Blockchain as Essential Means and Infrastructures for Transferring Digital Asset and Ownship in Digital Society

Ajin Jirachiefpattana, Ph.D.
National Statistical Office (NSO)
ajin_j@hotmail.com

Outline

- Security vs. Safety
- Cryptology
- Information Security Service requirements
- Brief history of Cryptography
- One-Way Hash function
- Digital Asset and Ownership
- Proof of Ownership
- Blockchain
- Key Characteristics of Blockchain Technology

Security vs. Safety

- **Security** : Being far from death.

ความมั่นคง คือ การห่างไกลจากความตาย จากการล่มสลาย จากการถูกทำลาย

- **Safety** : Being far from danger.

ความปลอดภัย คือ การห่างไกลจากอันตราย

- **Data Security vs. Data Privacy**

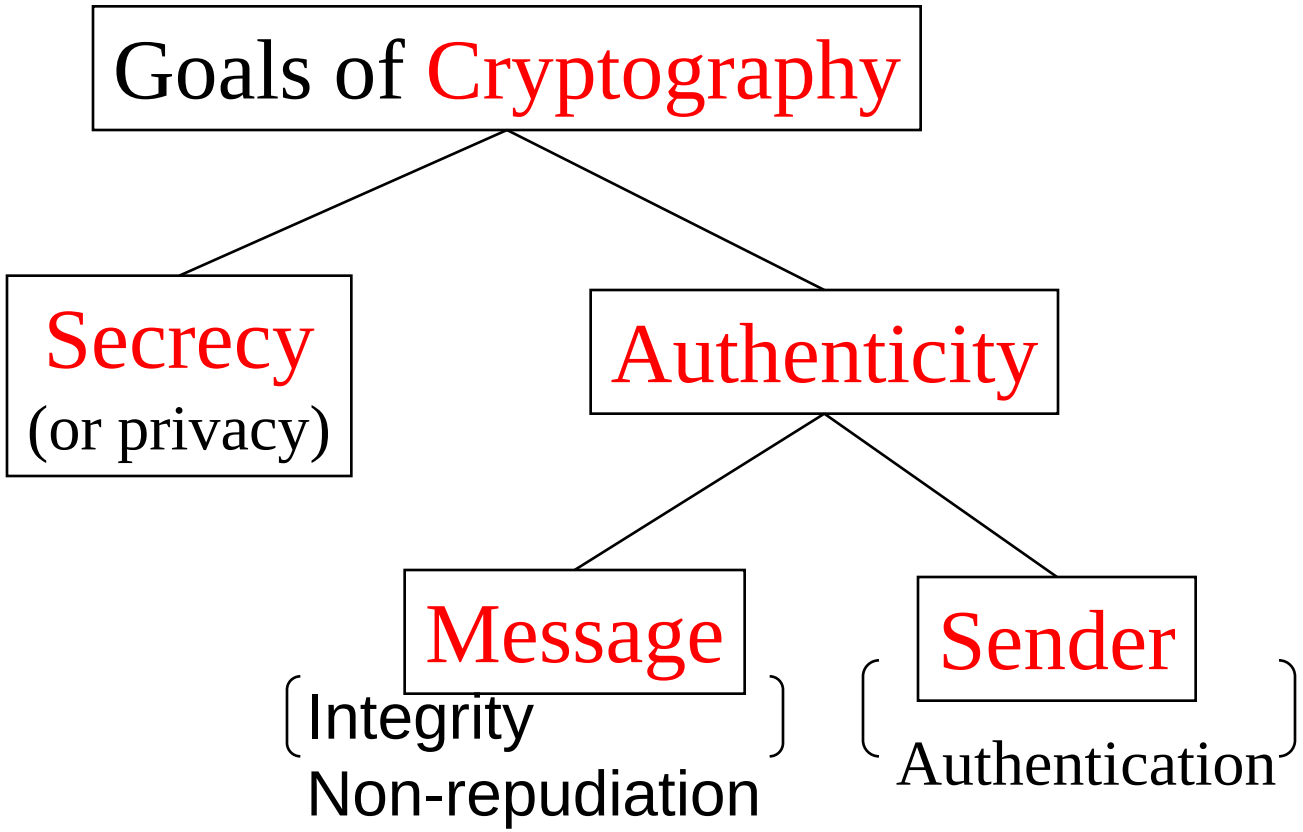
Cryptology

Cryptology
from the Greek for
"Greek *kruptos* (hidden) and *logos* (science),"

Cryptography
(code-making)

Cryptanalysis
(code-breaking)

Goals of Cryptography



Information Security Service requirements

- Integrity:

  Ensures that only authorized parties are able to modify computer system assets and transmitted information. Modification includes writing, changing, changing status, deleting, creating, and delaying or replaying of transmitted messages.

- Authentication:

  Ensures that the origin of a message or electronic document is correctly identified, with an assurance that the identity is not false.

- Non-repudiation:

  Requires that neither the sender nor the receiver of a message be able to deny the transmission.

Information Security Service requirements

- Confidentiality(or privacy):

  Ensures that the information in a computer system and transmitted information are accessible only for reading by authorized parties. This type of access includes printing, displaying, and other forms of disclosure, including simply revealing the existence of an object.

- Access control:

  Requires that access to information resources may be controlled by or for the target system.

- Non-replay attack:

Brief history of Cryptography

1949. C.E. Shannon first discussed the “Communication theory of secrecy systems”

1976 The Concept of PK was first proposed by Diffie and Hellman. However, they did not show how to design a public key cryptosystem and digital signature scheme.

1977 Data Encryption Standard (DES) was adopted as a federal standard in USA

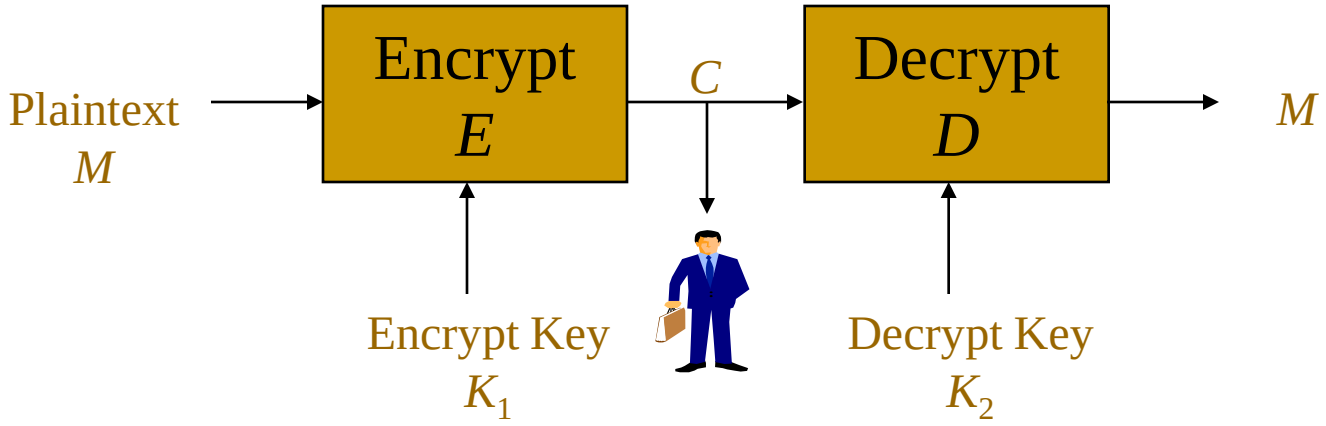
1978 The first PK Cryptosystem and Digital Signature was proposed by Rivest, Shamir and Adleman

1985. The concept of Zero Knowledge Interactive Proof (ZKIP) protocol was proposed by Goldwasser, Micali and Rackoff.

1991. NIST proposed the Digital Signature Algorithm (DSA and SHA-1) for use in Digital Signature Standard (DSS)

2000. The AES Algorithm was announced (Oct,2nd) by NIST and it was adopted as standard in 2001.

Encryption and Decryption



- When $K_1 = K_2$, the system is called **symmetric encryption system**.
- When $K_1 \neq K_2$, the system is called **asymmetric encryption system** or **public encryption system**, where K1 is called public key and K2 is secret key.

Symmetric Encryption

- Based on substitution and transposition, the computation is fast, and is used on the encryption and decryption of a large quantity of data.
- Classification:

  (1) *Block Cipher*

  Ex:DES, Triple DES, IDEA, AES

  (2) *Stream Cipher*

  Ex: RC4

The well known Symmetric Standards

Name	Key length	Block length	Rounds	Year	FIPS
DES	56	64	16	1977	Pub 46
3DES	56/112/168	64	16*3	1979	Pub 97
IDEA	128	64	8	1990	
Skipjack	80	64	32	1993	
AES	128/192/256	128	10/12/14	2001	Pub 197

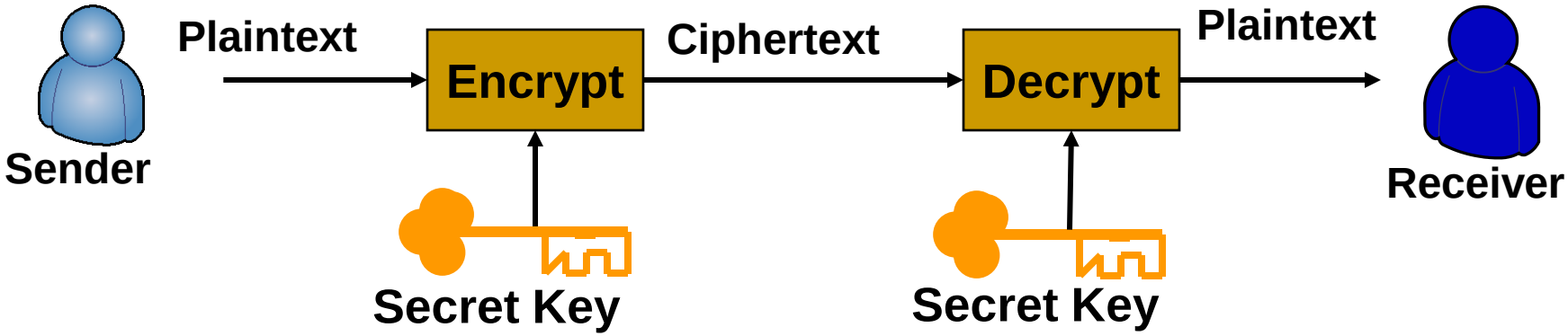
Asymmetric Encryption

- Based on the concept of mathematic logic. The operation is slow, but there is no need to consider key distribution. It is used on the encryption and decryption of a smaller quantity of data, such as protecting session keys or users' personal information.

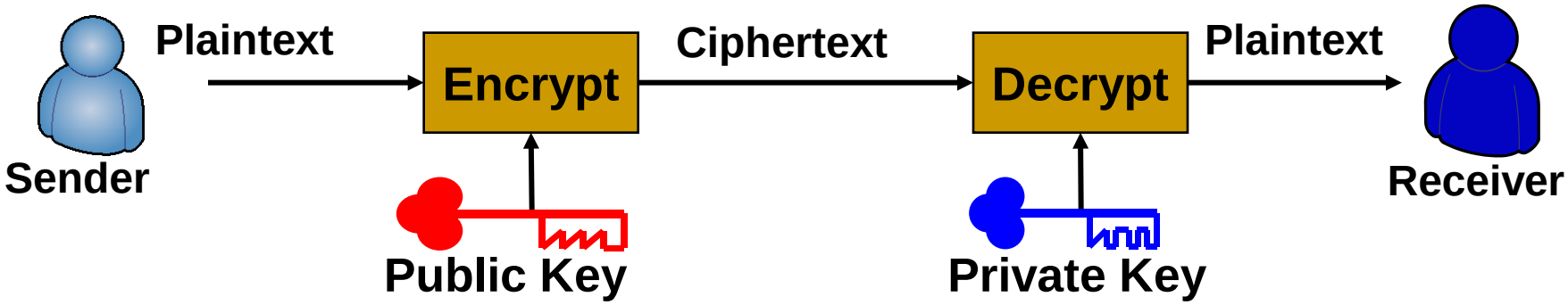
Ex: RSA , ElGamal

The Concept of Symmetric and Asymmetric Ciphers

Symmetric



Asymmetric



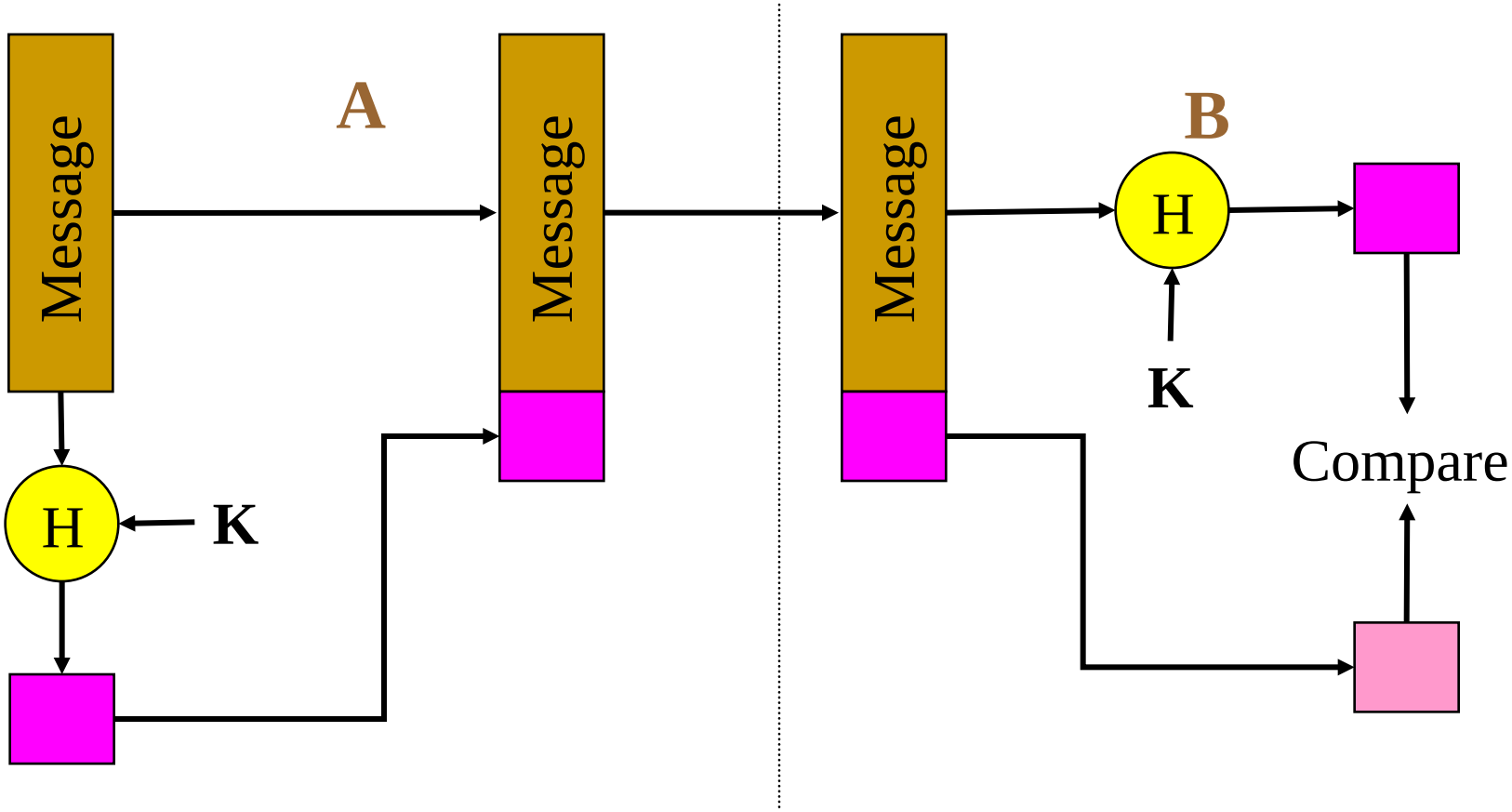
One-Way Hash function

- Message of arbitrary length mapped to string of fixed length
- Unkeyed hash functions
  - Used in digital signatures
  - Examples are MD5, SHA
- Keyed hash functions
  - Message integrity

One-Way Hash Function Requirements

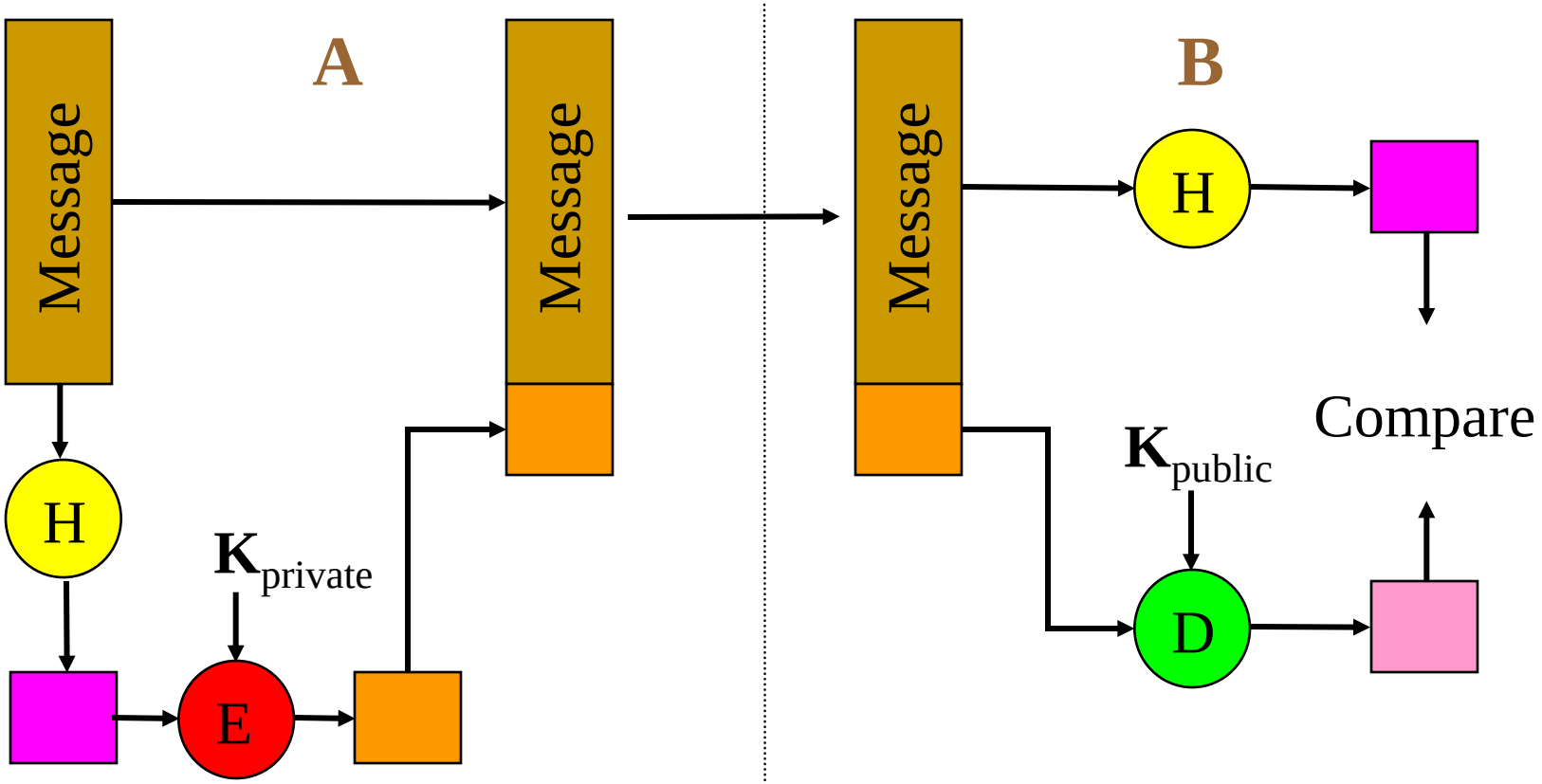
- **A hash function H must have the following properties:**
  1. H can be applied to a block of data of any size
  2. H produces a fixed-length output
  3. H(x) is relatively easy to compute for any given x, making both hardware and software implementations practical
  4. For any given code h, it is computationally infeasible to find x such that H(x)=h
  5. For any given block x, it is computationally infeasible to find $y \neq x$ with H(y)=H(x)
  6. It is computationally infeasible to find any pair (x, y) such that H(x)=H(y)

Message Authentication Using a One-way Hash Function (1)



Using keyed one way hash function

Digital signature Using unkeyed One-way Hash Function (2)

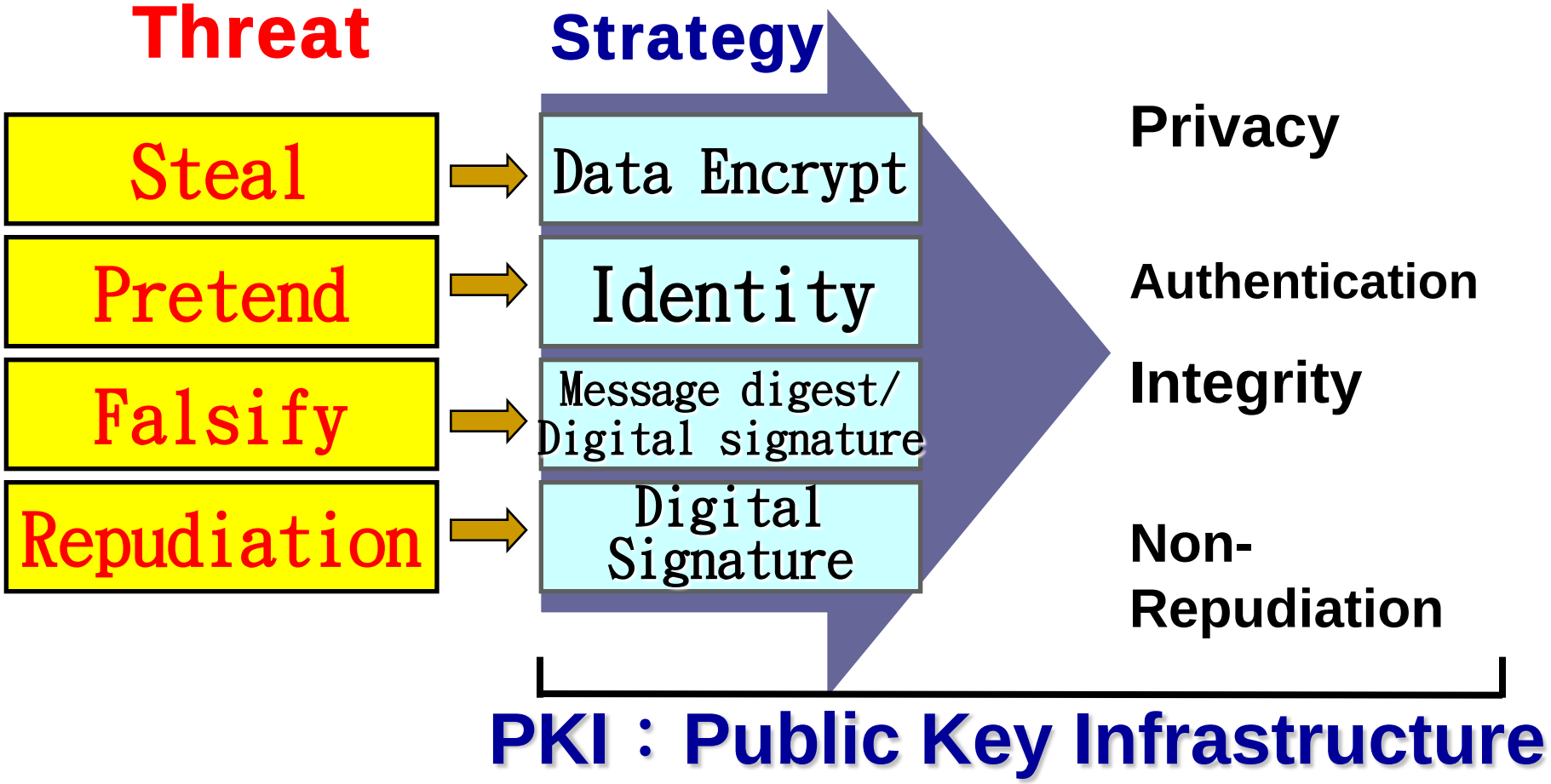


Using public-key encryption (Digital Signature)

Comparison of MD5 & SHA-1 & SHA-2

Difference	MD5	SHA-1	SHA-2
Year	1982	1993	2002
Length of Digest	128 bits	160 bits	224/256/384/512
Operate rounds	64	80	64/80
Count of logic function	4	4	8
Count of constant	64	80	6

Threat and strategy of network Security



Structure of Standard Certificate

DSA with SHA-1

Usually X.500 Format

Usually X.500 Format

(Usually omitted)

(Usually omitted)

DSA with SHA-1

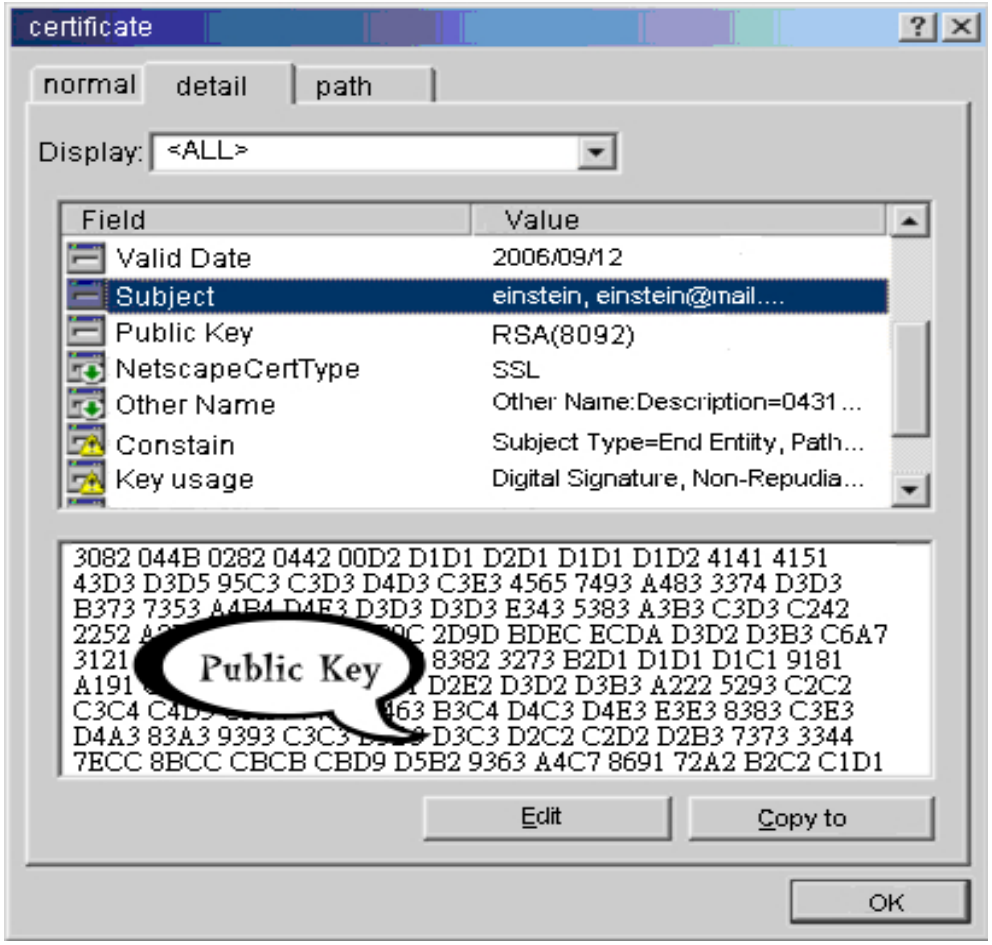
version
serialNumber
signature
issuer
validity
subject
subjectPublicKeyInfo
issuerUniqueID
subjectUniqueID
extensions
signatureAlgorithm
signatureValue

Options

Certificate Contents

Tamper Evident Envelop

Standard Certificate in X.509



Digital Asset and Ownership

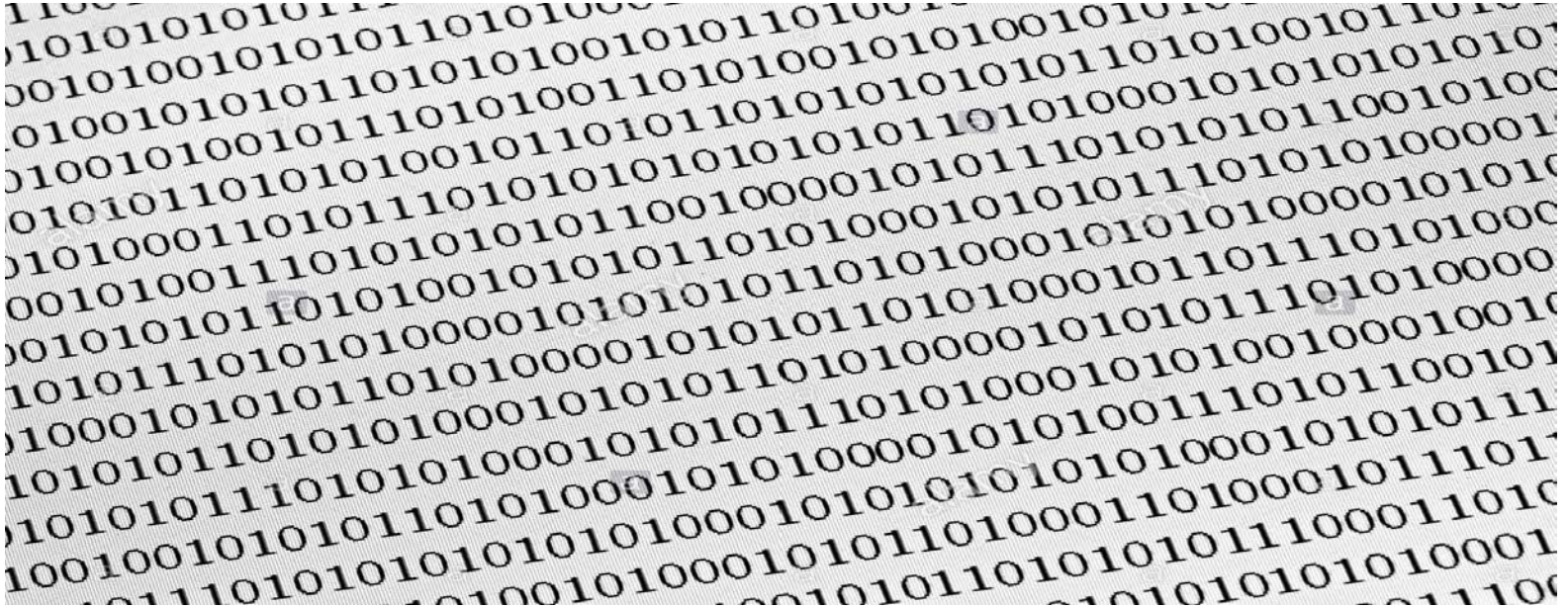
- **Many copies** of digital data or asset can **easily** be made, stored, disseminated within networks.
- All of these copies are **very hard** to identify any differences or which one is original or which ones are copies.
- Without a central authority and through a peer-to-peer network, **how to prove or verify who holds the rights or ownership of such digital data or asset**.

Proof of Ownership

- Central Authority
- Possession
- Witness (all participants)
- Legal Document or Ledger or Deed
- Regulation and Law


THE UNITED STATES OF AMERICA
JE 51817534 A
TEN
DOLLARS


FRANCE
POSTE AERIENNE
40f
+10f



Blockchain

- Blockchains are **tamper evident** and **tamper resistant digital ledgers** implemented in **a distributed fashion** (i.e., without a central repository) and **usually without a central authority** (i.e., a bank, company, or government).
- At their basic level, they enable a community of users to record transactions in a shared ledger within that community, such that **under normal operation of the blockchain network no transaction can be changed once published.**

Blockchain

- In 2008, the blockchain idea was **combined with several other technologies and computing concepts** to create modern cryptocurrencies: electronic cash protected through cryptographic mechanisms instead of a central repository or authority.
- The first such blockchain based cryptocurrency was **Bitcoin**.

Blockchain

- **Bitcoin users** can **digitally sign** and **transfer rights to that information** to **another user** and the Bitcoin blockchain **records this transfer publicly**, allowing all participants of the network to **independently verify the validity of the transactions**.
- The Bitcoin blockchain is **stored**, **maintained**, and **collaboratively managed** by a distributed group of participants.
- This, along with **certain cryptographic mechanisms**, makes the blockchain **resilient to attempts to alter the ledger later** (modifying blocks or forging transactions).

Blockchain

- Blockchains are **a distributed ledger** comprised of **blocks**. Each block is comprised of **a block header** containing metadata about the block, and **block data** containing a set of transactions and other related data.
- Every block header (except for the very first block of the blockchain) contains **a cryptographic link to the previous block's header**.
- Each transaction involves **one or more blockchain network users** and **a recording of what happened**, and it is **digitally signed by the user who submitted the transaction**.
- How **the participants in the network** come to agree on **whether a transaction is valid**. This is called "**reaching consensus**."

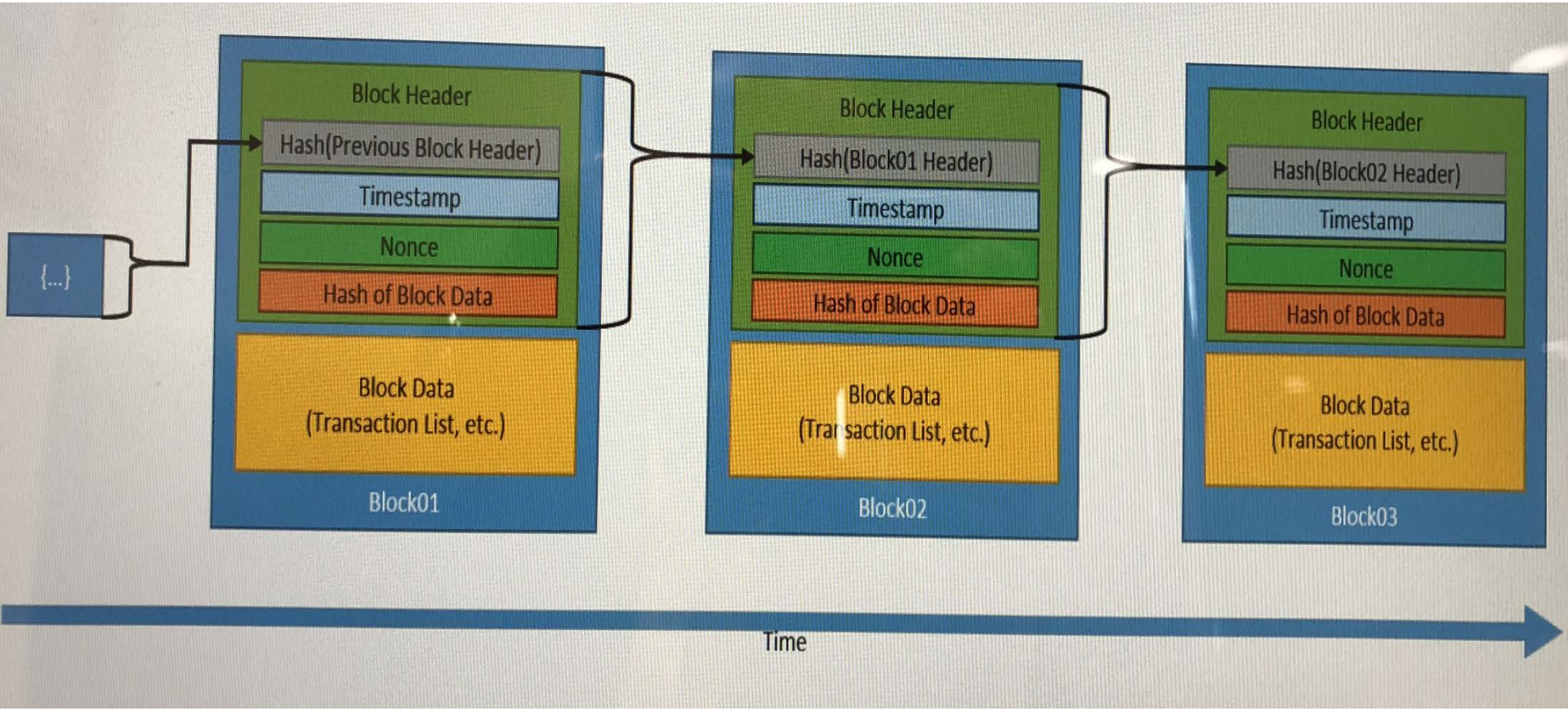
Blockchain

- Two general high-level categories for blockchain approaches: **permissionless**, and **permissioned**.
- In a **permissionless** blockchain network anyone can read and write to the blockchain without authorization.
- **Permissioned** blockchain networks limit participation to specific people or organizations and allow finer-grained controls.

Key Characteristics of Blockchain Technology

- Ledger - the technology uses an append only ledger to provide full transactional history. Unlike traditional databases, transactions and values in a blockchain are not overridden.
- Secure - blockchains are cryptographically secure, ensuring that the data contained within the ledger has not been tampered with, and that the data within the ledger is attestable.
- Shared - the ledger is shared amongst multiple participants. This provides transparency across the node participants in the blockchain network.
- Distributed - the blockchain can be distributed. This allows for scaling the number of nodes of a blockchain network to make it more resilient to attacks by bad actors. By increasing the number of nodes, the ability for a bad actor to impact the consensus protocol used by the blockchain is reduced.

Generic Chain of Blocks



Reference

- **NISTIR 8202** "**Blockchain Technology Overview**" by Dylan Yaga, Peter Mell, Nik Roby, Karen Scarfone, October 2018.

  This publication is available free of charge from: https://doi.org/10.6028/NIST.IR.8202

The Need for AI


Thank You