TIBA

Lecture 1
Cryptographic Primitives

By Samuel Tang, TIBA

Fall 2020 @ Tsinghua University

TIBA

Goal: Understand the magic behind why blockchain works

TIBA

Content

- Cryptographic Hash functions
- Symmetric & Asymmetric Encryption
- Digital Signatures
- Cryptography enabled Blockchain
- Zero Knowledge Proof

TIBA

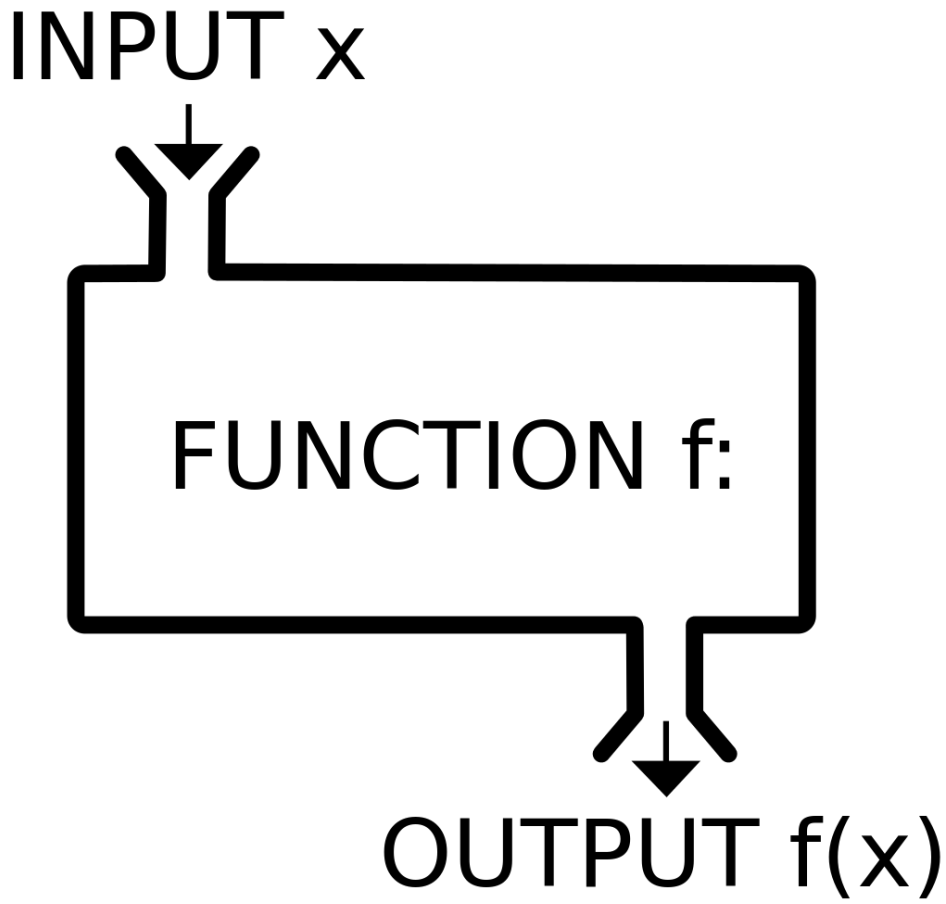
Cryptographic Hash functions

TIBA

What is a function?

Algebra Review

- Input -> function -> output
- ex. f(x) = 5x



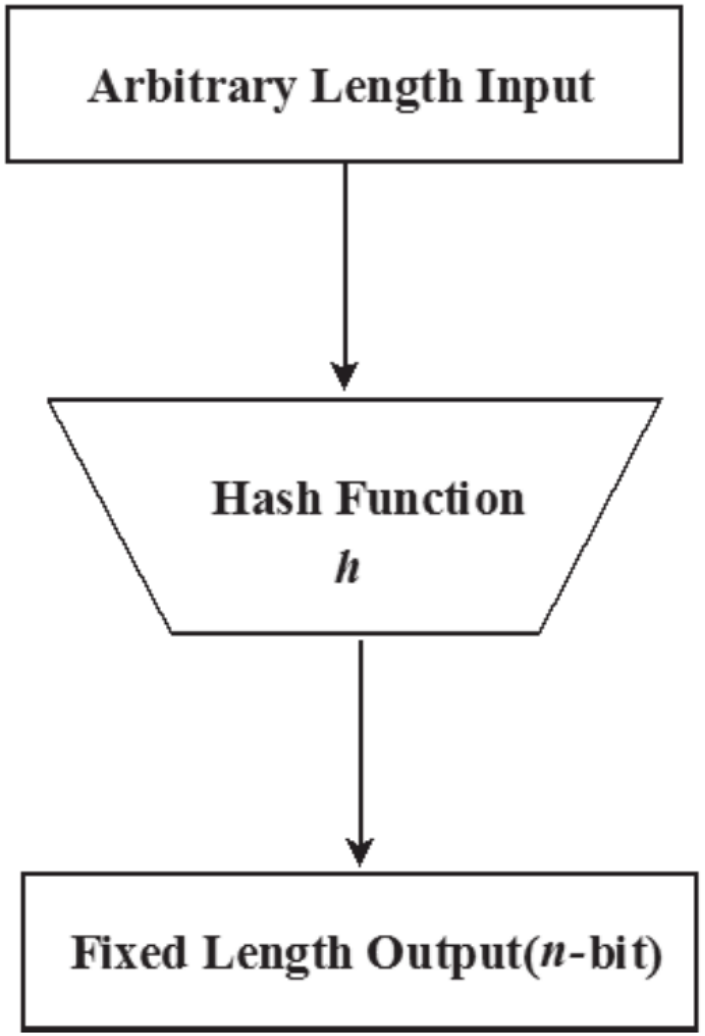
Img: https://en.wikipedia.org/wiki/Function_(mathematics)

TIBA

What is a “hash” function?

Blockchain Fundamental

- Input -> hash function -> output
  - Arbitrary-size input (aka message)
  - Hash function = mathematical transformation
  - fixed-size output (aka digest, hash)

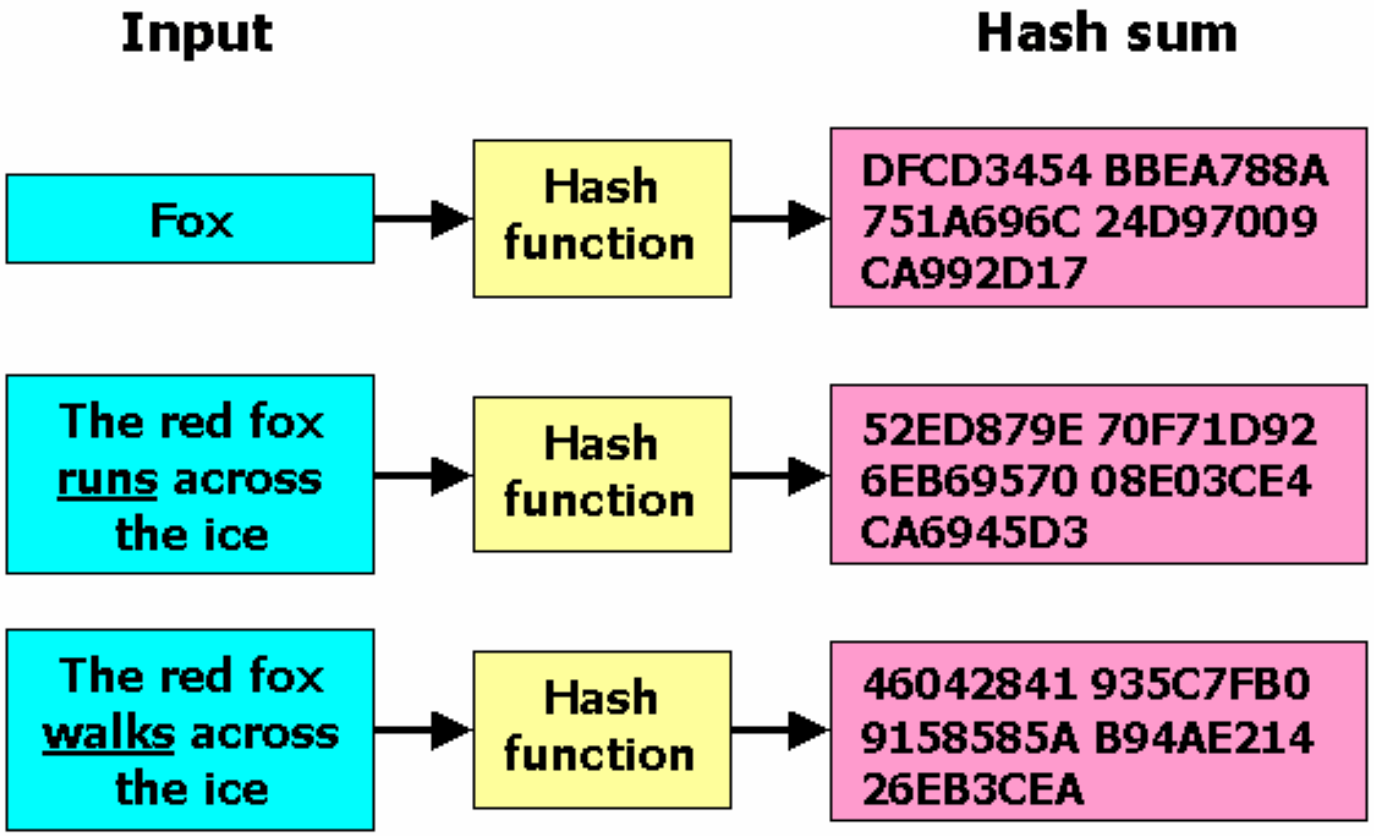


Img: https://www.researchgate.net/figure/Cryptographic-hash-function-Formally-a-hash-function-can-be-shown-as-0-1_fig1_322094216

TIBA

What is a “hash” function?

Example



Img: https://www.researchgate.net/figure/Cryptographic-hash-function-Formally-a-hash-function-can-be-shown-as-0-1_fig1_322094216

TIBA

Hash Function Properties

Things to know about Hash Functions

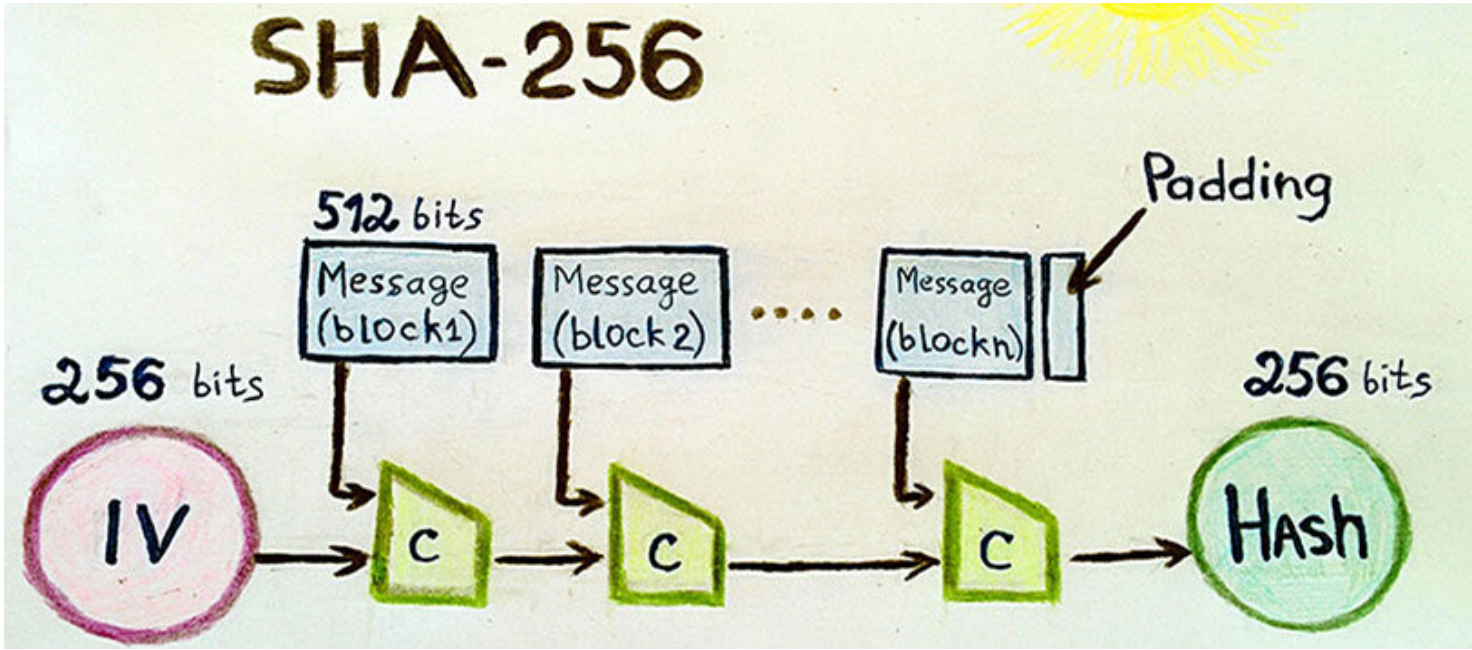
- Deterministic - same input same output
- Collision-free - different input different output
  - practically but not theoretically
- Hiding - one way function
  - given an output, infeasible to find the input
- Puzzle-friendly - given the output and part of the input, difficult to find the input
- Computationally Efficient – doesn't require too much computational power

TIBA

Hash Function Algorithm

SHA-256

- **SHA-256**
  - part of the SHA-2 cryptographic hash functions family
  - Output size: 256 bits
  - Used in Bitcoin



Img: https://waytomine.com/sha-256-algorithm-function-bitcoin-network/

TIBA

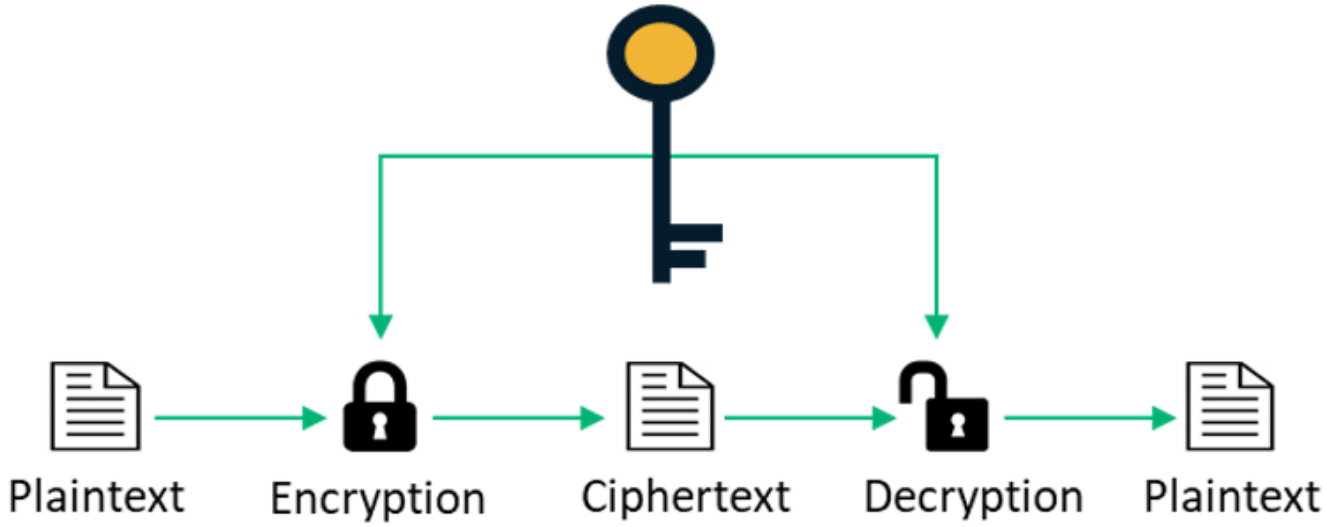
Symmetric & Asymmetric Encryption

TIBA

Symmetric Encryption

Blockchain Fundamental

- same key is used for both encrypting and decrypting messages
- security depends on keeping the key safe

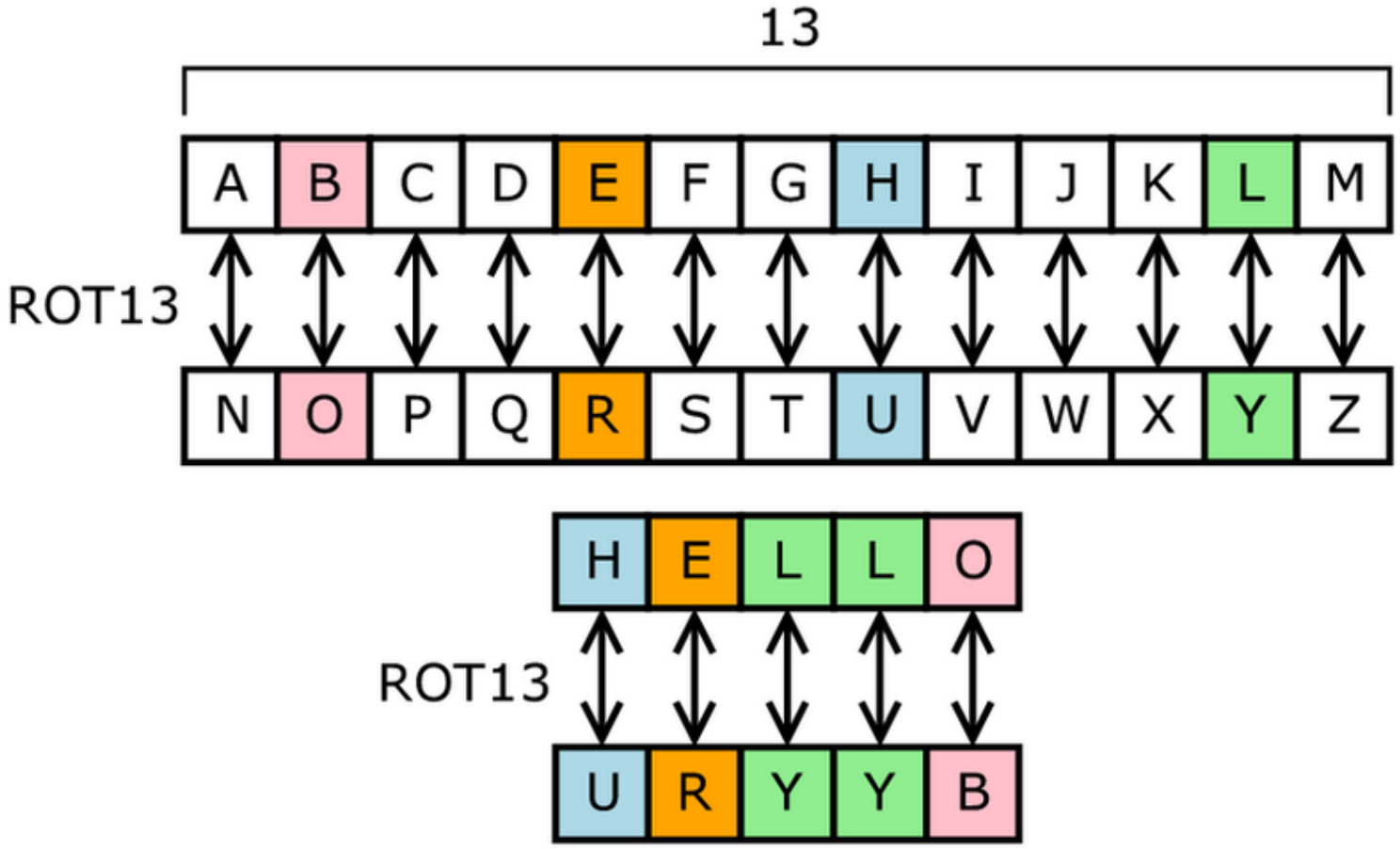


Img: https://sectigostore.com/blog/5-differences-between-symmetric-vs-asymmetric-encryption/

TIBA

Symmetric Encryption

Example

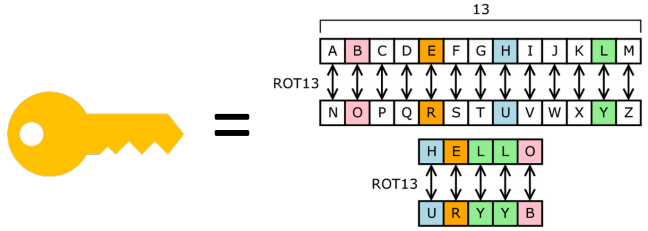


Img: https://sectigostore.com/blog/5-differences-between-symmetric-vs-asymmetric-encryption/

TIBA

Symmetric Encryption

Example



HELLO -> URYYB

URYYB -> HELLO

URYYB???

Alice

Christopher

Bob

Img: https://sectigostore.com/blog/5-differences-between-symmetric-vs-asymmetric-encryption/

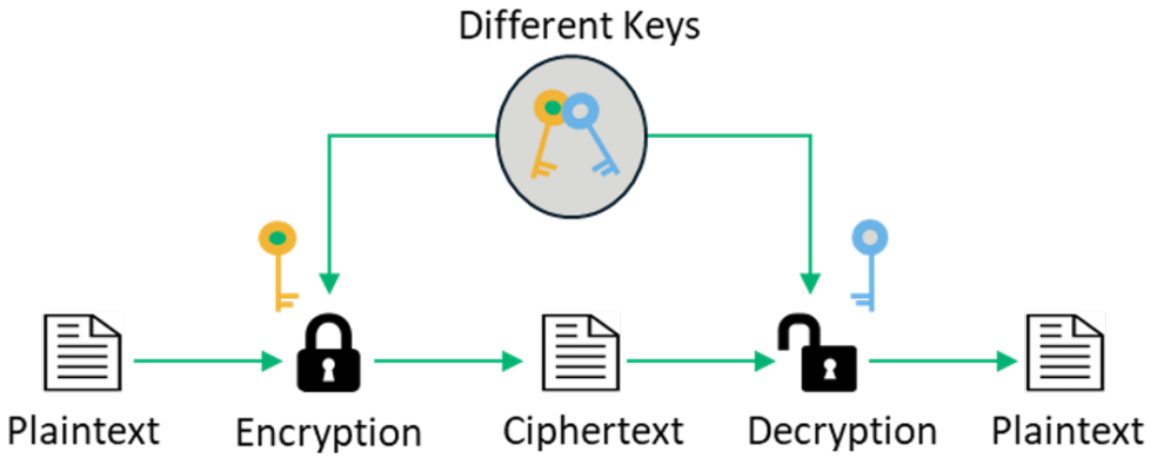
TIBA

Asymmetric Encryption

aka Public-Key Cryptography

- Two keys: public key and private key
  - Mathematically related
  - Public key: accessible to everyone
  - Private key: only yourself

- If use public key encrypt, then use private key decrypt
- If use private key encrypt, then use public key decrypt
- Security depends on keeping your own private key safe

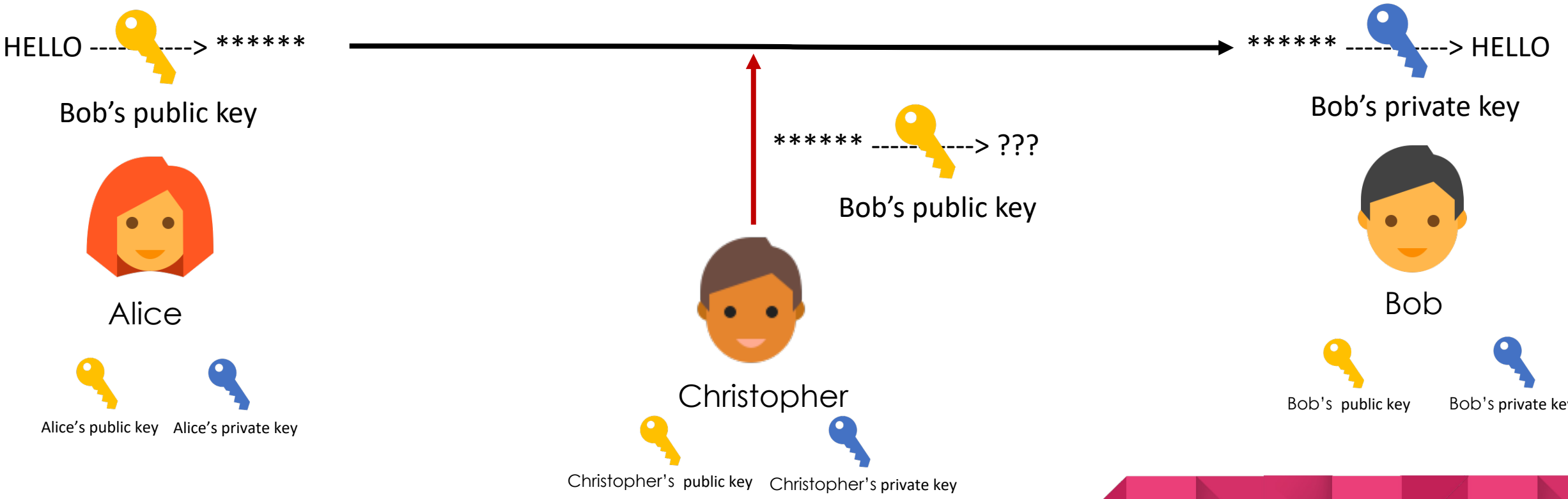


Img: https://sectigostore.com/blog/5-differences-between-symmetric-vs-asymmetric-encryption/

TIBA

Asymmetric Encryption

Example



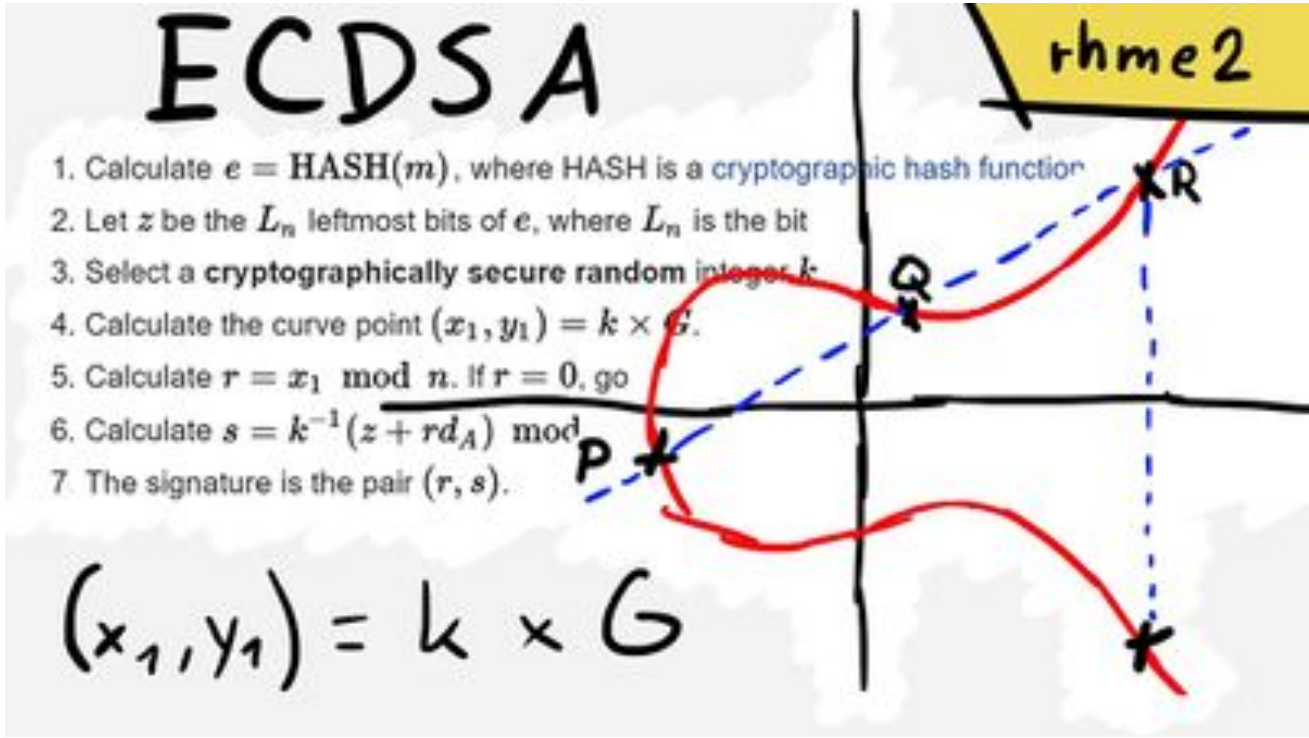
Img: https://sectigostore.com/blog/5-differences-between-symmetric-vs-asymmetric-encryption/

TIBA

Elliptic Curve Digital Signature Algorithm

ECDSA

- Digital Signature Algorithm (DSA) which uses keys derived from elliptic curve cryptography (ECC)
- Used in Bitcoin to produce private and public key pair



Img: https://en.bitcoinwiki.org/wiki/Elliptic_Curve_Digital_Signature_Algorithm

TIBA

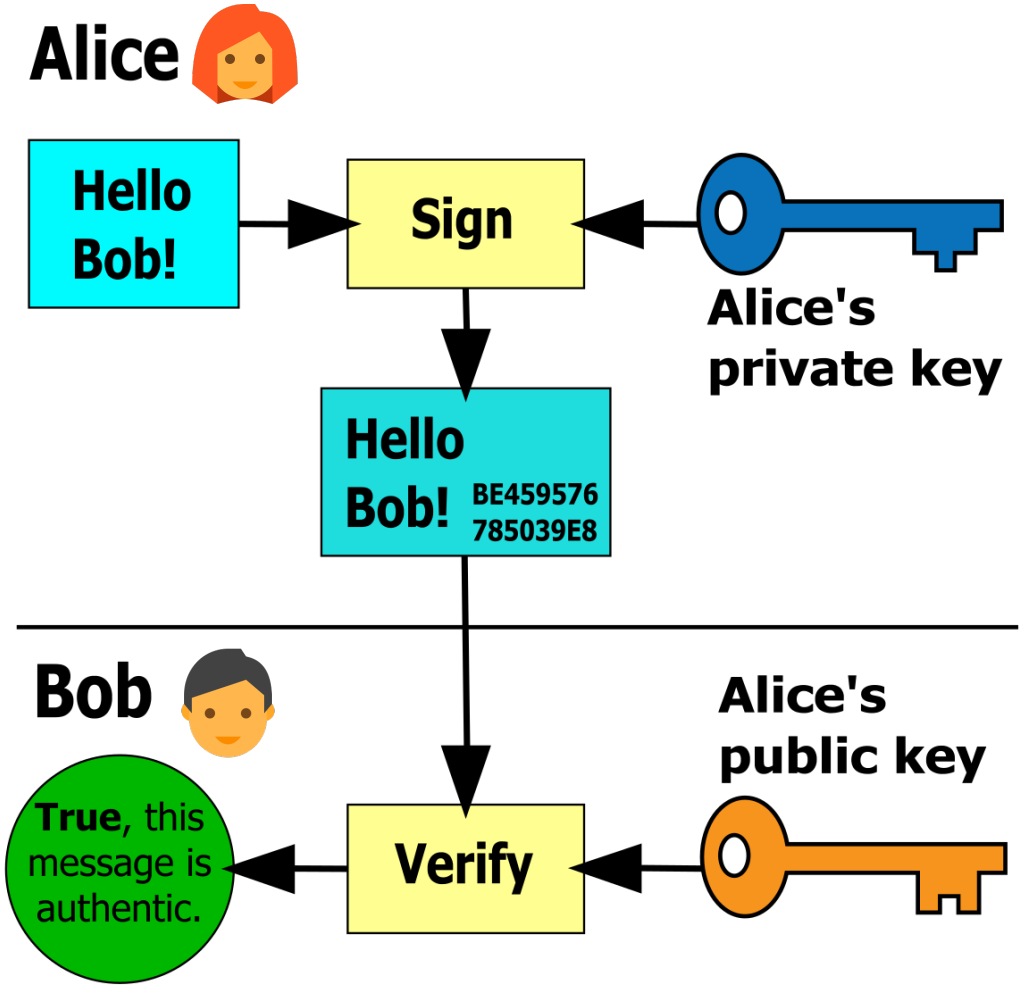
Digital Signatures

TIBA

Digital Signature

Proving Identity

- **Digital Signature**
  - to generate:
    private key + message
  - to verify:
    public key + message + digital signature
  - in **Bitcoin**:
    message == transaction

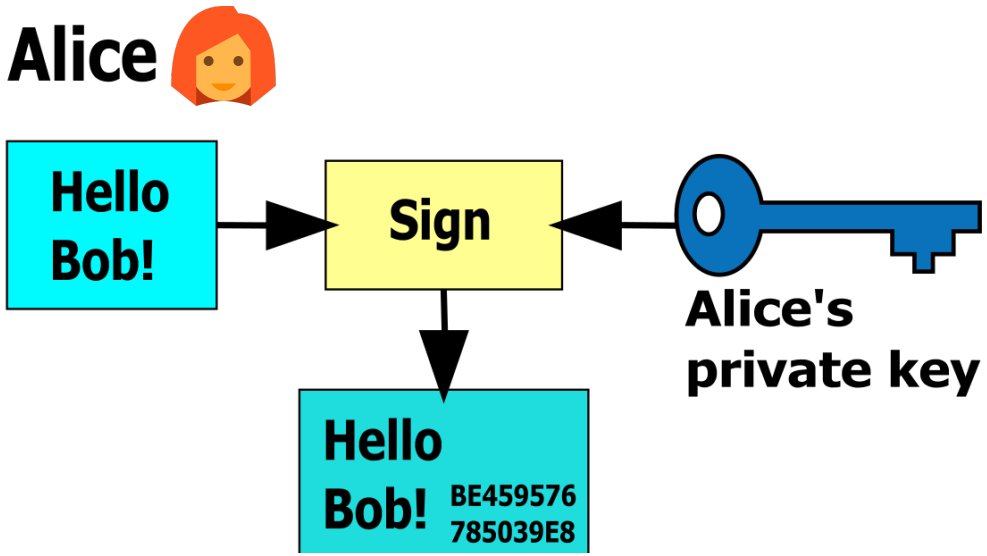


Source: https://en.wikipedia.org/wiki/Digital_signature

Digital Signature

Proving Identity

- **Alice has a private-public key pair**
  - Signing key (private key)
  - Verification key (public key)
- Sign the message with her private key
- Publish: original message, Alice's public key, Signed message



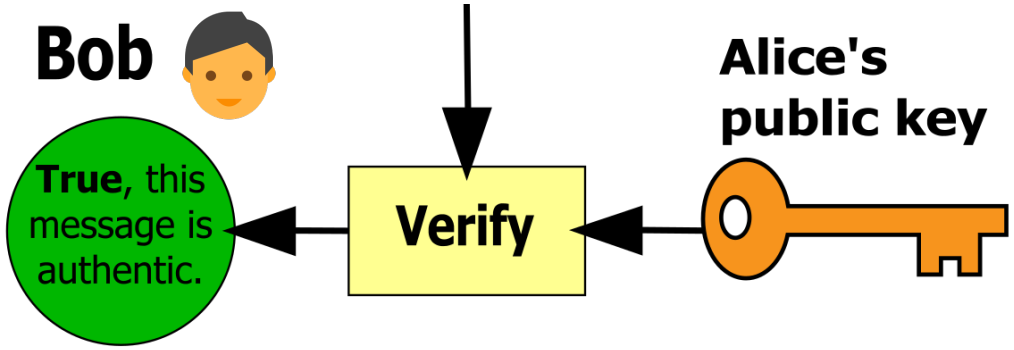
Source: https://en.wikipedia.org/wiki/Digital_signature

TIBA

Digital Signature

Proving Identity

- **Bob uses Alice's public key to verify the message was sent from Alice and not anyone else**

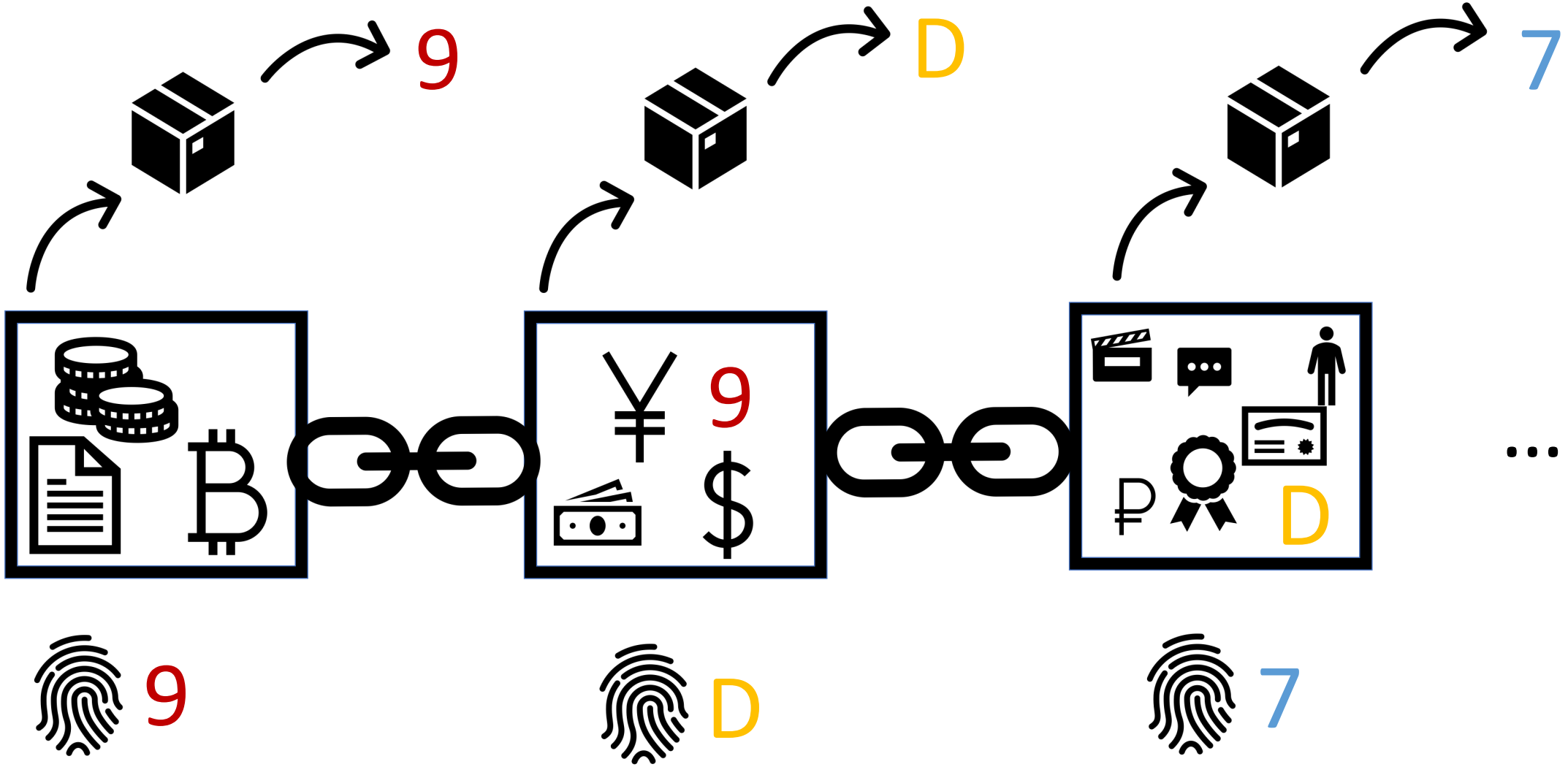


Source: https://en.wikipedia.org/wiki/Digital_signature

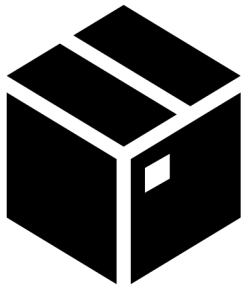
TIBA

Cryptography-enabled Blockchain

TIBA

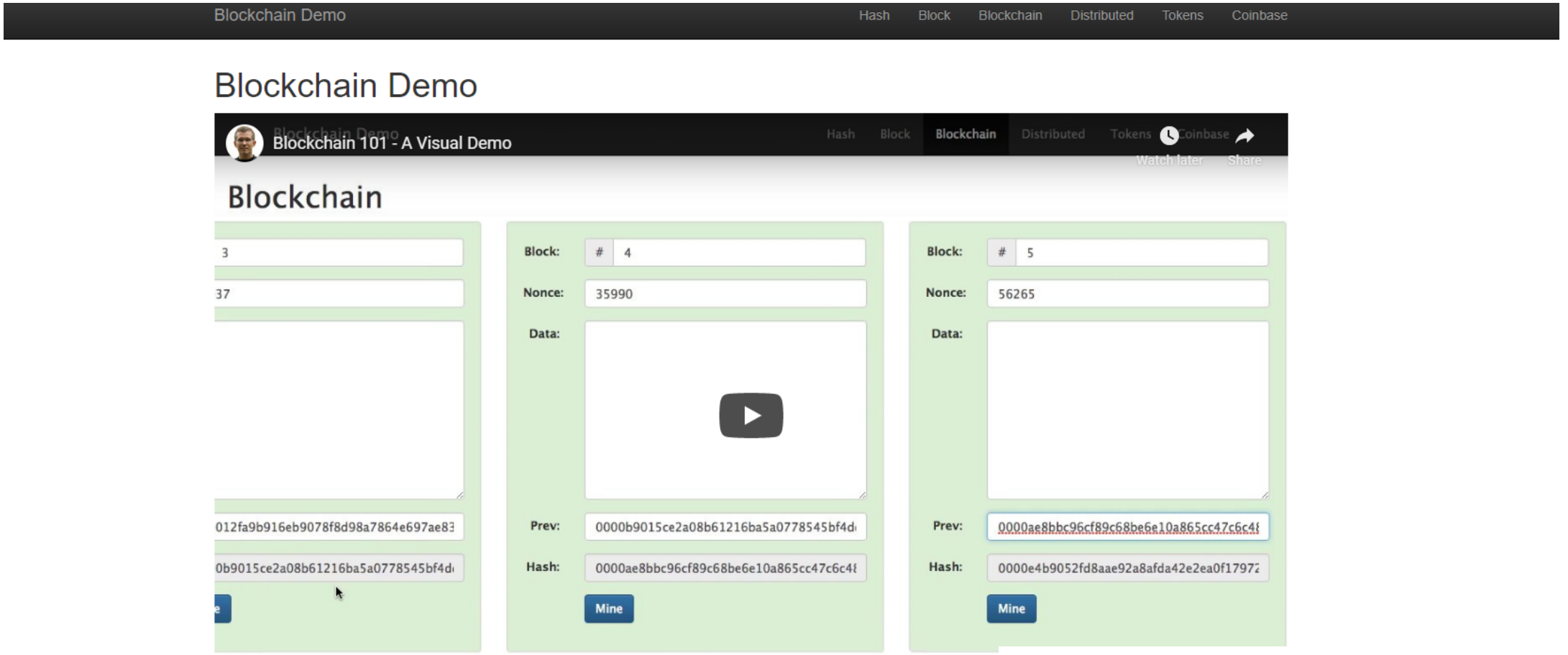


TIBA



= Hash Function

Blockchain Visual Demo



Source: https://andersbrownworth.com/blockchain/

TIBA

Zero Knowledge Proof

TIBA

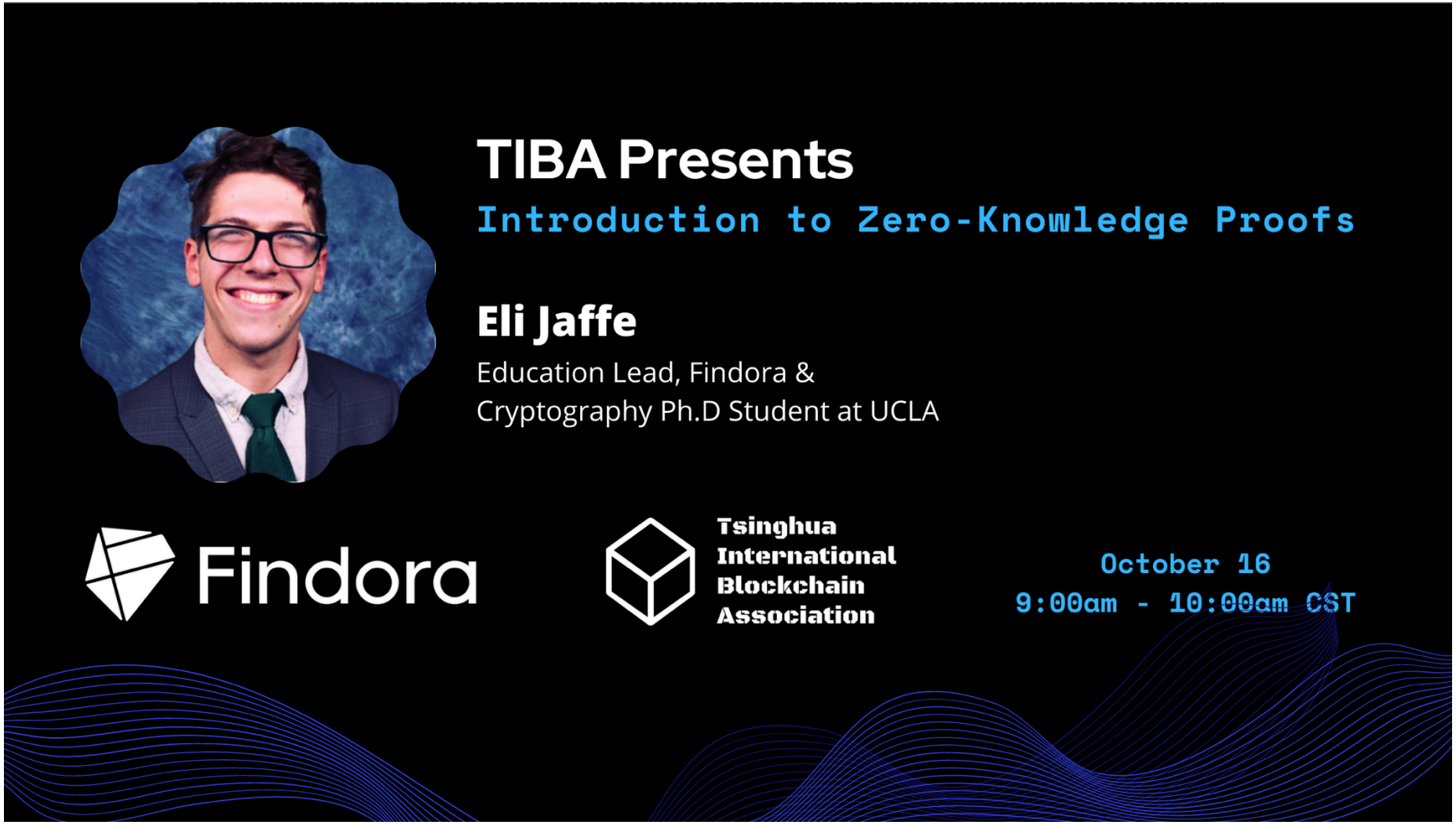
Zero Knowledge Proof

Proving without Revealing

- Proving you know a secret without revealing the secret
- Isn't 100% proof, but it minimizes the probability that someone is lying

Readings: https://blog.goodaudience.com/what-is-zero-knowledge-proof-and-why-you-should-care-36977d738339
https://www.wired.com/story/zero-knowledge-proofs/;

TIBA Workshop #1 Oct 16



TIBA

Questions?

TIBA

Homework Assignments

- Blockchain 101 - A Visual Demo
- Blockchain 101 - Part 2 - Public / Private Keys and Signing
  - Demo website
- How secure is 256 bit security?
- Asymmetric encryption - Simply explained
- Digital Signatures and Signing transactions explained
- [optional] How SHA-2 Works Step-By-Step (SHA-256)

TIBA

Extra Material – ZK Proof

- Zero Knowledge Proof – ZKP
- Zero Knowledge Proofs - Computerphile
- Security and Privacy for Crypto with Zero-Knowledge Proofs
- Zero-knowledge proofs intro with Str4d (Zcash)
- Zero Knowledge Proofs and Their Future Applications by Elad Verbin at Web3 Summit 2018
- WTF is Zero-Knowledge Proof

TIBA

Cryptographic Primitives
by
Samuel Tang

Thank you for listening!
See you next week!