



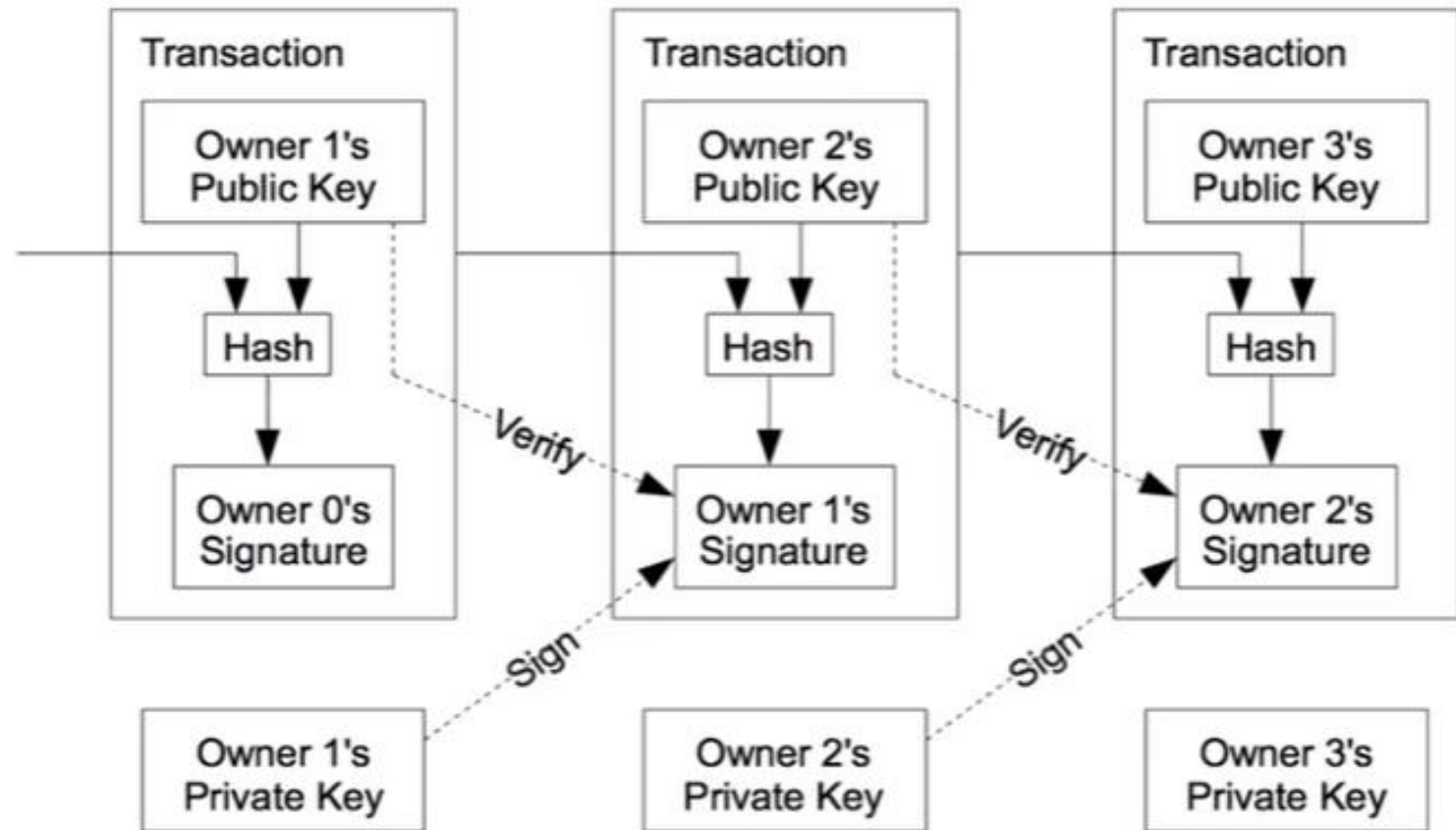
# **Roadmap to Building the Blockchain: Guided by the Bitcoin White Paper**

# bitcoin.pdf

- Published on October 31st, 2008.
- White paper is an official document outlining proposals on an issue.
- Satoshi Nakamoto
- 8 pages - 12 sections.



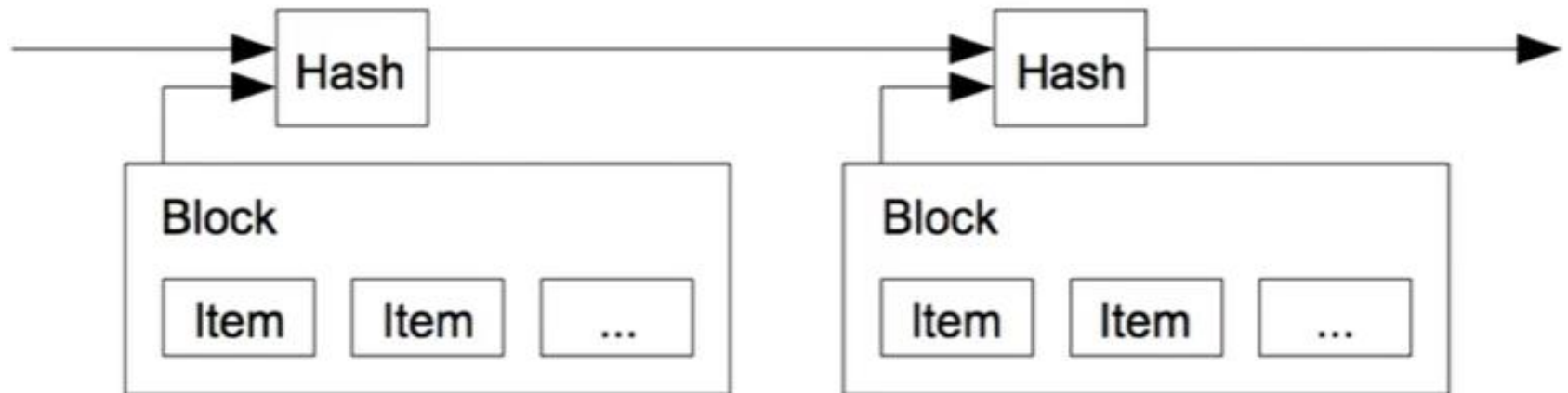
## 2. Transactions



The follow diagrams and text are from the original bitcoin.pdf white paper.

### 3. Timestamp Server

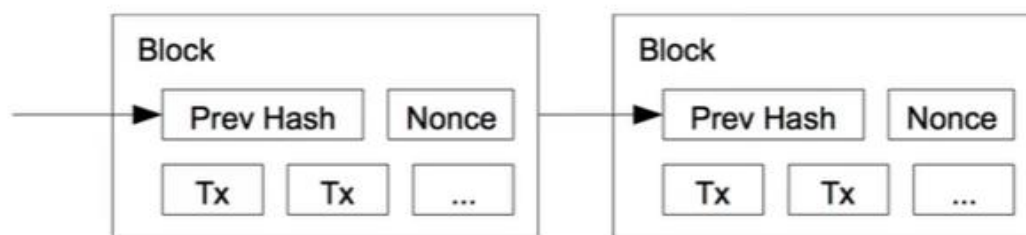
- Timestamps order blocks in the chain.



## 4. Proof-of-Work

To implement a distributed timestamp server on a peer-to-peer basis, we will need to use a proof-of-work system similar to Adam Back's Hashcash [6], rather than newspaper or Usenet posts. The proof-of-work involves scanning for a value that when hashed, such as with **SHA-256**, the hash begins with a number of zero bits. The average work required is exponential in the number of zero bits required and can be verified by executing a single hash.

For our timestamp network, we implement the proof-of-work by incrementing a nonce in the block until a value is found that gives the block's hash the required zero bits. Once the CPU effort has been expended to make it satisfy the proof-of-work, the block cannot be changed without redoing the work. As later blocks are chained after it, the work to change the block would include redoing all the blocks after it.





**5. Network**

**6. Incentive**

- 
- 7. Reclaiming Disk Space**
  - 8. Simplified Payment Verification**
  - 9. Combining and Splitting Value**
  - 10. Privacy**
  - 11. Calculations**





# **Bitcoin: A Peer-to-Peer Electronic Cash System**

Satoshi Nakamoto  
satoshin@gmx.com  
[www.bitcoin.org](http://www.bitcoin.org)



