

Blockchain

Blockchain & Money



Curso 2024/2025



Francisco Hernando Gallego



fhernando@uva.es



Diego Martín de Andrés



diego.martin.andres@uva.es

Clase 3 – Temas Principales

- Revisión de la Clase 2
- Características de diseño de Bitcoin
- Funciones hash criptográficas
- Registros inmutables con sello temporal
- Cabeceras de bloque y árboles de Merkle
- Criptografía asimétrica y firmas digitales
- Direcciones de Bitcoin
- Conclusiones

Revisión de la Clase 2

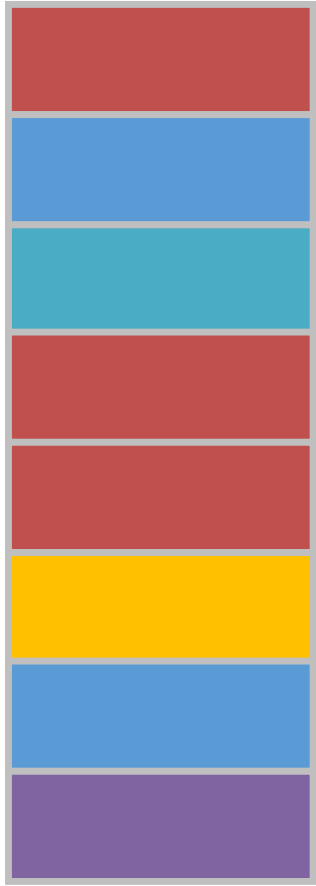
- El dinero es un consenso social y económico
- El dinero fiduciario es solo la etapa actual en una larga evolución del dinero
- La moneda fiduciaria también ha enfrentado desafíos e inestabilidades
- Los libros contables (ledgers) son una herramienta clave para registrar la actividad económica y las relaciones financieras
- La banca central y el sistema financiero se construyen sobre una red de libros contables
- Actualmente vivimos en una era de moneda electrónica
- Se han realizado numerosos intentos previos de crear monedas digitales criptográficas
- El artículo de Nakamoto "*Bitcoin: Un sistema de efectivo electrónico entre pares*" representa un hito en esta evolución

Bitcoin: A Peer-to-Peer Electronic Cash System

- From: Satoshi Nakamoto <satoshi <at> vistomail.com>
Subject: Bitcoin P2P e-cash paper
Newsgroups: gmane.comp.encryption.general
Date: Friday 31st October 2008 18:10:00 UTC
- “I've been working on a new electronic cash system that's fully peer-to-peer, with no trusted third party.”

Blockchain Technology

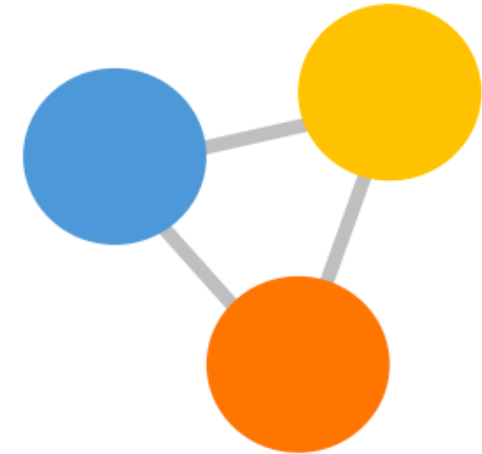
timestamped
append-only log



auditable database



network consensus protocol



Secured via cryptography

- Hash functions for **tamper resistance** and **integrity**
 - Digital signatures for **consent**
- Consensus for **agreement**

- Addresses '**cost of trust**'
(Byzantine Generals problem)
- Permissioned
 - Permissionless

Bitcoin – Características Técnicas

- Funciones hash criptográficas
- Registros inmutables con sello temporal (bloques)
- Cabeceras de bloque y árboles de Merkle
- Criptografía asimétrica y firmas digitales
- Direcciones
- Consenso mediante prueba de trabajo (Proof of Work)
- Red descentralizada de nodos
- Moneda nativa (bitcoin como unidad de valor)
- Entradas y salidas de transacciones
- Salida de transacción no gastada (UTXO)
- Lenguaje de scripts

Cryptography:

Communications in the presence of adversaries



Scytale Cipher
Ancient Times

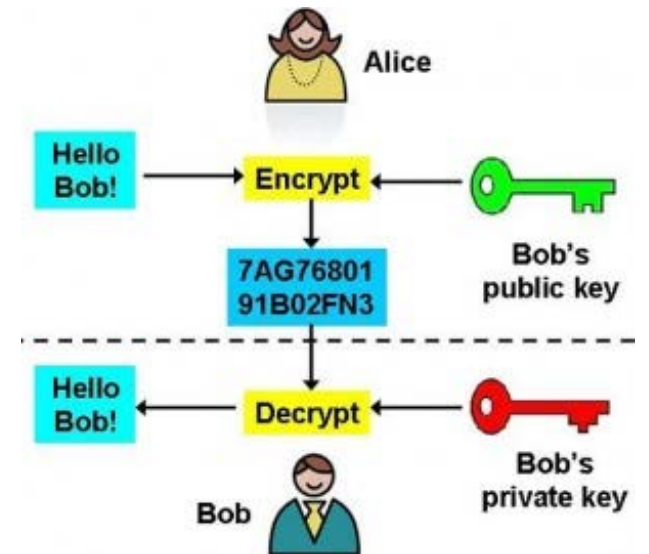
© Luringen on Wikimedia Commons.
License CC BY-SA. All rights reserved.
This content is excluded from our
Creative Commons license. For more
information, see

<https://ocw.mit.edu/help/faq-fair-use/>



Enigma Machine
1920s - WWII

Image by the [CIA](#) and is in the public domain via Wikimedia Commons.



Asymmetric Cryptography
1976 to today

Image is in the [public domain](#) via Wikipedia.

Funciones Hash Criptográficas

Huellas digitales para los datos

Propiedades generales

- Asocian una entrada x de cualquier tamaño a una salida de tamaño fijo: el hash
- **Deterministas:** el mismo input siempre produce el mismo hash
- De cálculo eficiente

Funciones Hash Criptográficas

Propiedades criptográficas

- **Resistencia a preimagen** (función unidireccional): es inviable obtener x a partir de $\text{Hash}(x)$
- **Resistencia a colisiones**: es inviable encontrar dos entradas distintas x y y tal que $\text{Hash}(x) = \text{Hash}(y)$
- **Efecto avalancha**: un pequeño cambio en x cambia completamente el $\text{Hash}(x)$
- **Dificultad tipo rompecabezas**: incluso conociendo parte de x y su $\text{Hash}(x)$, es muy difícil recuperar el resto

Funciones Hash Criptográficas

Usos y funciones en Bitcoin

Usos como:

- Nombres (identificadores únicos)
- Referencias
- Punteros (para estructuras encadenadas como la blockchain)
- Compromisos criptográficos

Funciones Hash Criptográficas

Funciones hash usadas en Bitcoin:

- **SHA-256**: para cabeceras de bloque y árboles de Merkle
- **SHA-256 + RIPEMD-160**: para generar direcciones de Bitcoin

 Estas funciones son fundamentales para garantizar la seguridad e integridad de la red Bitcoin.

'How to Time-Stamp a Digital Document'

Habor & Stornetta (1991)

Surety 1995 - present



Universal Registry Entries:
Zone2-

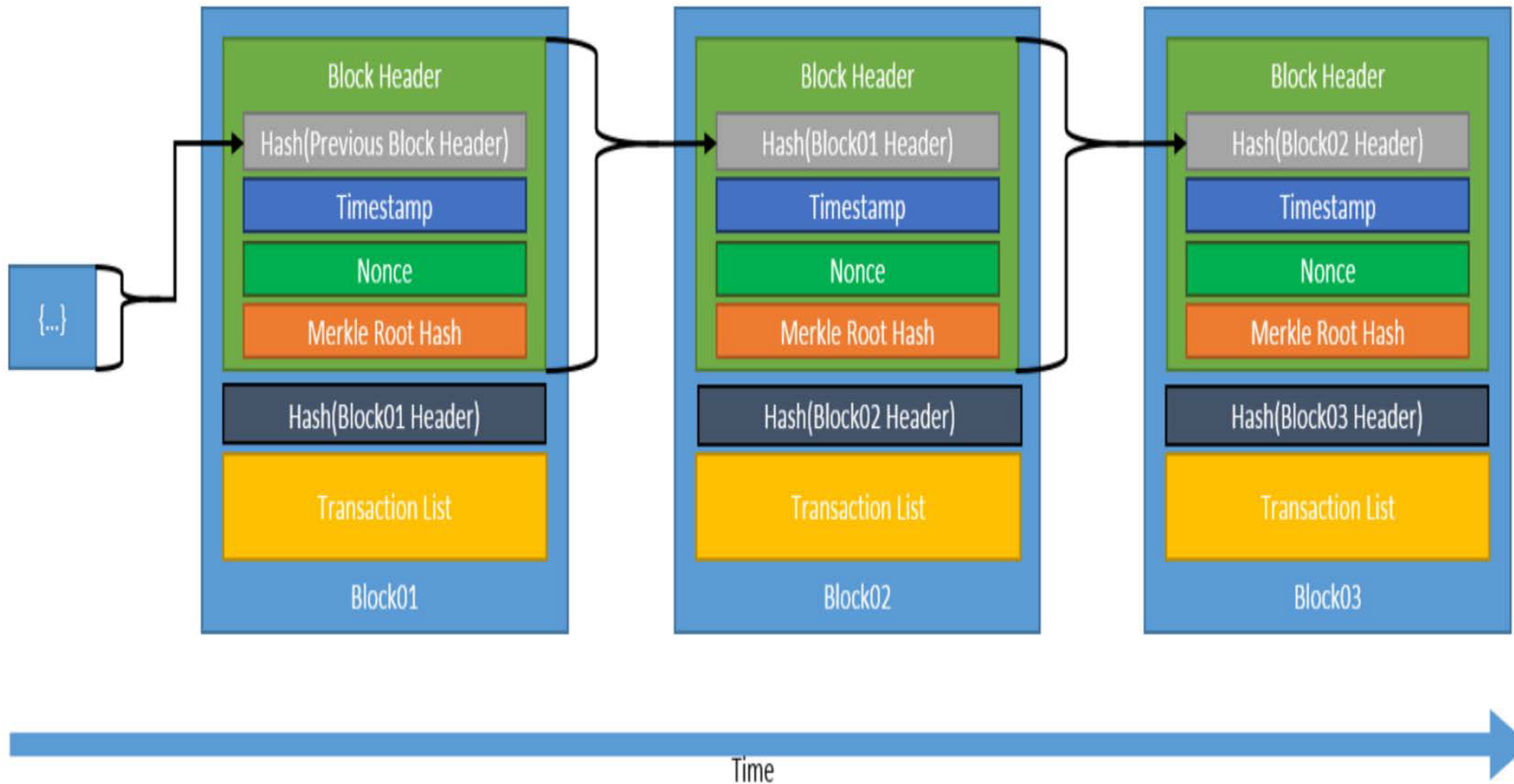
dS8492cgVOFAoP9kyE1XzMORQ
HgEwzkVbVafNylkUz99ava8/ME
p5y9EFSG8XxzMBaIGQQ==

Zone3-

JnFCg+HCmvhj8GmmUP7VZna71
NgZup/RfuKUQNzCHWXMuaLK
durxHQVSpSHLaBGPRiy+mg==

These base64-encoded values represent the combined fingerprints of all digital records notarized by Surety between 2009-06-03Z 2009-06-09Z.
www.surety.com 571-748-5800

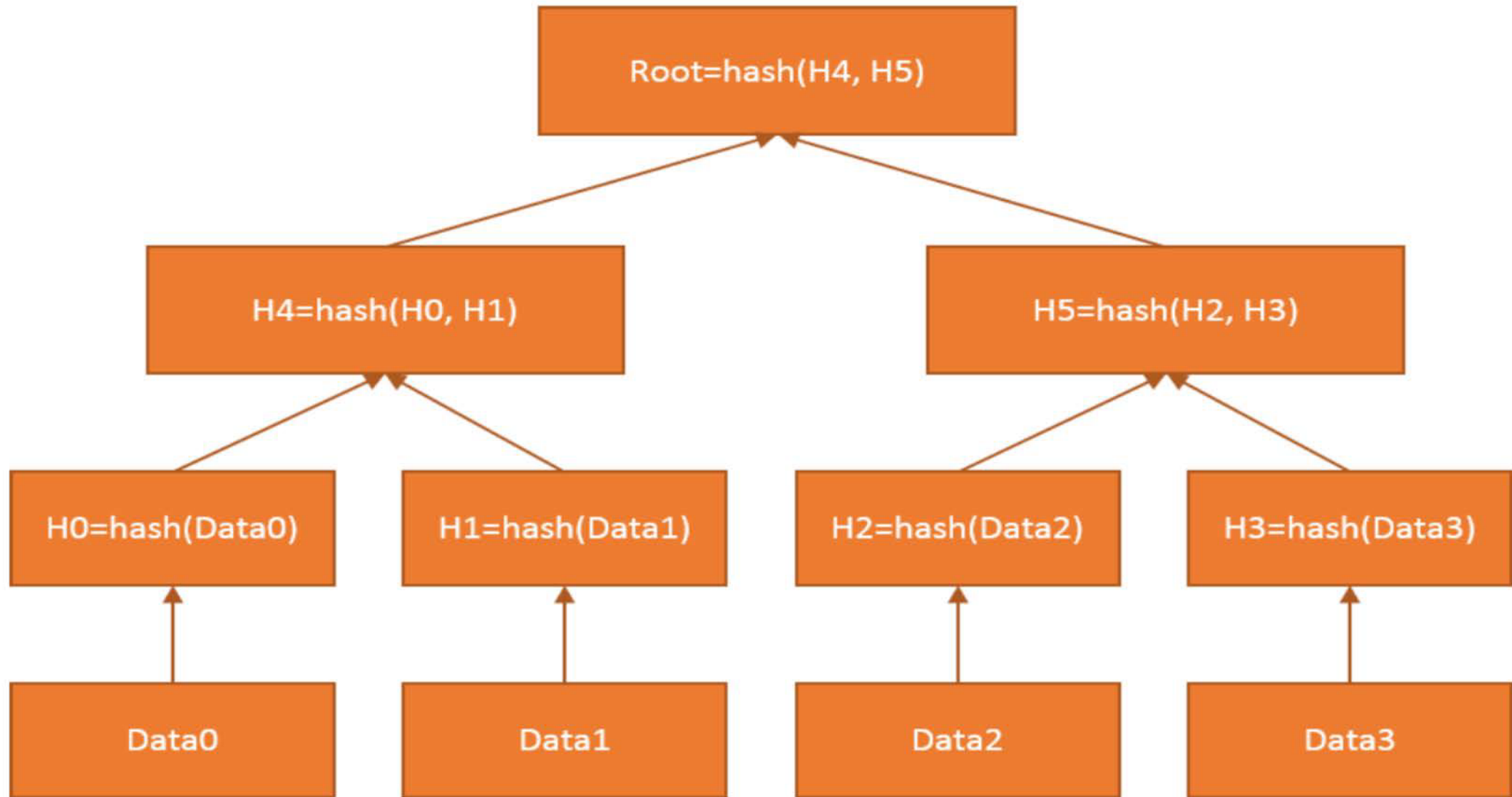
Timestamped Append-only Log - Blockchain



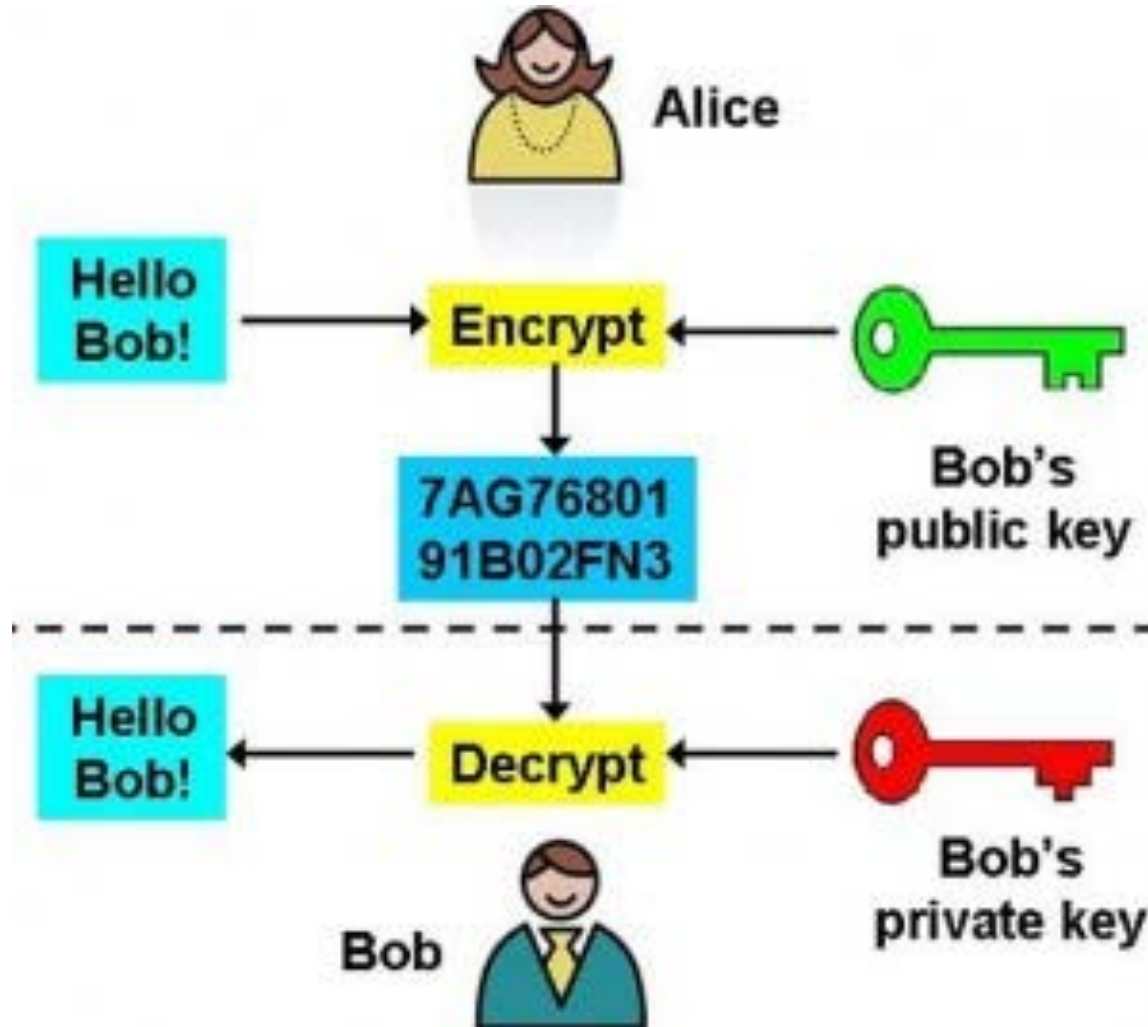
Block Header

- Version
- Previous Block hash
- Merkle Root hash
- Timestamp
- Difficulty target
- Nonce

Merkle Tree – Binary Data Tree with Hashes



Asymmetric Cryptography & Digital Signatures



Criptografía Asimétrica y Firmas Digitales

Algoritmos de Firma Digital

- **Generación de claves:** se genera un par de claves a partir de un número aleatorio
 - Clave pública (**PK**)
 - Clave privada (**sk**)
- **Firma:** se crea una firma digital (**Sig**) a partir de un mensaje (**m**) y la clave privada (**sk**)
- **Verificación:** permite comprobar si una firma (**Sig**) es válida para un mensaje (**m**) y una clave pública (**PK**)

Criptografía Asimétrica y Firmas Digitales


Propiedades

- Es computacionalmente inviable obtener la clave privada (**sk**) a partir de la clave pública (**PK**)
- Todas las firmas válidas pueden verificarse correctamente
- Las firmas son **inviables de falsificar** sin la clave privada correspondiente

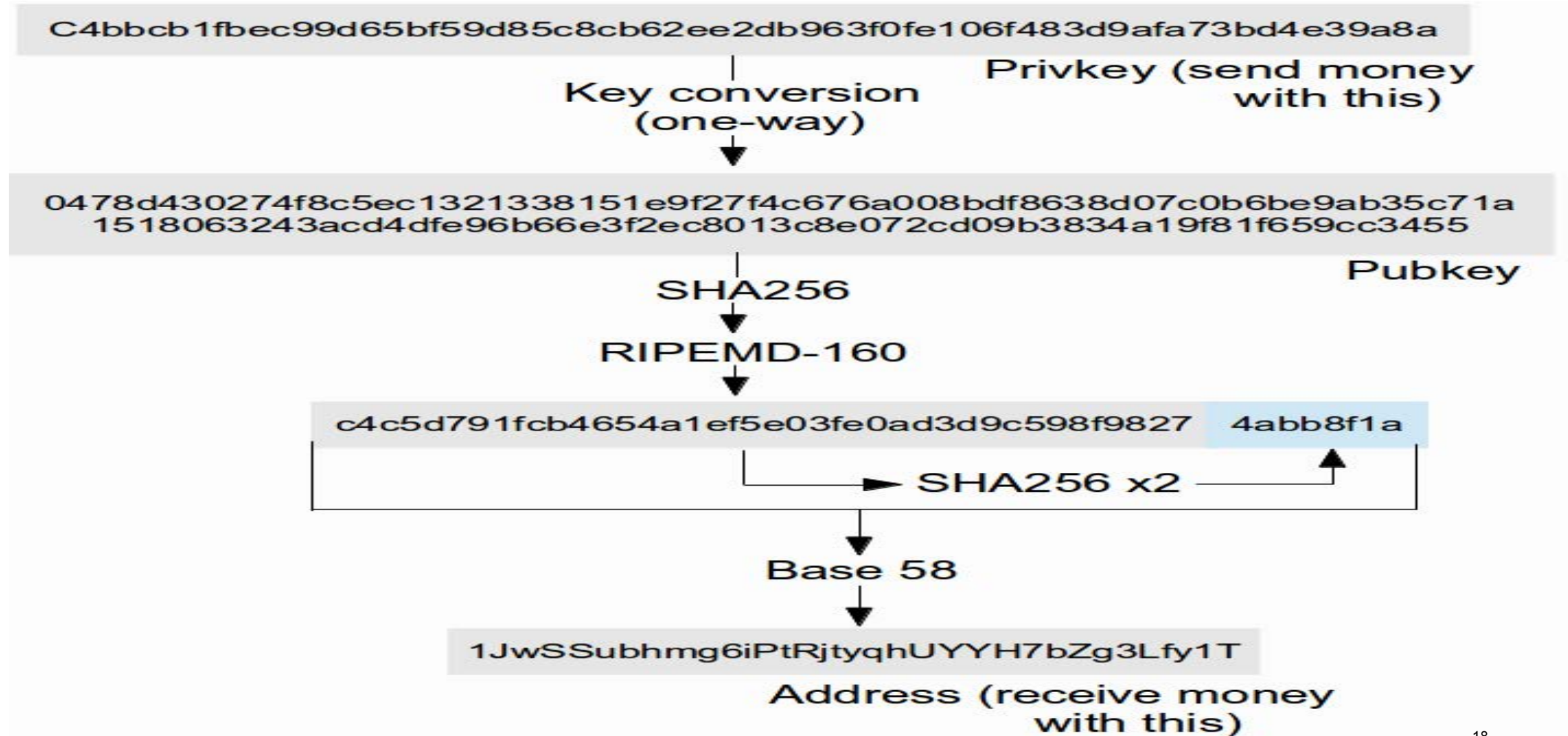
Criptografía Asimétrica en Bitcoin

Función de Firma Digital en Bitcoin

- **Algoritmo de Firma Digital con Curvas Elípticas (ECDSA)**
 - Curva utilizada: $y^2 = x^3 + 7$

 Este sistema permite que los usuarios firmen transacciones con su clave privada y que cualquiera pueda verificar su validez usando solo la clave pública.

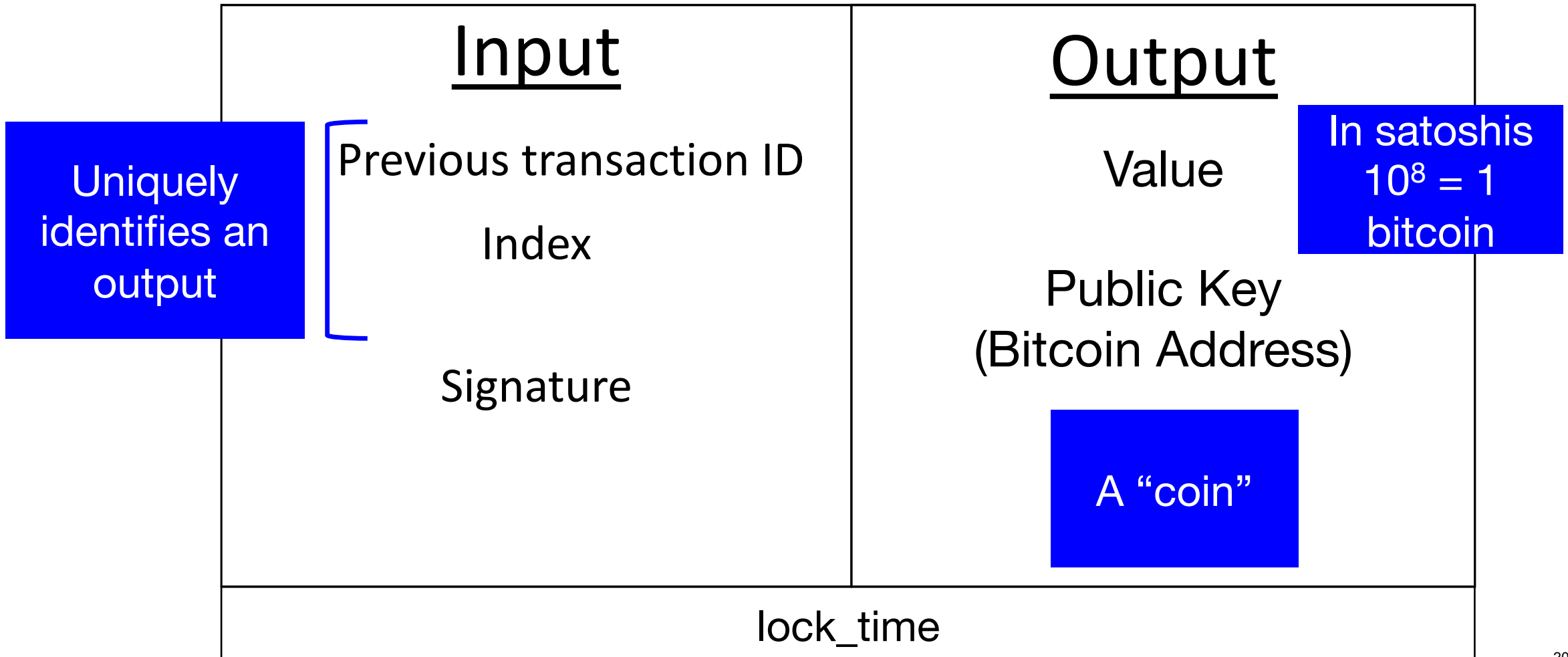
Bitcoin Addresses



Deposits & Negotiable Orders



Transaction format



Preguntas de Estudio

- ¿Qué es el problema de los Generales Bizantinos? ¿Cómo lo resuelven la prueba de trabajo (Proof of Work) y la minería en Bitcoin?
¿Y de forma más general, cómo lo aborda la tecnología blockchain?
- ¿Qué otros protocolos de consenso existen? ¿Cuáles son las ventajas e inconvenientes de los algoritmos alternativos como proof-of-work, proof-of-stake, etc.?
- ¿Cómo registra Bitcoin las transacciones? ¿Qué es una **salida de transacción no gastada** (UTXO)?
¿Qué código de script está incrustado en cada transacción de Bitcoin y qué tan flexible es como lenguaje de programación?

Conclusiones de la Clase 4

Diseño de Bitcoin

- Registros inmutables con sello temporal (bloques)
- Asegurados mediante funciones hash criptográficas y firmas digitales


Protocolo de Consenso

- Consenso alcanzado mediante prueba de trabajo (Proof of Work)
- Red descentralizada de nodos
- Moneda nativa (bitcoin)

Conclusiones de la Clase 4

Registro de Transacciones

- Entradas y salidas de transacción
- Salidas de transacción no gastadas (**UTXO**)
- Lenguaje de scripting embebido en cada transacción

 Estos elementos permiten que Bitcoin funcione como un sistema descentralizado, verificable y programable de transferencias de valor.