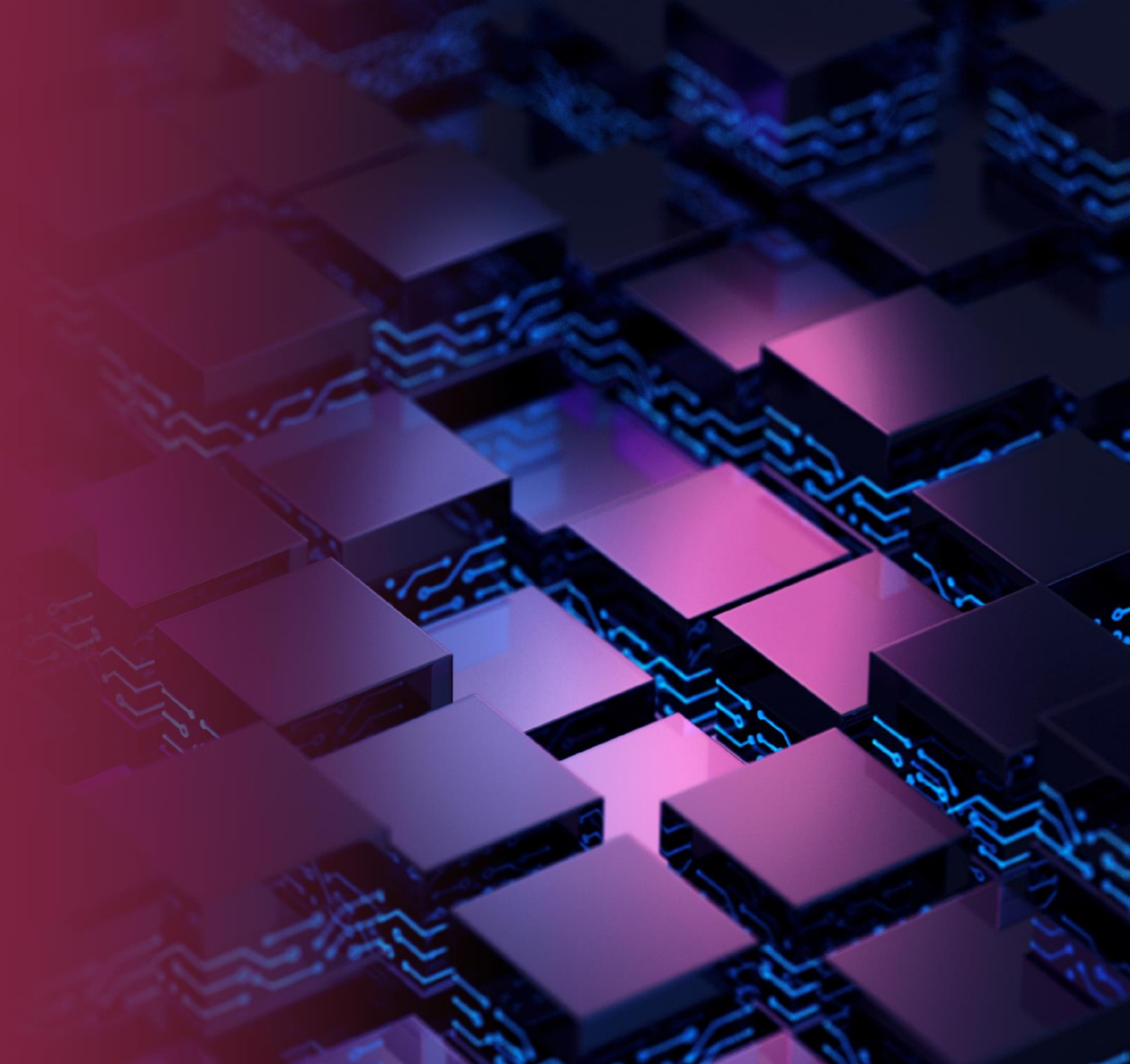
NANYANG TECHNOLOGICAL UNIVERSITY SINGAPORE

CC0007 Science and Technology for Humanity

Blockchain Revolution

Asst Prof Li Yi, NTU

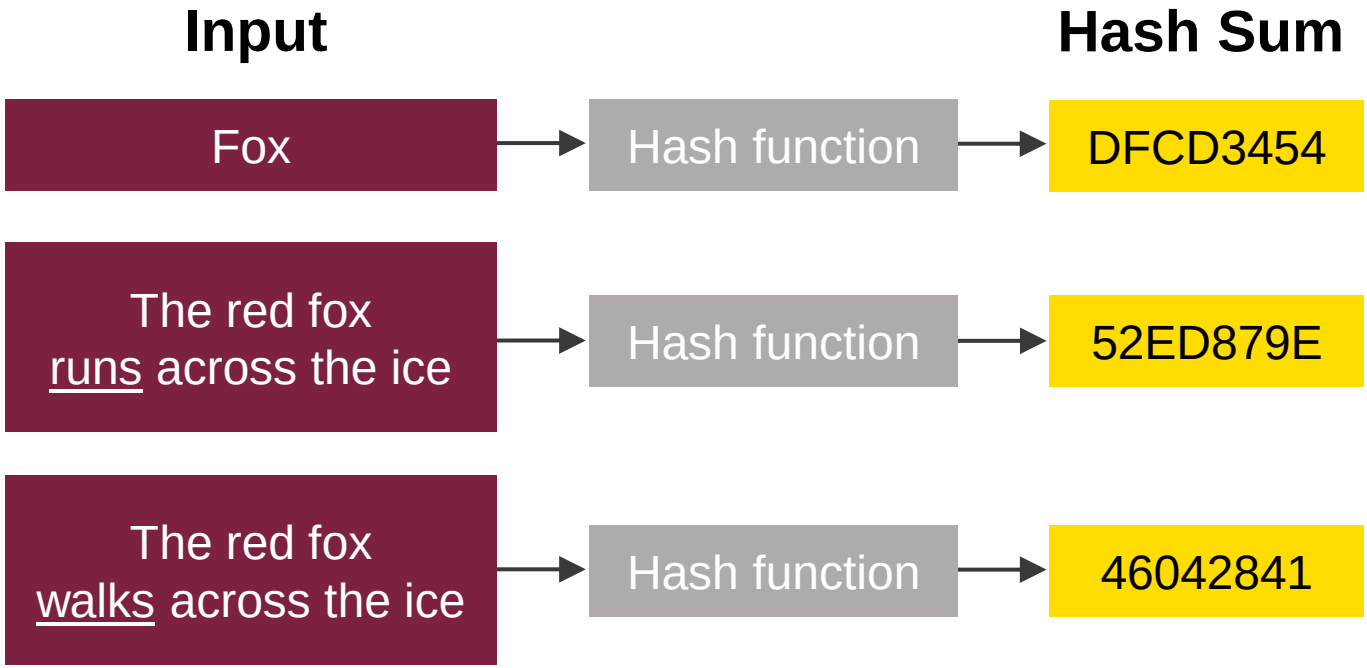
Blockchain Primer



Hash Function

Same lenght

- A **hash function** is a mathematical function that converts a variable-length string of characters into a **fixed-size** numerical value
- **Cryptographic hash function:** one-way function – easy to compute, hard to invert

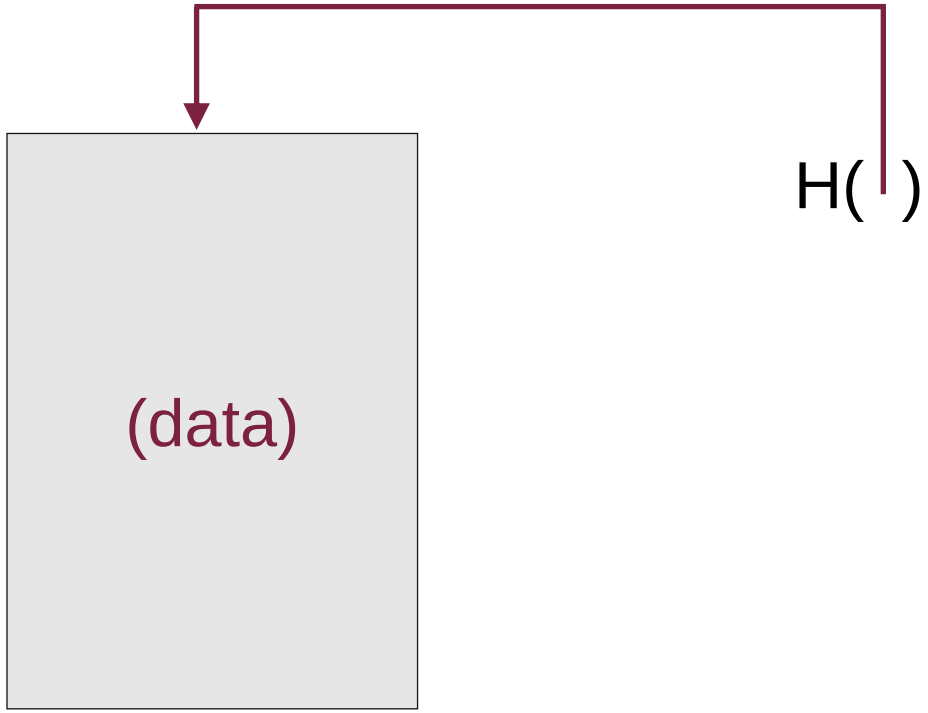


E.g., MD5, SHA-1, SHA-256, …

Lowery, J. M. (2020). *MD5 vs SHA-1 vs SHA-2 - Which is the most secure encryption hash and how to check them*. freeCodeCamp. https://www.freecodecamp.org/news/md5-vs-sha-1-vs-sha-2-which-is-the-most-secure-encryption-hash-and-how-to-check-them/

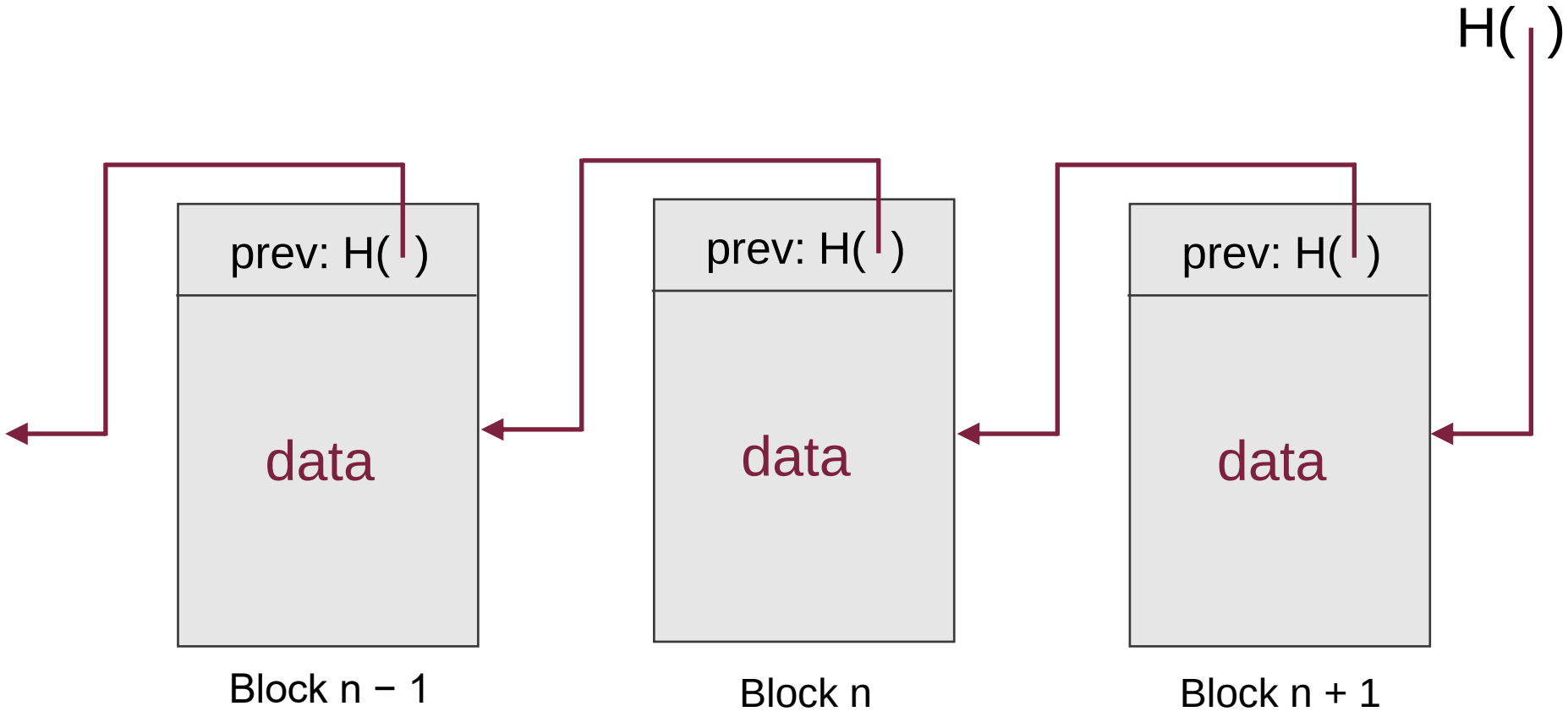
Hash Pointer

- A pointer to where data is stored together with a cryptographic hash of the value of that data at some fixed point in time
- Difference from a regular pointer: This also gives you a way to **verify that the information hasn't been changed**.



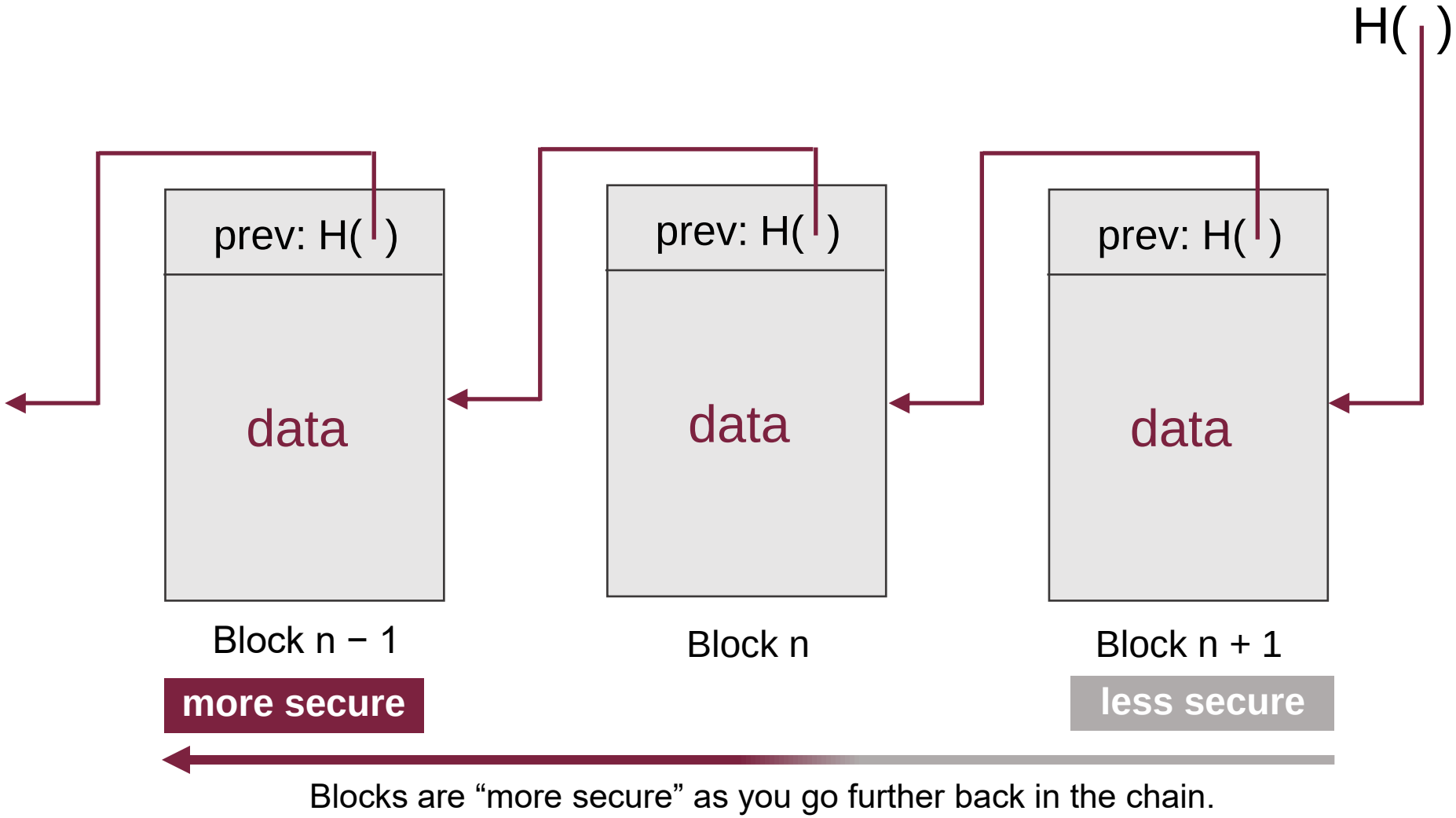
Narayanan, A., Bonneau, J., Felten, E., Miller, A. & Goldfeder, S. (2016). *Bitcoin and cryptocurrency technologies: A comprehensive introduction*. Princeton University Press.

Blockchain



Narayanan, A., Bonneau, J., Felten, E., Miller, A. & Goldfeder, S. (2016). *Bitcoin and cryptocurrency technologies: A comprehensive introduction*. Princeton University Press.

Blockchain

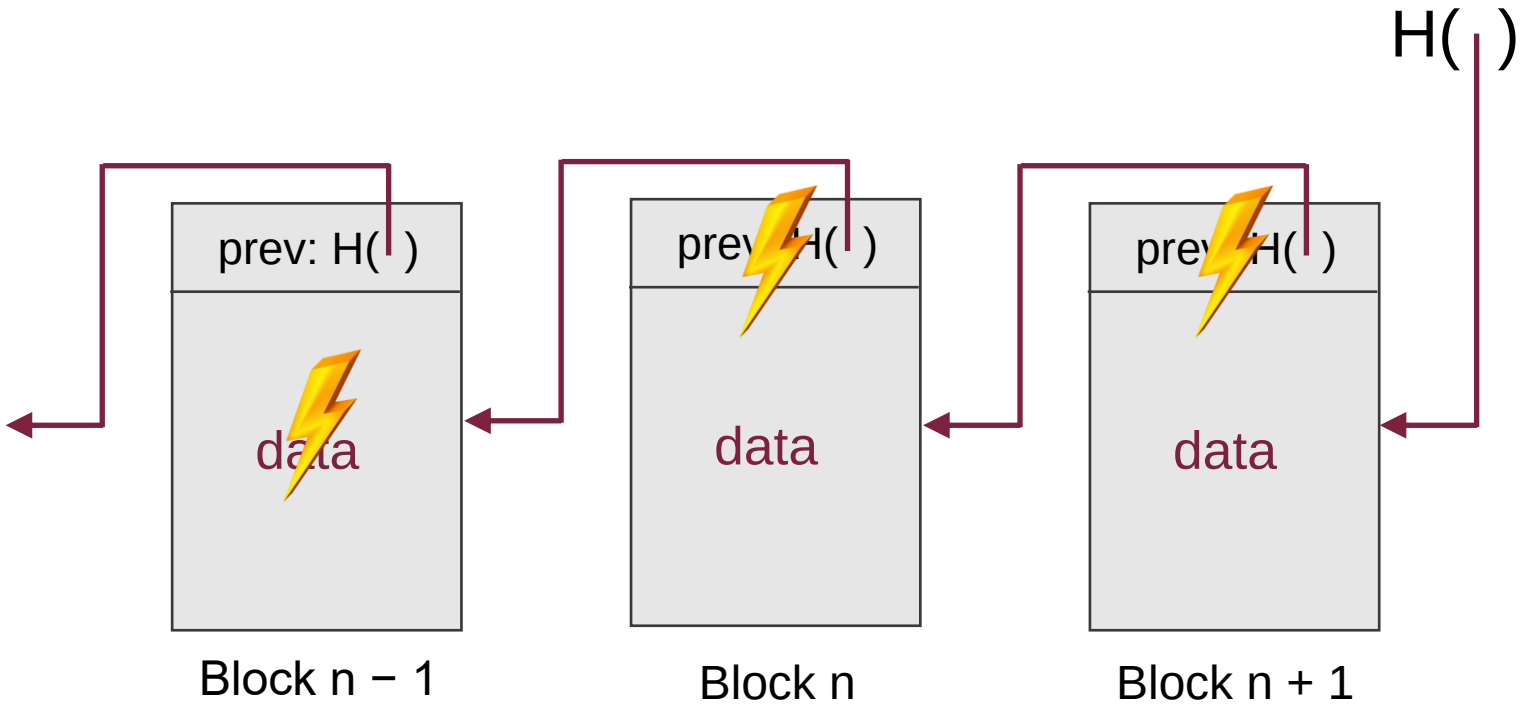


Narayanan, A., Bonneau, J., Felten, E., Miller, A. & Goldfeder, S. (2016). *Bitcoin and cryptocurrency technologies: A comprehensive introduction*. Princeton University Press.

Blockchain as a Tamper-Evident Log

If an adversary modifies data in block n − 1:

- The hash in block n, which is a hash of the entire block n − 1, is not going to match up.
- We will detect the **inconsistency**.

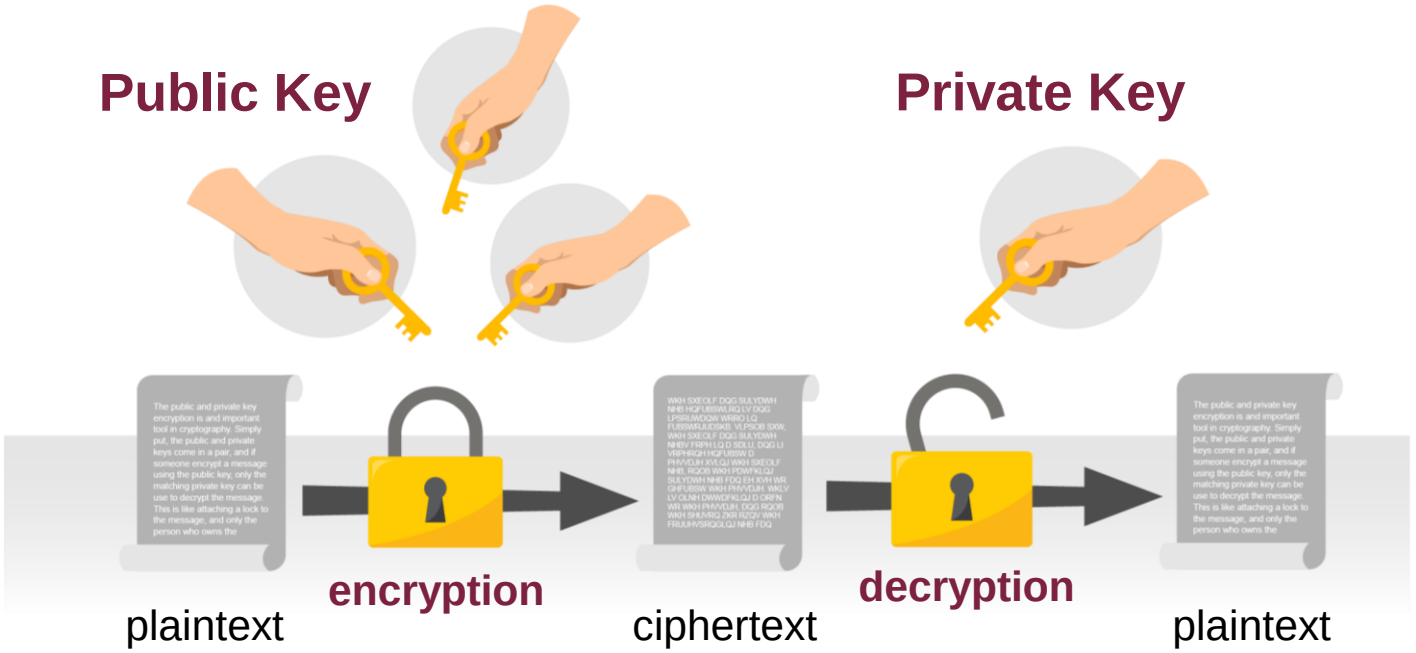


Narayanan, A., Bonneau, J., Felten, E., Miller, A. & Goldfeder, S. (2016). *Bitcoin and cryptocurrency technologies: A comprehensive introduction*. Princeton University Press.

Public and Private Keys

In cryptography:

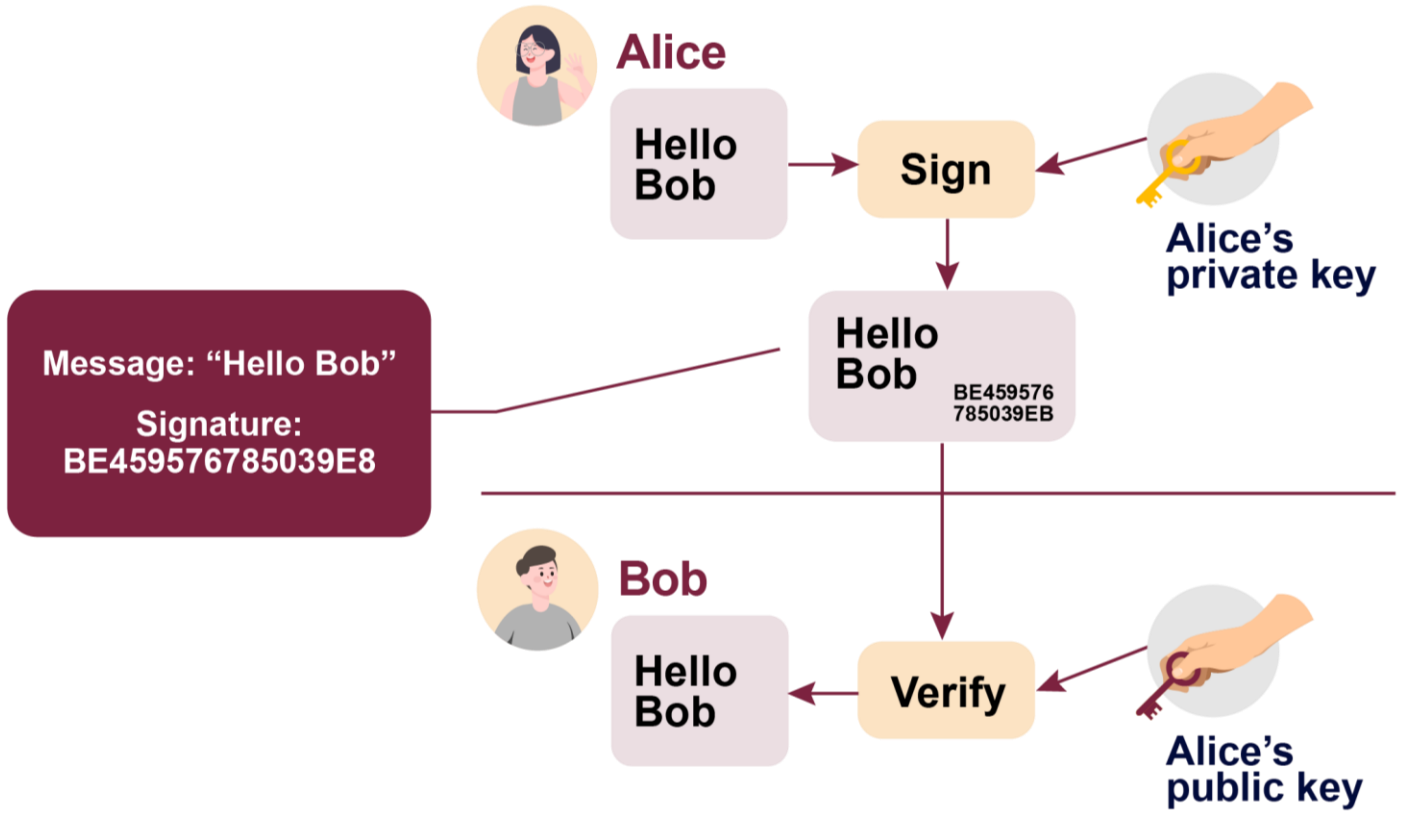
- The public key is used to encrypt, and the private key is used to decrypt.
- It is computationally infeasible to compute the private key based on the public key.



GlobalSign. (n.d.). *What is public-key cryptography?* Retrieved July 20, 2022 from https://www.globalsign.com/en/ssl-information-center/what-is-public-key-cryptography

Digital Signatures

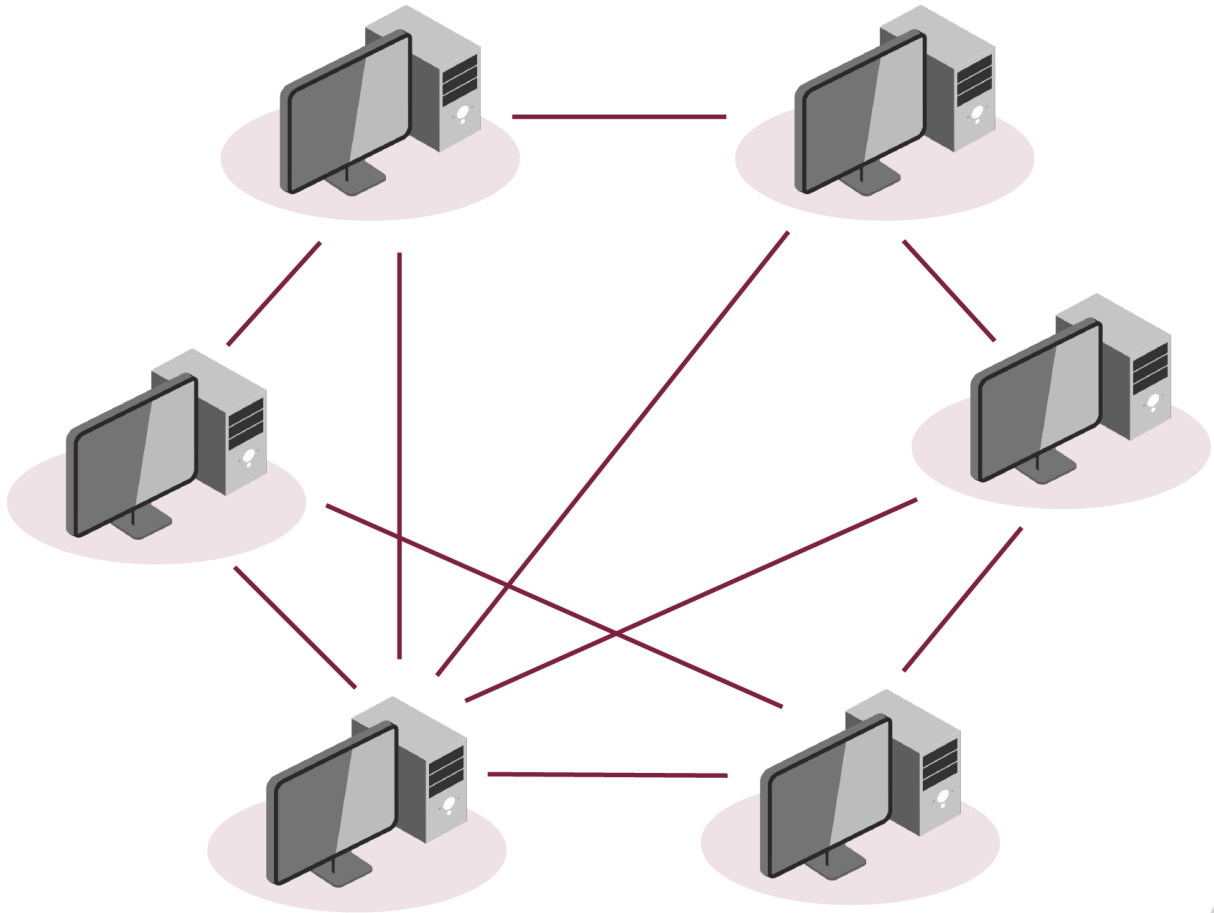
- The digital analog to a handwritten signature on paper.
- **Properties:**
  - Only you can make your signature, but anyone who sees it can verify that it's valid.
  - The signature to be tied to a particular document.



Adapted from FlippyFlink. (2019). *Example showing digital signing* [Illustration]. Wikimedia Commons. https://commons.wikimedia.org/wiki/File:Private_key_signing.svg. CC BY-SA 4.0.

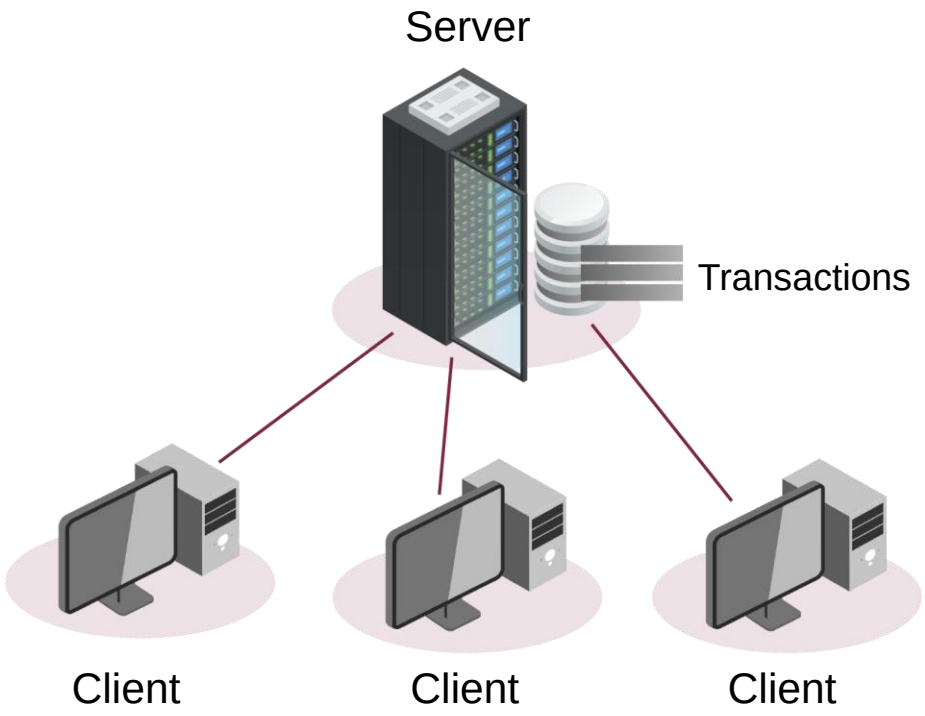
Peer-to-Peer (P2P) Network

- Identical information in each server/node
- Allow the participants of the market to trade directly with each other without any trusted third party to process all trades
- Offer high resistance to transaction censorship
- Cheap to use; private and secure, at least when realised properly
- use for file sharing

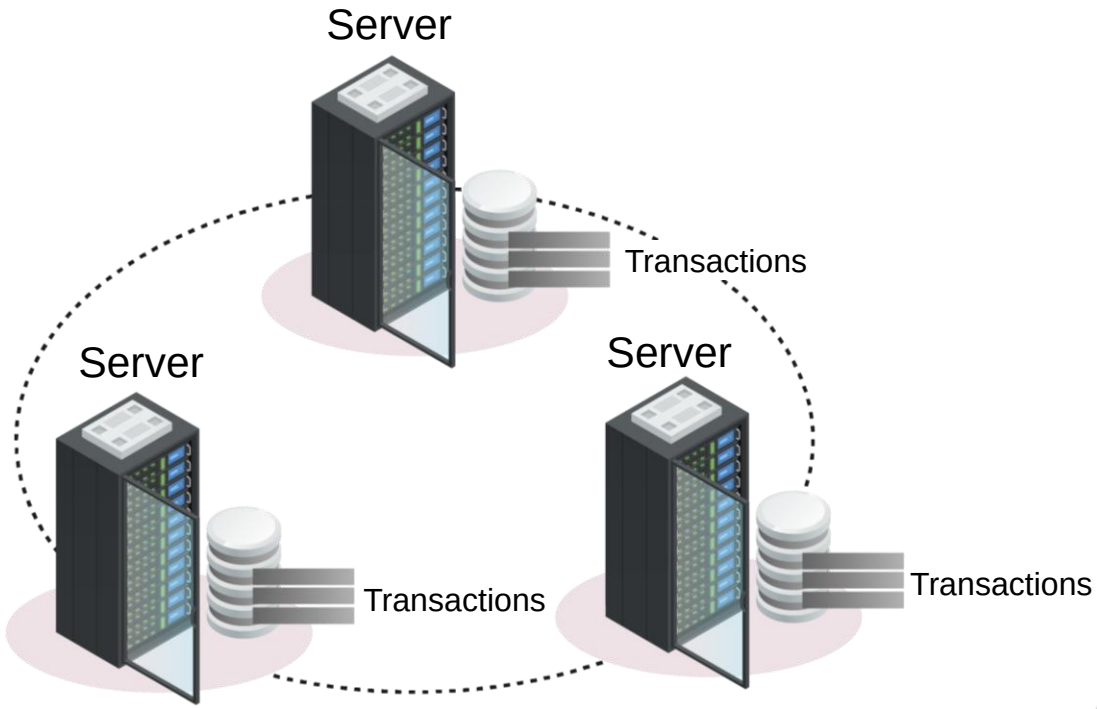


Marshall, A. (2017). *P2P cryptocurrency exchanges, explained*. Cointelegraph. Retrieved July 20, 2022 from https://cointelegraph.com/explained/p2p-cryptocurrency-exchanges-explained

Centralised vs. Decentralised Data Storage

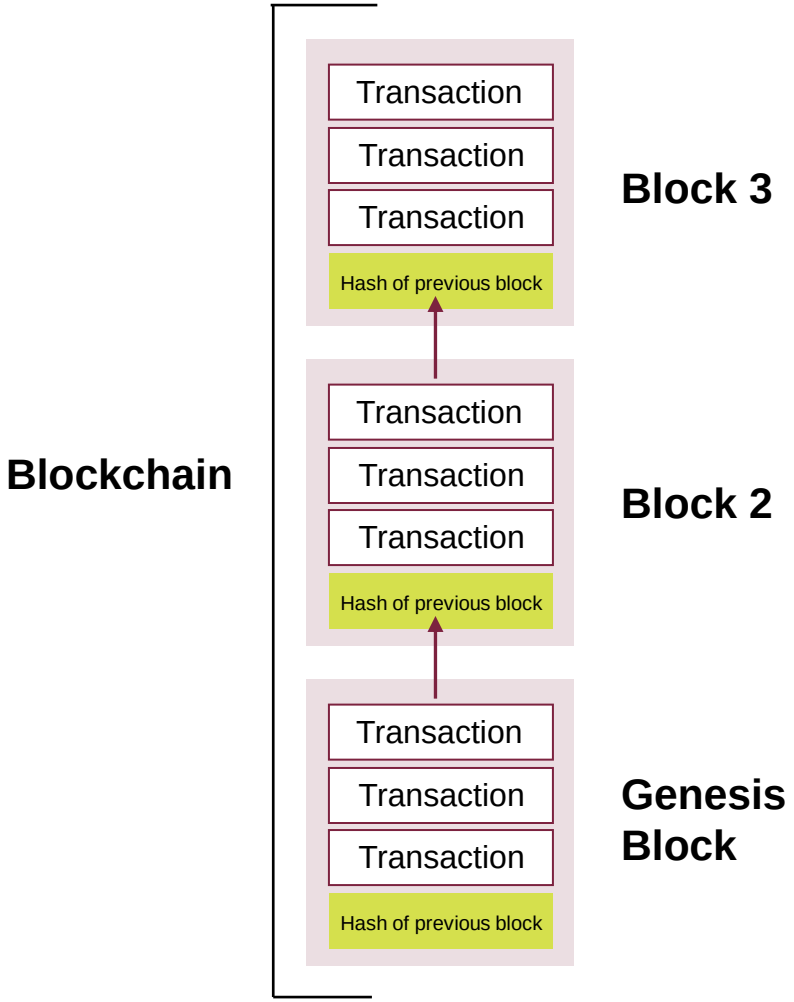


Centralised data storage



Decentralised data storage

Linking Blocks to Form a Blockchain



Nodes in blockchain network