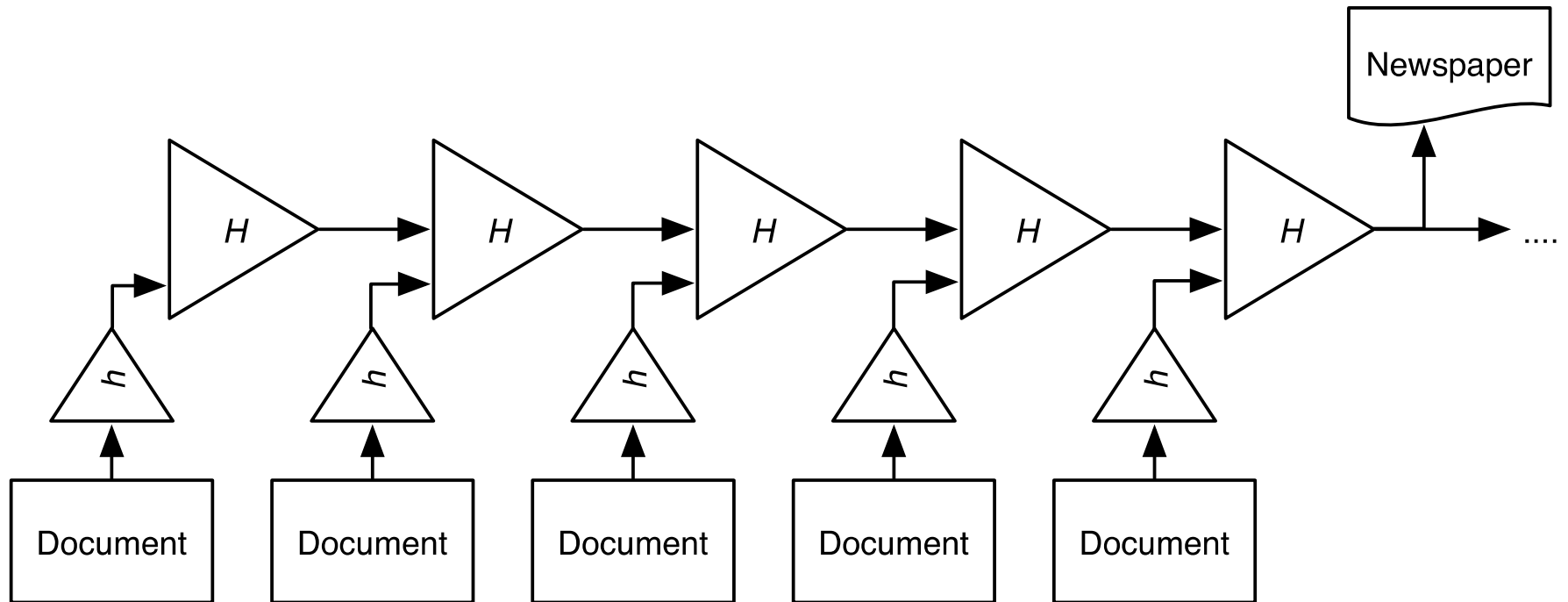


Blockchain (Bitcoin)

Four ideas

- Hash chaining – Unalterable history
- Public key cryptography – Signatures
- Addition/Subtraction – General ledger
- Notarization – Proof of validity

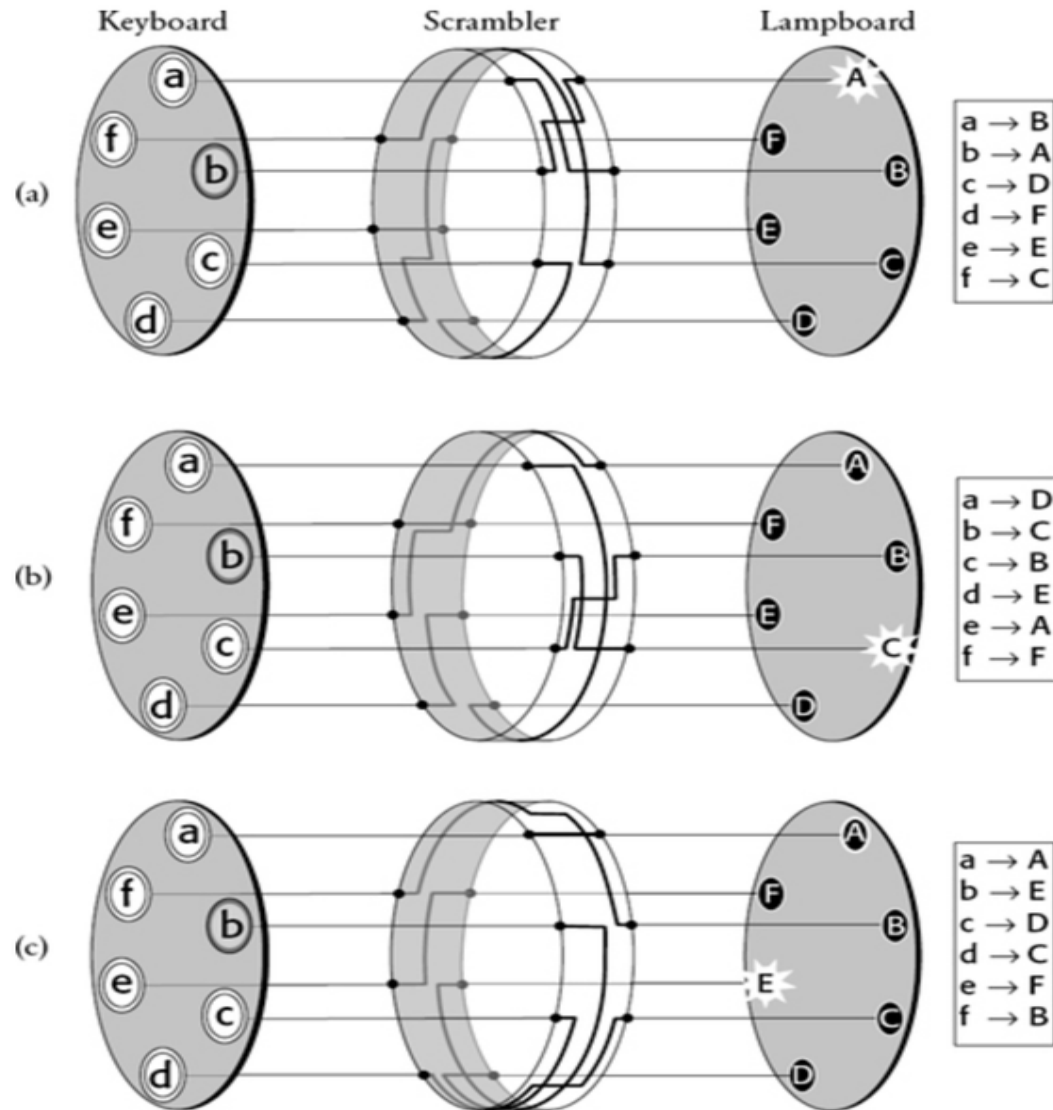
Hash chaining



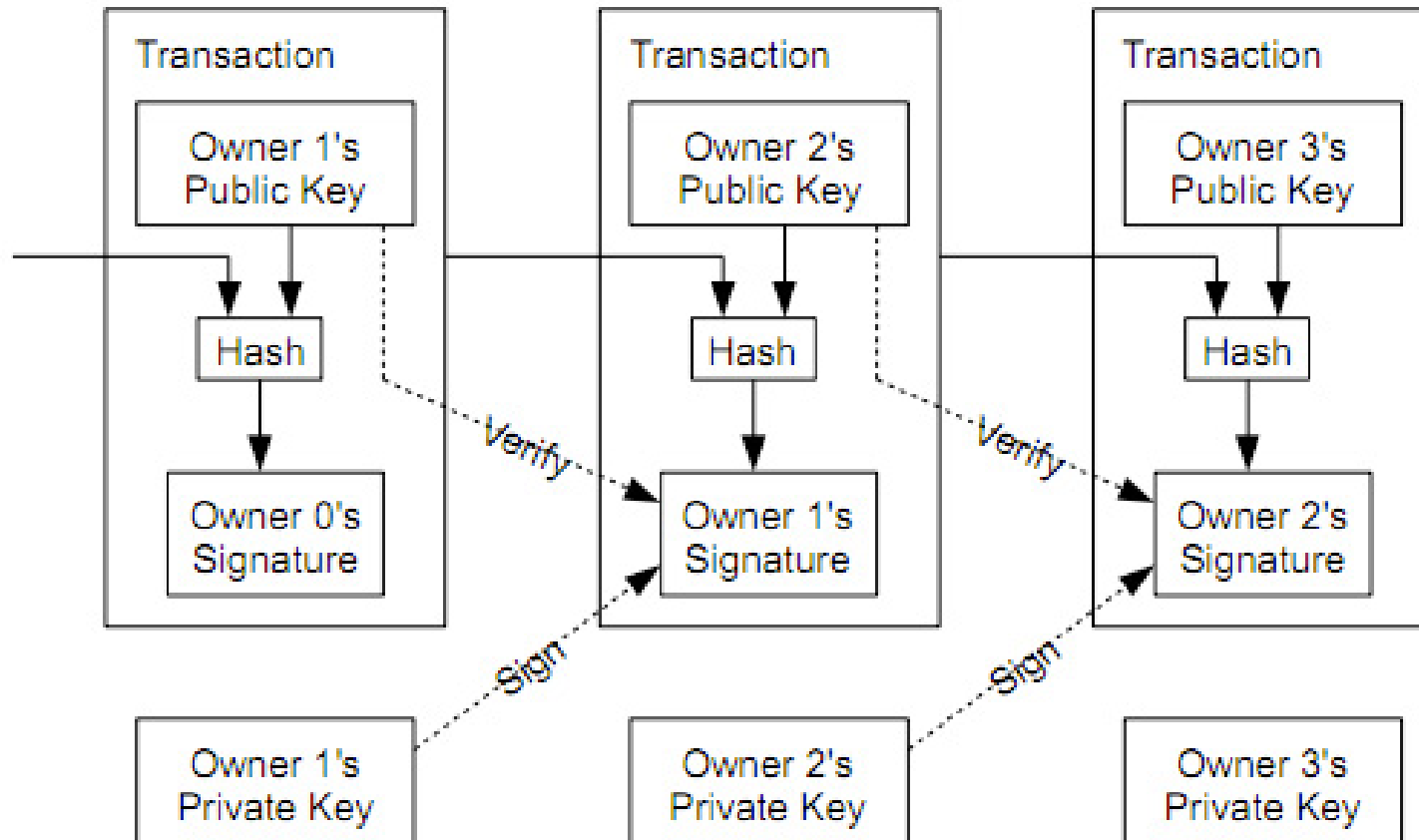
Enigma machine



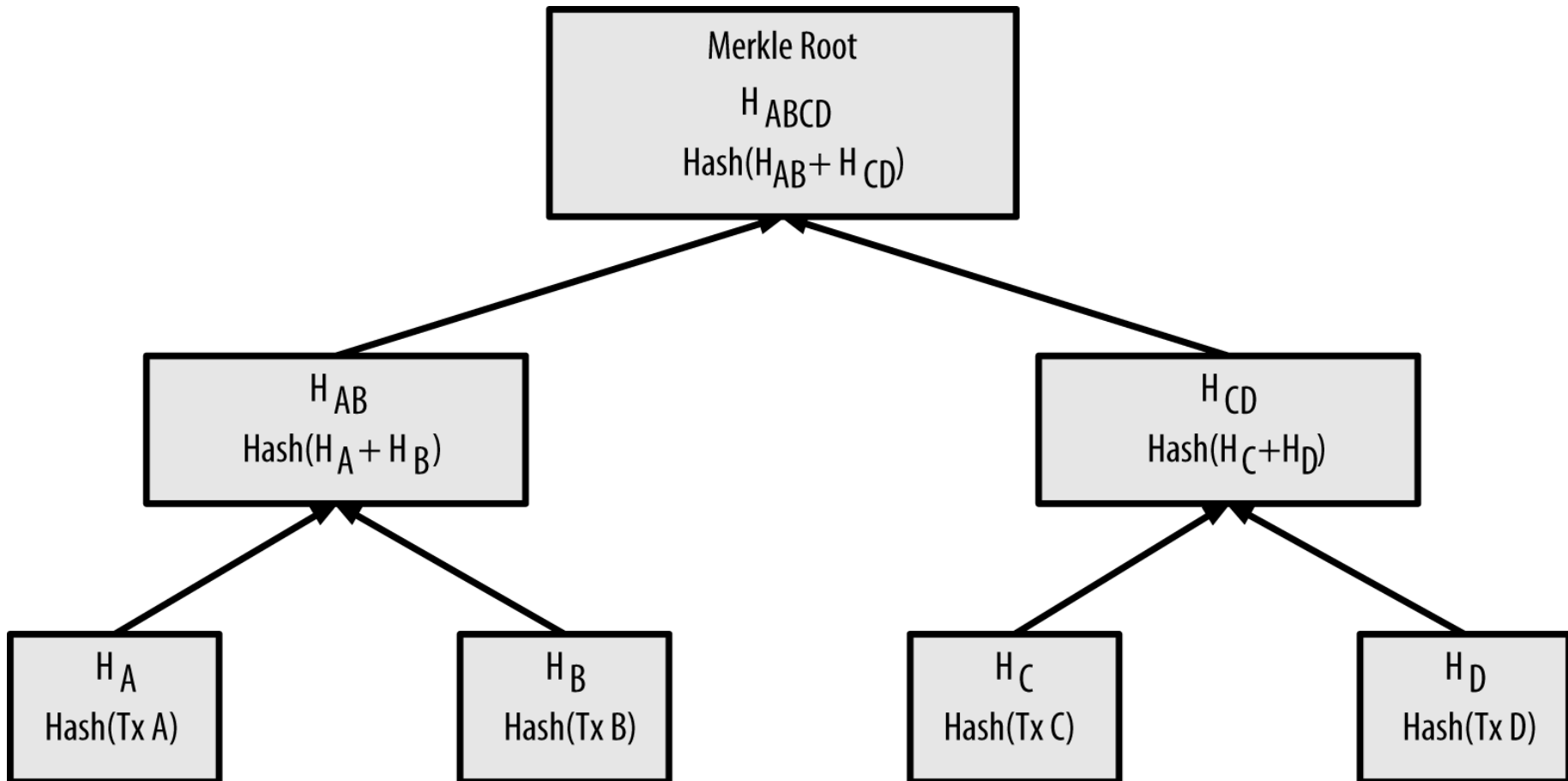
Enigma rotors



Transaction Hash chaining



Hash tree – Merkle tree



Blockchain (Bitcoin)

Four ideas

- Hash chaining – Unalterable history
- Public key cryptography – Signatures
- Addition/Subtraction – General ledger
- Notarization – Proof of validity

General Ledger

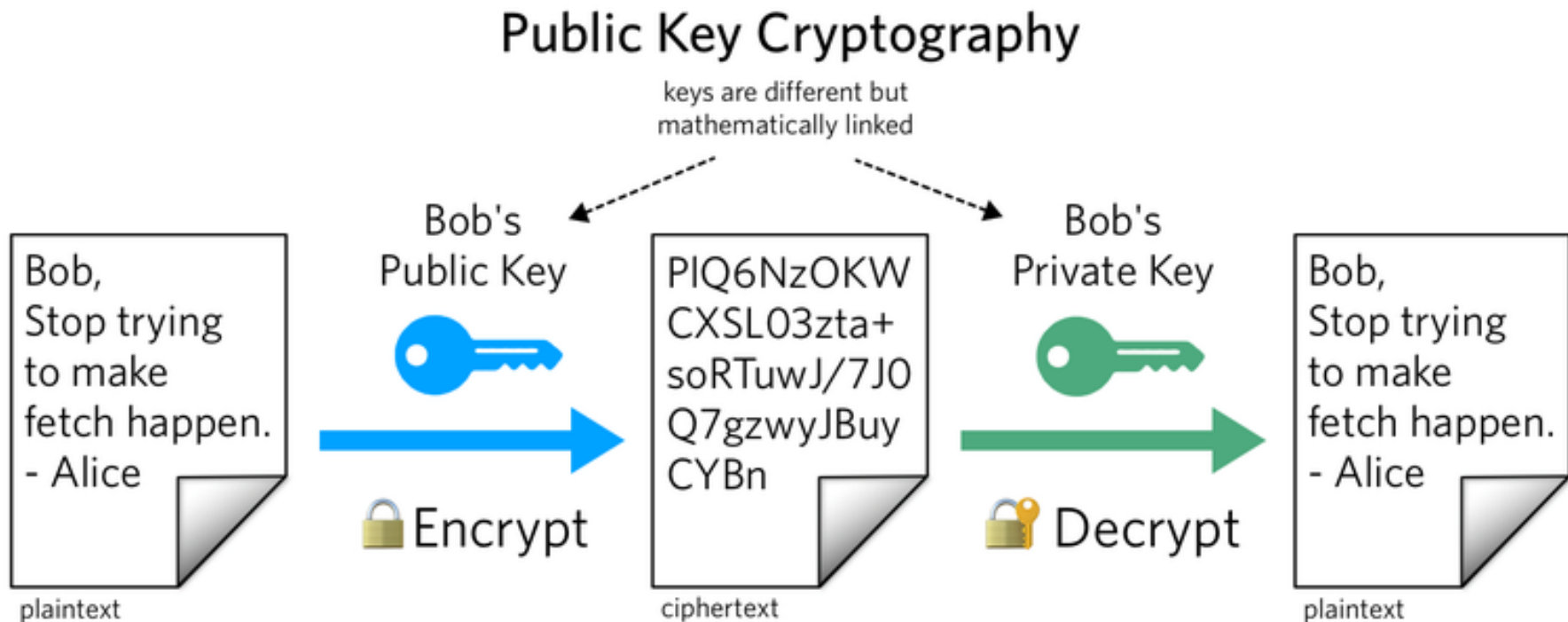
	To record investment by Fizbo		
Jan 3	Car	5,000	
	Accounts payable		5,000
	To record purchase of car on credit		
Jan 5	Advertising expense	100	
	Cash		100
	To record Facebook advertising		

Blockchain (Bitcoin)

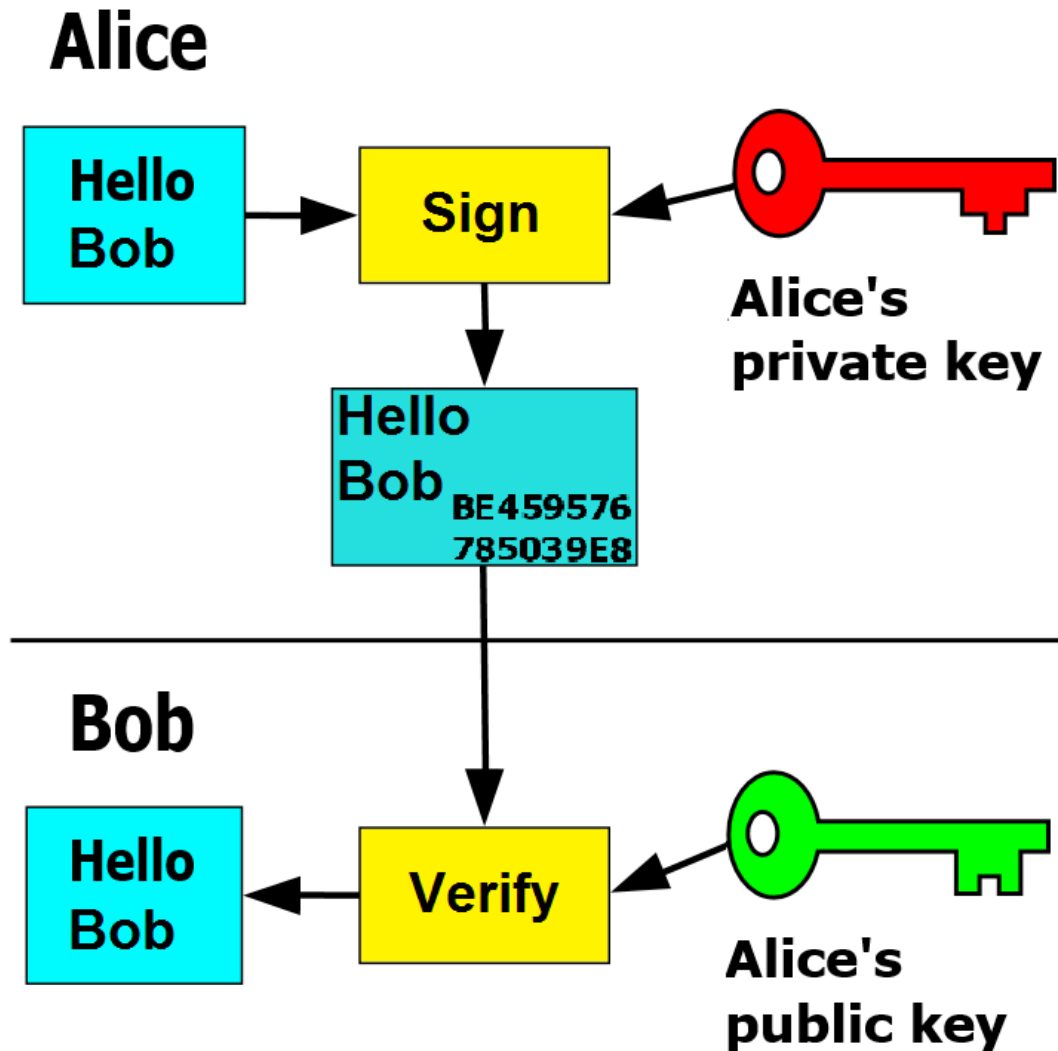
Four ideas

- Hash chaining – Unalterable history
- Public key cryptography – Signatures
- Addition/Subtraction – General ledger
- Notarization – Proof of validity

Plaintext - Cryptext



Public Key Signatures



Rivest Shamir Adleman - 1977

RSA Algorithm

Key Generation

Select p, q	p and q , both prime; $p \neq q$
Calculate $n = p \times q$	
Calculate $\phi(n) = (p-1)(q-1)$	
Select integer e	$\gcd(\phi(n), e) = 1; 1 < e < \phi(n)$
Calculate d	$de \bmod \phi(n) = 1$
Public key	$KU = \{e, n\}$
Private key	$KR = \{d, n\}$

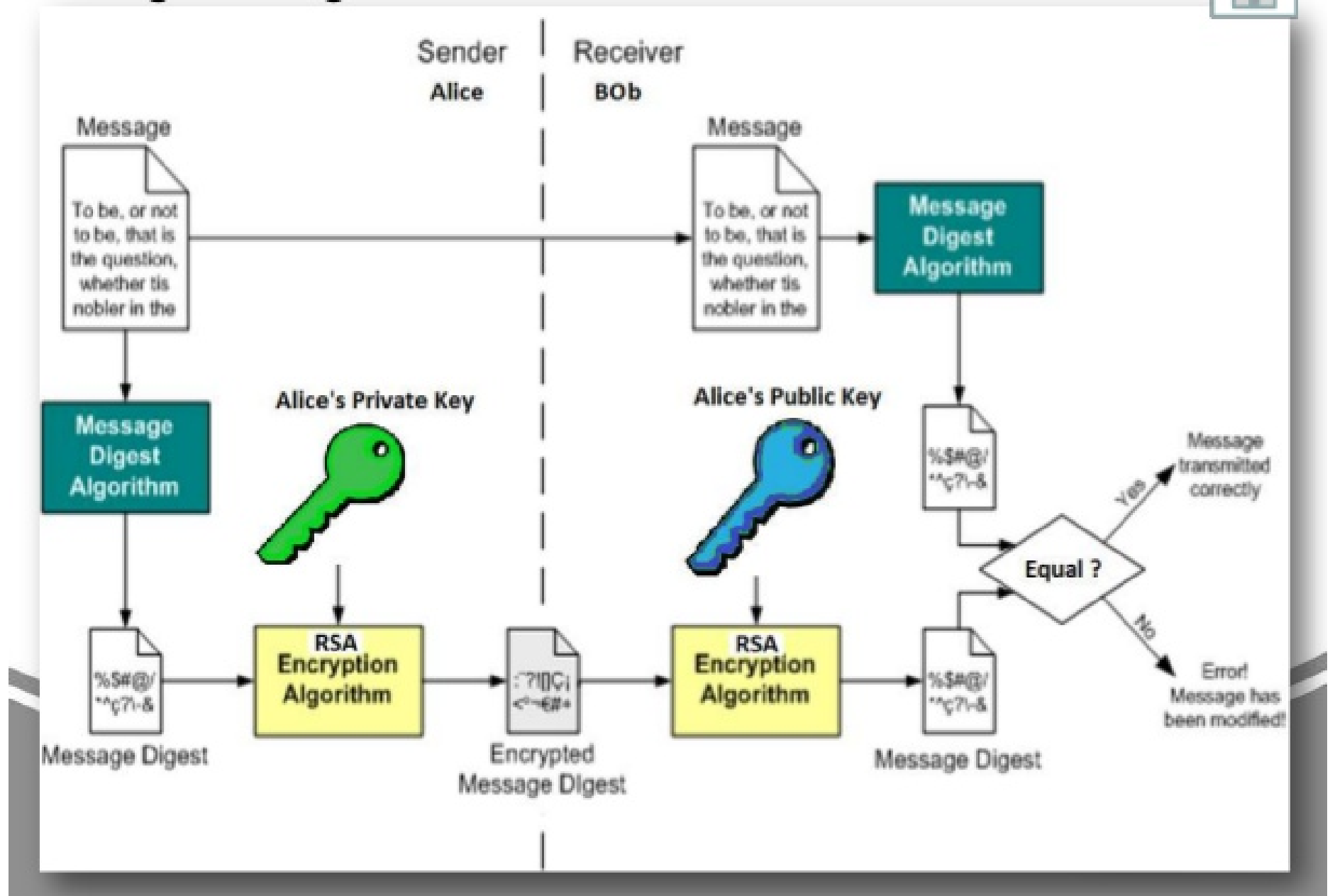
Encryption

Plaintext:	$M < n$
Ciphertext:	$C = M^e \pmod{n}$

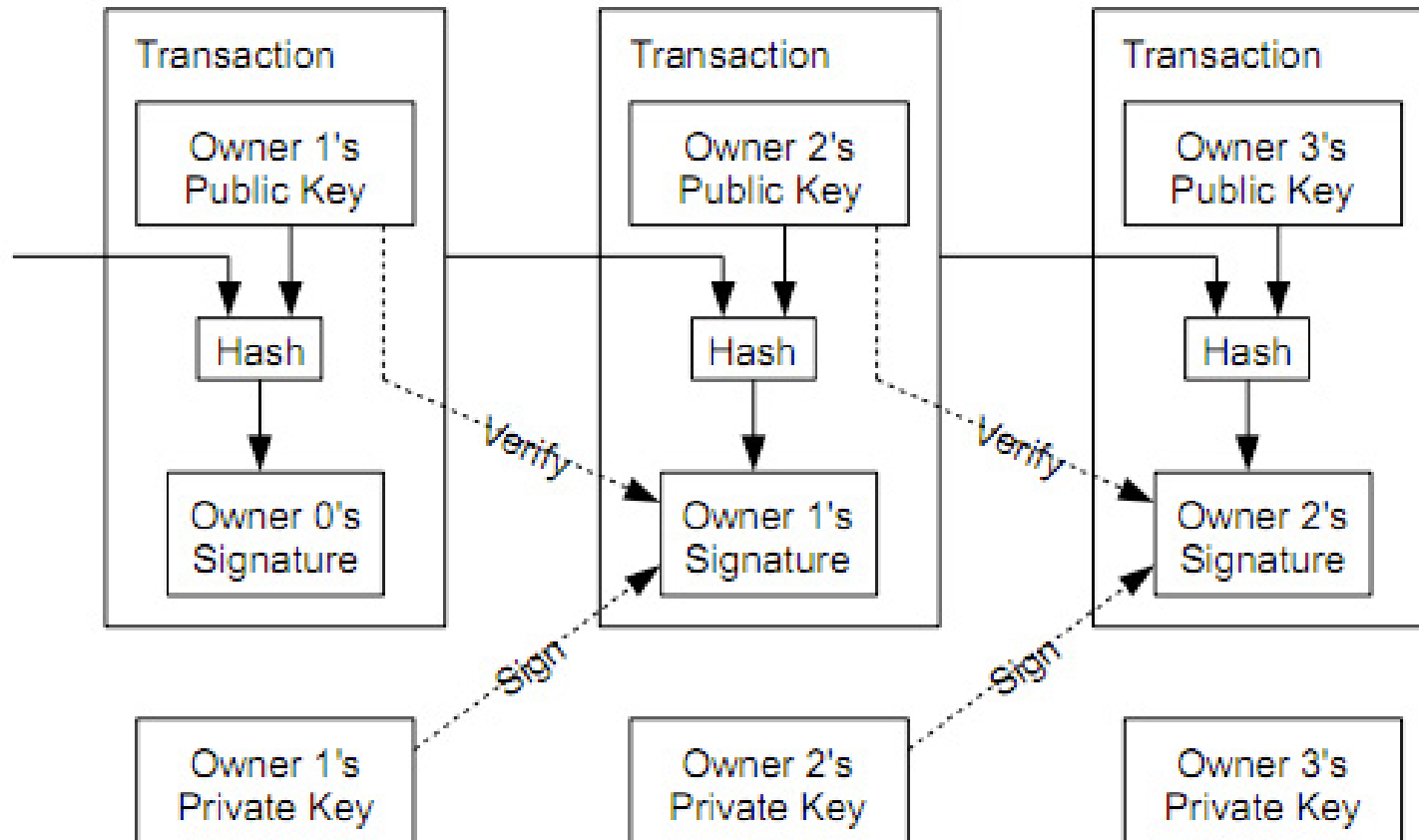
Decryption

Plaintext:	C
Ciphertext:	$M = C^d \pmod{n}$

Digital Signature on RSA



Transaction Hash chaining



Blockchain (Bitcoin)

Four ideas

- Hash chaining – Unalterable history
- Public key cryptography – Signatures
- Addition/Subtraction – General ledger
- Notarization – Proof of validity

Notarization

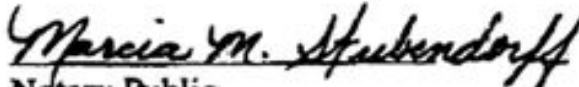
this statement, is a "covered report":

- Apple Computer, Inc. Annual Report on Form 10-K for the fiscal year ended September 29, 2001;
- all reports on Form 10-Q, all reports on Form 8-K and all definitive proxy materials of Apple Computer, Inc. filed with the Commission subsequent to the filing of the Form 10-K identified above; and
- any amendments to any of the foregoing.


Steven P. Jobs
Chief Executive Officer
August 8, 2002

RECEIVED
OFFICE OF THE SECRETARY
AUG 8 2002

Subscribed and sworn to
before me this 8th day of August, 2002.


Notary Public
My Commission Expires: May 21, 2006



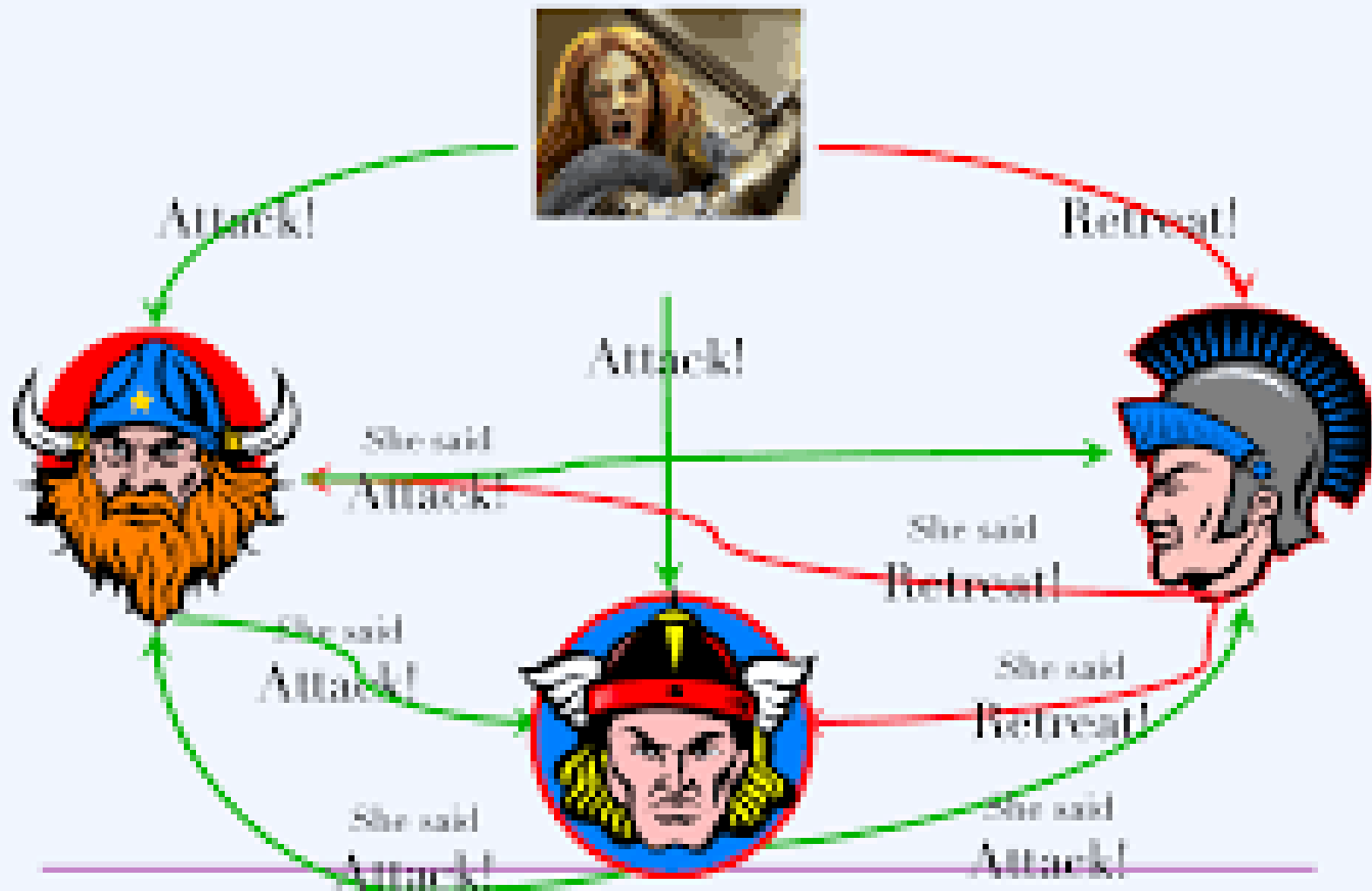
Byzantine Generals



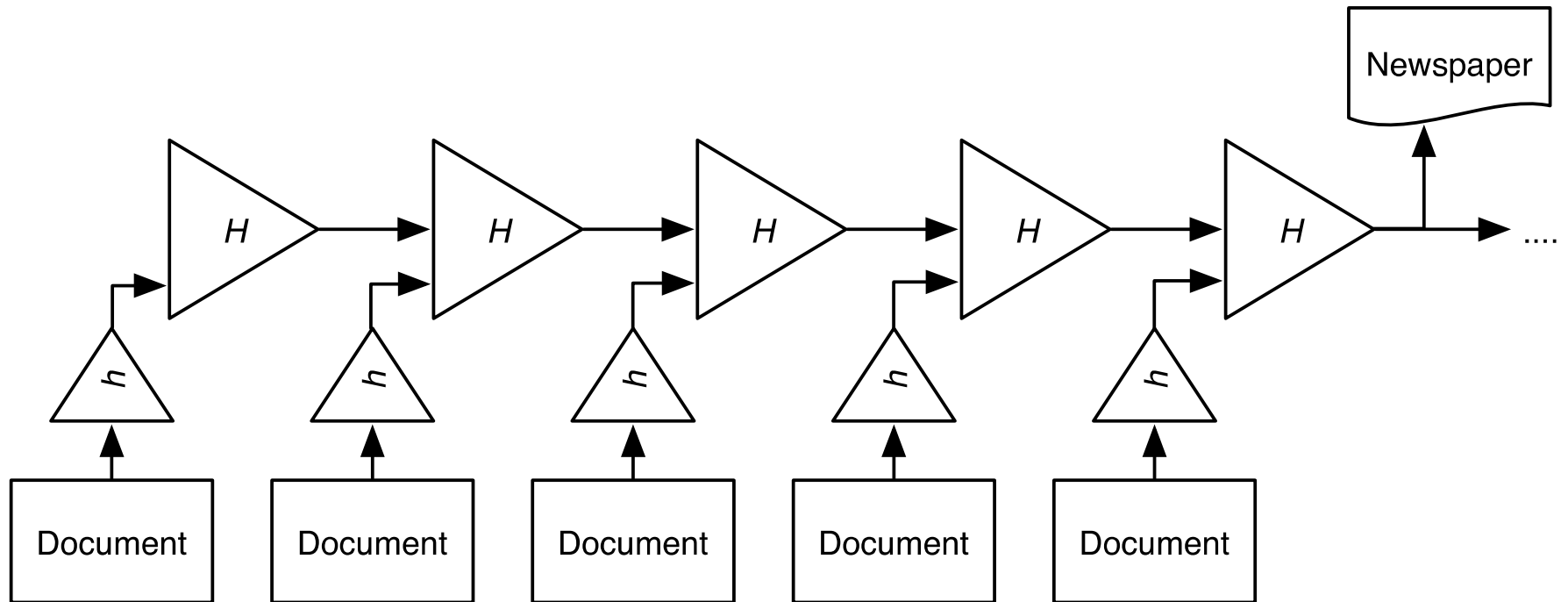
The Byzantine Generals Problem



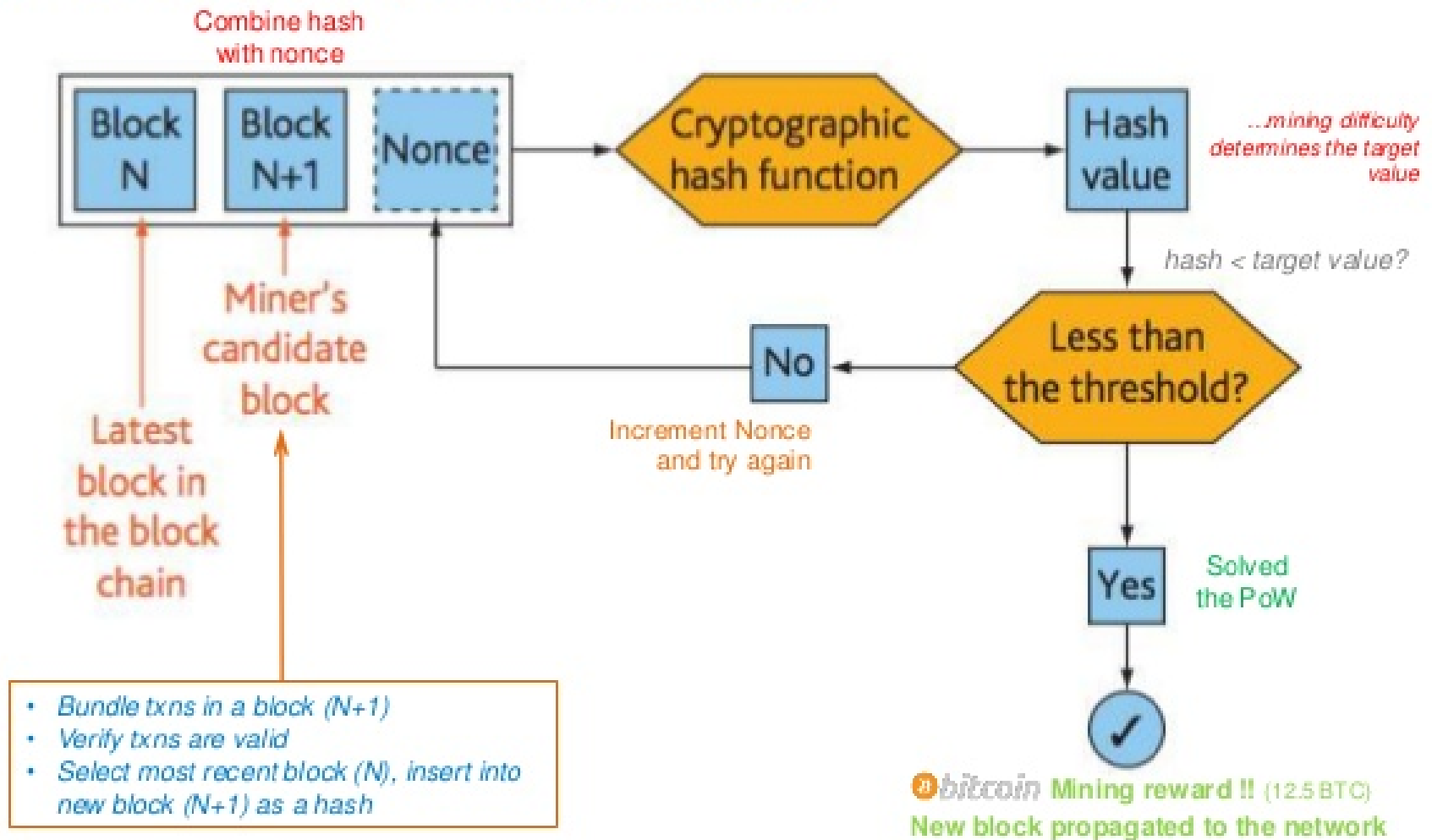
[4,1] Byzantine Generals Problem



Solution: Chained Notarizations!



#Hash - Bitcoin's proof of work scheme



Blockchain (Bitcoin)

Four ideas + Reward

- Hash chaining – Unalterable history
- Public key cryptography – Signatures
- Addition/Subtraction – General ledger
- Notarization – Proof of validity
- Proof of work – Mining

Bitcoin is Evil ! ! !!!!

- Vast waste of electricity!
- Strongly deflationary!
 - Today GDP=100 BTC=100
 - Tomorrow GDP=105 BTC=100
 - Don't spend! Wait till tomorrow!
- Not Enough BTC for world population
 - 21 Million BTC total

Phew. Now Lets go Crazy!

- Addition, Subtraction...
 - Multiplication, division, if-then-else, loops...
 - General programming!
 - *Ethereum* – smart legal contracts
 - DAO – Decentralized Autonomous Organizations
- Proof of Work...
 - Proof of Stake
 - Gossip Protocols

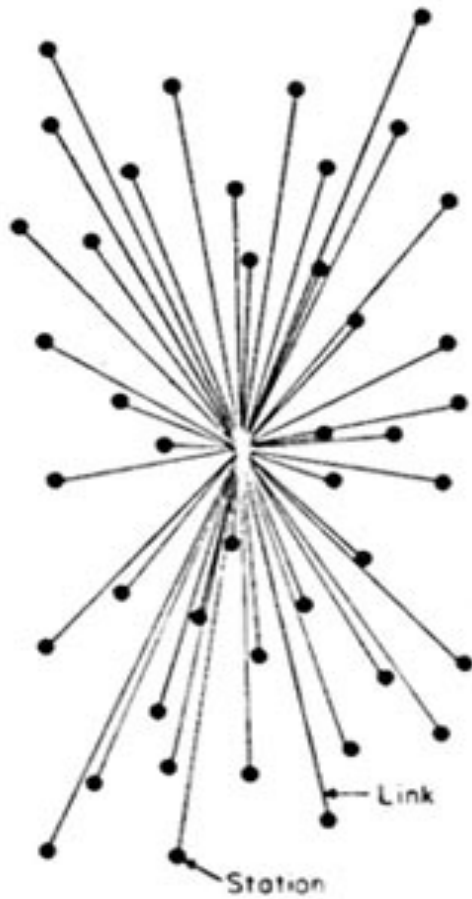
Lets Go Crazy!

- Uneraseable, uncorruptible database
 - Append-only logs
 - Git – dat:// – IPFS
 - Log structured merge tree (LSM)
- Authenticated identity
 - Banking, voting, UBI ... and social interaction
- Identity hiding
 - Financial, medical records
 - Journalism, secret organizations
 - Crime

Lets Go Crazy!

- Singleton (centralized) blockchain...
 - Decentralization
 - Distributed Hash Table
 - LSM, Secure Scuttlebutt
- Not just money, contracts!
 - Chat, email, social media, file sharing
 - Not just music, but science data! Or web pages!
 - Identity, Liquid democracy, UBI, Value flows, ERP

Decentralized Social Media



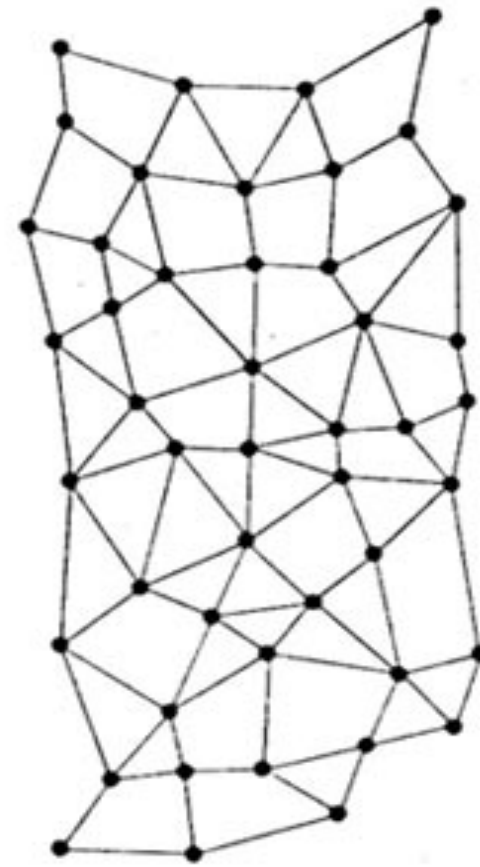
CENTRALIZED
(A)

Centralized



DECENTRALIZED
(B)

Federated



DISTRIBUTED
(C)

Decentralized