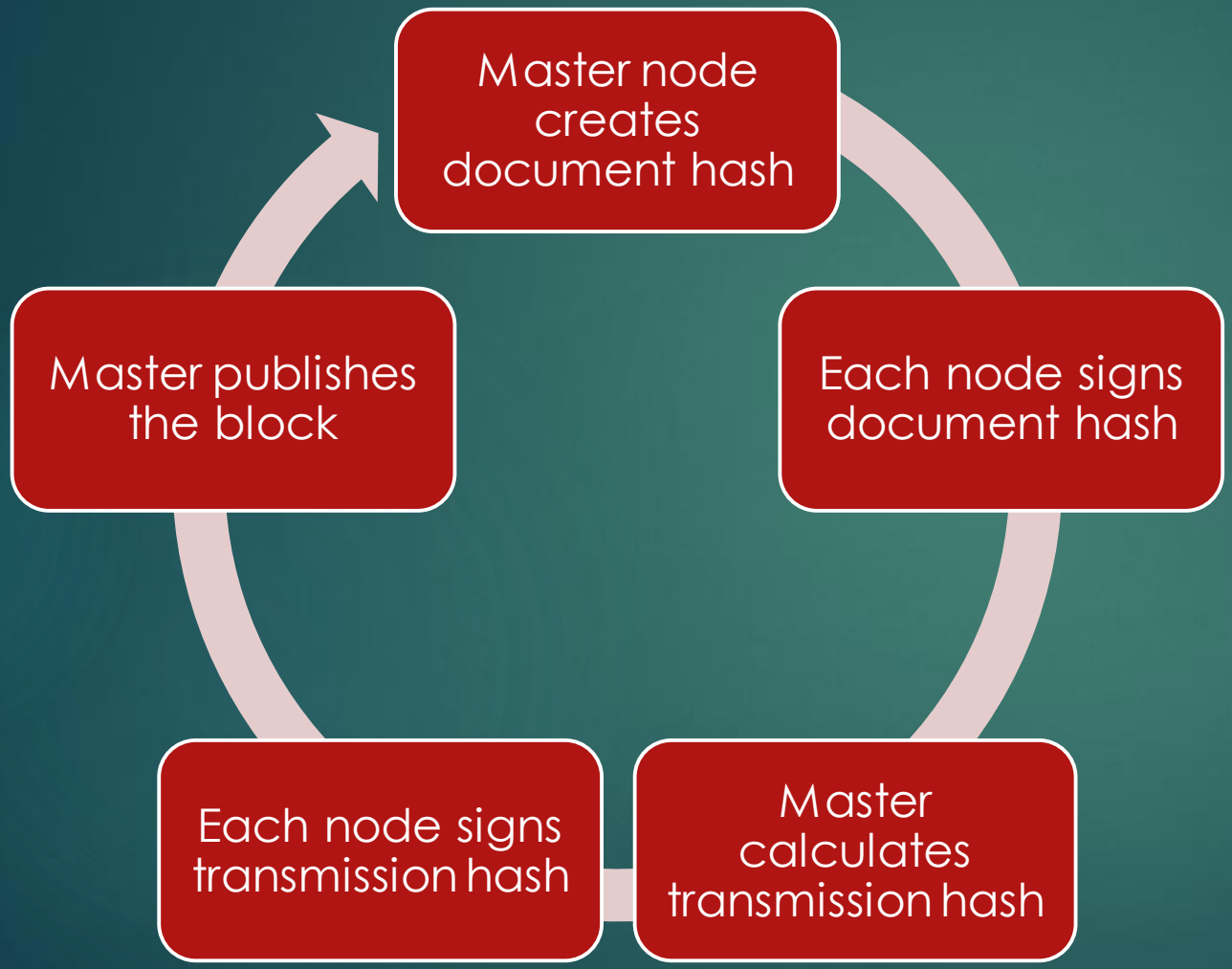
Local storage based on LevelDB

IP registry based on Python Flask

BLOCK STRUCTURE

Hash of previous block
List of public keys
Hash of document
Signed Hash of document
Signed Hash of the block

creating a block



BLOCK STRUCTURE

- Hash of previous block
- Timestamp
- List of public keys
- Hash of document
- Signed Hash of document
- Signed Hash of the block

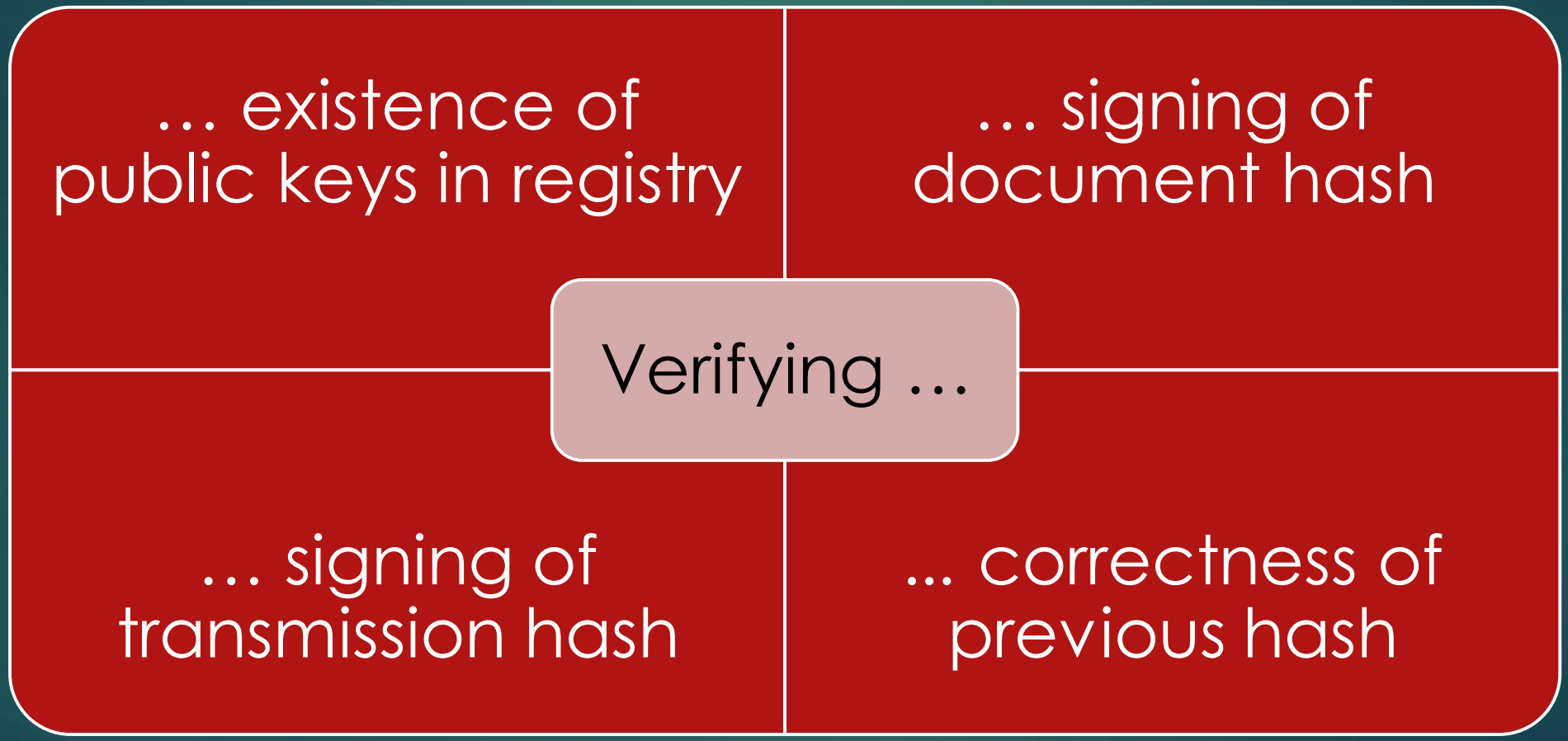
publishing a block

Step 1
- Creating new block
- Adding block to local chain

Step 2
- Get IP list from IP server
- Broadcast the new block

Step 3
- Each recipient verifies new block
- On success, add to own chain

verifying a block



summary

- Problem:
  - How to store and verify legal documents cost efficiently
- Solution:
  - Store using a blockchain
  - Verify using RSA-based signing
- Limitations:
  - Requires a state governed key registry
  - Appropriate fees for multiple key ownership to avoid spamming
  - No incentive for people to maintain a server for clients

Conclusion:
Attractive alternative to paper contracts with option to uniquely identify contracts partners