Money, Blockchain and Cryptocurrency : 3 Interlinking Stories

Dr A S Ramasastri

Director, IDRBT

Story of Money

From thousands of years ago . . .

Money

Uses of Money

- Medium of Exchange
- Unit of Account
- Store of Value

Kinds of Money

- Asset Money
- Paper Money
- Deposit Money

Characteristics of Money

- Durability
- Portability
- Divisibility
- Uniformity
- Limited Supply
- Acceptability
- Anonymity

Currency and Payments

Paper Currency

- Central Bank Issues
- through Banking Channels
- for Public Transactions

- No Record of Individual Public Transactions
- No Double Spend Possible
- Counterfeit Possible

Payment Systems

- RBI, NPCI
- RTGS, NEFT, IMPS
- Centralized Transactions Record

Digital Wallets

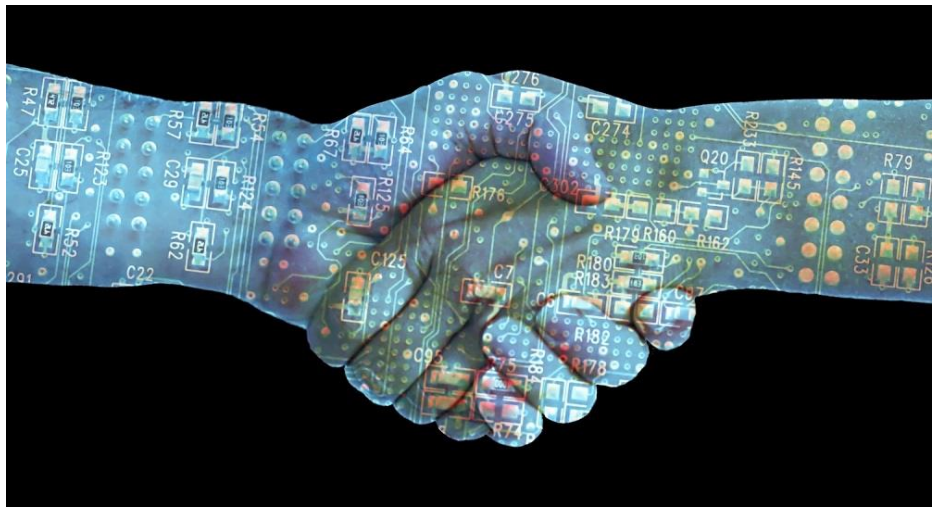
- Banks and PPI Issuers
- SBI Buddy, Jio Money, PayTm
- Centralized Transactions Record

Currency Digitization

- Handling increasing volumes, counterfeit, illegal funding are concerns
- Digitization of Currency – Cost Effective, Efficient, Elegant
- Electronic Payment Systems provide reliable and fast transfer systems; They are NOT digital currency
- Digital Wallets convert and reconvert paper / deposit money to digital money; They are NOT digital currency
- Virtual Currencies issued by non-central banks do not have the legal tender status; They are NOT digital currency
- Search and research is on for technology that supports all characteristics of money, including no double spend possibility

Story of Blockchain

From 1991 . . .



Blockchain - Evolution

- Certifying documents (text, audio, picture, and video) created in digital form on easily modifiable media is a concern
- A cryptographically secured chain of blocks was described in 1991
- Efficiency improvement for it was derived in 1992
- Distributed blockchain was conceptualised in 2008
- Was implemented as core component of Bitcoin in 2009
- It serves as the public ledger for all transactions.

DL and BC

- Distributed ledger (also called shared ledger) is a consensus of replicated, shared, and synchronized digital data geographically spread across multiple sites. There is no central administrator or centralised data storage.
- Blockchain (originally called Block Chain) is a distributed ledger that is used to record transactions across many participants so that the record cannot be altered retroactively without the alteration of all subsequent blocks

Blockchain – Scientific Underpinnings

Peer-to-Peer Networking

Peer-to-peer (P2P) networking is a distributed application architecture that partitions tasks between peers. Peers are equally privileged, equipotent participants in the application.

Distributed Consensus

Consensus is a fundamental problem in distributed systems, where the objective is to achieve overall system reliability in the presence of a number of potentially faulty processes.

Fault Tolerance

Fault tolerance is an important property desired of a distributed system for guaranteeing its ability to continue operating properly in the event of the failure of some of its components.

Cryptography

Cryptography enables secure communication in the presence of third parties, and plays a vital role in establishing trust, security and privacy in a distributed system.

Blockchain – Components

Cryptographic

- Hash Function
- Hash Pointer
- Tamper-Evident Link List
- Merkle-Tree
  - Tamper-Evident Binary Tree
- Patricia-Tree
  - Tamper-Evident Tree

Functional

- Network
- Transactions
- Ledger
- Verification
- Consensus
- Smart Contracts

Land Registry the Apt BC Application?

- “As on today, title deeds are paper documents showing the chain of ownership for land and property. They can include: conveyances, contracts for sale, wills, mortgages and leases.”
- Titles are blockchains currently held in a central repository
- Instead of miners, succession is verified by notaries.
- Titles are meaningful candidates for being treated on DL / BC
- State Governments thinking of such applications

IDRBT White Paper and PoC

- Trade Finance
- Cross-border Payments
- KYC
- Securities Servicing
- Loan Syndication
- Supply Chain Financing
- Consortium Accounts

Pre Requisites

Business Related

- Need a critical mass of participants for adoption of blockchain solution to be successful
- Blockchain is a fundamentally different way of asset management and value creation, and therefore requires a shift in business thinking
- Blockchain adoption requires a number of changes to existing practices, which may increase costs and risks
- From a business perspective, flexible settlement timeframes may be preferable – to instant settlements enabled by blockchain – for performing compliance checks or to fund positions

Technology Related

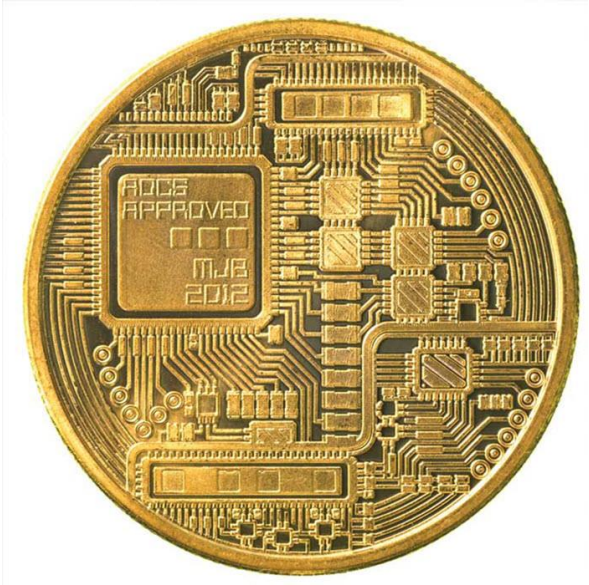
- Adopting blockchain requires achieving sufficient scale of operations, and interoperability with legacy systems and other blockchain systems
- Given the critical role of cryptography in achieving trust and transparency in blockchains, it is imperative that the cryptographic keys and access credentials are managed effectively
- Smart contracts are executed at every node for validating and settling transactions. Verification of smart contracts for preventing malicious behaviour is very important

Potential Risks

- Cryptography could be used to conceal identities and undertake fraudulent activities
- Cyber risk and the risk of fraudulent activities, risk to fair competition and orderly markets, risk to financial stability through increased market volatility or interconnectedness
- Quick dissemination of errors: a mistake in the coding of smart contracts or reference data might quickly affect a number of participants
- What information to share: competitors, privacy laws and regulations

Story of Cryptocurrency

From 2008 . . .



Was World Waiting For?

- International Currency
- Algorithmic Currency
- Decentralized Governance
- Virtual Currency
- Illegal Funding
- Speculation Opportunities

A Bit of Old Story

- David Chaum's eCash system (online) of 1983
- Chaum and Naor's system (offline) of 1990
- David Chaum's concern for eCash relates to privacy aspects of online financial transactions
- The systems could not provide anonymity and prevent double-spend problems.

Bitcoin

Digital token
that relies on cryptography
for chaining together token transfers
in a peer-to-peer network
(decentralized authority)

World is Watching

- Most countries treat it as a commodity
- Most countries don’t recognize it as legal tender
- However, its use is not illegal
- In some countries, buying goods/services is taxed
- Conversion to/from fiat currency is not taxed

National Plans

- Project Ubin – places a tokenized form of the Singapore dollar on DLT
- China's central bank developed a prototype of a cryptocurrency
- Bank of Russia thinks that it is time for national cryptocurrencies
- Denmark considers minting E-Krone
- Canada has been experimenting with CAD-COIN
- UK is researching the economic factors and implications of central bank issued digital currency (CBDC)
- International Monetary Fund (IMF) proposes central bank digital currencies (CBDCs) to contain the rise of cryptocurrencies

Central Bank Digital Currencies

- Authorized Participants
- Structure of Transactions
- Verification Algorithms
- Access Control Structures
- Appropriate Consensus Algorithm
- Incentives for Honesty

- Permissioned???

Blockchain Classification

Permissionless

- All entities can
  - Submit transactions
  - Validate transactions
  - Create blocks
  - Participate in the consensus
  - Access the blockchain
- Illustrations
  - Bitcoin
  - Ethereum

Permissioned

- Designated roles to entities
  - **End-users** can only submit and access their transactions
  - **Validating peers** can only validate and access their transactions
  - **Consensus servers** can only create blocks and participate in the consensus
- Illustrations
  - Hyperledger Fabric (IBM)
  - Sawtooth Lake (Intel)
  - Corda (R3 Consortium)

Back to Basics

Eternal . . .

Potential Areas of Research

Security and Privacy

- Existing security solutions can only provide point-to-point security, while blockchain being a distributed system with decentralized authority demands end-to-end security
- Several advanced security policies such as information-flow controls are being actively pursued in the computer security literature.

Potential Areas of Research

Scalability and Consensus

- Adopting blockchain for practical applications requires several orders of magnitude increase in the throughput.
- Government’s increased focus on digitizing the banking transactions will only push these numbers further higher.

Potential Areas of Research

Monetary and Other Policies

- Impact on Money Supply, Money Multiplier, Velocity of Money, Deposit Money, Interest Rates and Monetary Policy Measures
- Impact on Transparency, Visibility, Black Money, Counterfeiting, Money Laundering, Privacy, Illegal Funding, Tax Collection

Blockchain is a foundational technology,
and thus has the potential to create new foundations
for our economic and social systems.

While foundational innovations can have enormous impact,
it will take decades for them to seep into
our economic and social infrastructure

- Harvard Business Review

Wishing the Event A Grand Success

asramasastri@idrbt.ac.in