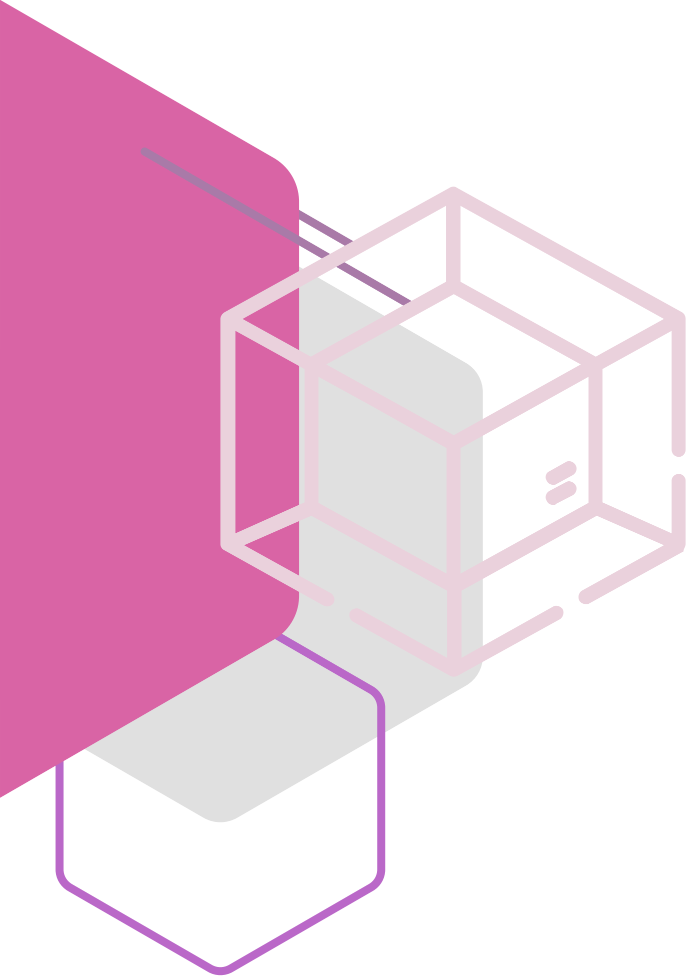
EMALI

EMALI in CIExpo

Blockchain Infopack



EMALI

1 Blockchain 101

2 Trinity of Digital Trust

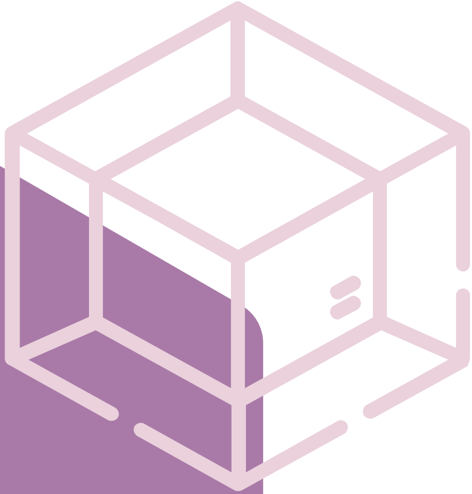
3 Smart Contract

4 Digital Signature and Identification

01

Blockchain 101

A chain that changes the world.



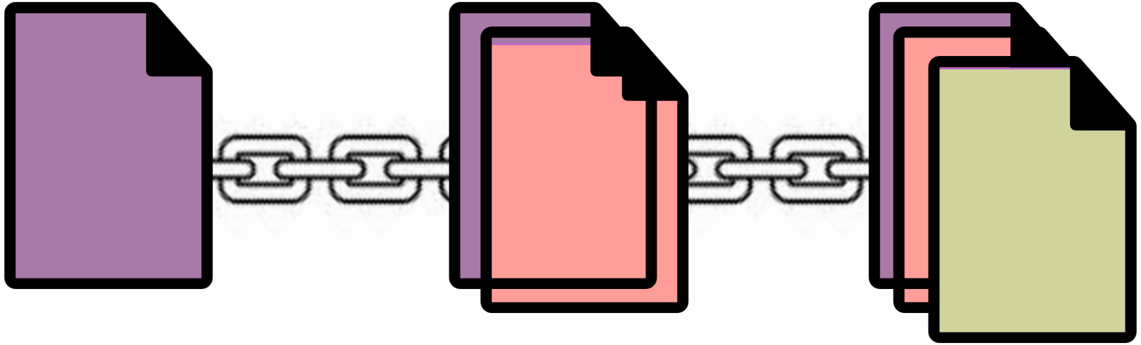
What is blockchain?

A Distributed ledger with single truth by consensus algorithm.

Distributed ledger

Ledger stores valid data. The old stack of data is also stored in the last ledger .

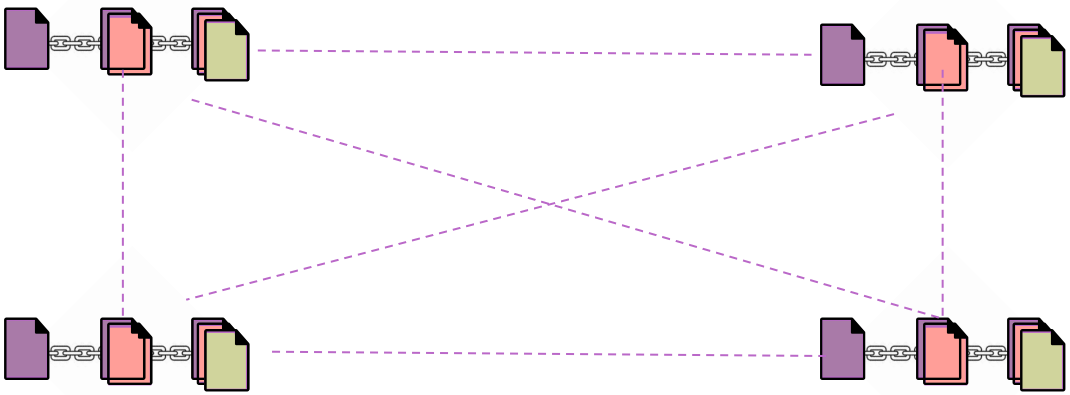
- The stack storage gives the “Append-only” characteristic to a ledge. It makes it very hard to amend the content of the previous data



Distributed ledger

A ledger is shared to many parties. Now, every parties own a single copy of the ledger.

- To amend the data, you need to compromise different parties to make the changes



Consensus algorithm

A consensus algorithm is needed to make sure all participants in the network knows how to agree on a single copy of ledger

The Desirable properties are:

1. **Consistency**

- System validates data under the same algorithm

2. **Availability**

- The system keeps running even inaccurate transaction occurs

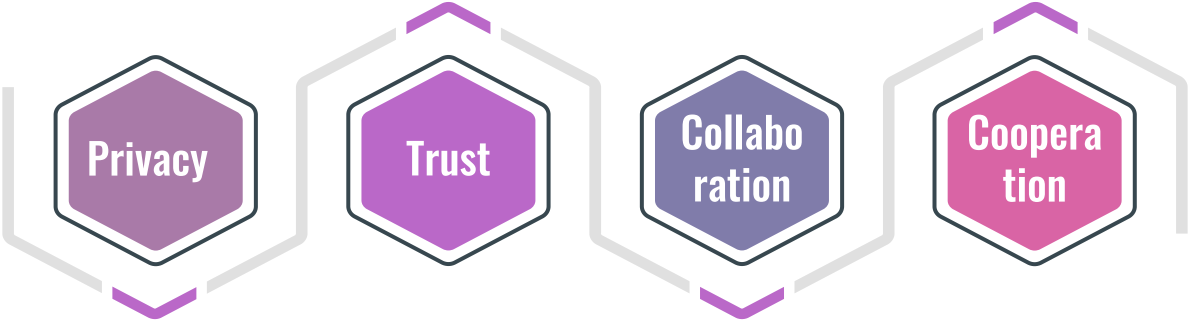
Four Pillars of Blockchain Design

CONSENSUS

Transactions are endorsed by relevant participants

SHARED LEDGER

Append-only distributed system of records shared across business network



CRYPTOGRAPHY

Ensuring appropriate visibility; transaction are secure, authenticated,and verifiable

SMART CONTRACT

Business terms embedded in transactions records and executed automatically

02

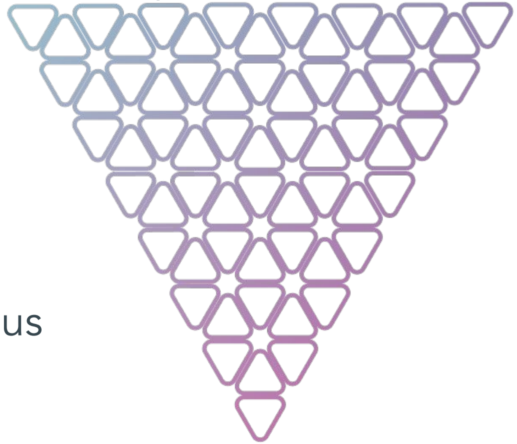
Trinity of Digital Trust

A balance between privacy, confidentiality and authenticity

Trinity of Digital Trust

Privacy

Ensure that only the necessary information is provided, and the other information remains protected



Confidentiality

Ensure that the data is protected against malicious parties

Authenticity

Ensure that the source of data is the expected personnel(s)

Privacy

Ensure that only the necessary information is provided, and the other information is protected

- Data sovereignty is done with a comprehensive access control protocols

Privacy: Zero-knowledge proof (ZK proof)

ZK proof is a way that allows provers to proof themselves without showing any other informations to the verifier.

- Example: To buy a beer, you need to proof that you are over 18-year-old. However, you do not want to show the staff HKID cards as it consist many sensitive informations.

A classic ZK proof (Schnorr protocol) contains 3 stages:

1. Commit

The prover make some commitment that he/she cannot be changed in later stages

2. Challenge

The verifier send some random challenge for prover

3. Response

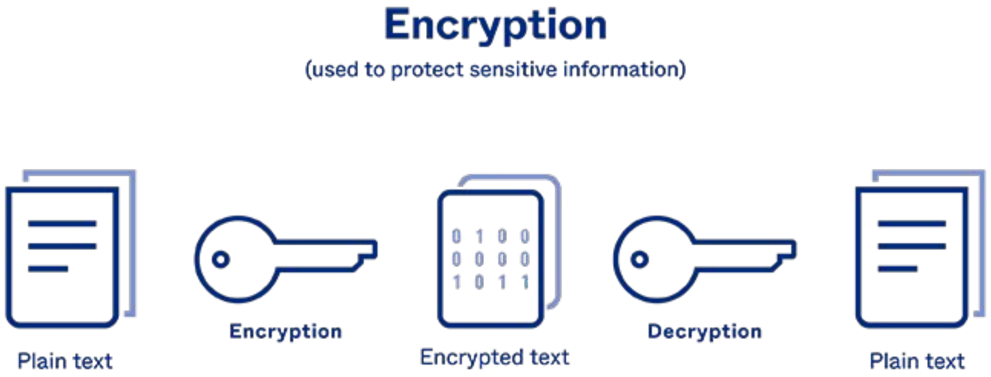
The prover compute the proof based on the challenge and secret

Confidentiality

Ensure that the data is protected against malicious parties

- Encryption prevent data from leaking to the third party.

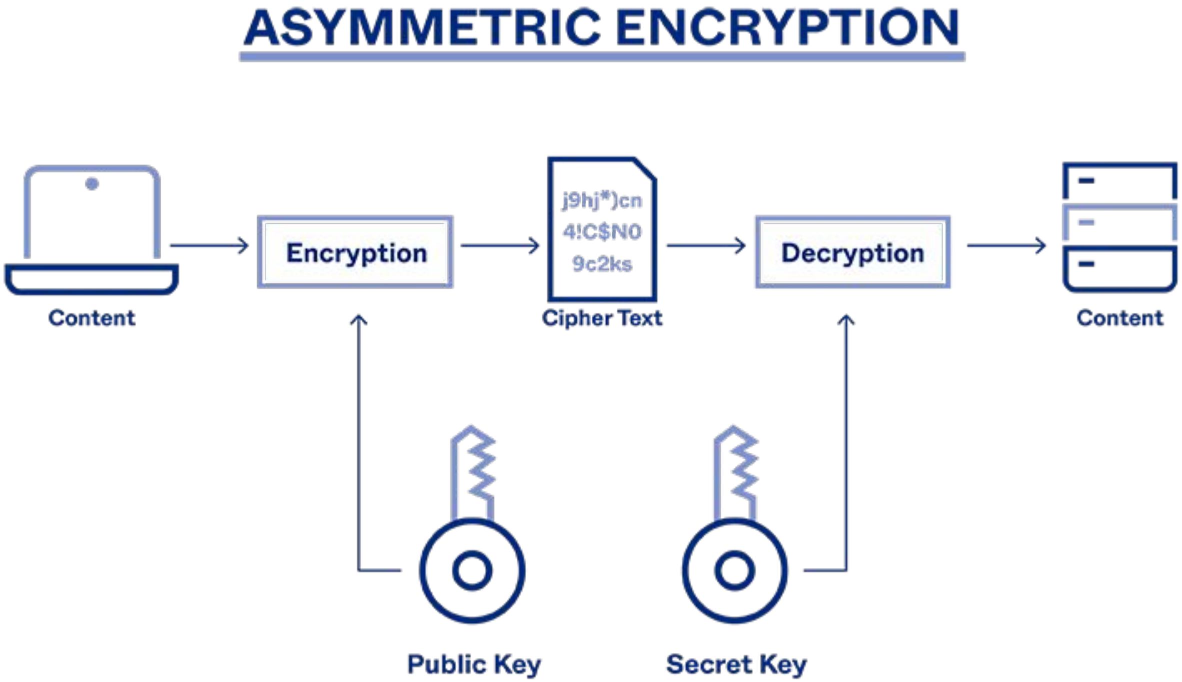
Confidentiality: Encryption



Example: Bob wants to send a secret message to Alice.

- Bob can encrypt the message with alice’s public key
- No one knows the message during delivery as it is encrypted
- Alice decrypt the message with her private key

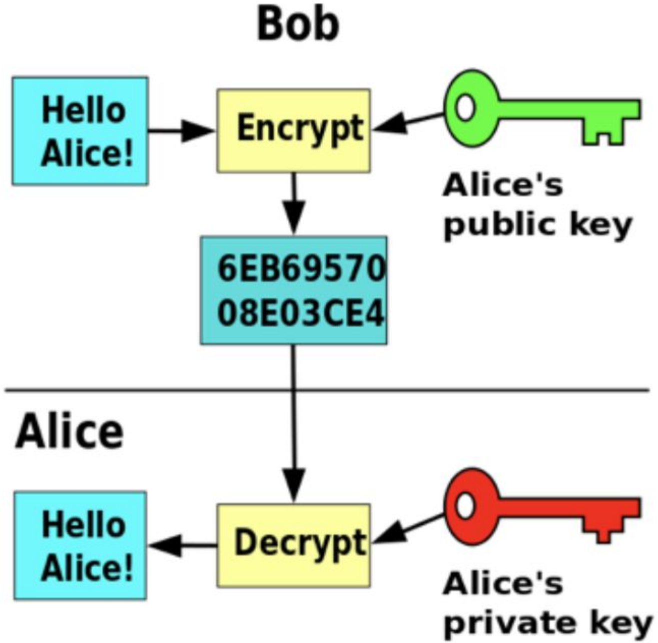
Confidentiality: Asymmetric Encryption



Confidentiality: Encryption

Bob wants to create a specific secret message for **Alice**

Alice wants to read the secret message from **Bob**



Bob wants to send a secret message to Alice:

- Bob can encrypt the message with alice’s public key
- No one knows the message during delivery as it is encrypted
- Alice decrypt the message with her private key

Authenticity

Ensure that the source of data is the expected personnel(s)

- Immutable record on data supported by blockchain (seen in section 1)
- Digital signature and DID (seen in section 4)

03

Smart Contract

Technology based promise that foster trust

Smart Contract

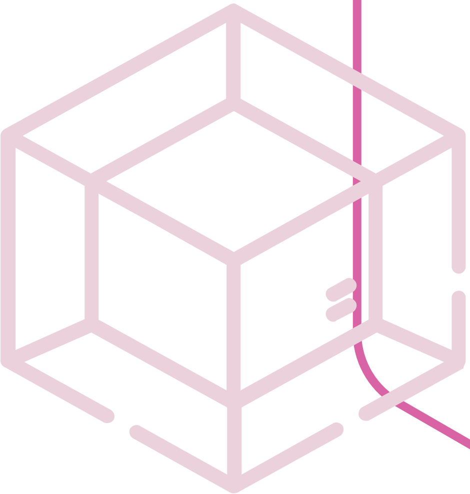
Immutability:
Publicly available across the parties in the ledger

Smart Contract Analogy:
Code executes

Privacy Preserving:
Access control and data sovereignty

04
Digital Signature and Identification

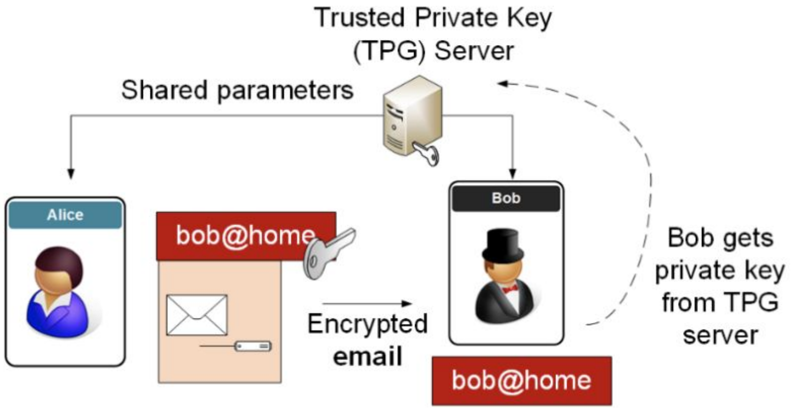
Own an unique identity in the ever-changing digital world



Identity based encryption

Method explanation:

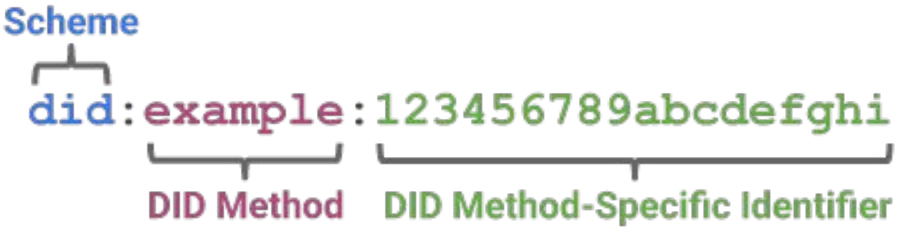
- ID as public key: Bob encrypted the message with the ID of Alice
- Private key stored at TPG server: Alice decrypt the message with the private retrieved from a trusted private key server



Compare to classic public key encryption

- Less difficult in memorising public key

Decentralised Identifier (DIDs)



Scheme

did:example:123456789abcdefghi

DID Method

DID Method-Specific Identifier

What is a DID?

- A globally unique identifier
- A component of the digital identity infrastructure
- Standardized by W3C

How can it help with data authorship?

- No more “identity theft” , user can own their identity no limited to certain platform
- An identifier for web 3.0

Digital signature vs PDF signature

Digital Signature Algorithms:

- Generate Key Pair – Public Key (PK) & Private Key (sk)
- Signature – Creates Digital Signature (Sig) from message (m) and Signer's Private Key (sk)
- Verification – Verifies if a signature (Sig) is valid for a message (m) by Signer's Public Key (PK)

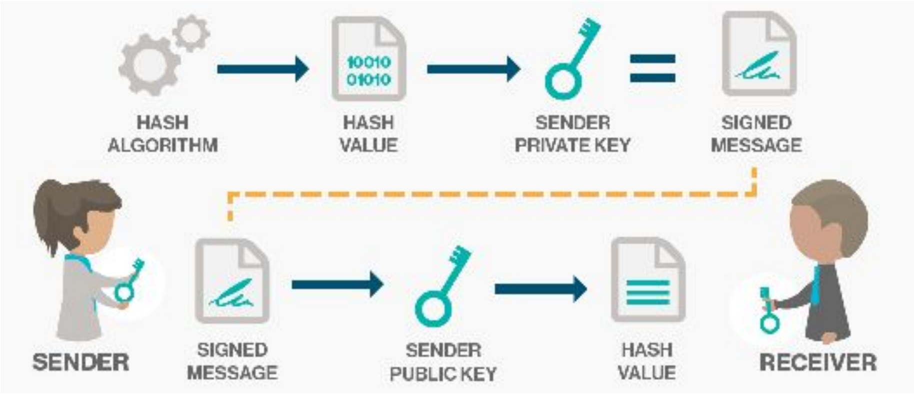
Property of Digital signature

- All valid signatures verify
- Signatures infeasible to forge

Key pair verification

How does it works:

- Alice sign on a data with Alice's private key
- Verifier Bob verify the identity of Alice by trying to opening the data with Alice's public key
- In this way, Alice does not need to give anyone her private key proof that she is alice



EMALI

ABOUT EMALI

EMALI specialised in AI, blockchain, cryptography, security, and privacy technologies.

Emali's latest fintech solution is Hong Kong Monetary Authority's Commercial Data Interchange (CDI).