Bitcoin: A Peer-to-Peer Electronic Cash System

By Timothy Chen
Introduction

• Bitcoin uses peer-to-peer technology to operate with no central authority or banks

• Managing transactions and the issuing of bitcoins is carried out collectively by the network.

• Bitcoin is open-source. Its design is public, nobody owns or controls Bitcoin and everyone can take part.
Transactions

- Public key - verify the ownership of signature.
- Private key - Use to sign the coin for owner verification.
Timestamp Server

- Peer to peer let everybody know a coin history
- Prevent give use same coin twice, and all transition has to be public
- Example: User give some one coin then let everyone know at what time you give coin
How Do we Get bitcoins

- Use SHA 256 hash general a hash give 32 bits number, which we call mining
- Verify the node to node.
Calculations

\[ p = \text{probability an honest node finds the next block} \]
\[ q = \text{probability the attacker finds the next block} \]
\[ q_z = \text{probability the attacker will ever catch up from } z \text{ blocks behind} \]

\[ q_z = \begin{cases} 
1 & \text{if } p \leq q \\
(q/p)^z & \text{if } p > q 
\end{cases} \]
Conclusion

- Bitcoin is a framework of coins made from digital signature, which provides strong control of ownership, and prevent a from double spending.