Cryptocurrency: An Overview

Palash Sarkar

Indian Statistical Institute
http://www.isical.ac.in/~palash

February 4, 2019

Reserve Bank of India, Kolkata

Structure of the Presentation

- A general overview.
- A glimpse into blockchain technology.

A General Overview

What is a cryptocurrency?

Some kind of a virtual or digital token/asset.

- Based on cryptography and distributed computing.
- Maintained by a network of computers.
- Make payments in return for goods/services; hold as an asset.

Potentially disruptive technology

Bitcoin

Proposed by (the pseudonymous) Satoshi Nakamoto in 2009.

- White paper and software released in January 2009.
- Has grown from an obscure software to command a present day market capitalisation of more than US$ 60 billion.
- Kick started an immense amount of activity in cryptocurrency.
  - More than 1600 cryptocurrencies have been proposed till date.
- Based on distributed ledger implemented using blockchain technology.
  - Tremendous potential much beyond cryptocurrency.
  - Many major banks, financial institutions and companies are presently exploring possibilites to incorporate some kind of blockchain technology.

Features of Bitcoin (and Other Cryptocurrencies)

- **Decentralised:** Everything is maintained by a network of nodes (computer servers).
- **Trustless:** Users do not need to trust any single authority; trust comes implicitly from the network.
- **Permissionless:** No permission is required to join the network; anybody can download the software and become a node in the system.

Cryptocurrency Community

- **Users:** entities which make and receive payments using the cryptocurrency.
- **Nodes/servers:** these run the cryptocurrency software.
- **Miners:** entities with significant computational resources which confirm transactions and create new amounts of the currency.
- **Cryptocurrency exchanges:** sites where cryptocurrencies can be exchanged for each other or for fiat currencies.

Regulatory Status

Cryptocurrency, by virtue of being decentralised, is hard to regulate; it is possible, however, to criminalise entire activity, thus, enforcing an effective ban.

- *Absolute ban:* Algeria, Bolivia, Egypt, Iraq, Morocco, Nepal, Pakistan and United Arab Emirates.
- *Implicit ban:* Bahrain, Bangladesh, China, Colombia, the Dominican Republic, Indonesia, Iran, Kuwait, Lesotho, Lithuania, Macau, Oman, Qatar, Saudi Arabia and Taiwan.
- *Legal:* EU, USA, Mexico, Japan, South Korea.
- *Not illegal but, banking ban:* Canada, India.

Central Bank Interest

Central banks of several countries are interested in introducing **centralised, trusted, permissioned** digital currencies.

- Bank of England, People's Bank of China, Bank of Israel.
- Saudi Arabia and UAE have launched a pilot cryptocurrency for easier cross border payments.
- The Central Bank of Singapore has launched projects to improve inter-bank payments and to facilitate bank users exchange currencies with each other.
- ...

International Payments

Distributed ledger not based on blockchain:

- **Ripple**.
- **R3:** Corda.

Based on blockchain:

- **IBM blockchain:** a solution for the banking industry.
- **J. P. Morgan Chase:** Quorum (a permissioned version of Ethereum).

Blockchain Applications

- **Smart contracts:** Creation of self-executable and autonomous contracts.
- **Logistics management:** shipping industry (paperless cargo system); ...
- **Supply chain management:** sensor data management.
- **Governance:** land records, statutory certificates, ...
- ...

A Glimpse into Blockchain Technology

Background Science

Cryptography:

- Hash function.
- Digital signature scheme.

Distributed Computing:

- Peer-to-peer (P2P) network.
- Consensus algorithm.

Cryptography: Hash Function

Compressing Information

A hash function compresses arbitrary information to a short fixed length string called the digest.

Examples of information that can be compressed by a hash function.

- An SMS/text message,
- A digital photo,
- An MP3 file,
- A book (e.g. ‘War and Peace’).

The amount of information to be compressed varies, but, in each case, the compressed information will be a string of some fixed size.

Hash Function

Formally

$$H : \bigcup_{i=0}^{L} \{0,1\}^i \rightarrow \{0,1\}^n.$$

- Typically n is at least 160.
- L should be "sufficiently large".
- Arbitrary information is encoded as a bit string.

Examples:

- 256-bit digest: SHA256 (used by Bitcoin), SHA-3 or, Keccak (used by Ethereum).
- 160-bit digest: RIPEMD160 (used by Bitcoin).

Why Are Hash Functions Important?

- The ability to efficiently compress information is very useful.
- Computational task: Given x, compute $H(x)$.
  - Software: very fast and small memory.
  - Hardware: small hardware area, low power.
- Other algorithms work on the compressed information to realise different cryptographic primitives.

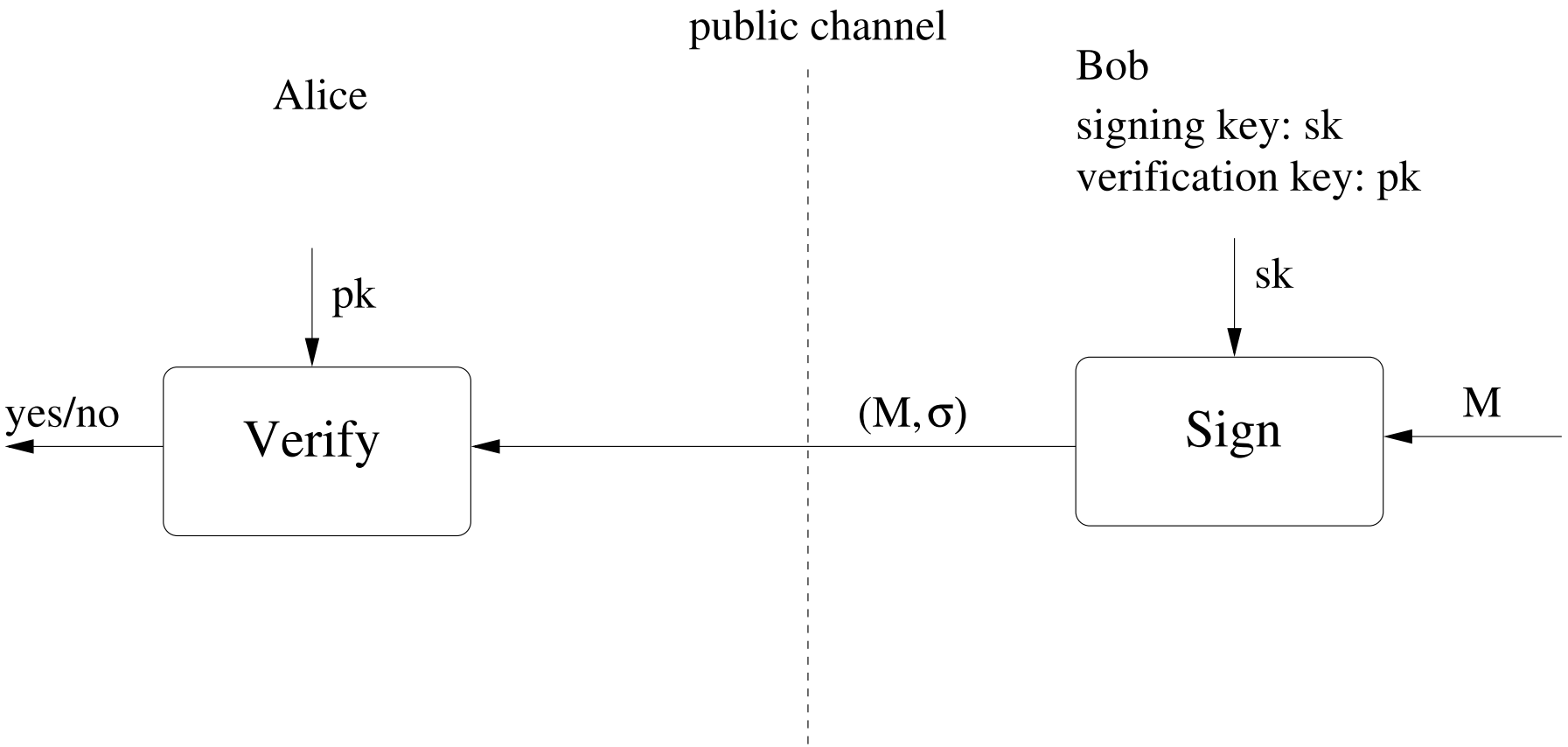
Some Basic Properties

- **Pre-Image Resistance (One-Wayness):** Given an n-bit string y, it should be *computationally infeasible* to find an x such that $H(x) = y$.
- **Collision Resistance:** It should be *computationally infeasible* to find two distinct strings x_1 and x_2 such that $H(x_1) = H(x_2)$.
- **Second Pre-Image Resistance:** Given x_1 it should be *computationally infeasible* to find x_2 such that $H(x_1) = H(x_2)$.

The actual properties required of a hash function depend on the application.

Cryptography: Digital Signature Scheme

Overview of Digital Signature Scheme



Digital Signature Scheme

Consists of three procedures: (Setup, Sign, Verify).

- **Setup:** generates (pk_B, sk_B) for Bob;
  pk_B is made public (placed in a public directory).
- **Sign:** Bob signs message M using sk_B to obtain signature σ.
- **Verify:** Alice can verify the validity of (M, σ) using pk_B;
  Alice does not need any secret information to verify a signature.

Blockchain Basics Through Bitcoin

Basic Components: Address

An address is the hash (or digest) of a public key.

- Currency is assigned to addresses.
- To participate, a user generates a signing-public key pair; the hash of the public key is the address to which currency can be assigned.
- To spend the currency associated to an address, a user needs to remember the signing key; if the signing key is lost, then there is no way to spend the associated currency.

Basic Components: Transaction

A transaction is a statement transferring currency from input address(es) to output address(es).

- To be valid, a transaction has to be signed by the signing key(s) associated with the input address(es).
- The output sum must be at most the input sum; transaction fee is input sum minus output sum.
- Any user can initiate a transaction.

Basic Components: Block

A block is essentially a list of transactions.

- A block $B = (h, R, \eta)$, where
  - h is the hash (or digest) of a previous block;
  - R is the list of transactions in the block B;
  - η is a nonce.
- A block also contains some additional metadata such as the timestamp of creation.

Basic Components: Blockchain

$$B_0 = (R_0, \eta_0) \leftarrow B_1 = (h_1, R_1, \eta_1) \leftarrow \cdots \leftarrow B_r = (h_r, R_r, \eta_r).$$

- B_0 is the genesis block.
- h_1 is the hash of B_0; h_2 is the hash of B_1; ...
- B_r is the present head of the block chain.

Basic Components: Nodes

Nodes are computers which run the Bitcoin software.

- Nodes are connected through a peer-to-peer (P2P) network; communicate using a gossip protocol.
- Users can initiate transactions through nodes; these are propagated to the network using the gossip protocol.
- Nodes maintain a local copy of the blockchain; there is no concept of a central copy of the blockchain.
- Nodes also maintain a list of valid addresses and their associated currency amount; this information is available from the blockchain.

The blockchain constitutes the distributed ledger.

Block Mining

Difficulty indicator d: (difficulty is inversely proportional to d).

Consider a node v:

- B_r: blockchain header; let h_{r+1} be the hash of B_r.
- v makes a list R_{r+1} from the currently pending transactions.
- **Proof-of-work:** node v obtains a value η_{r+1} such that $H(h_{r+1}, R_{r+1}, \eta_{r+1}) < d$.

New copy of the blockchain at v:

$$B_0 \leftarrow \cdots \leftarrow B_r = (h_r, R_r, \eta_r) \leftarrow B_{r+1} = (h_{r+1}, R_{r+1}, \eta_{r+1}).$$

Node v propagates block B_{r+1} to the network.

Generating a Proof-of-Work

To find η_{r+1} such that $H(h_{r+1}, R_{r+1}, \eta_{r+1}) < d$:

- Since H is one-way, the only way to obtain η_{r+1} is to successively try values $0, 1, \ldots$
- Each trial requires a single evaluation of H.
- Assuming that the outputs of H are independent and uniform random, about $2^n/d$ trials are required.
- Smaller the value of d, the more difficult it is to find a proof-of-work.

Difficulty Updation

- Miners employ special purpose hardware to obtain proof-of-work.
- As hashing speed increases, the time to mine a block decreases.
- To compensate for this, the difficulty is increased (i.e., d is decreased) so that mining each block requires about 10 minutes.
- Difficulty is updated after every 2016 blocks.

Block Reward

To incentivise miners, successful mining of a block carries a reward.

- New currency is generated on successful mining of a block.
  - Originally, this was 50 BTC.
  - Halves after every 210,000 blocks (roughly 4 years).
  - Will become zero after about 21 million BTC have been generated (around the year 2140).
  - Satoshi: 10^{-8} BTC.
- Transaction fees of all the transactions in a block.

Coinbase transaction: has an output address and no input address; used for assigning the block reward.

Consensus Mechanism: Problem

- Many miners are asynchronously trying to mine the next block.
- All miners which mine a block immediately propagate it to the network.
- A particular node may receive more than one block; it has to decide which block it should append to its local copy of the blockchain.

Consensus Mechanism: Protocol Rule

Choose the more difficult block.

- If two blocks have the same difficulty, choose the one which was first received.

Consequences:

- Leads to the blockchain which required a greater amount of work; longest chain, if all blocks have the same difficulty.
- If a node falls behind due to network delays, then later it may have to discard one or more blocks from its copy of the blockchain.

The protocol ensures that all connected nodes have the same copy of the blockchain (with the possible exception of a few most recent blocks).

Confirmation of Transaction

- A transaction gets included in a block which is then mined and added to the head of the blockchain. This is a confirmation of the transaction on the blockchain.
- As successive blocks are mined and further appended to the blockchain, the transaction receives new confirmations.
- It is recommended that a transaction should be buried 6 blocks deep to be considered finally confirmed.

Immutability of the Blockchain

Suppose an adversary changes a transaction somewhere in the blockchain:

- The block containing the transaction has to be mined anew.
- All subsequent blocks have to be mined anew.
- Adversary has to play catch-up: do all of the above **before** the honest miners have been able to successfully generate a new block.

51% Attack: If the adversary controls more than 50% of the hash rate, then the above attack becomes feasible.

No Double Spending

- An adversary issues a transaction making a payment from an address.
  - It gets confirmed on the blockchain.
  - The adversary receives the goods/services for the payment.
- Next the adversary issues a new transaction making another payment from the same address.
  - Normally, this transaction will get rejected.
- The adversary tries to modify the blockchain to erase the previous transaction.

Immutability of the blockchain prevents this from happening.

Summary

- An overview of the exciting new field of cryptocurrency and blockchain technology.
- A brief sketch of how the blockchain for Bitcoin works.
- Much remains unsaid.

Thank you for your kind attention!