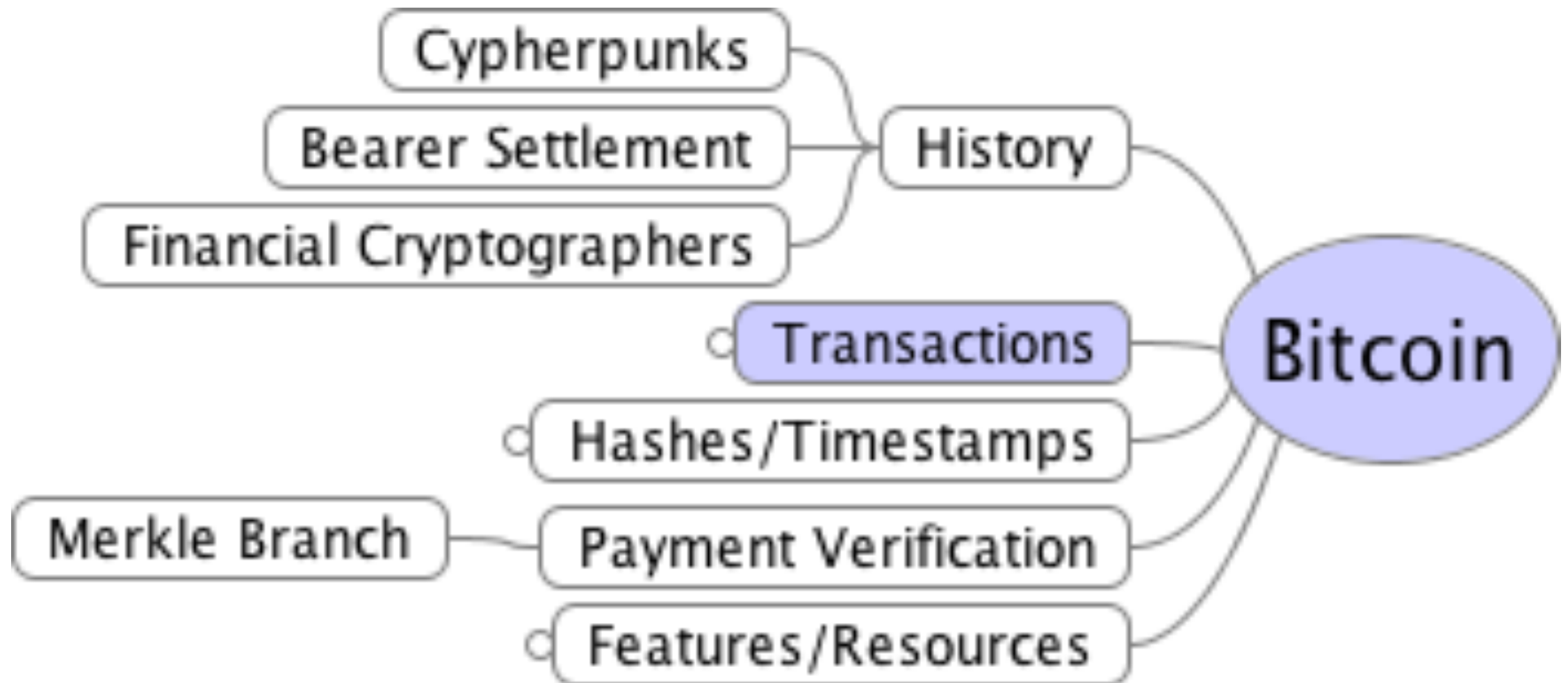


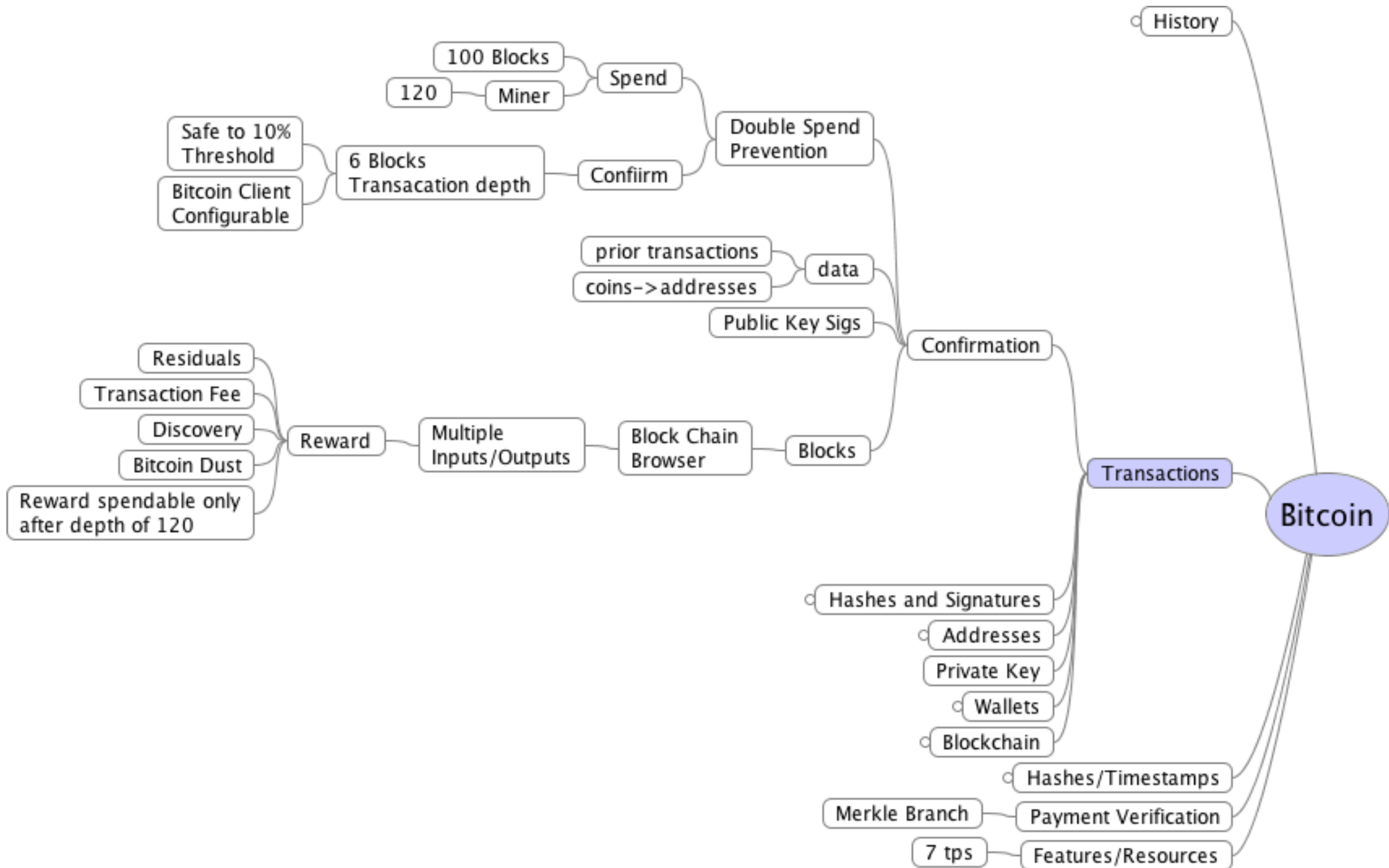
Bitcoin - Future Currency or Terrorist Bank?

Graeme Burnett

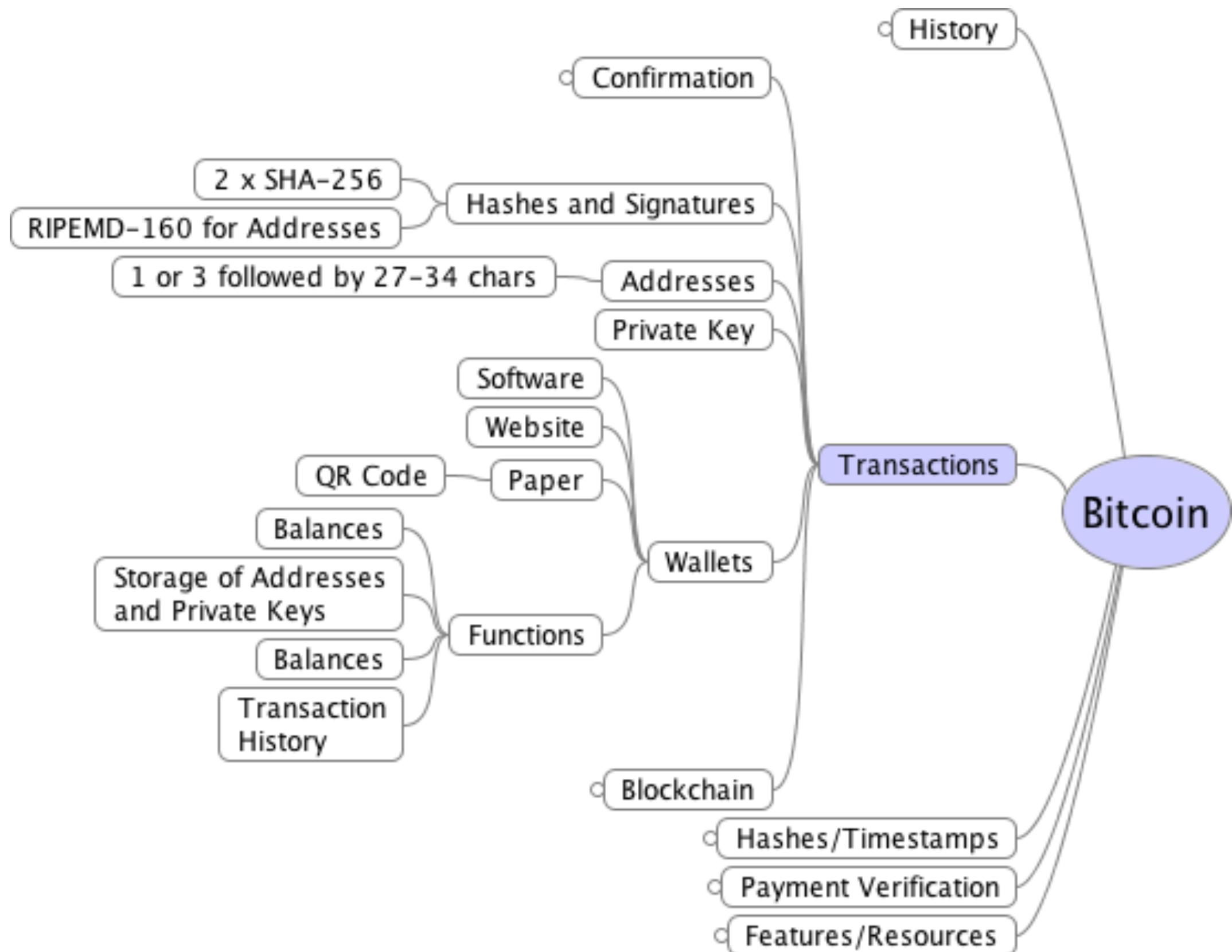
Apr 2016



Bitcoin Transactions - Confirmation



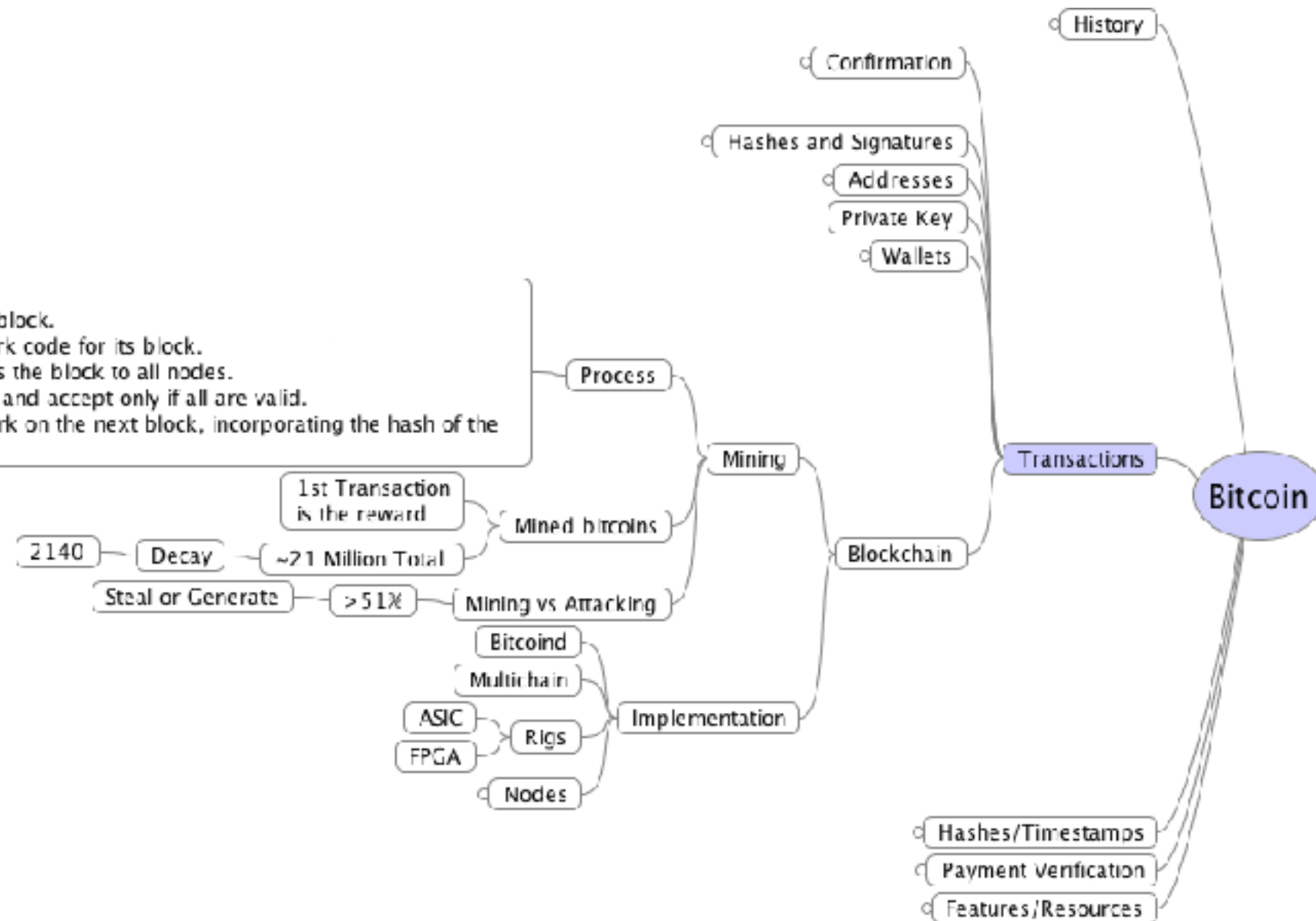
Bitcoin - Hashes, Signature and Addresses



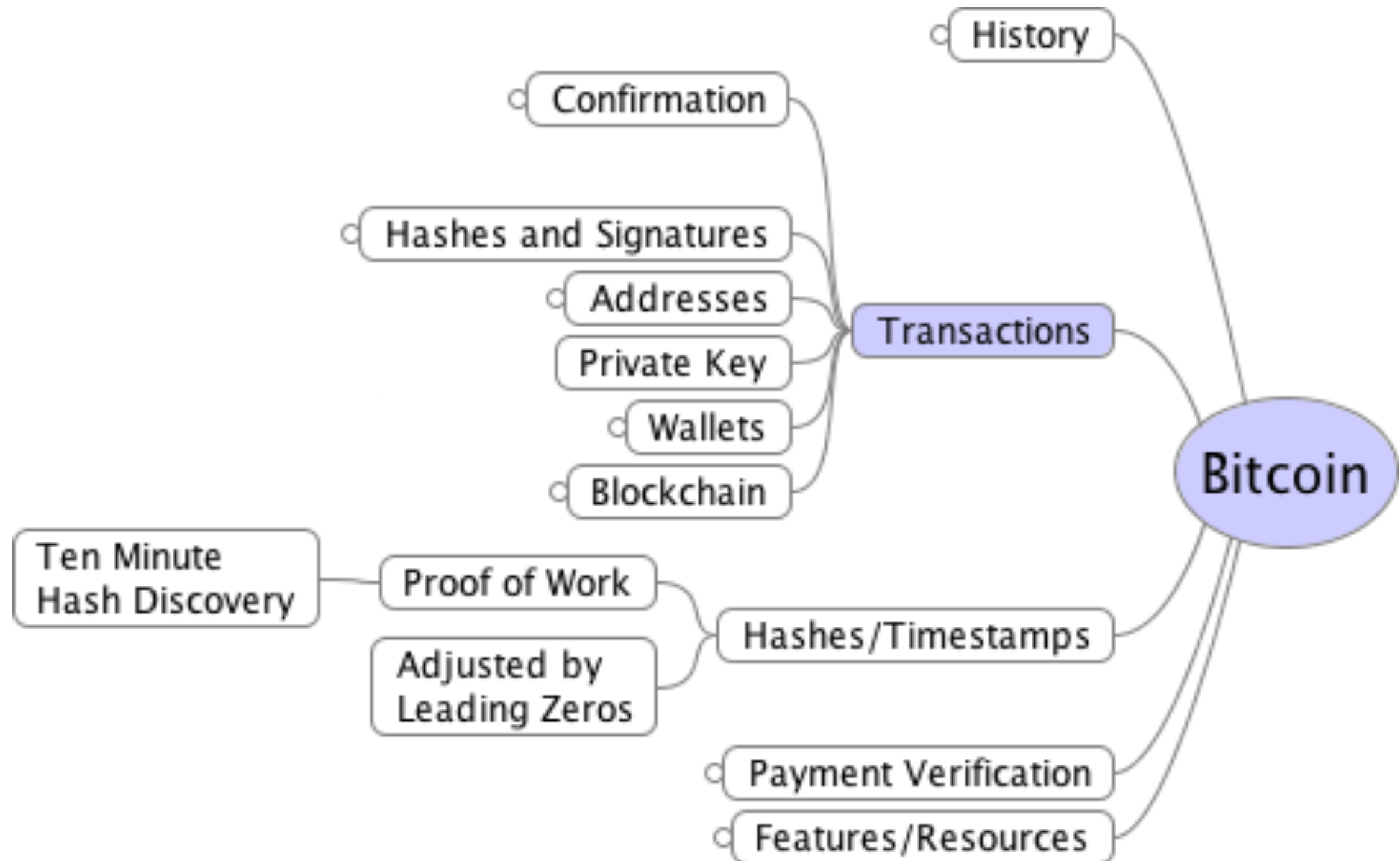
Bitcoin - Blockchain



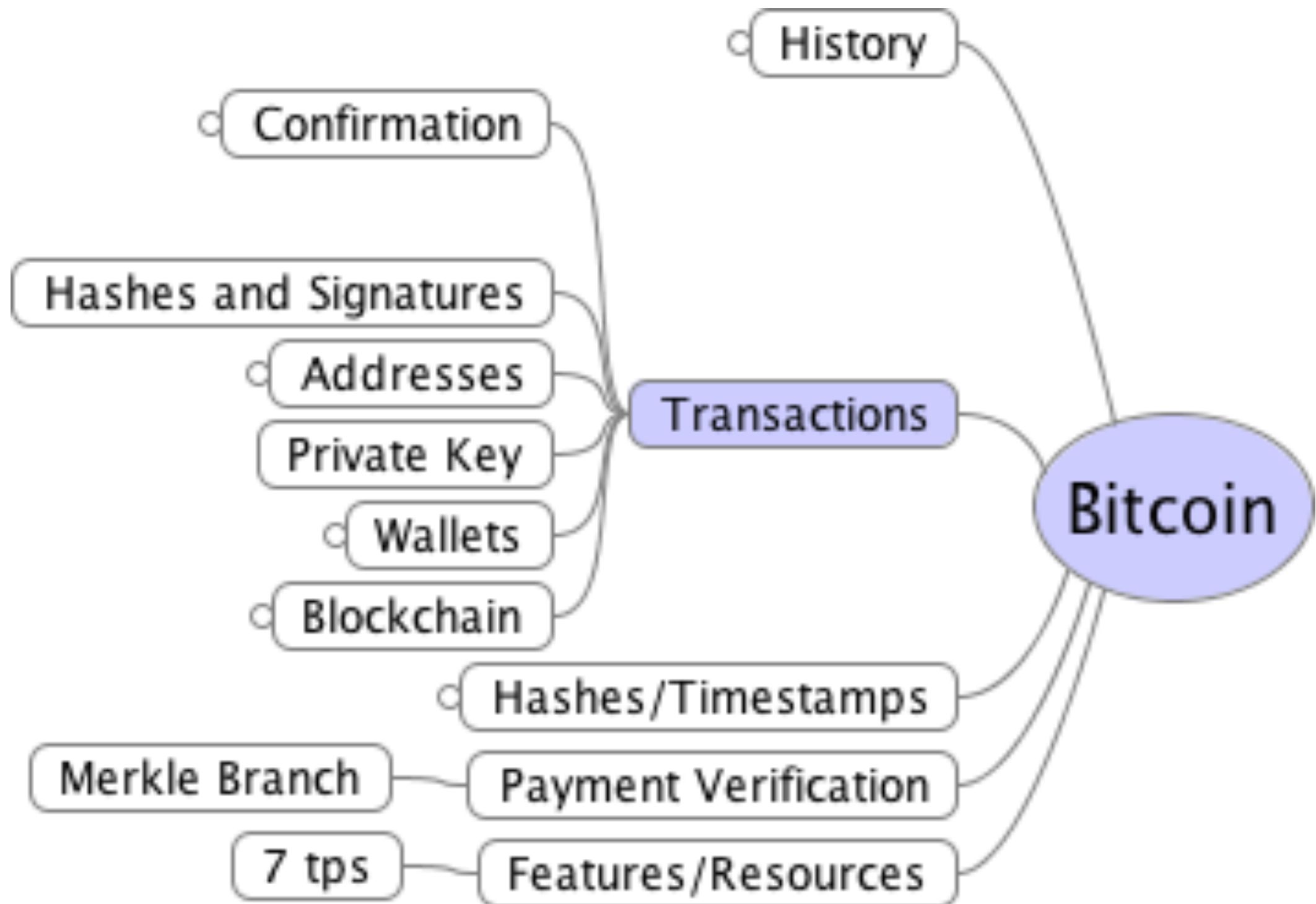
1. New transactions are broadcast to all nodes.
2. Each miner node collects new transactions into a block.
3. Each miner node works on finding a proof-of-work code for its block.
4. When a node finds a proof-of-work, it broadcasts the block to all nodes.
5. Receiving nodes validate the transactions it holds and accept only if all are valid.
6. Nodes express their acceptance by moving to work on the next block, incorporating the hash of the accepted block.



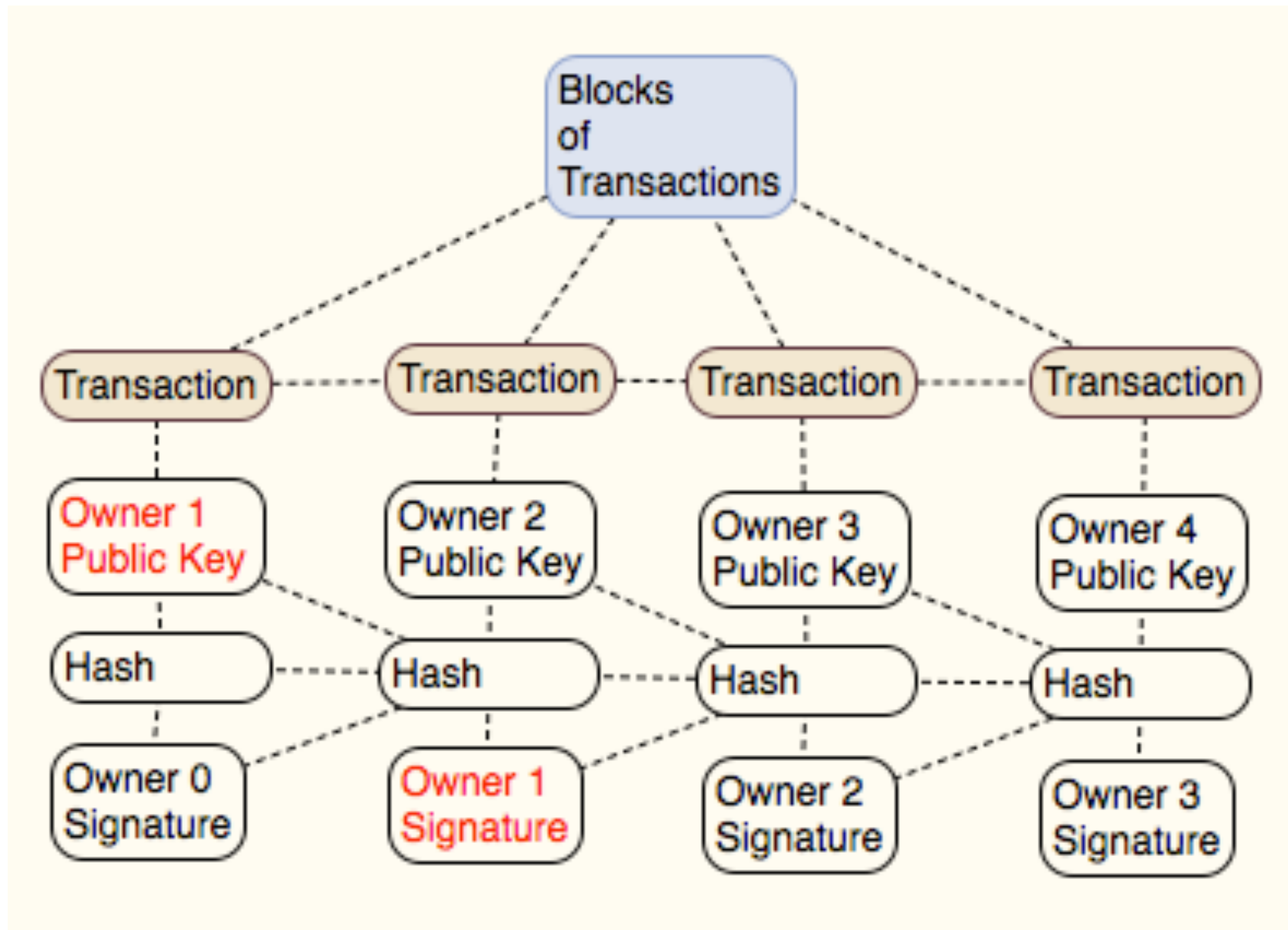
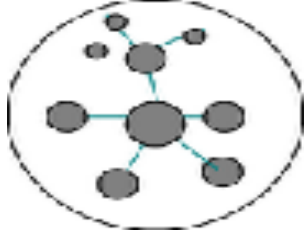
Bitcoin - Hashes/Timestamps



Bitcoin - Payment Verification



Appendix - Blockchain



Conclusion



- It's all about blockchain
- Blockchain == non-repudiation
- Bitcoin 1.0 is vulnerable
- Red funding? Too insecure, too much complexity
- Bitcoin 2.0 - it's not blockchain
- Commercial diversification