



BLOCKCHAIN TECHNOLOGY

Asymmetric Cryptography

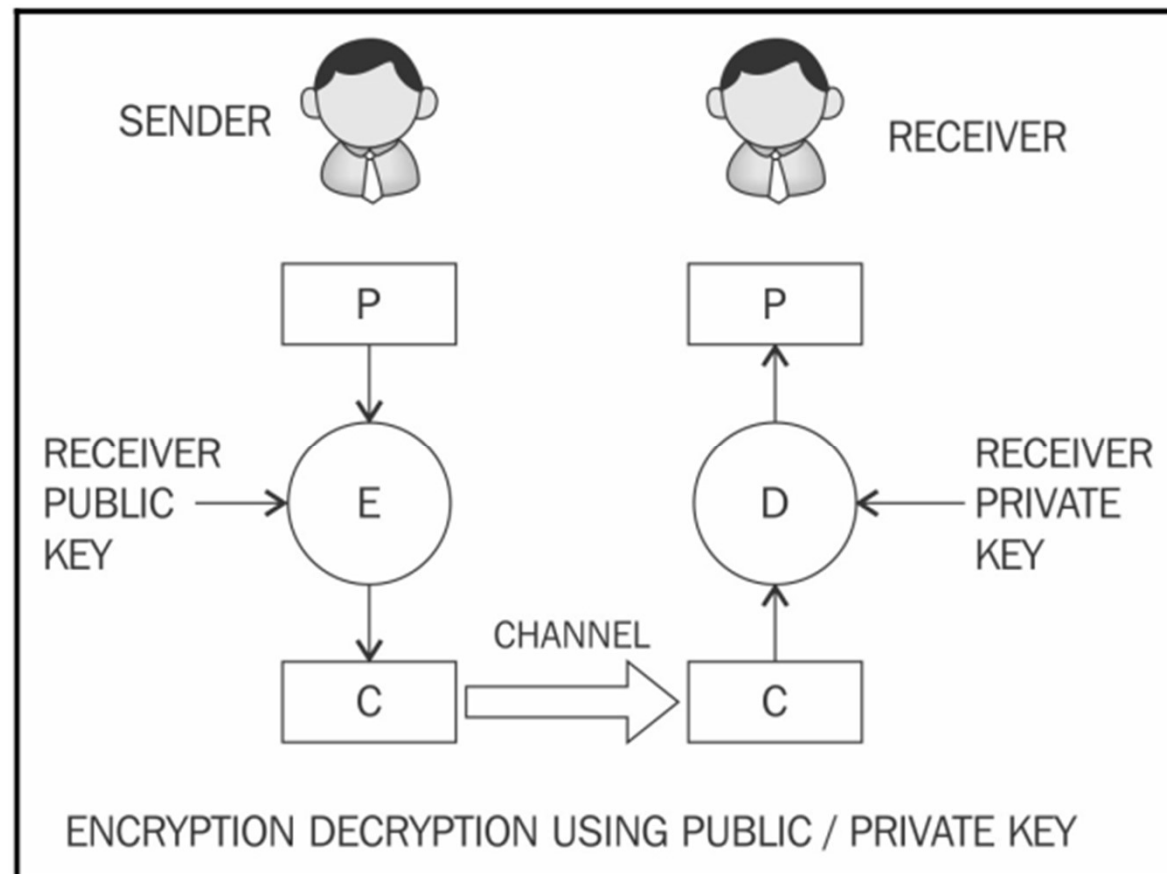


Asymmetric cryptography

- Asymmetric cryptography
 - the key for encryption is different from the key for decryption
 - Also known as public key cryptography
 - uses public and private keys to encrypt and decrypt data, respectively

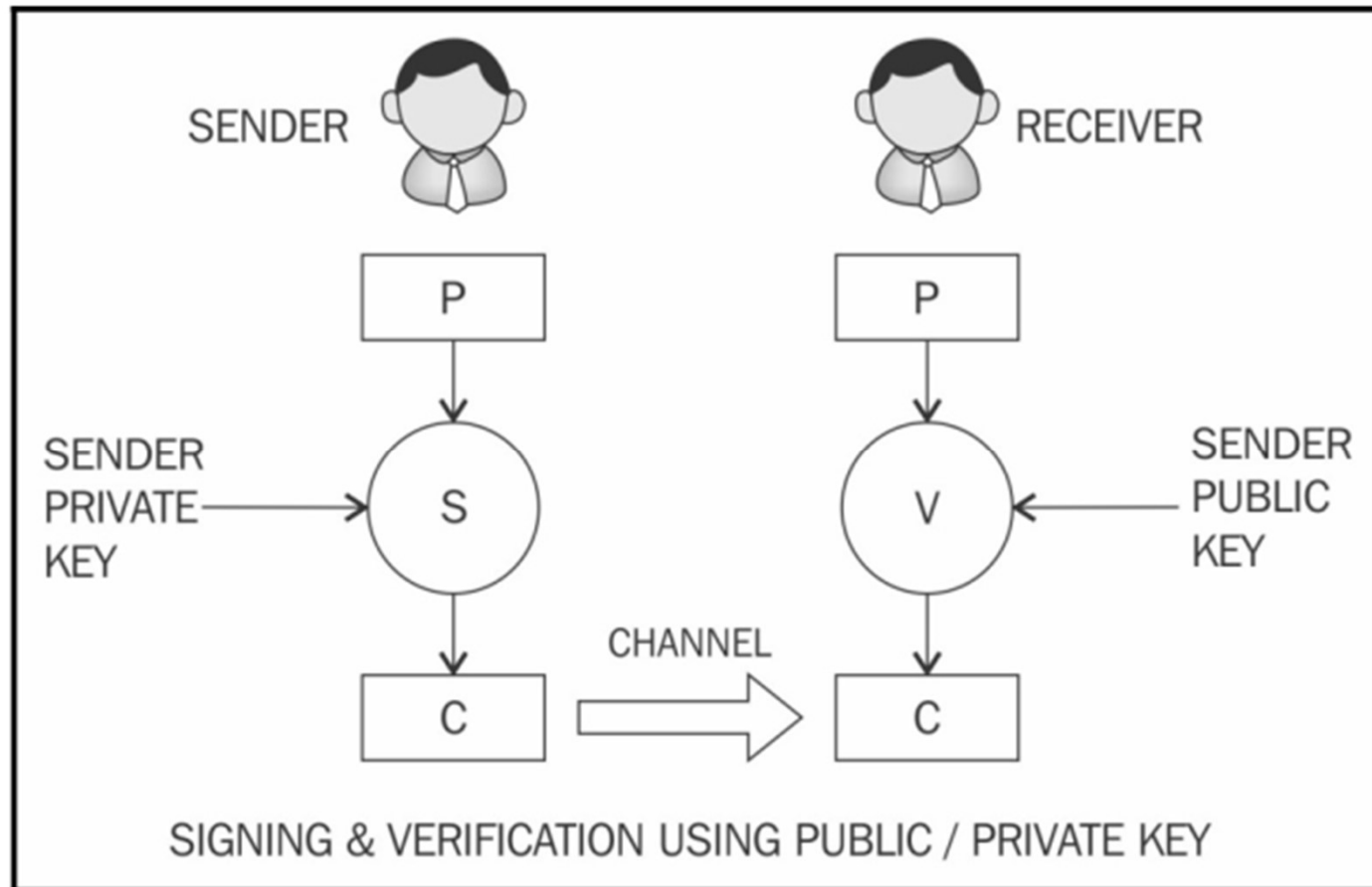
Asymmetric cryptography

- Asymmetric cryptography
 - Encryption/Decryption



Asymmetric cryptography

- Asymmetric cryptography
 - Signing/Verification





Asymmetric cryptography

- they are slower in terms of computation than symmetric key algorithms.
 - They are not commonly used in the encryption of large files or the actual data
 - They are usually used to exchange keys for symmetric algorithm.




Asymmetric cryptography

- The three main categories
 - Integer factorization
 - Discrete logarithm
 - Elliptic curves





Asymmetric cryptography

- The three main categories
 - Integer factorization
 - Are based on the fact that large integers are very hard to factor
 - RSA is the prime example of this type of algorithm
- 

Asymmetric cryptography

- The three main categories
 - Discrete logarithm
 - based on a problem in modular arithmetic
 - It is easy to calculate the result of modulo function
 - but it is computationally impractical to find the exponent of the generator

$$3^2 \text{ mod } 10 = 9$$

- finding 2 (exponent) is extremely hard to determine
 - commonly used
 - Diffie-Hellman key exchange
 - digital signature algorithms

Asymmetric cryptography

- The three main categories
 - Elliptic curves
 - based on the discrete logarithm problem discussed earlier but in the context of elliptic curves
 - Elliptic curve can be defined as $y^2 = x^3 + ax + b$
 - has two integer variables a and b
 - Different curves can be generated by varying the value of a and/or b
 - can be defined over real numbers, rational numbers, complex numbers, or finite fields
 - For cryptographic purposes
 - an elliptic curve over prime finite fields is used
 - Additionally, the prime should be greater than 3.
 - Most commonly use cases
 - Elliptic Curve Digital Signature Algorithm (ECDSA)
 - Elliptic Curve Diffie-Hellman (ECDH) key exchange




Asymmetric cryptography

- Public and private keys
 - private key
 - a randomly generated number
 - kept secret
 - held privately by its users
 - no unauthorized access should be granted to that key
 - otherwise, the whole scheme is jeopardized
 - can be of various lengths depending on the type and class of algorithms used.
 - in RSA, typically a key of 1024-bits or 2048-bits is used.
 - The 1024-bit key size is no longer considered secure



Asymmetric cryptography

- Public and private keys
 - public key
 - freely available and published by the private key owner
 - Can be used to send the key owner an encrypted message
 - few concerns
 - authenticity and identification of the publisher of the public keys.
- 




Asymmetric cryptography

- RSA
 - based on the integer factorization problem
 - multiplication of two large prime numbers is easy
 - it is difficult to factor it back to the two original numbers



Asymmetric cryptography

- RSA

1. A key pair is generated by
 - Modulus generation
 - Select p and q as very large prime numbers
 - Multiply p and q , $n=p.q$ to generate modulus n
 2. Generate co-prime
 - Assume a number called e
 - e should satisfy a certain condition
 - should be greater than 1 and less than $(p-1)(q-1)$.
 - no number other than 1 can divide e and $(p-1)(q-1)$.
 - e is the co-prime of $(p-1)(q-1)$
- 

Asymmetric cryptography

- RSA

3. Generate the public key

- Public key is the pair of
 - The modulus generated in step 1
 - co-prime e generated in step 2
- p and q need to be kept secret

4. Generate the private key


- private key, called d , is calculated from p , q , and e

$$ed = 1 \text{ mod } (p-1)(q-1)$$



Asymmetric cryptography

- RSA

- anyone who knows p and q can easily calculate private key d
 - someone who does not know the value of p and q cannot generate d .
 - p and q should be large enough for the modulus n to become extremely difficult to factor
- 




Asymmetric cryptography

- Encryption and decryption using RSA

- Encryption:


$$C = P^e \text{ mod } n$$

- Decryption:

$$P = C^d \text{ mod } n$$




Asymmetric cryptography

- Elliptic Curve Cryptography
 - main benefit
 - Provides the same level of security with smaller key size
 - Two notable schemes
 - ECDH for key exchange
 - ECDSA for digital signatures
- 



Hash functions

- are used to create fixed-length digests of arbitrarily-long input strings.
- are keyless
- provide the data integrity service
- are usually built using iterated construction techniques
- Various families are available: MD, SHA-1, SHA-2, SHA-3, RIPEMD, and Whirlpool.
- are efficient and fast one-way functions
 - It is required that hash functions be very quick to compute regardless of the message size.
 - The efficiency may decrease if the message is too big
 - but the function should still be fast enough for practical use.
- have three security properties
 - preimage resistance
 - second preimage resistance
 - Collision resistance



Hash functions

- three security properties

- preimage resistance

$$h(x) = y$$

- x is considered a preimage of y
 - y cannot be reverse-computed to x
 - also called a one-way property

- second preimage resistance

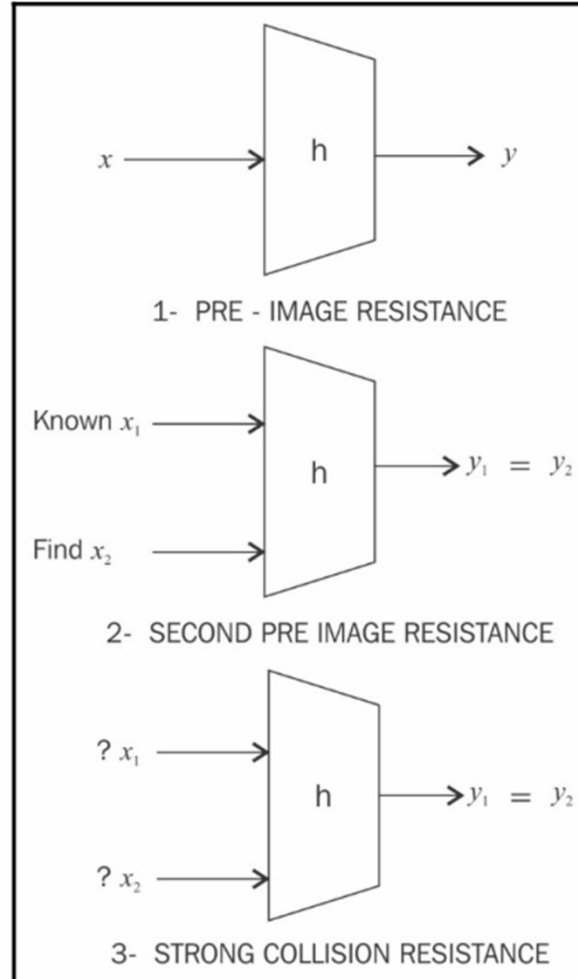
- given x and h(x),
 - almost impossible to find any m, where $h(m) = h(x)$.
 - also known as weak collision resistance

- Collision resistance

- two different input messages should not hash to the same output
 - also known as strong collision resistance.

Hash functions

- three security properties






Hash functions

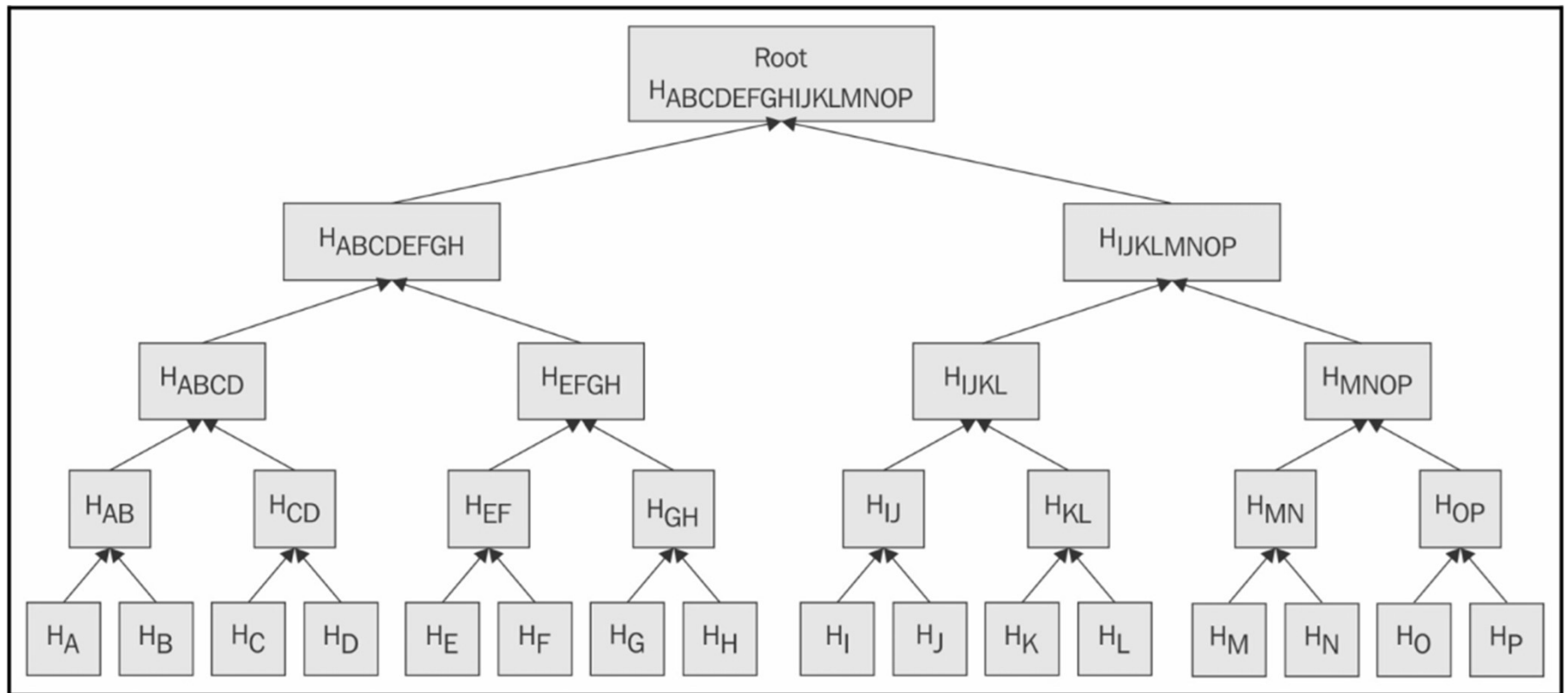
- hash functions will always have some collisions
 - they should be computationally impractical to find.
- avalanche effect is desirable in all hash functions
 - a small change will result in an entirely different hash output



Merkle trees


- is a binary tree in which
 - the inputs are first placed at the leaves
 - the values of pairs of child nodes are hashed together to produce a value for the parent node
 - until a single hash value known as Merkle root is Achieved
 - enable secure and efficient verification of large datasets
- 

Merkle trees



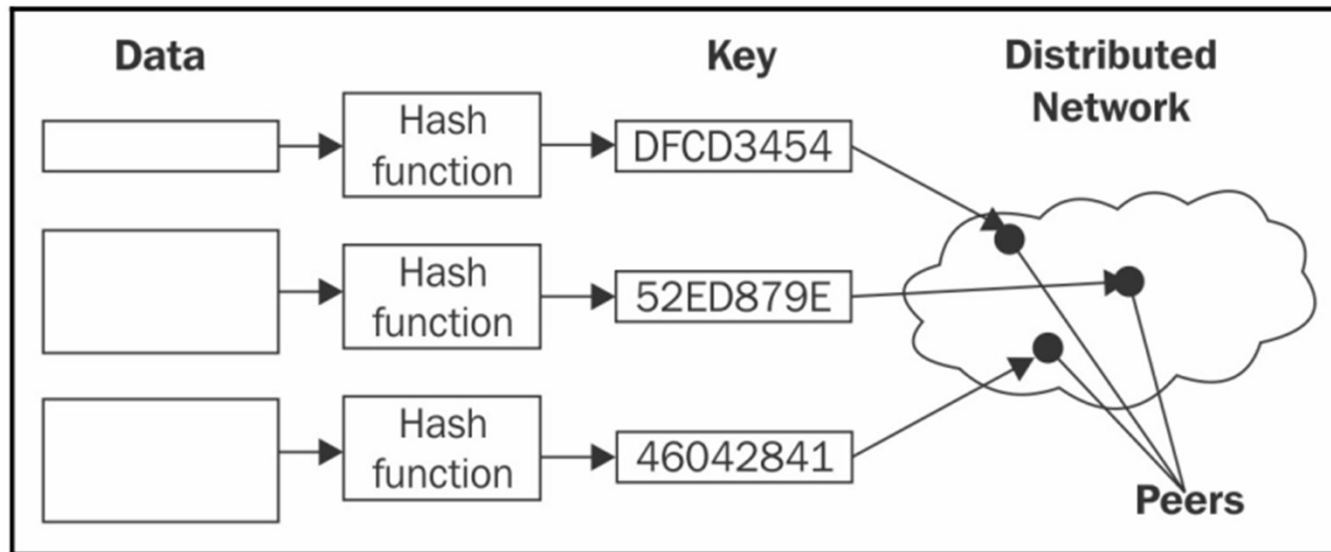


Distributed Hash Tables

- A hash table is a data structure that is used to map keys to values
 - Internally, a hash function is used to calculate an index into an array of buckets
 - Buckets have records stored in them using a hash key and are organized into a particular order.
 - DHT is a data structure where
 - data is spread across various nodes
 - nodes are equivalent to buckets in a peer-to-peer network
- 


Distributed Hash Tables

- The key is linked with the data (values) on the peer-to-peer network.
- When users request the data (via the filename)
 - the filename can be hashed again to produce the same key
 - any node on the network can then be requested to find the corresponding data
- DHT provides decentralization, fault tolerance, and scalability






Digital signatures

- are used in blockchain
 - The transactions are digitally signed by senders
 - using their private key before broadcasting the transaction to the network.
 - proves they are the rightful owner of the asset
 - The transactions are verified by other nodes on the network
 - to ensure that the funds indeed belong to the user
- 



Digital signatures

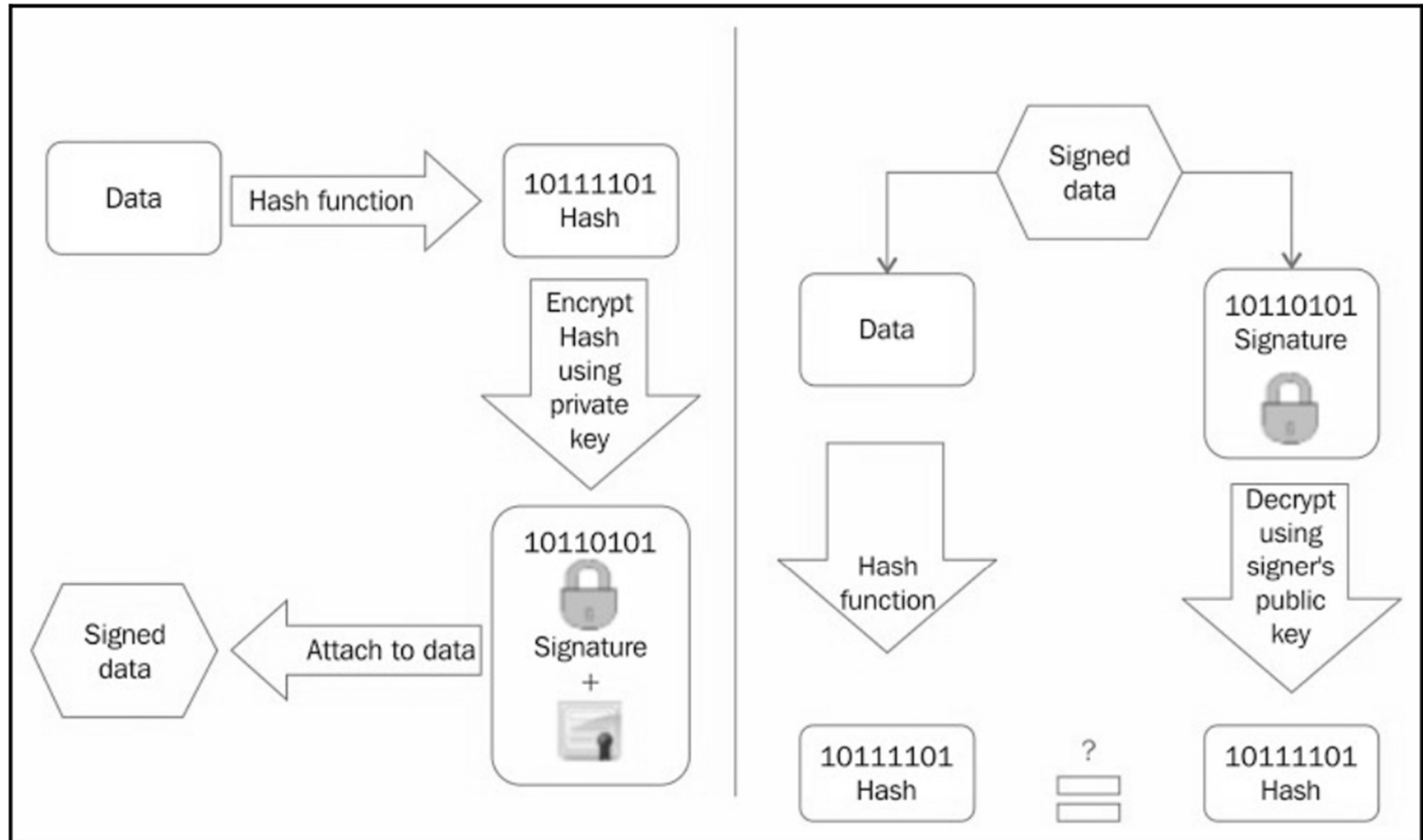
- RSA digital signatures are calculated in two steps
 1. Calculate the hash value of the data packet
 - provide the data integrity guarantee
 - the receiver can compute the hash and match it with the original hash
 - Technically, message signing can work without hashing the data first
 - but is not considered secure.
 2. Signs the hash value with the signer's private key
 - only the signer has the private key
 - the authenticity of the signature and the signed data is ensured.
- 



Digital signatures

- important properties of digital signature
 - Authenticity
 - the digital signatures are verifiable by a receiving party
 - Unforgeability
 - only the sender of the message can sign it using the private key
 - Nonreusability
 - the digital signature cannot be separated from a message and used again for another message

Digital signatures





Digital signatures

- Two methods to send an authenticated message
 - Encrypt then sign
 - the sender encrypts the data using the receiver's public key
 - then digitally signs the encrypted data
 - Sign then encrypt
 - the sender digitally signs the data using the private key
 - appends the signature to the data
 - then encrypts the data and the digital signature using the receiver's public key
 - This is considered more secure
- 




Useful topics in blockchain

- Homomorphic encryption
 - enable the processing of encrypted data without the need for decryption
 - have potential applications where
 - maintaining privacy is required
 - data is also mandated to be processed by potentially untrusted parties
 - can solve the problem of confidentiality and privacy in the blockchain



Useful topics in blockchain

- Signcryption
 - A primitive that provides all the functions of a digital signature and encryption
 - provide unforgeability, authentication, and non-repudiation
 - but with a cost less than
 - sign then encrypt
 - Encrypt then sign
- 



Useful topics in blockchain

- Zero-Knowledge Proofs (ZKP)
 - prove the validity of an assertion
 - without revealing any information whatsoever about the assertion
 - Three required properties
 - Completeness
 - if a certain assertion is true, then the verifier will be convinced of this claim by the prover
 - Soundness
 - if an assertion is false, then no dishonest prover can convince the verifier otherwise
 - zero-knowledge
 - the key property of ZKPs
 - absolutely nothing is revealed about the assertion except whether it is true or false



Useful topics in blockchain

- Zero-Knowledge Proofs (ZKP)
 - prove the validity of an assertion
 - without revealing any information whatsoever about the assertion
 - Three required properties
 - Completeness
 - if a certain assertion is true, then the verifier will be convinced of this claim by the prover
 - Soundness
 - if an assertion is false, then no dishonest prover can convince the verifier otherwise
 - zero-knowledge
 - the key property of ZKPs
 - absolutely nothing is revealed about the assertion except whether it is true or false



Useful topics in blockchain

- Zero-Knowledge Proofs (ZKP)
 - Are interested among researchers in the blockchain space
 - due to their privacy properties
 - An example is the Zcash cryptocurrency





Useful topics in blockchain

- **Blind signature**

- a form of digital signature in which
 - the content of a message is disguised (blinded) before it is signed
- be publicly verified against the original, unblinded message in the manner of a regular digital signature.
- are typically employed in privacy-related protocols where the signer and message author are different parties.
- Examples include cryptographic election systems and digital cash schemes.



General terminology related to trading

- Financial markets and trading
 - Money markets
 - short-term markets where money is lent to companies or banks to do interbank lending.
 - Credit markets
 - consist mostly of retail banks
 - they borrow money from central banks and loan it to companies or households in the form of mortgages or loans.
 - Capital markets
 - facilitate the buying and selling of financial instruments
 - mainly stocks and bonds.
 - can be divided into two types
 - primary markets
 - Stocks are issued directly by the companies to investors
 - secondary markets.
 - investors resell their securities to other investors via stock exchanges



General terminology related to trading

- Trading
 - an activity in which traders buy or sell various financial instruments
- Traders
 - have a short position if they have sold a contract
 - have a long position when they buy a contract.
- various ways to transact trades
 - through brokers
 - directly on an exchange
 - Over-The-Counter (OTC)
 - buyers and sellers trade directly with each other



General terminology related to trading

- Exchanges
 - are usually considered to be
 - a very safe
 - Regulated
 - reliable
 - electronic trading has gained popularity
 - traders send orders to a central electronic order book
 - orders, prices, and related attributes are published to all associated systems using communications networks



General terminology related to trading

- Orders
 - are instructions to trade
 - are the main building blocks of a trading system
 - have general attributes
 - The instrument name
 - Quantity to be traded
 - Direction (buy or sell)
 - The type of the order
 - Market orders
 - limit orders
 - stop orders

General terminology related to trading

- Trade life cycle
 - Pre-execution
 - An order is placed at this stage
 - Execution and booking
 - the order is matched and executed
 - it is converted into a trade
 - the contract between counterparties is matured.
 - Confirmation
 - both counterparties agree to the particulars of the trade.
 - Post booking
 - This stage is concerned with various inspection and verification processes required to ascertain the correctness of the trade
 - Settlement
 - the most vital part of trade life cycle
 - At this stage, the trade is final
 - Overnight (end-of-day processing):
 - include report generation, profit and loss calculations, and various risk calculations.

