Deep into Blockchain Series

Cryptography & Distributed Computing

Presenter(s): Founding Team

Event Organizers

dbcentrum Community

Connect | Collaborate | Create

Venue Sponsor

nagarro

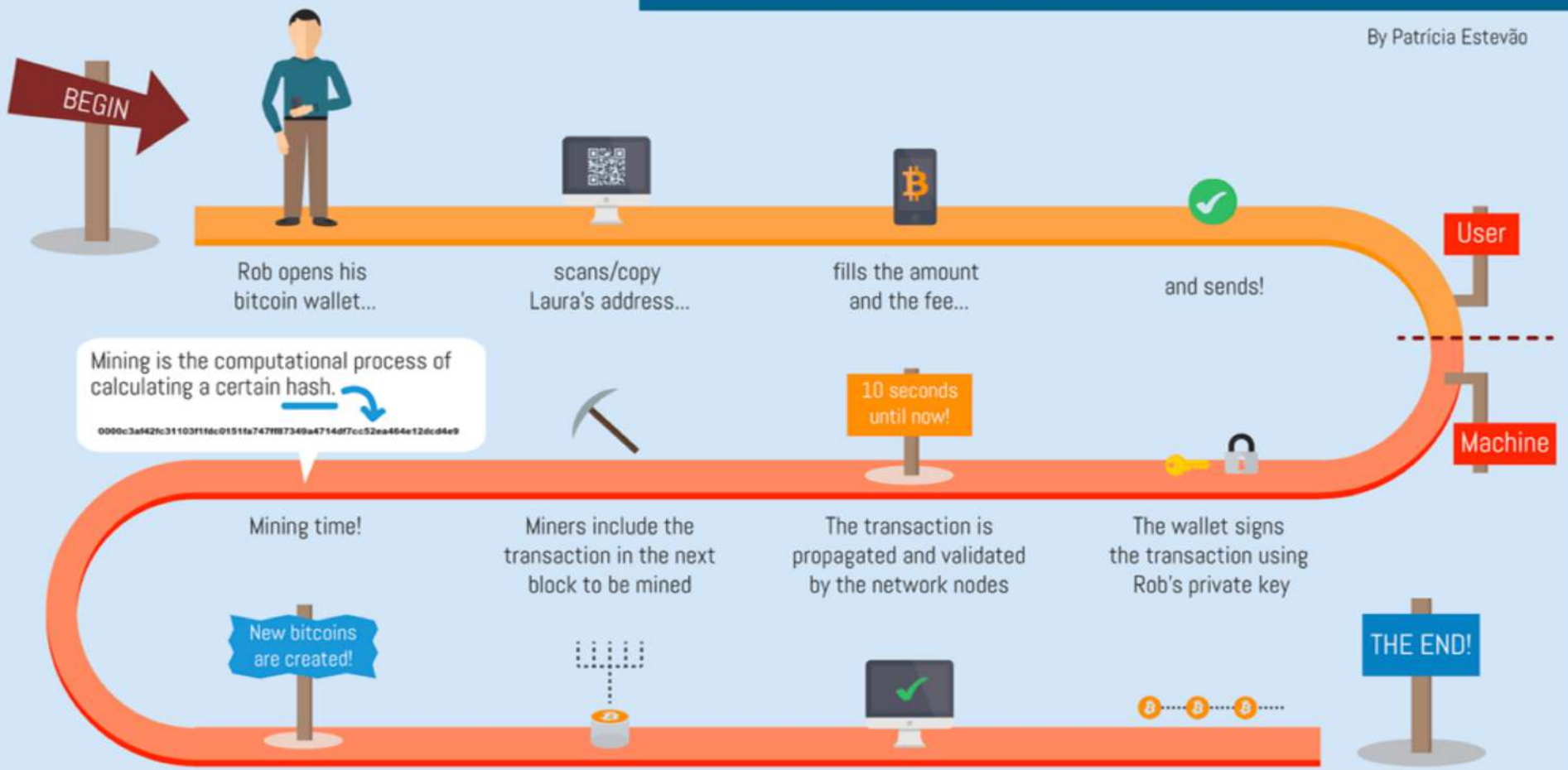
Let us try to find answers!

- Is the data transmitted on Blockchain encrypted?
- Can data encrypted by public key decrypted by public key?
- is there a difference between Hashing & Cryptographic hashing?
- Which cryptographic algorithm is used by popular Blockchains?
- When to use different types of encryption?
- What is the significance of digital signatures?
- How does a transaction use cryptography?

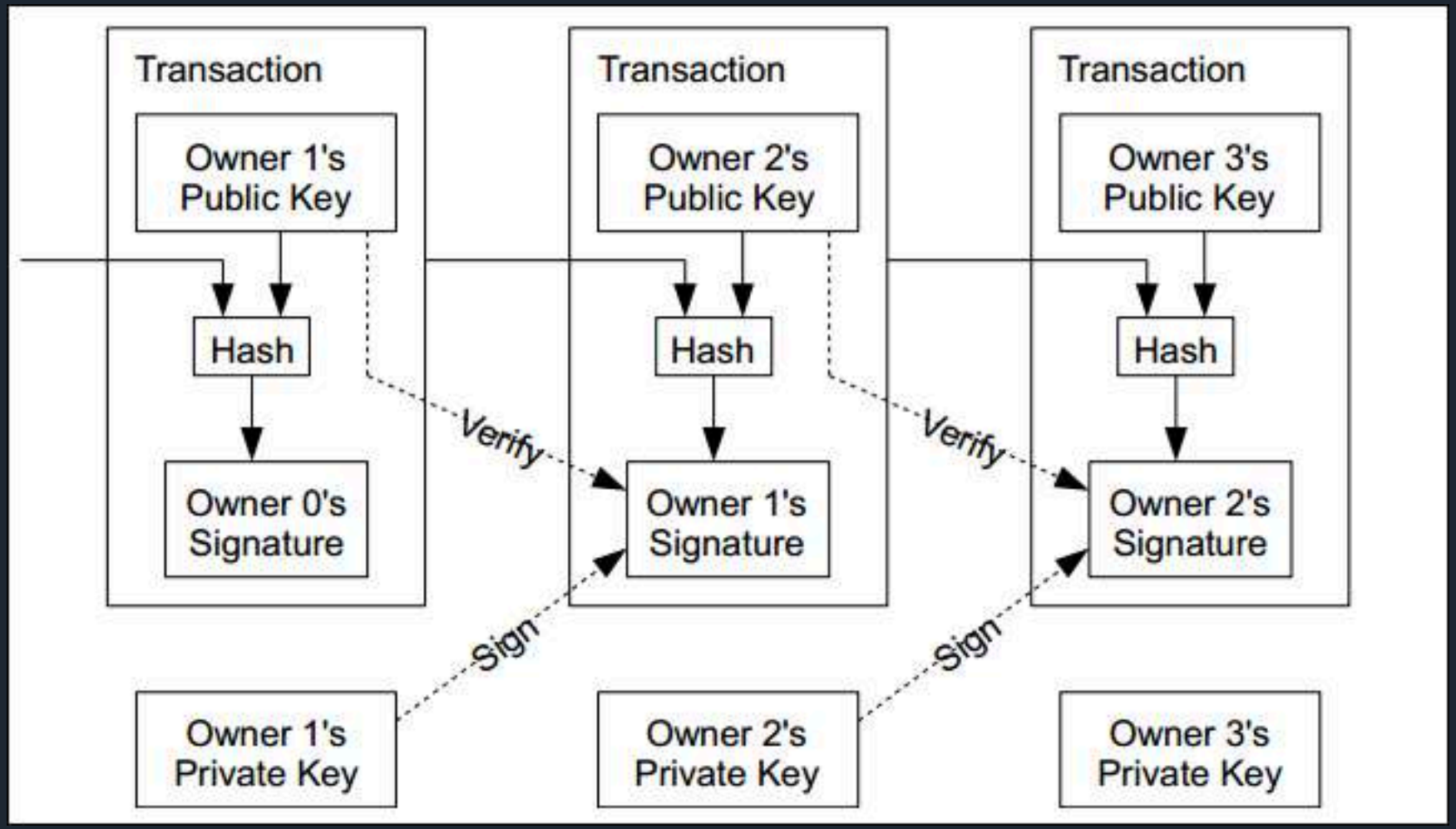
THE BITCOIN TRANSACTION LIFE CYCLE

Rob's quest to send 0.3 BTC to his friend Laura

By Patrícia Estevão



Importance of Cryptography in context of Blockchain



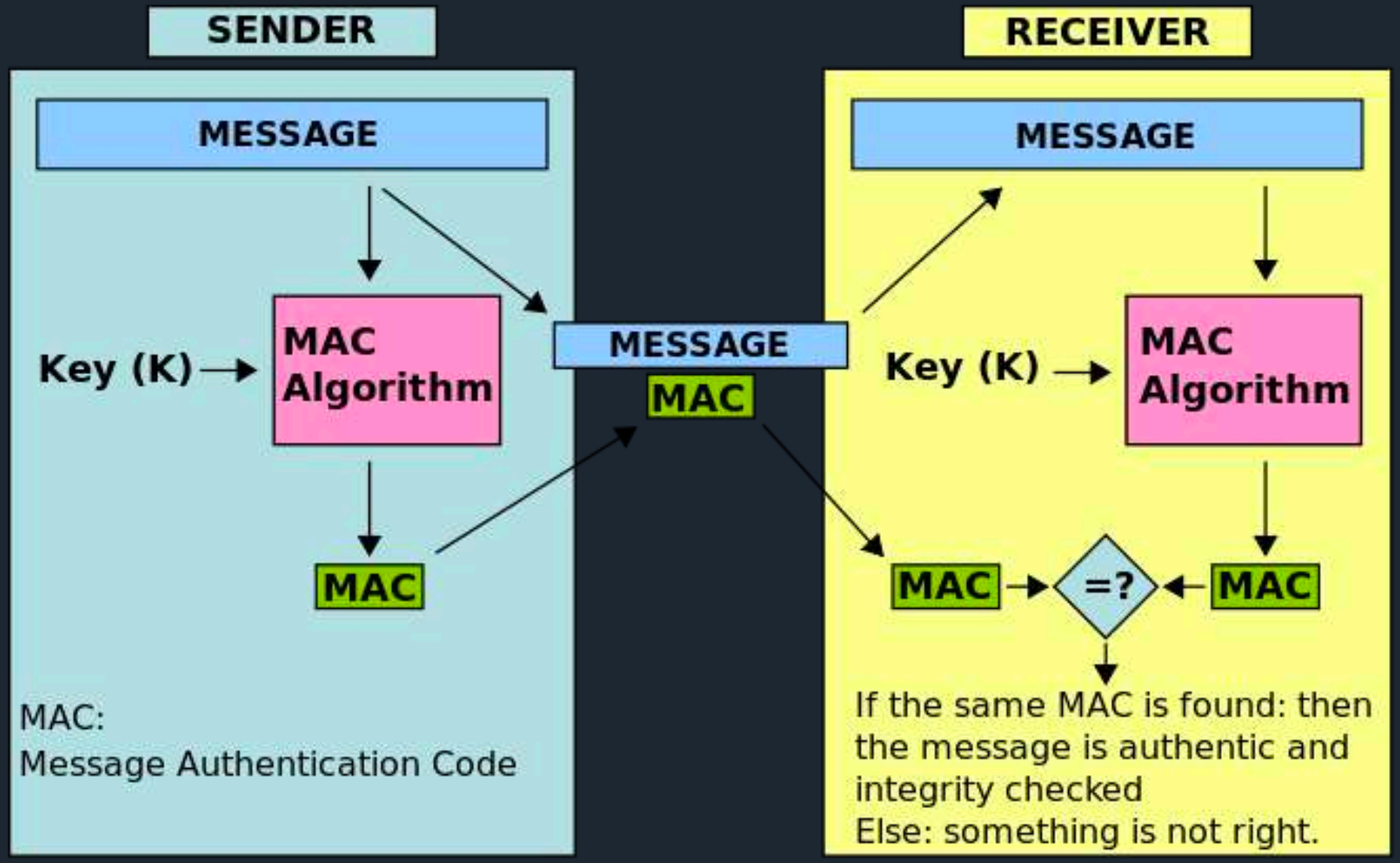
Mechanism of Hashing

- Hash functions are one way

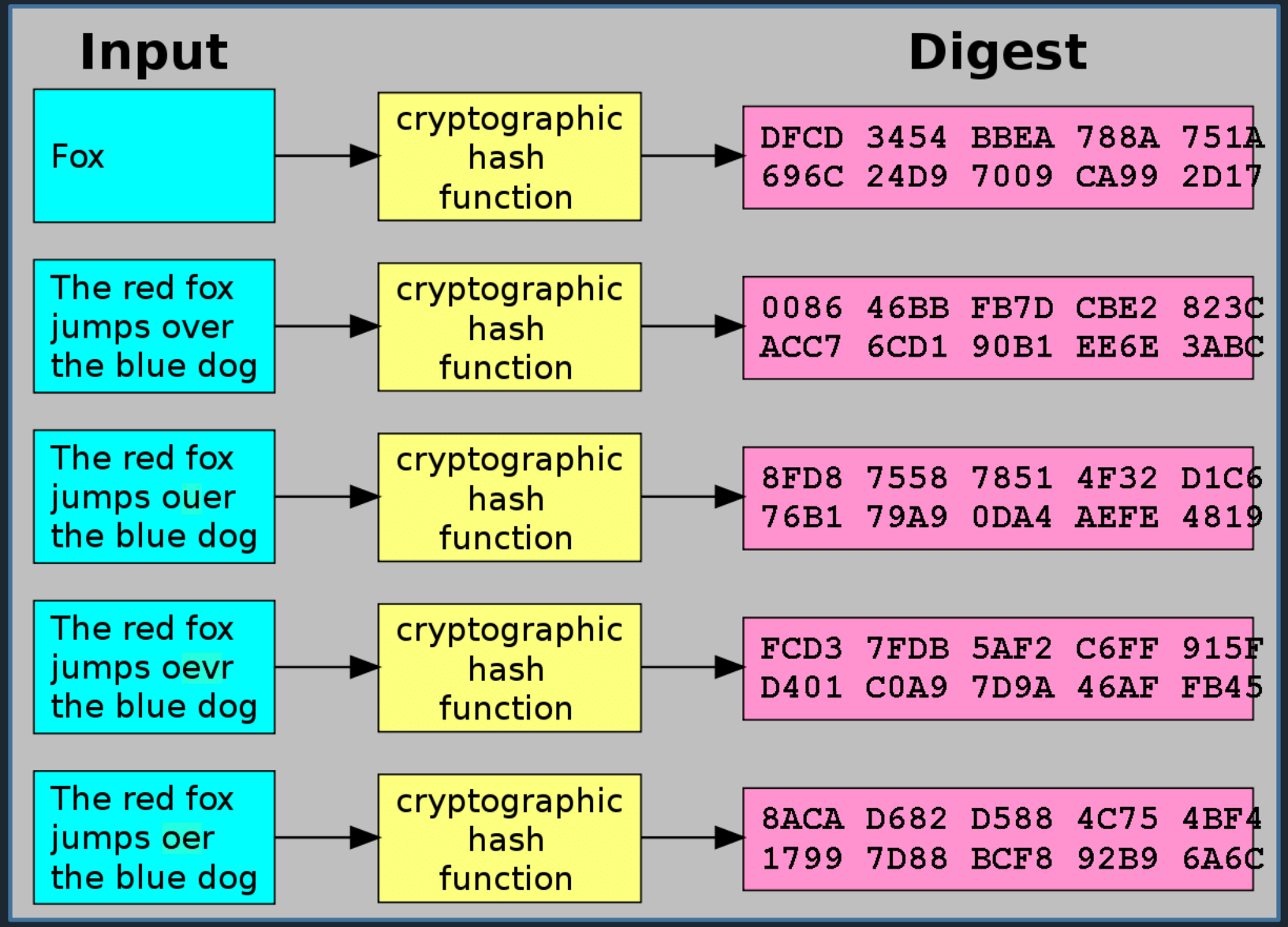
Algorithms

- MD5
- SHA-1
- SHA-256
- SHA-512

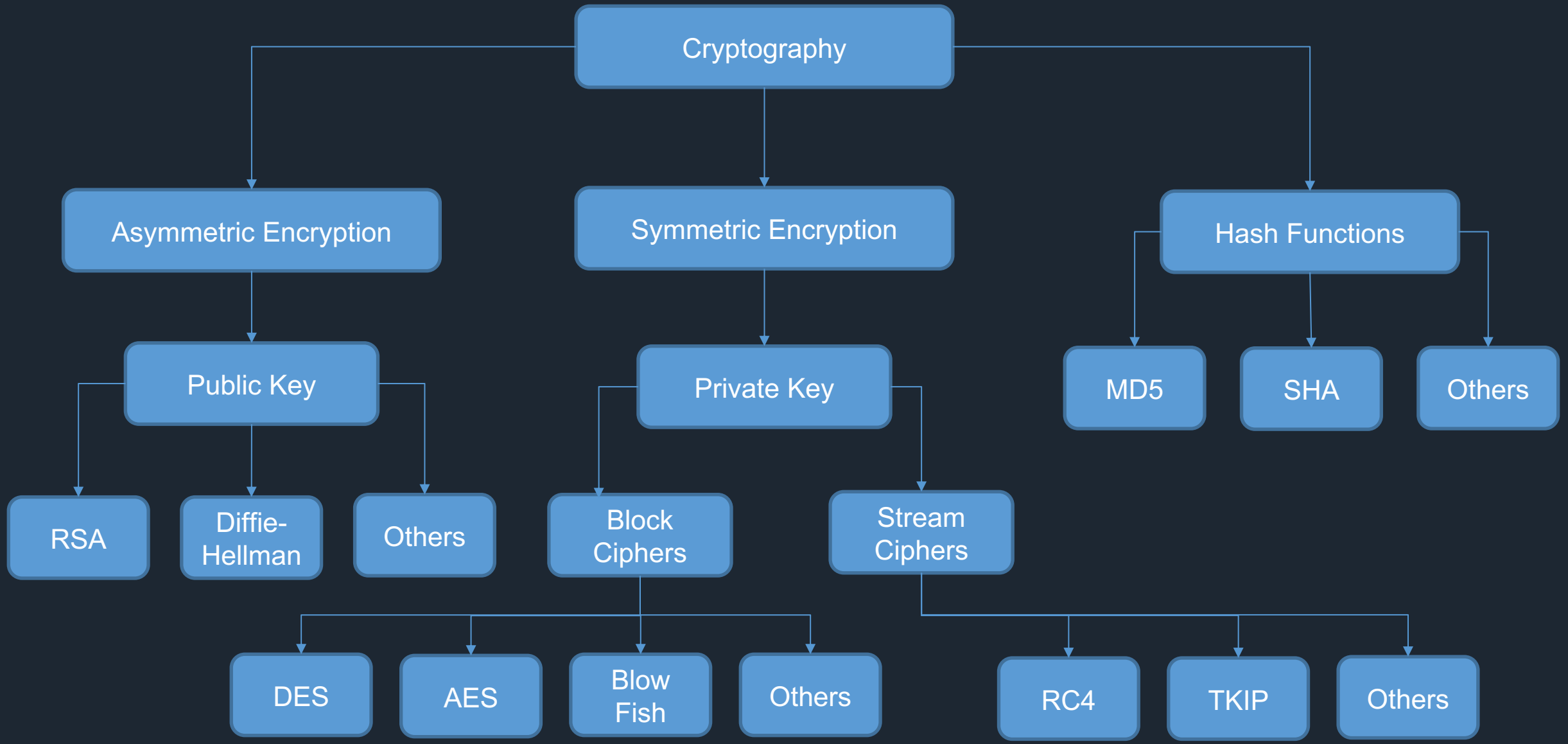
Mechanism of Hashing



Mechanism of Hashing



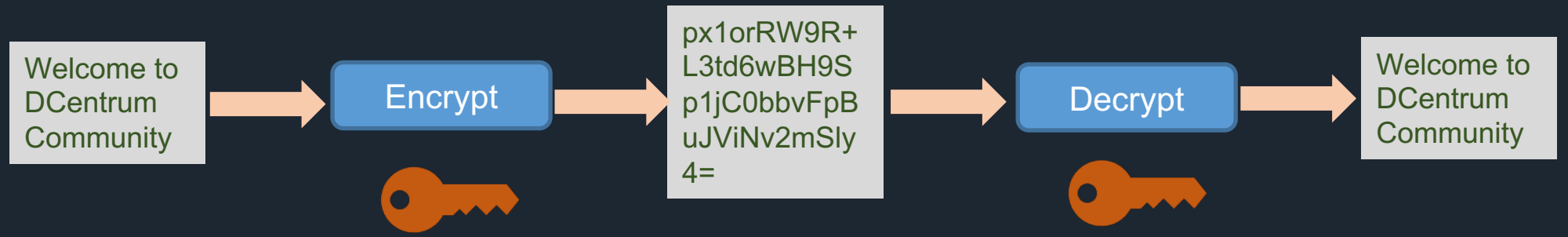
Cryptography tree



Importance of Cryptography in context of Blockchain

DES
Triple DES
AES
RC5

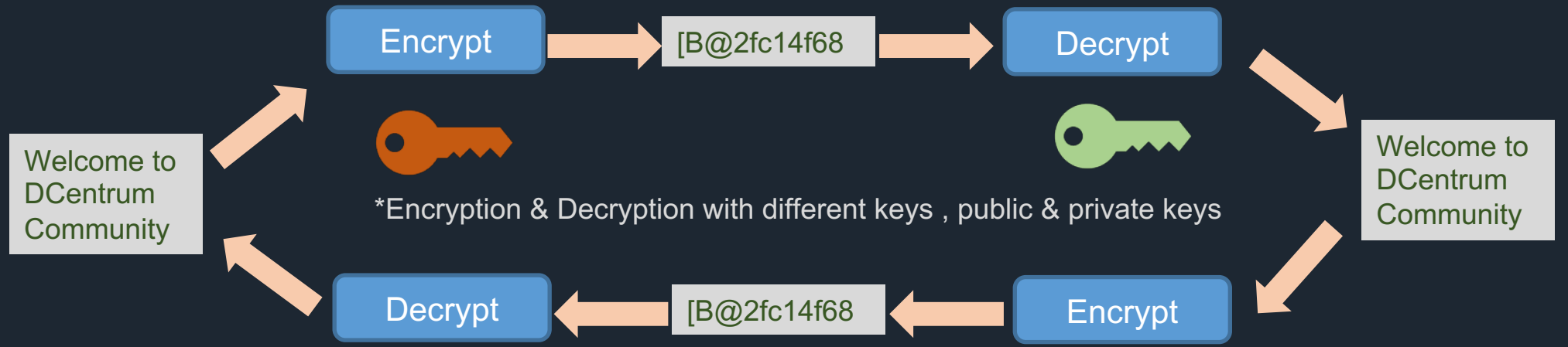
Symmetric Keys



*Encryption & Decryption use the same key

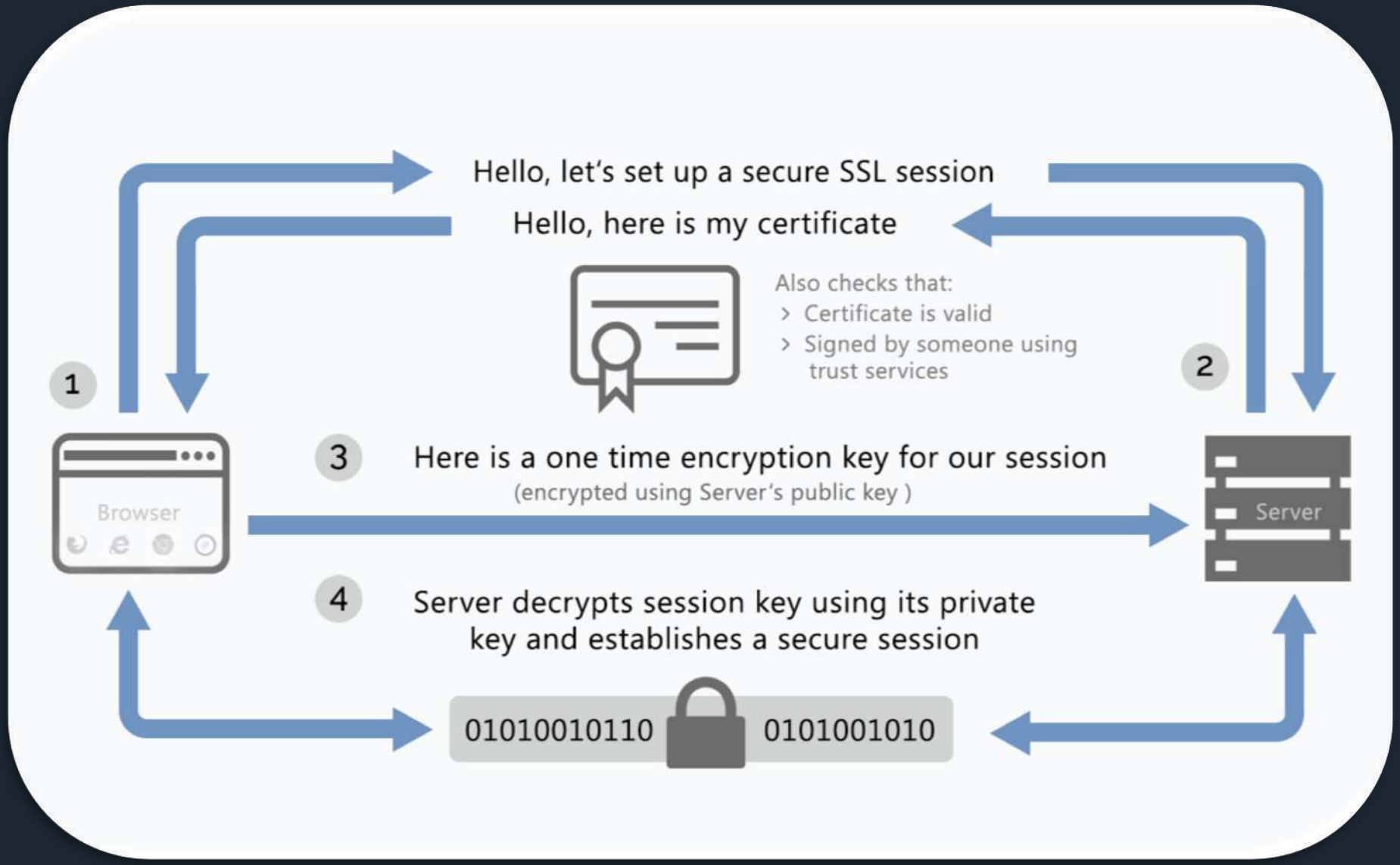
Asymmetric Keys

RSA
Elliptic Curve

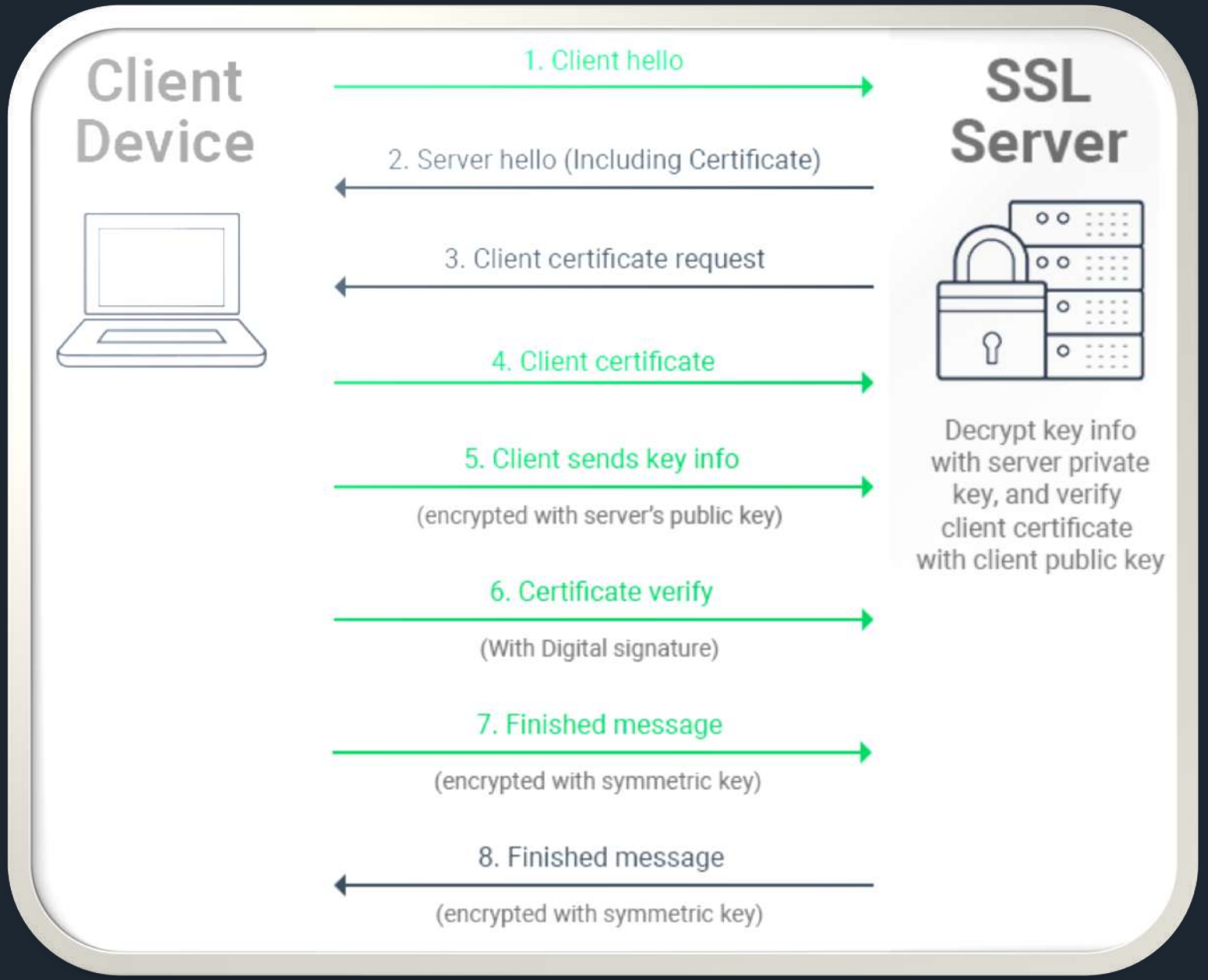


*Encryption & Decryption with different keys , public & private keys

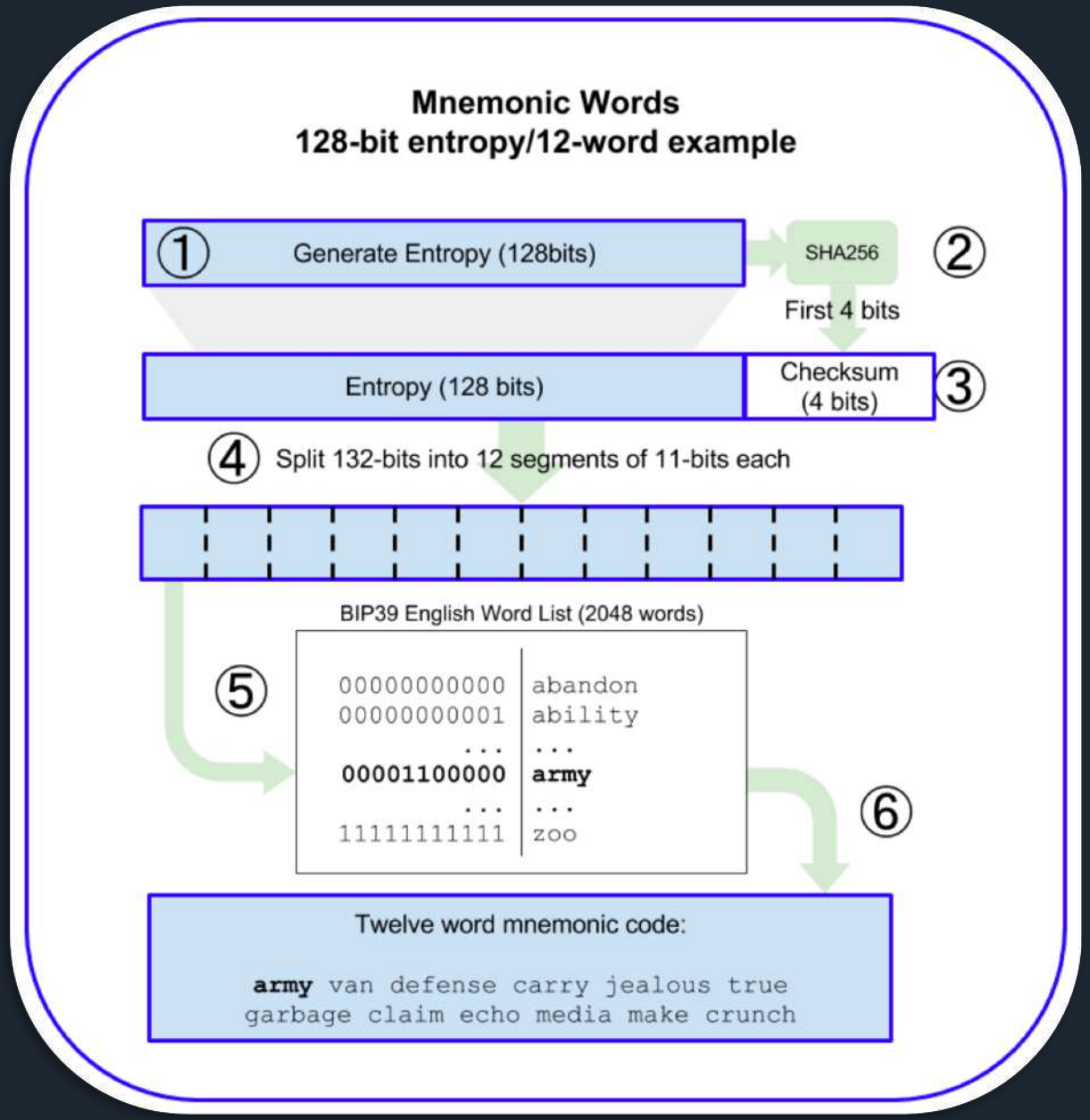
Cryptography & transmission of data via SSL



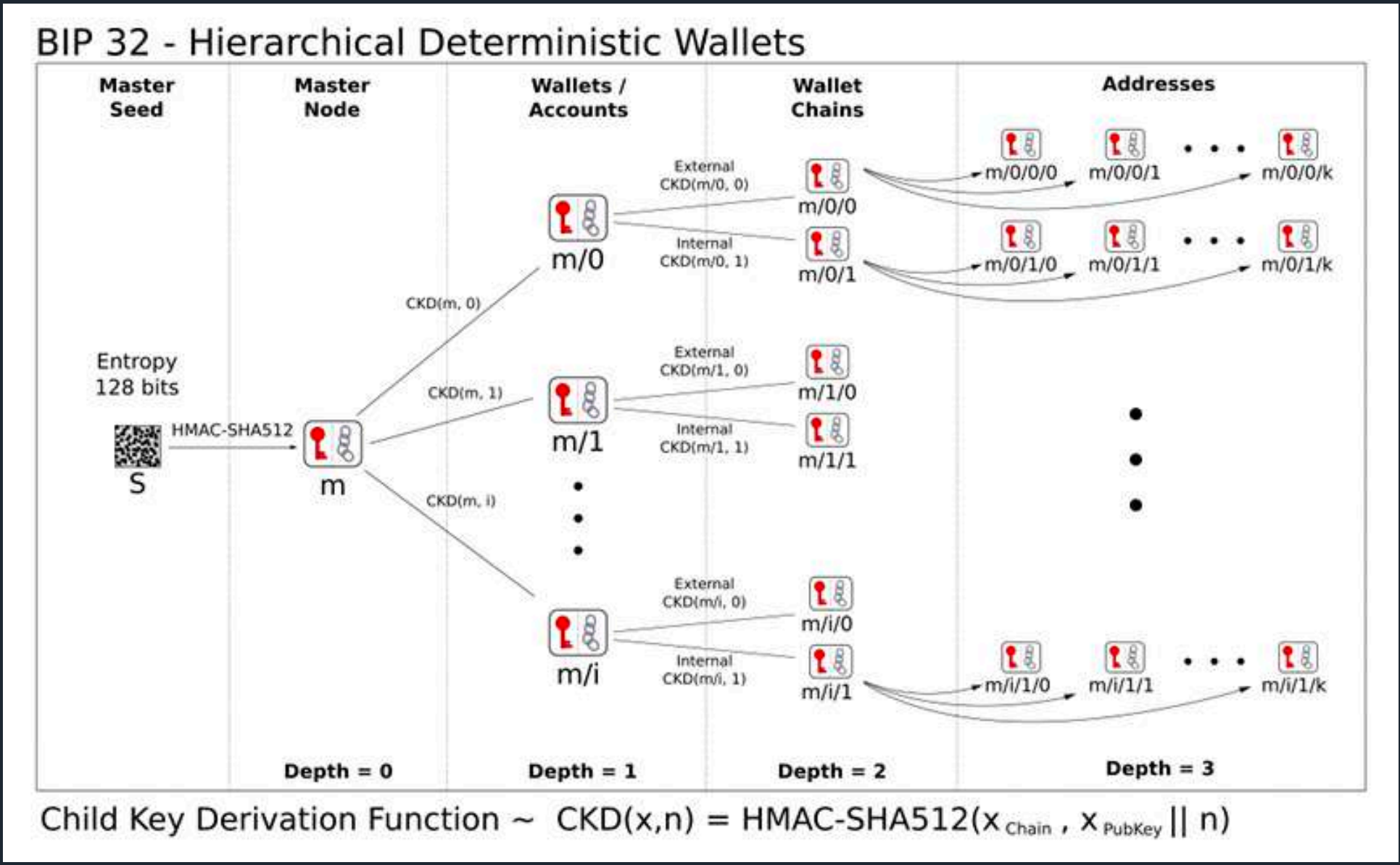
Cryptography & transmission of data via SSL



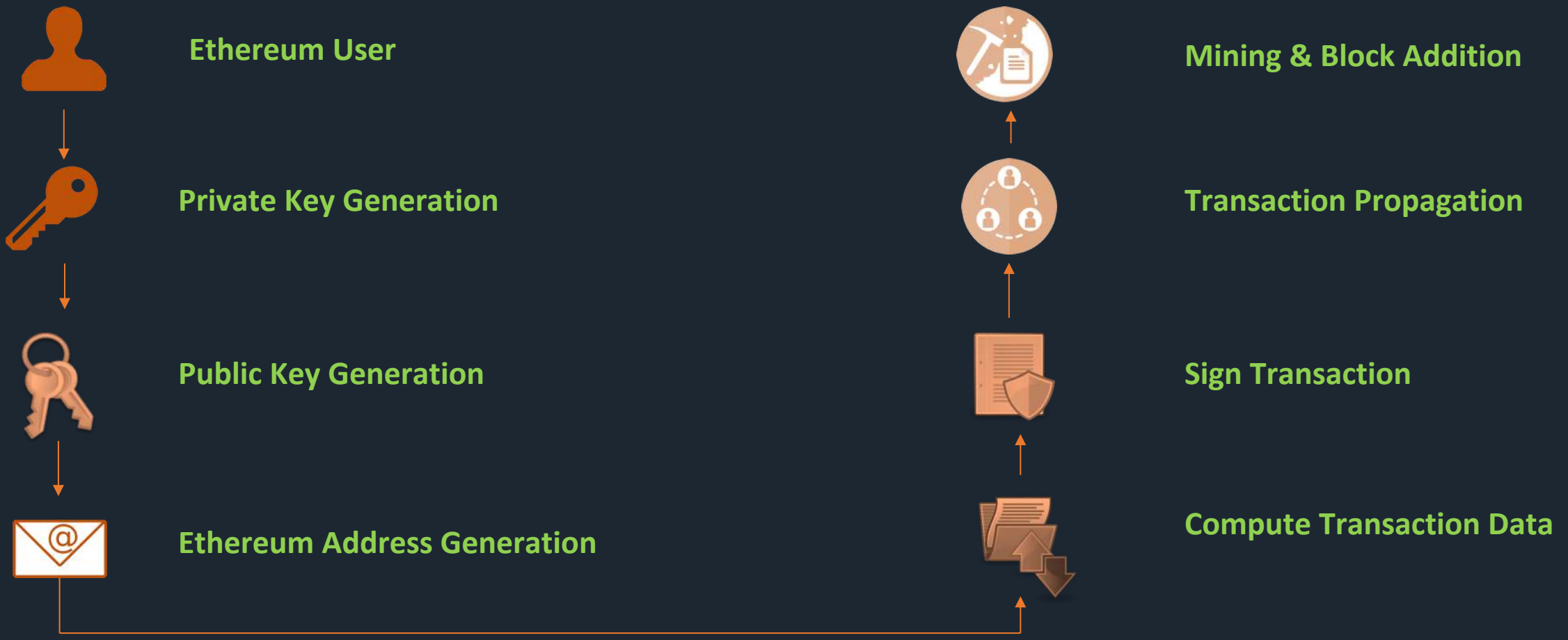
The need for mnemonics , BIP 32 and BIP 44 standards



The need for mnemonics , BIP 32 and BIP 44 standards



Transaction Cryptography Journey - Ethereum



Private Key Generation

User

Generate Private Key

Random 256 bit number

Human Source of Randomness

CSPRNG

SHA-256

or Keccak-256

Hashing Algorithm

Verify if the generated key is valid order of Elliptic Curve

f8f8a2f43c8376ccb0871305060d7b27b0554d2cc72bccf41b2705608452f315

Public Key Generation

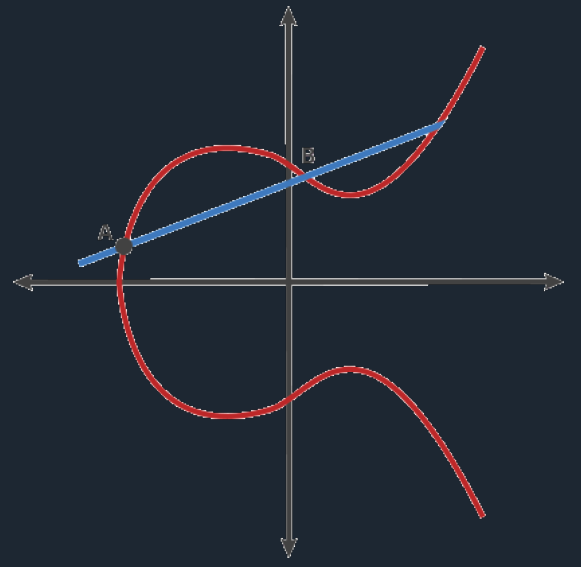
Private Key (k)

Elliptic Curve Multiplication

Public Key (K)

K = k * G

- G is a constant **Generator Point**
- Elliptic Curve Multiplication is a **one way function**
- Ethereum uses **secp256k1** standard of Elliptic Curve (**$y^2 = x^3 + 7$**)



A visualization of an secp256k1 elliptic curve

K = f8f8a2f43c8376ccb0871305060d7b27b0554d2cc72bccf41b2705608452f315 * G

K = (x,y)

x = 6e145ccef1033dea239875dd00dfb4fee6e3348b84985c92f103444683bae07b

y = 83b5c38e5e2b0c8529d7fa3f64d46daa1ece2d9ac14cab9477d042c84c32ccd0

04 + x-coordinate (32 bytes/64 hex) + y-coordinate (32 bytes/64 hex) → 130 Hex Characters (65 Bytes)

Ethereum Address Generation

Public Key (K)

Ethereum Address

- **Keccak256** hashing algorithm is used
- This is also a **one way function**

k = f8f8a2f43c8376ccb0871305060d7b27b0554d2cc72bccf41b2705608452f315

K = 6e145ccef1033dea239875dd00dfb4fee6e3348b84985c92f103444683bae07b83b5c38e5e2b0c8529d7fa3f64d46daa1ece2d9ac14cab9477d042c84c32ccd0

Keccak256(K) = 2a5bc342ed616b5ba5732269001d3f1ef827552ae1114027bd3ecf1f086ba0f9

Address = Last 20 Bytes = 001d3f1ef827552ae1114027bd3ecf1f086ba0f9

Ethereum Transaction Format

- Nonce
- Gas Price
- Gas Limit
- Recipient Address
- Value
- Data
- v,r,s - three components of an ECDSA digital signature of the originating EOA

Transaction message's structure is serialized using the Recursive Length Prefix (RLP) encoding scheme

Signing a Transaction

- **The digital signature algorithm used in Ethereum is the Elliptic Curve Digital Signature Algorithm (ECDSA)**
- **Purpose**
  - **Proves ownership**
  - **Guarantees Non-repudiation**
  - **Proves transaction data has not been and cannot be modified**

$$Sig = F_{sig}\left(F_{keccak256}(m), k \right)$$

k = Private Key
m = RLP Encoded Transaction
$F_{keccak256}$ = Keccak256 Hash Function
F_{sig} = Signing Algorithm
Sig = Resulting Signature

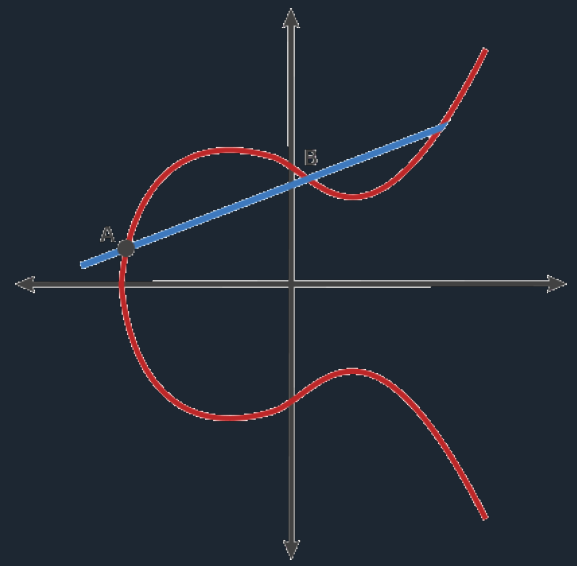
$$Sig = (r, s)$$

Verifying a Signature

- **Public Key Recovery (Using r and v)**

$$F_{sigV}\ (m\ ,\ K,\ Sig\ ) : Boolean$$

K = Public Key
m = RLP Encoded Transaction
F_{sigV} = Signing Algorithm
Sig = Signature



A visualization of an secp256k1 elliptic curve

Mining a Block

- **Ethereum uses *proof of work* consensus mechanism**
- **Ethereum uses Ethash POW algorithm**

The general route that the algorithm takes is as follows:

- There exists a **seed** which can be computed for each block by scanning through the block headers up until that point
- From the seed, one can compute a **16 MB pseudorandom cache**. Light clients store the cache
- From the cache, we can generate a **1 GB dataset**, with the property that each item in the dataset depends on only a small number of items from the cache. Full clients and miners store the dataset. The dataset grows linearly with time
- Mining involves grabbing random slices of the dataset and **hashing** them together. Verification can be done with low memory by using the cache to regenerate the specific pieces of the dataset that you need, so you only need to store the cache

Hashing Algorithm Used: **sha3_256** or **Keccak-256**

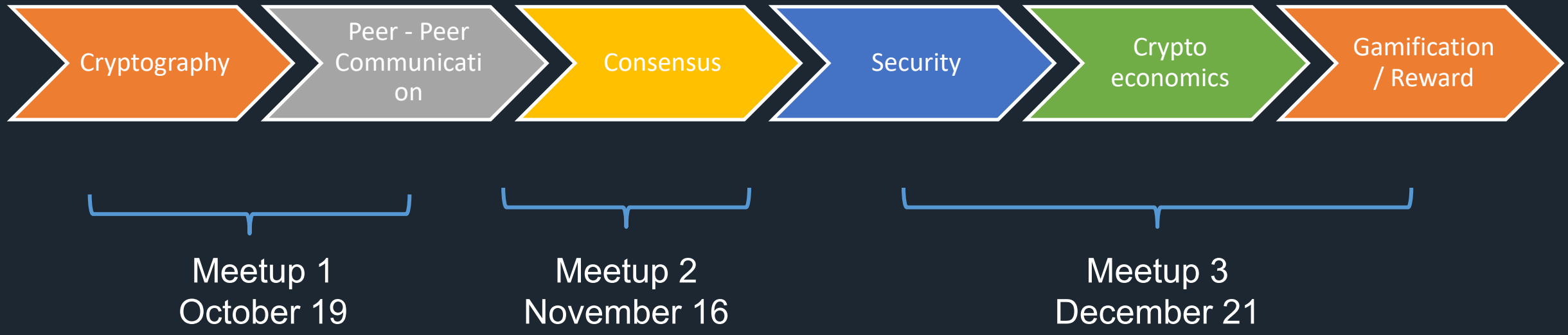
Comparative Study

Blockchain	Hashing Algorithm	Key Generation Mechanism
Ethereum	SHA-256, Keccak-256	Elliptic Curve Asymmetric Public Key Cryptography
Hyperledger Fabric	SHA3 SHAKE256	Elliptic Curve Asymmetric Public Key Cryptography
IOTA	Troika (New Ternary Hash Function)	Winternitz Hashing Algorithm

Comparison of various Distributed Ledger Platforms

Cryptocurrency Systems	Bitcoin	Ethereum	IOTA
Ledger technology	Blockchain	Blockchain	DAG (called Tangle)
Address formation	Begin with a random number as private key. Public key and address are derived from private key.	Begin with a random number as private key. Public key and address are derived from private key.	Begin with a random number as seed. Deterministic key and address pair are derived from a seed.
Address format	Base58Check encoded, usually 33-34 bytes	160 bits	81 trytes (see detail in IOTA part about trytes)
Where is the privacy held	Private key	Private key protected by passphrase	Secret
How to get balance from ledger	For each address, locate all unspent transaction output (UTXO) from blockchain and compute the total amount. A wallet can have multiple addresses and shows the total balance.	Balance, as a state of an account, is calculated from the transactions found in the blockchain.	From seed the list of addresses are generated, and summation of the balance of these addresses found in Tangle.

Comparative analysis of cryptography on various platforms



DEMO : Encryption & Decryption, P2P Networks

- DEMO : Encryption & Decryption, P2P Networks

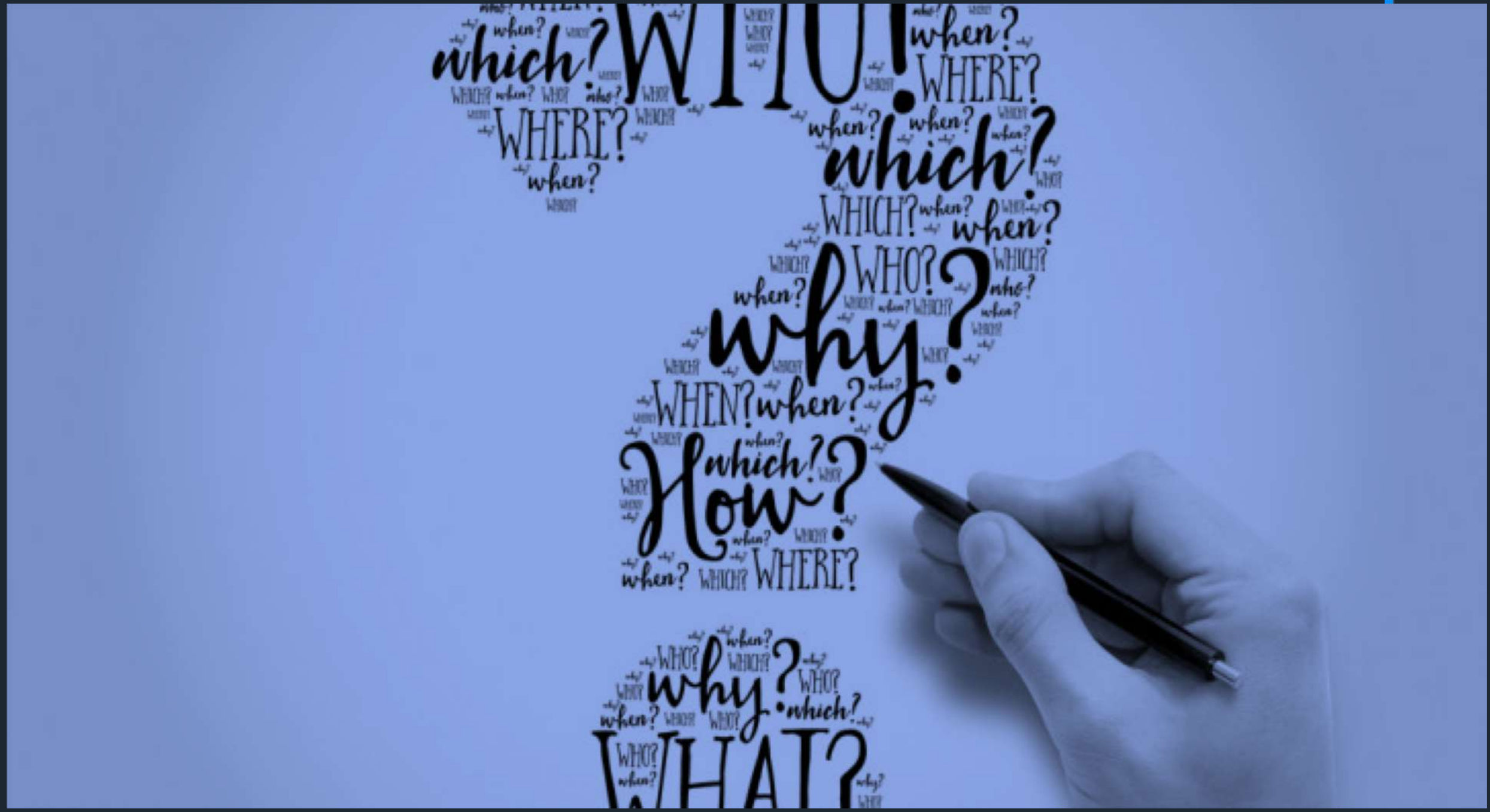
Supported by

nagarro

GOVERNMENT OF TELANGANA

bradsol
SIMPLIFYING BUSINESS

iDEALABS


WHERE?
when?
which?
WHO?
why?
WHEN?
How?
WHERE?
WHAT?