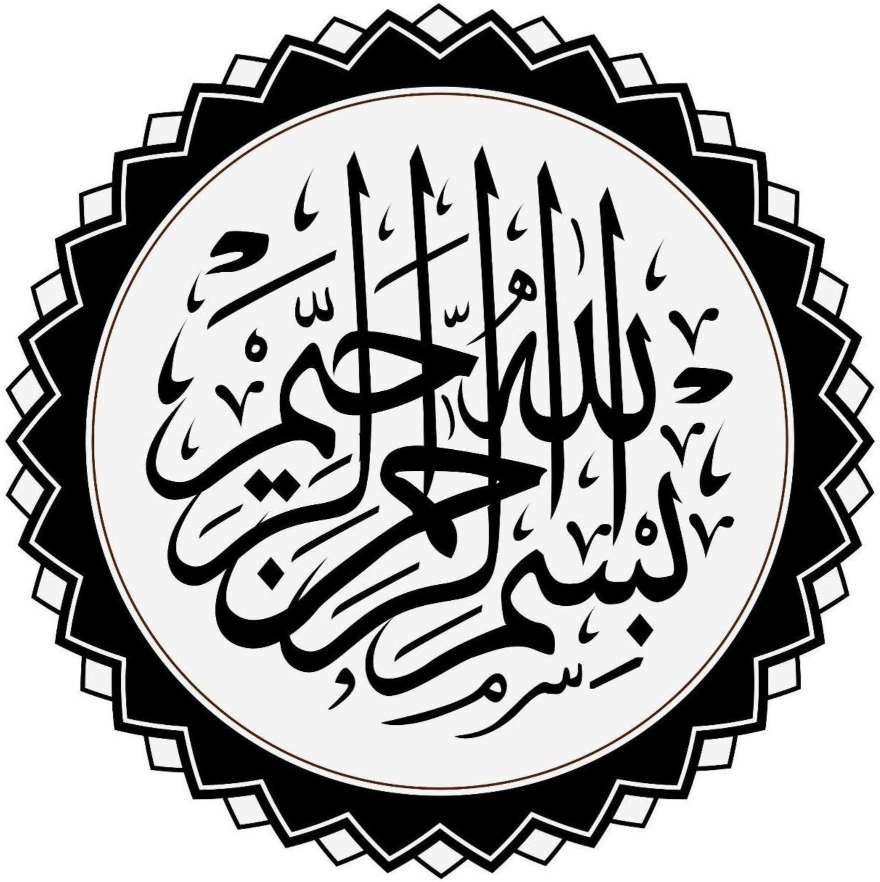

بسم الله الرحمن الرحيم

Blockchain-A Decentralized & Distributed Ledger Technology

Presented By:

Course Instructor: Dr. Kashif Mehboob Khan

kashifmehboob@neduet.edu.pk

https://www.linkedin.com/in/dr-kashif-mehboob-khan/

https://scholar.google.com/citations?user=jKVCoTMAAAAJ&hl=en

Brief Profile

- **Qualification**:
  - Ph.D. (**Blockchain Security**)
  - MS CS
  - BS Computer Engg.
- **Experience**: (**17 years**)
  - 5 years as System Analyst/Programmer
  - 2010 to present at NED University
- **Certifications**:
  - Introduction to Amazon Elastic Compute Cloud (EC2)
  - Introduction to AWS Solutions
  - Essential Features of .NET Framework
  - Microsoft Certified Technology Specialist (Windows Share point)
  - Windows Phone 7 Development
- **Awards**:
  - Best Researcher Award 2021 by NED
  - E-Invoicing App award by TCS
- **Financial Rewards**:
  - – Received a financial reward of 7 hundred thousand PKR for blockchain security related publications from NED University.
- **Affiliations/Membership**:
  - – NED University
  - – Member of **Blockchain Community, IEEE**, Membership No. 95502101
- **Blockchain Technology Collab**:
  - – Engaged in international Blockchain Project worth a funding amount of up to €123k.
  - – Research Collaboration with **Daniel Kraft, chief scientist at Namecoin**
  - – Technical collaboration with Apptron Technologies Pvt. Ltd. as a **lead external consultant. (2021)**
  - – Idea selected for pitching in International **ONTO CHAIN Summit 2022 at Berlin, Germany**
  - – Presented Blockchain security model at **University of West London, UK.**

AGENDA

- **Goal**
- **Motivation**
- **Relevance**
- **Blockchain & Cryptocurrency**
  - Hashing ---10 min. (approx.)
  - Data Structure, Decentralized, Public ledger, Immutability--- 20 min. (approx.)
  - Real World Applications of Blockchain---------------------------- 10 min. (approx.)
  - Misconceptions Regarding Blockchain---------------------------- 20 min. (approx.)
  - Key Research Areas--- 20 min. (approx.)
- **Blockchain in Banking**
  - Assets Creation --- 20 min. (approx.)
  - Transaction Processing through Public addresses --------------- 20 min. (approx.)
  - Implementation of Interesting Use-Cases ------------------------ 20 min. (approx.)
- **What is Next**
  - API based Banking DApps--- 20 min. (approx.)
- **Q/A** --- 20 min. (approx.)
- **Acknowledgement**

Goal

“To Provide Strong Theoretical and Practical Foundation for Building and Deploying Distributed Decentralized Architecture for real world problems.”

Motivation

The Presentation will address the rising issue of transferring asset from one entity to another in a conventional centralised environment by proposing and implementing a distributed and decentralized architecture using public ledger.

Relevance

The topic is about one of the most emerging technologies in distributed computing which is blockchain. The technology does not require any trusted party to run the system over the network and has been successful in variety of domains including well-known cryptocurrency, Bitcoin.

If you can't explain it simply, you don't understand it well enough.

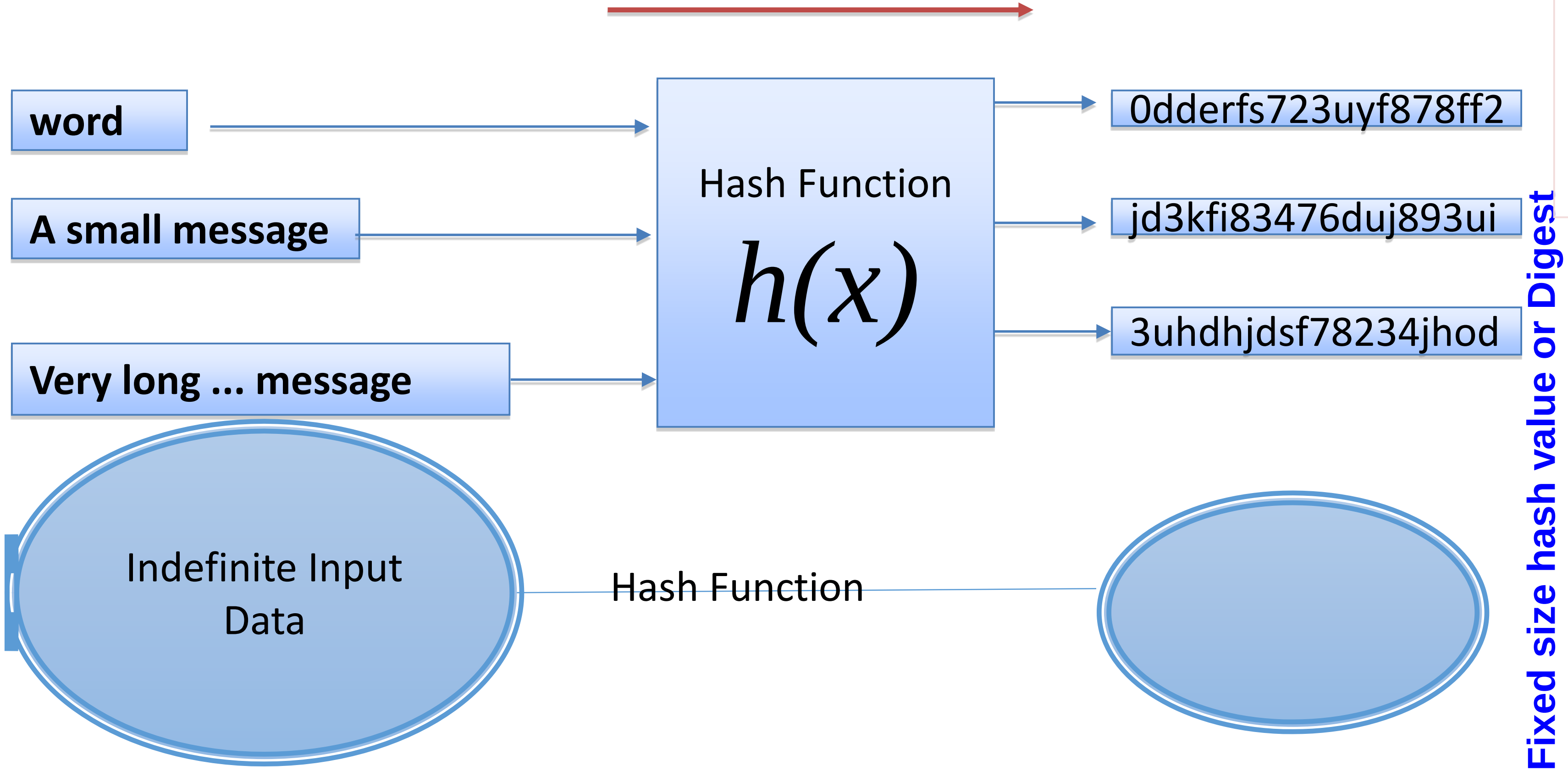
Blockchain & Cryptocurrency

- What is this?
- Why is it gaining importance?
- Point of Concerns.

Cryptographic Hash Function (CHF)

- A procedure that takes an arbitrary block of data and returns a fixed-size bit string, the (cryptographic) hash value, such that an accidental or intentional change to the data will change the hash value

Application: Can be used for password storage!, integrity check, etc…



Blockchain & Cryptocurrency:
Evolution to Crypto

1. ERA-I (No such thing like money)

- Trading used to be done through exchanging objects.
- **Issue**
  - We may be interested in giving away our object but not interested in getting the particular object in exchange.
  - This may lead to cancellation of the deal.
  - Solution demands to move into ERA-II.

2. ERA-II (Precious Coins—Gold, Silver etc.)

- Accepted by a large number of population. (1 pound)
- This era allows the resolution of issue, raised in era-I.
- Accept the coin, trade it with someone else to get what you want (as it is made up of precious material).

Blockchain & Cryptocurrency: Evolution to Crypto

ERA-I (No such thing like money)

Trading used to be done through exchanging objects.

Issue

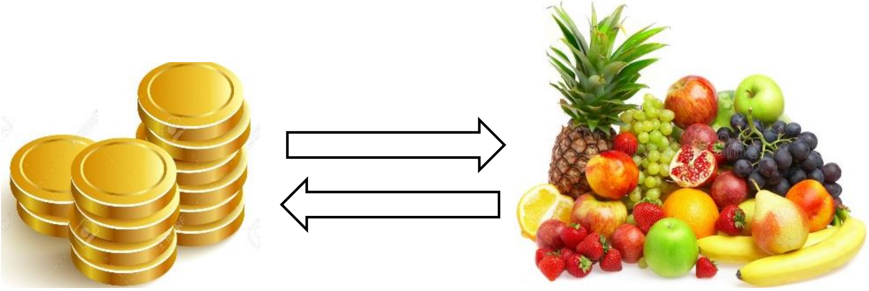
- We may be interested in giving away our object but not interested in getting the particular object in exchange.
- This may lead to cancellation of the deal.
- Solution demands to move into ERA-II.

[1]

Blockchain & Cryptocurrency: Evolution to Crypto – Contd.

ERA-II (Precious Coins—Gold, Silver etc.)

- Accepted by a large number of population. (1 pound)
- This era allows the resolution of issue, raised in era-I.
- Accept the coin, trade it with someone else to get what you want (as it is made up of precious material).

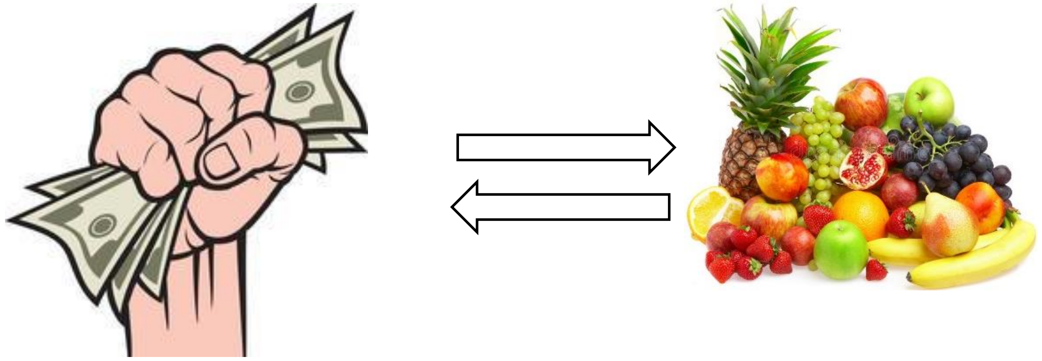


[2]

Blockchain & Cryptocurrency: Evolution to Crypto – Contd.

ERA-III (Paper Money—A Receipt)

- Banks were established and governments started to takeover producing a trusted system.
- Moving away from the need of carrying precious material.
- Introducing receipt (paper money of zero value) as a promise from the government (a proof that we have a certain amount against this.)



[2]

Blockchain & Cryptocurrency: Evolution to Crypto – Contd.

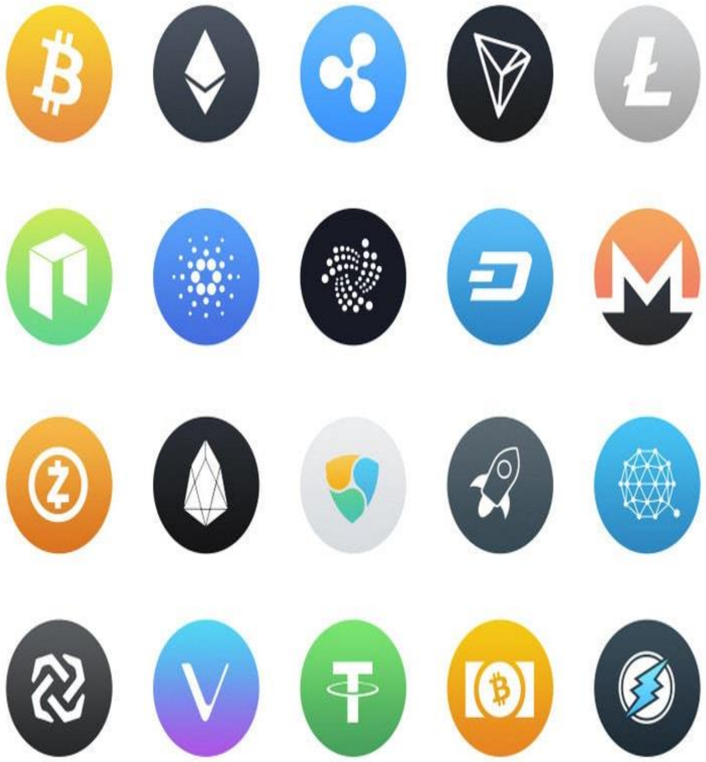
ERA-IV (Records on Spreadsheet)

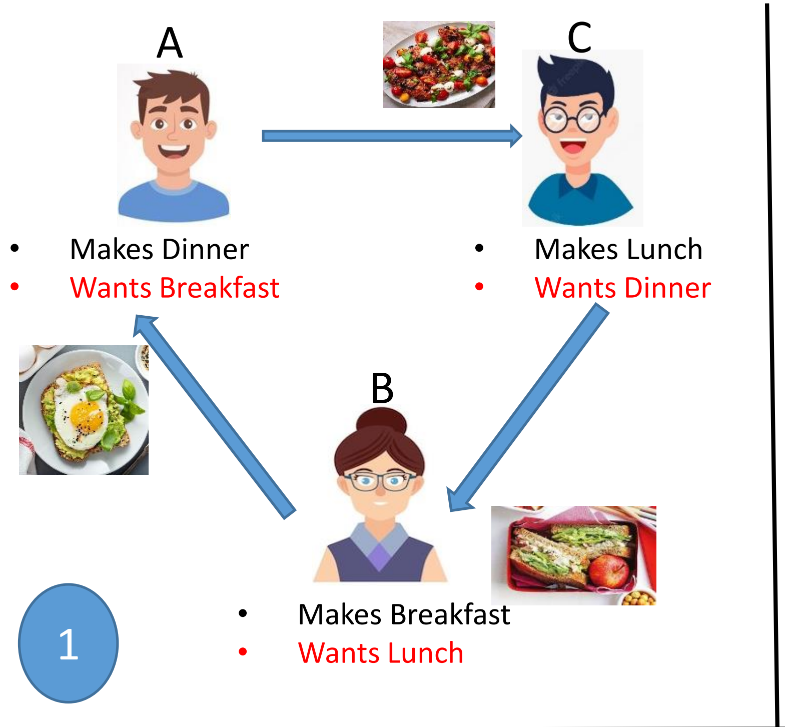
- No paper notes/ no coins/no objects exchange
- Online buying & Selling
- Making and moving entries from one account to another. (Debit/Credit of values between buyer & Seller)

Blockchain & Cryptocurrency: Evolution to Crypto – Contd.

ERA-V (Cryptocurrency)

- Completely virtual
- No gold/no silver/no paper
- Transfer of digital assets (But the concept behind is similar)
- Just continuously manipulating spreadsheets. (Who has paid how much to whom)
- Instead of multiple banks, keeping their separate records, in crypto there is one really BIG sheet of all the transactions which have ever occurred (Ledger).
- So, why everyone is getting crazy about it? Move to next slide!!

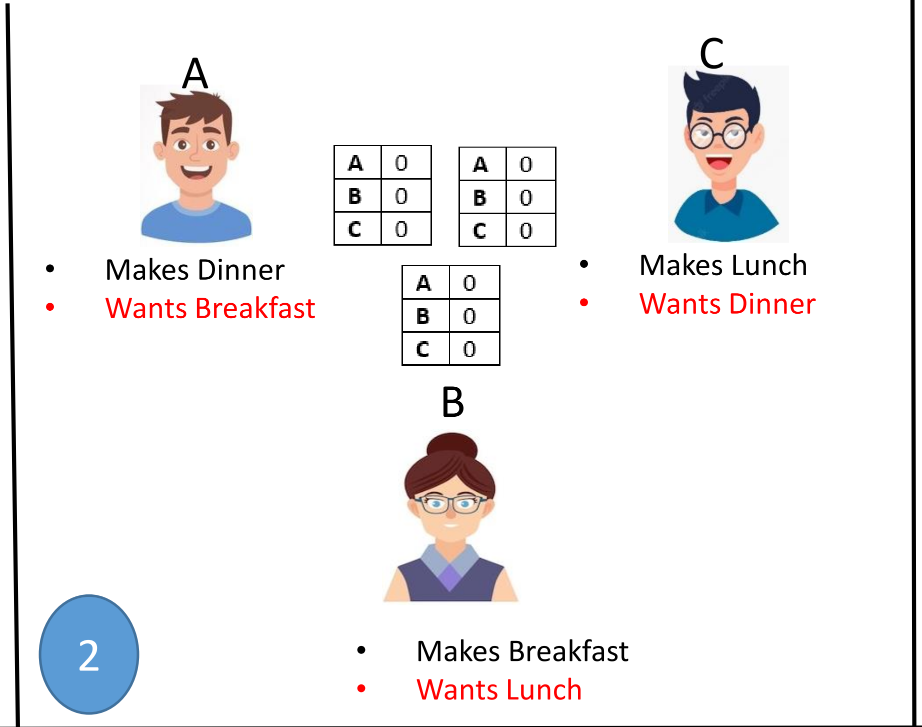




- Makes Dinner
- Wants Breakfast

- Makes Lunch
- Wants Dinner

- Makes Breakfast
- Wants Lunch



A	0
B	0
C	0

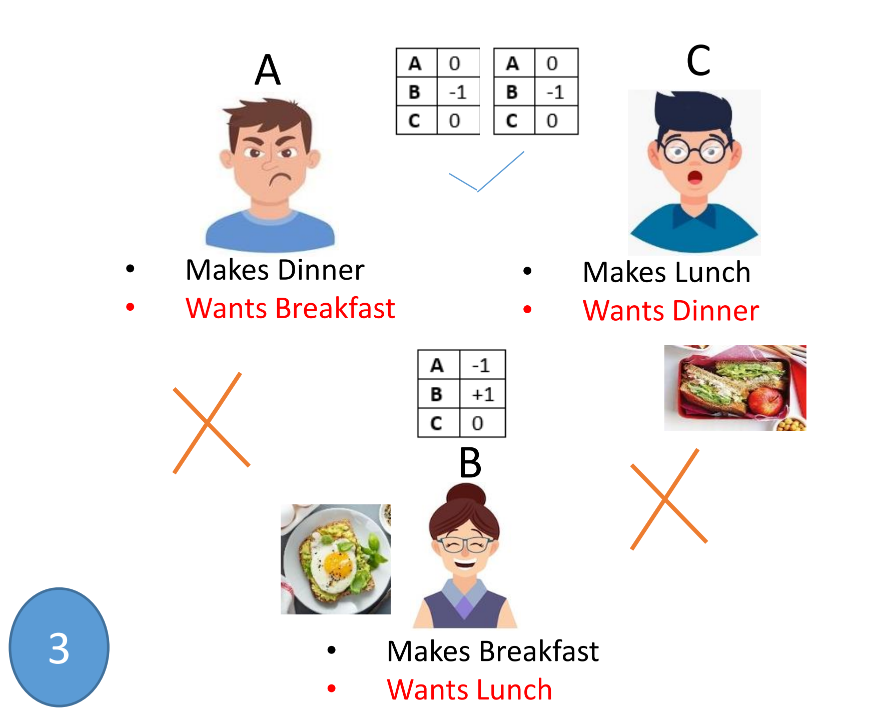
A	0
B	0
C	0

A	0
B	0
C	0

- Makes Dinner
- Wants Breakfast

- Makes Lunch
- Wants Dinner

- Makes Breakfast
- Wants Lunch



A	0
B	-1
C	0

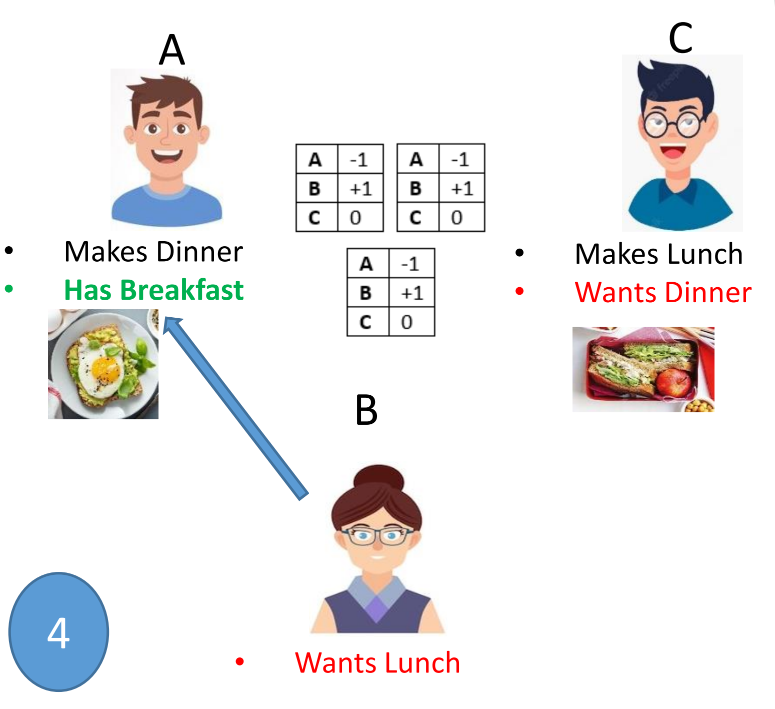
A	0
B	-1
C	0

A	-1
B	+1
C	0

- Makes Dinner
- Wants Breakfast

- Makes Lunch
- Wants Dinner

- Makes Breakfast
- Wants Lunch



A	-1
B	+1
C	0

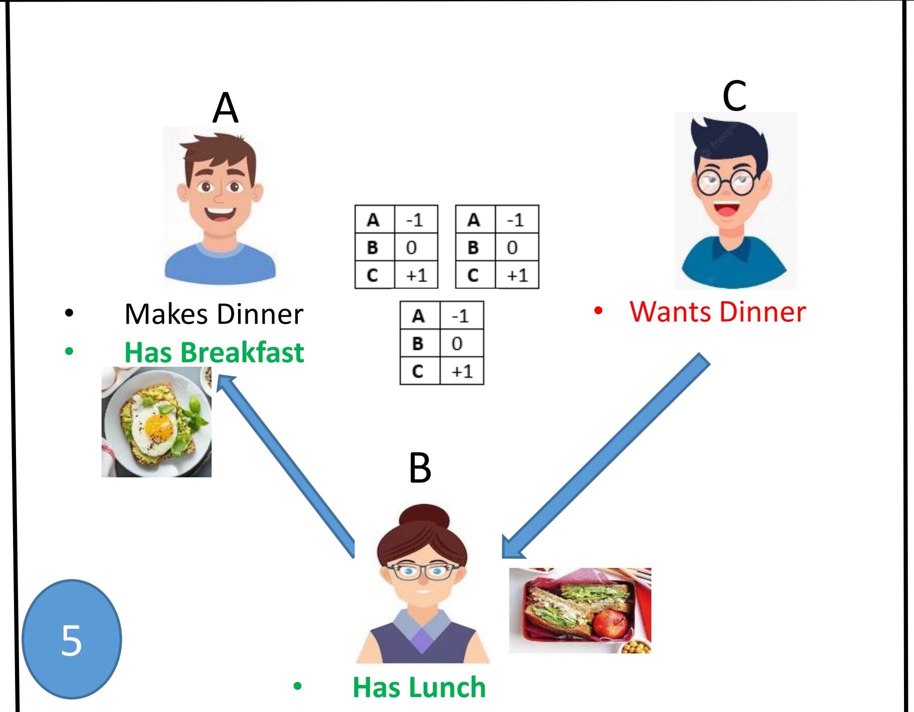
A	-1
B	+1
C	0

A	-1
B	+1
C	0

- Makes Dinner
- **Has Breakfast**

- Makes Lunch
- Wants Dinner

- Wants Lunch



A	-1
B	0
C	+1

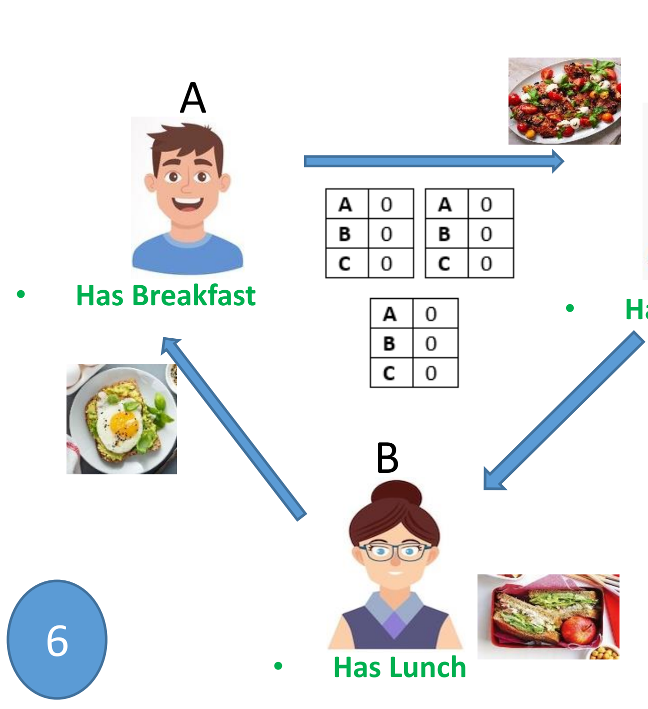
A	-1
B	0
C	+1

A	-1
B	0
C	+1

- Makes Dinner
- **Has Breakfast**

- Wants Dinner

- **Has Lunch**



A	0
B	0
C	0

A	0
B	0
C	0

A	0
B	0
C	0

- **Has Breakfast**

- **Has Dinner**

- **Has Lunch**

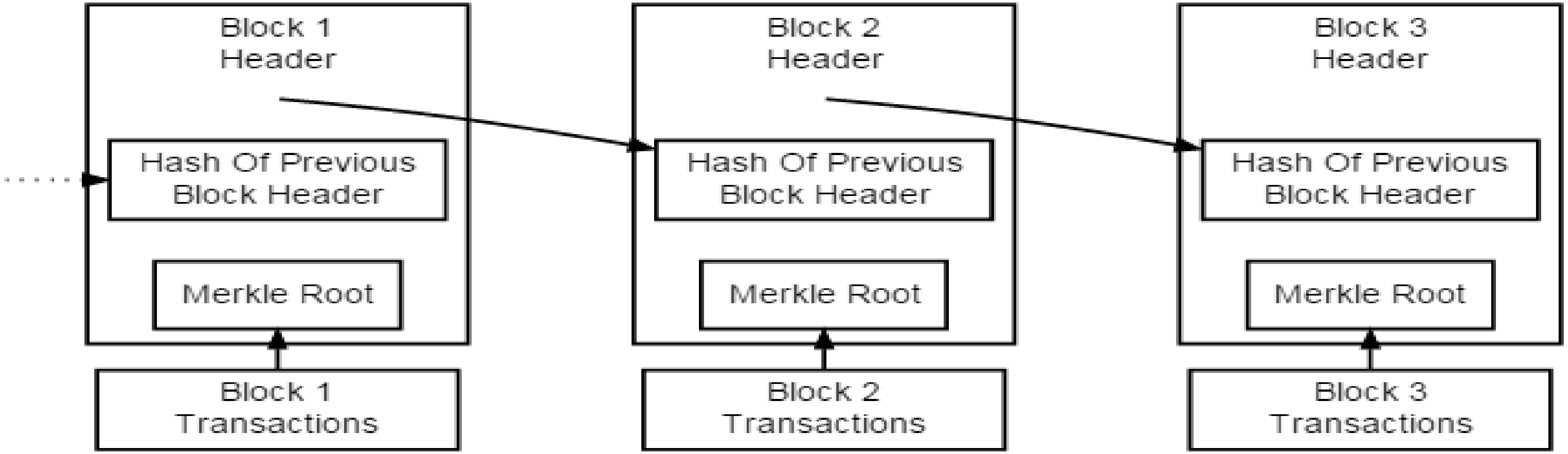
Blockchain & Cryptocurrency: Evolution to Crypto – Contd.

ERA-IV (Records on Spreadsheet)

- No paper notes/ no coins/no objects exchange
- Online buying & Selling
- Making and moving entries from one account to another. (Debit/Credit of values between buyer & Seller)

Blockchain—Core Concepts

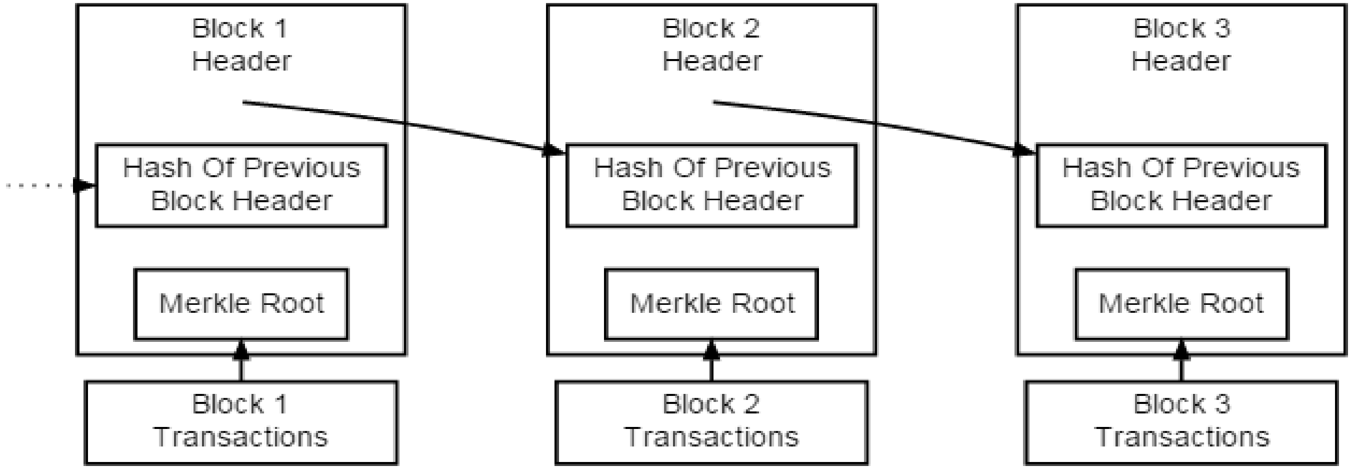
- Data Structure
- Decentralized (Peer to Peer)
- Public ledger
- Immutable



Simplified Bitcoin Block Chain

Blockchain---Contd.

- **Data Structure**
- Decentralized (Peer to Peer)
- Public ledger
- Immutable



Simplified Bitcoin Block Chain

Blockchain---Contd.

- **Data Structure**
- Decentralized (Peer to Peer)
- Public ledger
- Immutable

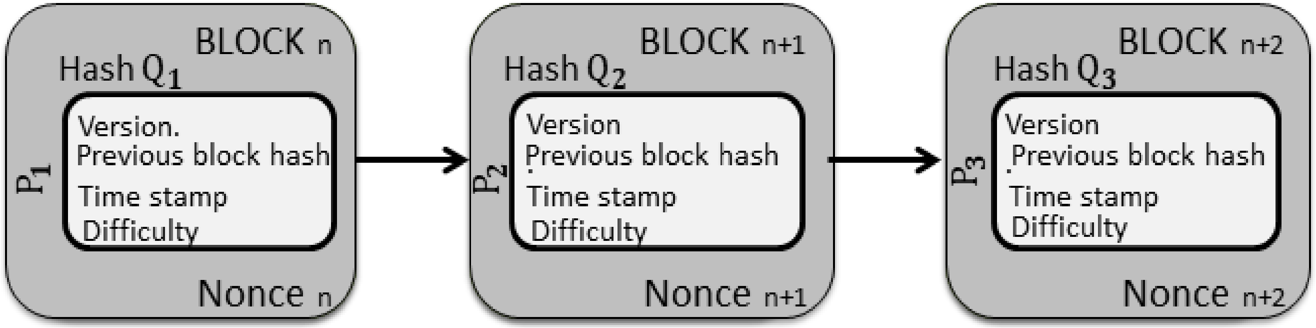
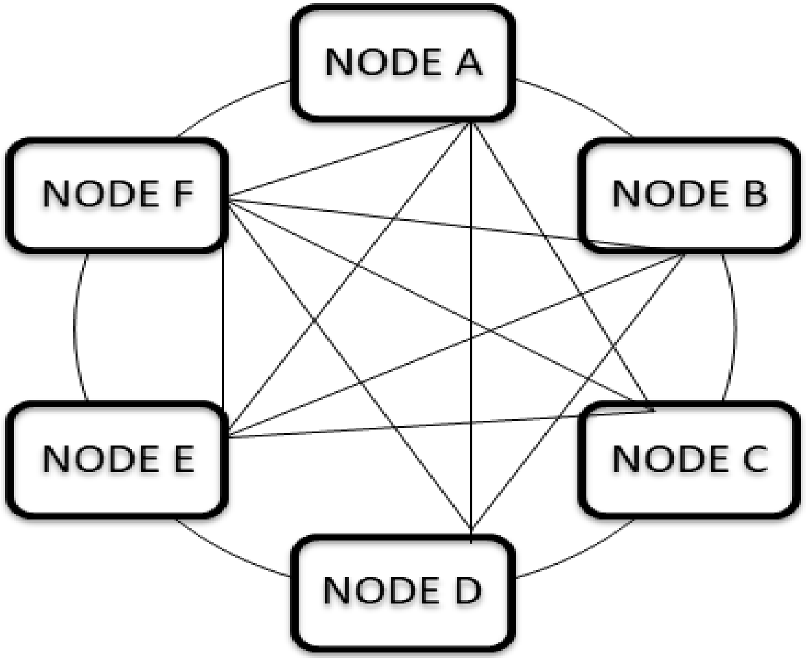


Figure 02

- Block 1 has the information of P_1 with the hash value of Q_1
- Block 2 has the information of P_2 with the hash value of Q_2
- Block 3 has the information of P_3 with the hash value of Q_3

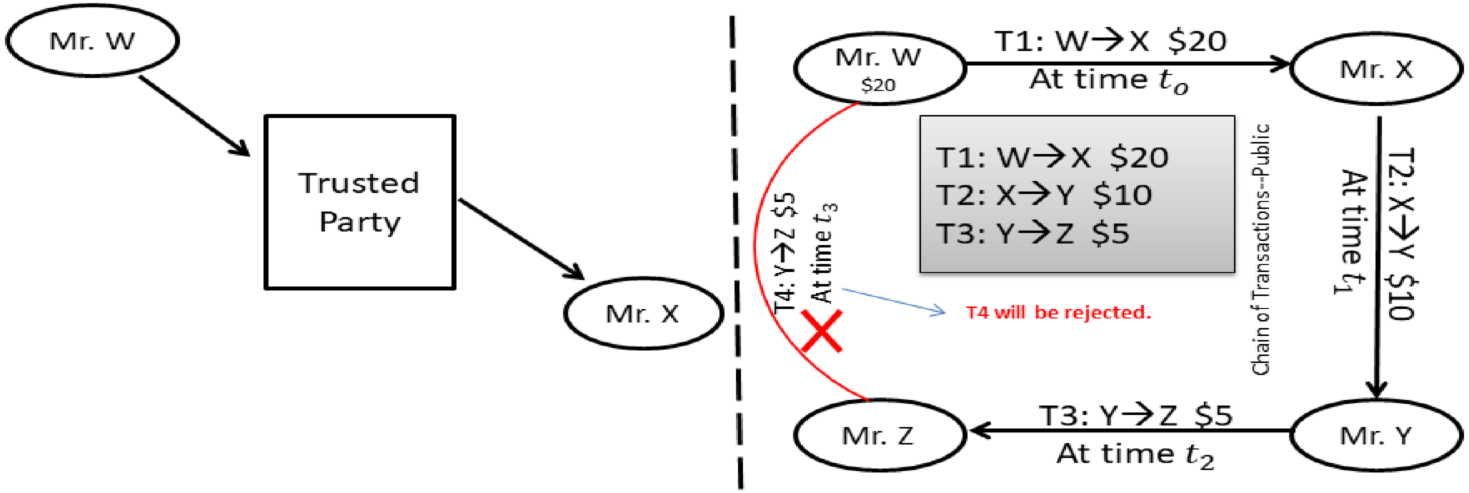
Blockchain---Contd.

- Data Structure
- **Decentralized (Peer to Peer)**
- Public ledger
- Immutable



Blockchain---Contd.

- Data Structure
- Decentralized (Peer to Peer)
- **<u>Public ledger –Money Transfer via Open Ledger</u>**
- Immutable



- Takes some time to transfer.
- Charges Fee.
- Data is private & centrally located.

- Takes less time to transfer.
- Charges very nominal Fee.
- Distributed Open Ledger.
- Every node keeps full copy of chain.

Blockchain---Contd.

- Data Structure
- Decentralized (Peer to Peer)
- Public ledger
- **Immutable**

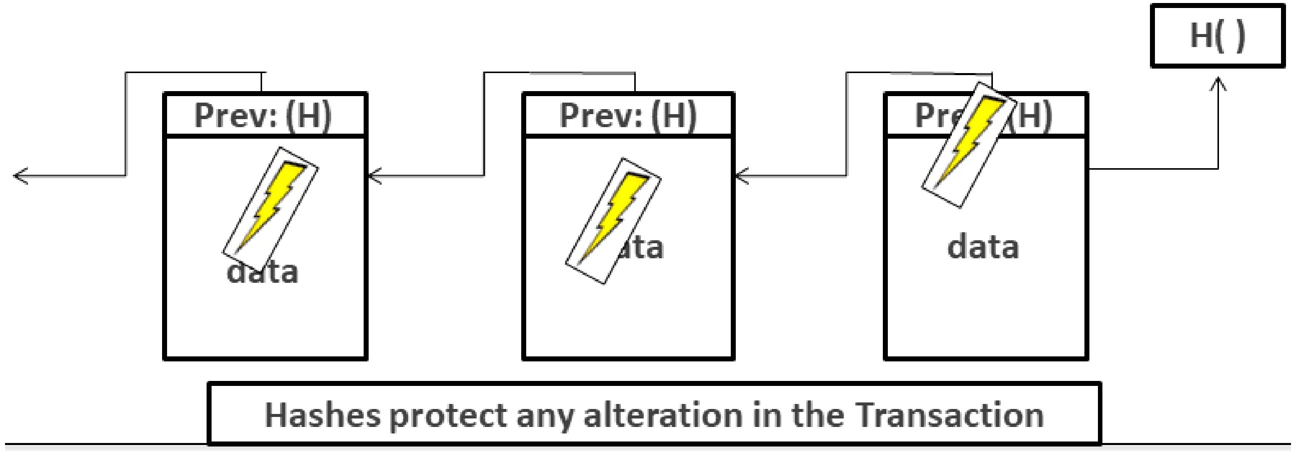


Figure 5: Centralised Vs Blockchain based Decentralized Distributed Public Ledger

➢ Any tampering in the block is restricted by chaining the blocks through hashes.

Blockchain—Real World Applications

- Electronic Voting
- Real State
- Supply Chain Management
- Provenance Tracking

Blockchain—Clarifying Misconceptions

- Bitcoin is digital money.
- Blockchain is a technology which enables Bitcoin to move from one account to another securely.
- They are not same. But since Bitcoin has been the face of blockchain in the recent past, it would be good to build the fundamental concepts in the context of Bitcoin.
- Blockchain attempts to solve the problem of asset transfer.
- Transactions traditionally occur through a trusted third party in blockchain.

Blockchain—Key Areas

- Learning Based Consensus Algorithm using Business Model Intelligence.
- Subscription Based Mining For Private Blockchain
- Collaborative Public Blockchain for Key Information Sharing
- Provenance Enabled Integrated Intelligent Algorithm for Attack Protection

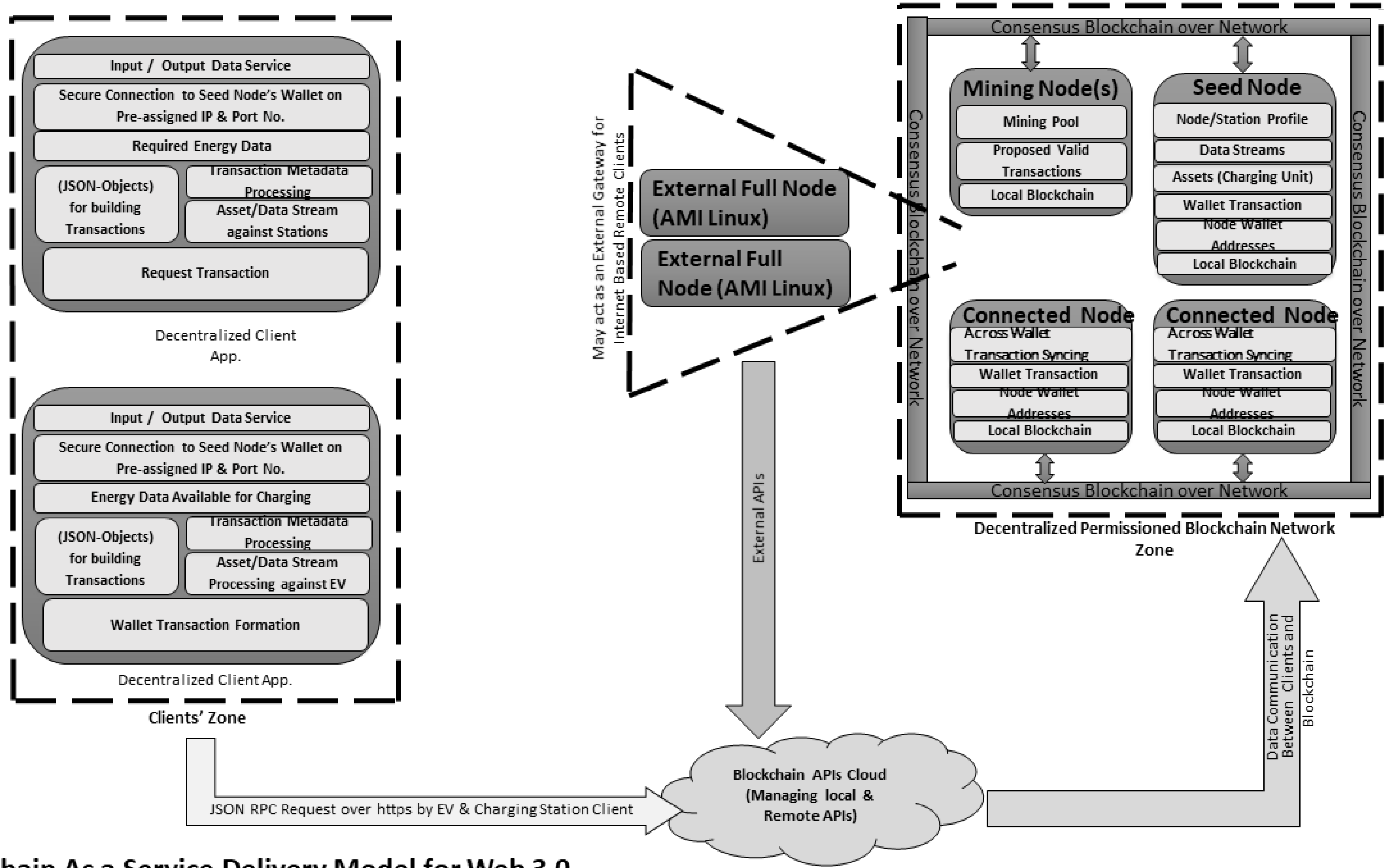
Blockchain (NOT Bitcoin) in Banking—Asset Management

- Assets: Anything of value
- Transactions: A complete activity from account to account
- Wallet Addresses: May be thought of as an account number
- Ledger: A large public spreadsheets contains transaction which have ever occurred.
- Use-Cases:
  - P2P fund Transfer (Transfer of ownership for assets)
  - Blockchain in Remittance Payment (Use in Pakistan)
  - From Central Bank to Consumer Bank (State Bank Scenario)
- Some Practical Demonstration/Implementation

What is Next!

- API based DApps.

Our Proposal for Blockchain Based Consumer Banking


Input / Output Data Service
Secure Connection to Seed Node's Wallet on Pre-assigned IP & Port No.
Required Energy Data
(JSON-Objects) for building Transactions
Transaction Metadata Processing
Asset/Data Stream against Stations
Request Transaction
Decentralized Client App.
Input / Output Data Service
Secure Connection to Seed Node's Wallet on Pre-assigned IP & Port No.
Energy Data Available for Charging
(JSON-Objects) for building Transactions
Transaction Metadata Processing
Asset/Data Stream Processing against EV
Wallet Transaction Formation
Decentralized Client App.
Clients' Zone
JSON RPC Request over https by EV & Charging Station Client
May act as an External Gateway for Internet Based Remote Clients
External Full Node (AMI Linux)
External Full Node (AMI Linux)
External APIs
Blockchain APIs Cloud (Managing local & Remote APIs)
Data Communication Between Clients and Blockchain
Consensus Blockchain over Network
Mining Node(s)
Mining Pool
Proposed Valid Transactions
Local Blockchain
Seed Node
Node/Station Profile
Data Streams
Assets (Charging Unit)
Wallet Transaction
Node Wallet Addresses
Local Blockchain
Connected Node
Across Wallet Transaction Syncing
Wallet Transaction
Node Wallet Addresses
Local Blockchain
Connected Node
Across Wallet Transaction Syncing
Wallet Transaction
Node Wallet Addresses
Local Blockchain
Consensus Blockchain over Network
Consensus Blockchain over Network
Consensus Blockchain over Network
Decentralized Permissioned Blockchain Network Zone

Blockchain As a Service Delivery Model for Web 3.0

Q/A

Special Thanks

• **Dr. Sarosh Hashmat Lodi**, Vice Chancellor, NED University of Engineering & Technology	
• **Dr. Saad Ahmed Qazi**, Dean Faculty of Electrical & Computer Engineering, NED University of Engineering & Technology • **(Course Lead)**	
• **Dr. Muhammad Mubashir Khan**, Chairman, Department of Computer Science & Information Technology, NED University of Engineering & Technology • **(Course co-ordinator)**	