BlockChain Fundamentals

ABOUT BLOCKCHAIN

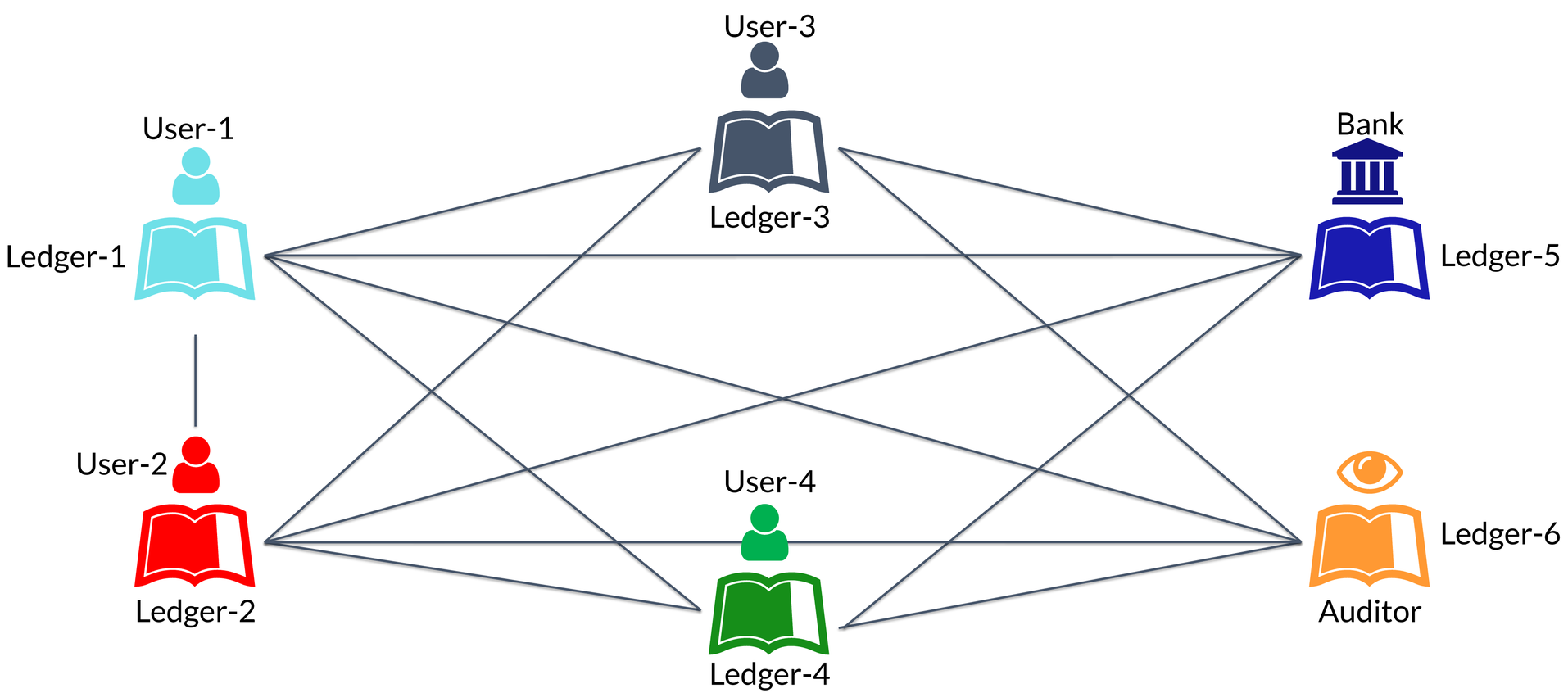
BlockChain and BitCoin are not same; In fact, BitCoin is just ONE application of BlockChain

- BitCoin is a CURRENCY
- Primary purpose is mining
- There are 21 million BitCoins
- It does not have a fixed value
- More than 50% are with 880 individuals
- There are similar currencies like LiteCoin, RippleCoin etc.

- BlockChain is a TECHNOLOGY
- Distributed & Shared Ledger
- Cryptography (Private Key, Hashing)
- Based on Consensus
- Implements Smart Contracts
- Impacts all Business Segments

ABOUT LEDGERS

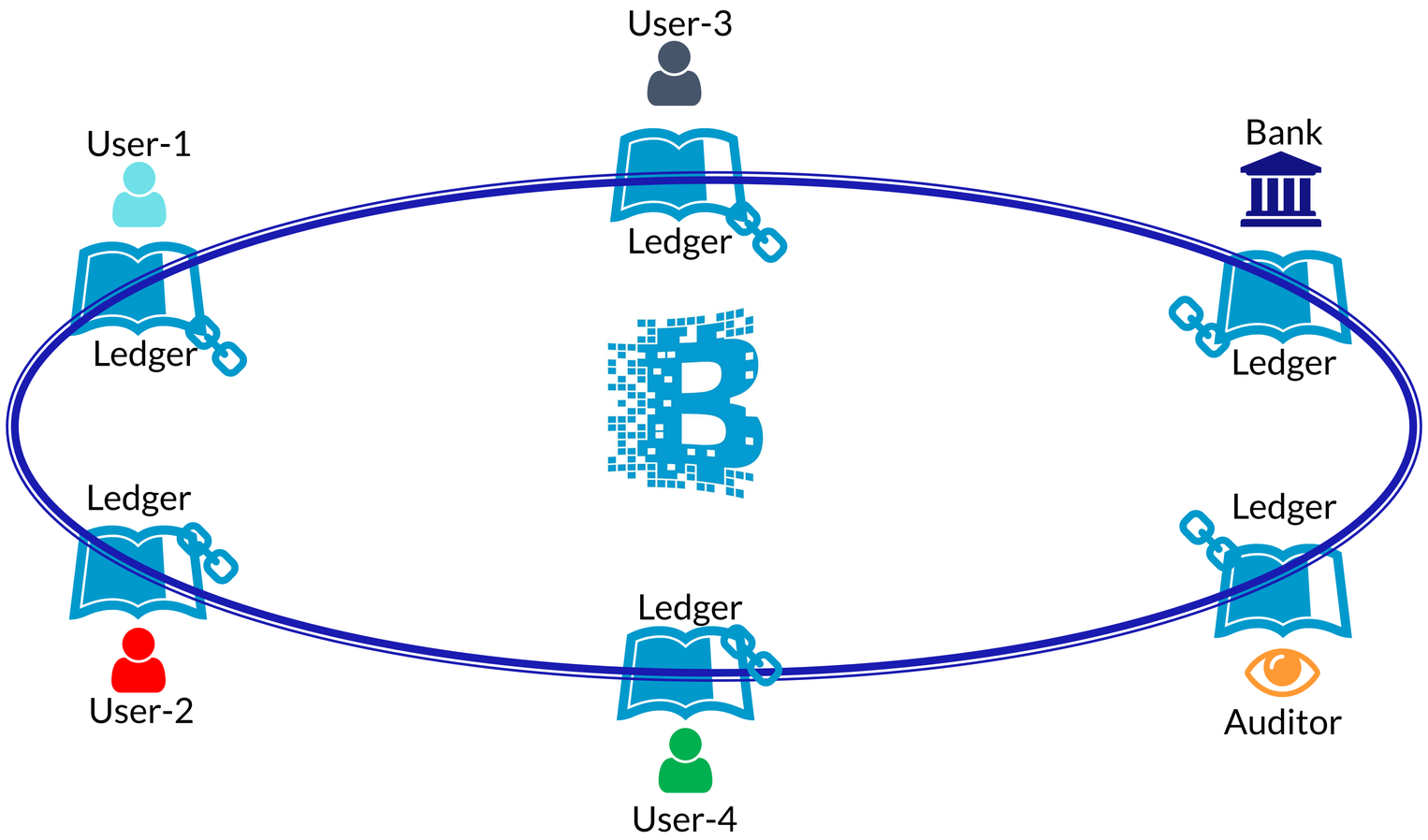
Current Scenario – Individual Ledgers



- Inefficient
- Error Prone
- Vulnerable
- High Cost

ABOUT LEDGERS

BlockChain concept – Shared Ledgers



- Resilient
- Consistent
- Secured
- Efficient

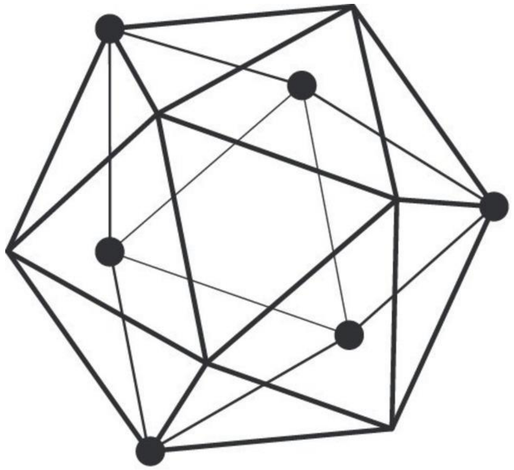
ABOUT BLOCKCHAIN

4 Main Pillars

Consensus

Cryptography

Distributed Shared Ledger



Smart Contract

TECHNOLOGY OVERVIEW

Cryptographic Hash

The Hash Function: Collision Free, Hiding

Input (any length)	Hash Function	Output (Fixed Length)
Kiran	Hash (Input)	DF60AF
Kiran is a nice guy	Hash (Input)	ACD055
Kiran likes cold coffee	Hash (Input)	349ACD

Collision Free

No body can find x and y such that x!=y AND H(x) = H(y)
Corollary: If H(x) == H(y), THEN x = y

Hiding

If we know H(x), THEN its infeasible to find x
To achieve this:
Instead of computing H(x), compute H(k | x)
“k” is chosen from a distribution of high min-entropy

TECHNOLOGY OVERVIEW

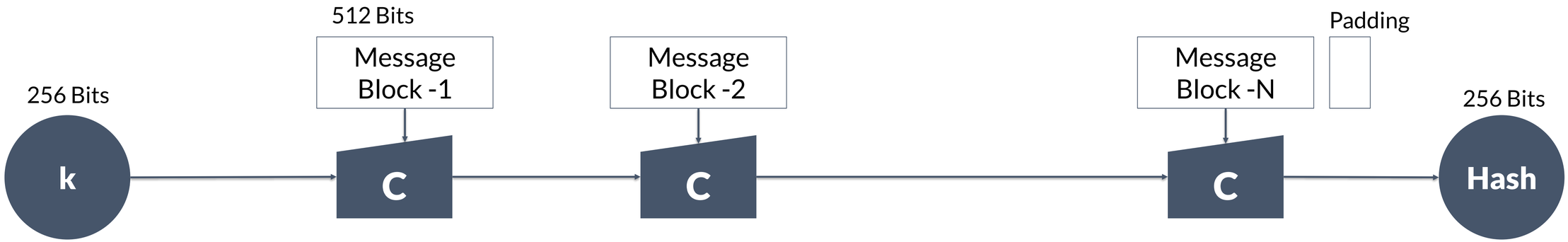
Commitment

The Commitment: Want to seal a value into an envelope NOW and open the envelope LATER

How is it implemented digitally in BlockChain? – Commitment API

Commit(msg) = (H(key | msg), key)
Verify(commit, key)

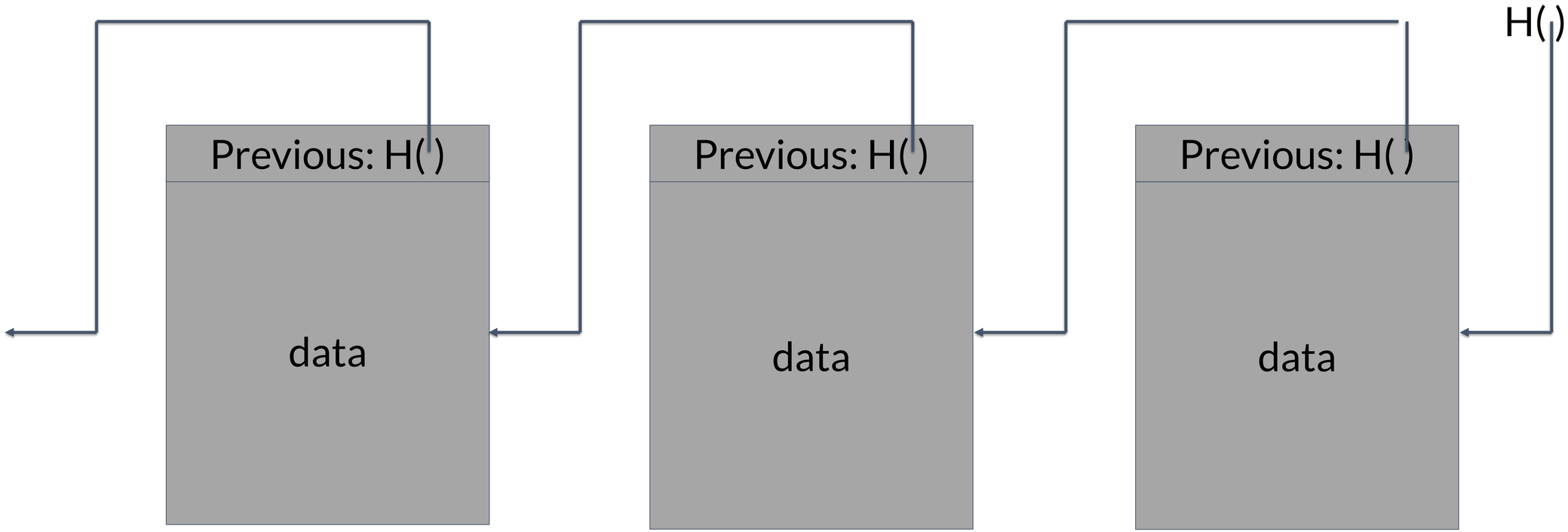
Example: Use case of BitCoin using SHA-256 Hash Function



TECHNOLOGY OVERVIEW

So, how do all these add up towards BlockChain?

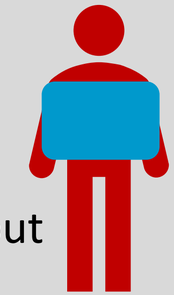
The Hash Pointer: (1) Pointer to where INFO is stored, AND (2) Hash of the INFO



BLOCKCHAIN IN ACTION

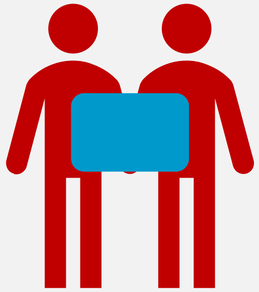
How does it all work?

Each Transaction is put into a Block



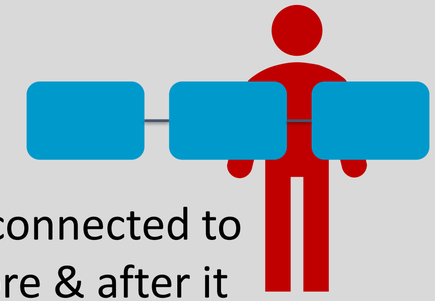
Transaction can by anything like filling a form, depositing a check, applying for credit etc. etc.

Transaction gets consensus



Every party getting affected by the transaction has to consense. For example, the party receiving a form and party filling a form should arrive at a consensus for the form's completion.

Block is connected to one before & after it



Block (with the transaction) is time stamped and put in a chain of Blocks which can never be deleted. All involved parties have the copy of the this Block and the previous blocks, making the chain of transactions tamper proof.

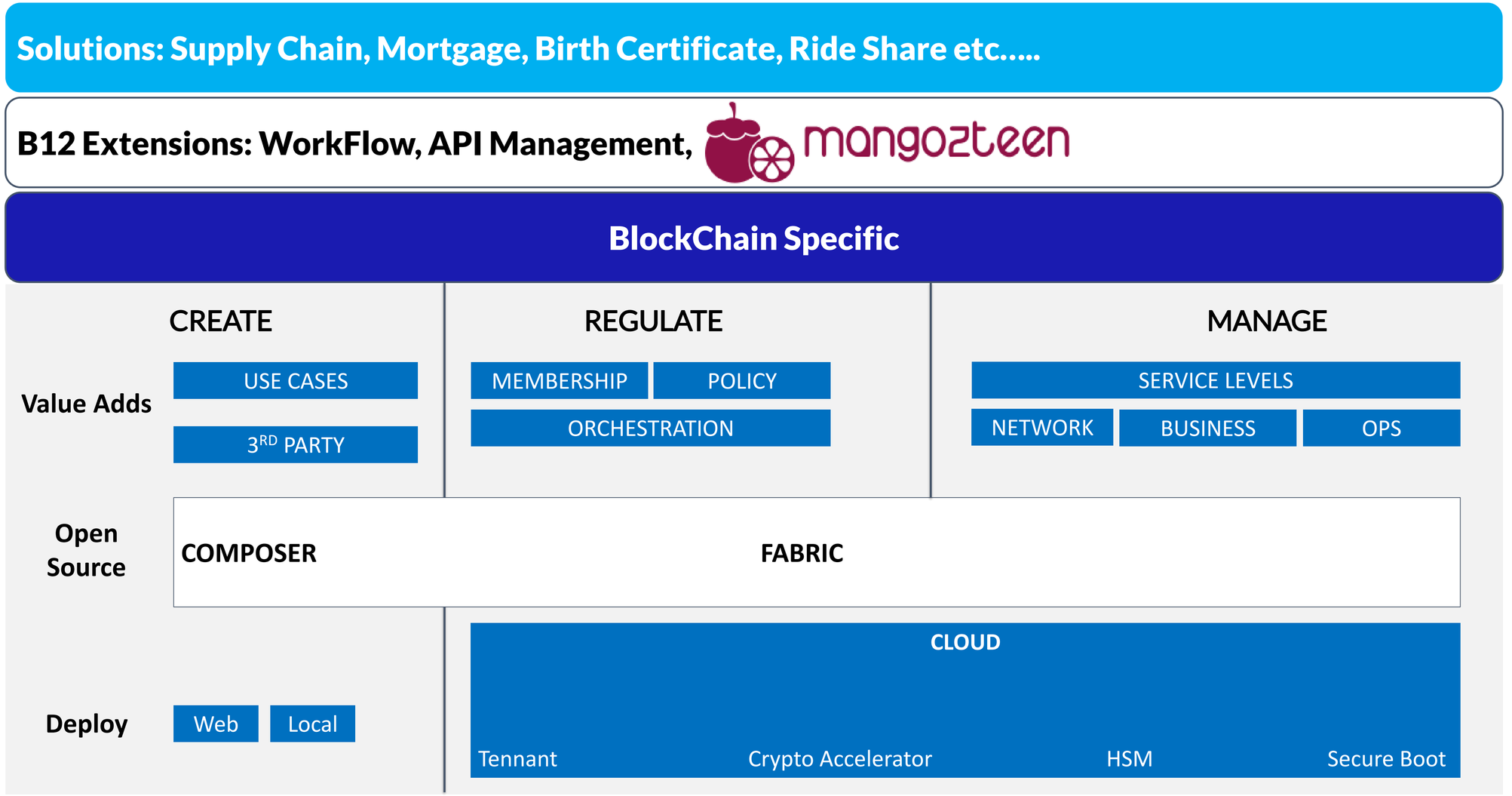
Automated action based on Smart Contract

Smart Contract is automated and is a business logic. It always executes based on fulfilment of an input trigger. For example: If the form is duly filled, then an ACTION will always be taken.

- Facilitate Escrow services
- Acts as Notary of transactions
- Can't be modified easily

SOLUTION ARCHITECTURE

End – End offering along with TE IoT



THIRDEYE OFFERING

How can we help?

BLOCKCHAIN ADVISORY

- Technology Advisory
- Training
- Consulting
- Roadmap
- Integration
- QA

GESTATION

- Technology Assessment
- Use Case definitions
- Prototyping
- Lab incubation

SOLUTIONS

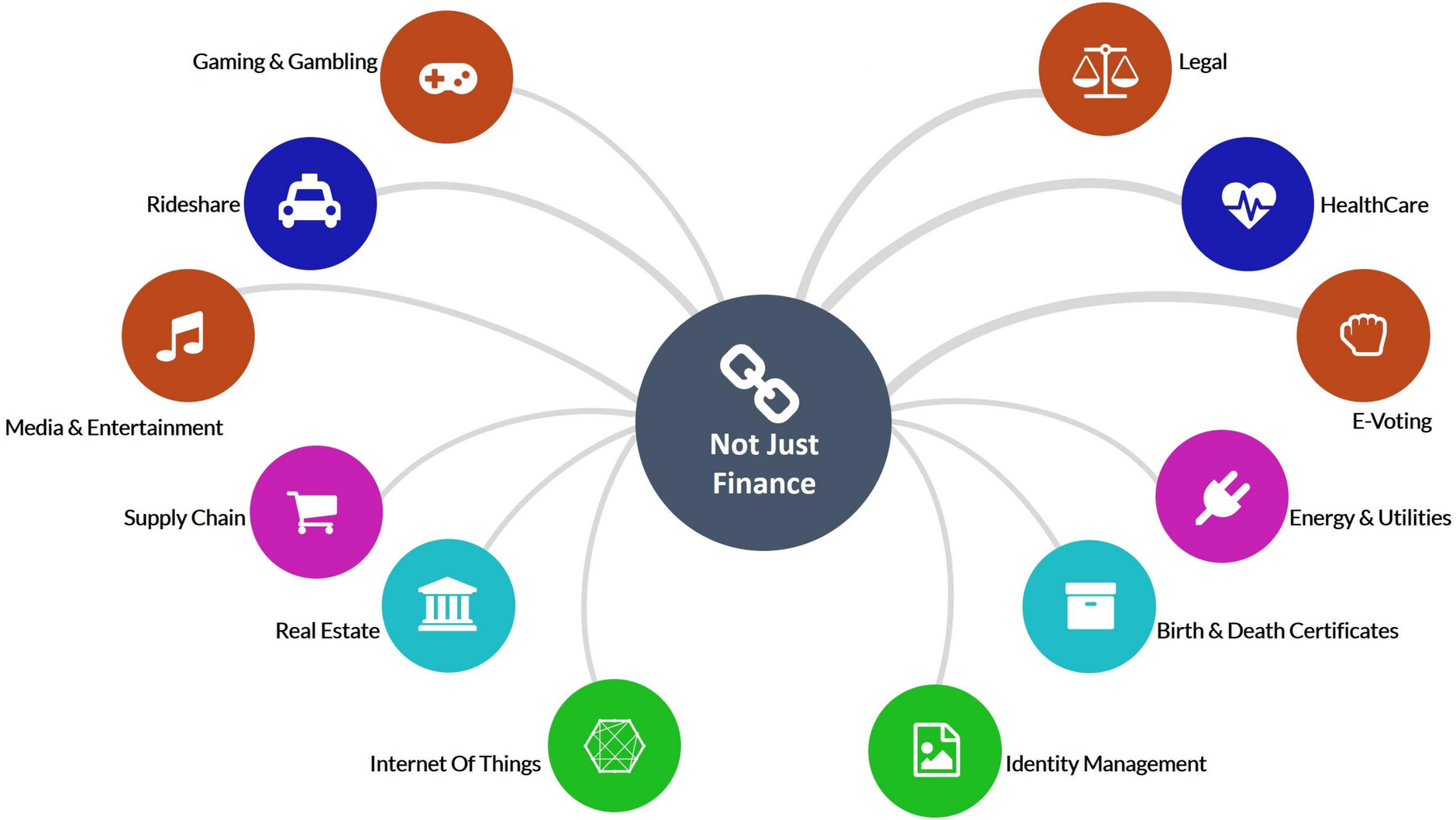
- Industry specific
- Integrations
- IOT Enablement

PLATFORM ECOSYSTEM

- Ecosystem Building
- Platform Enablement

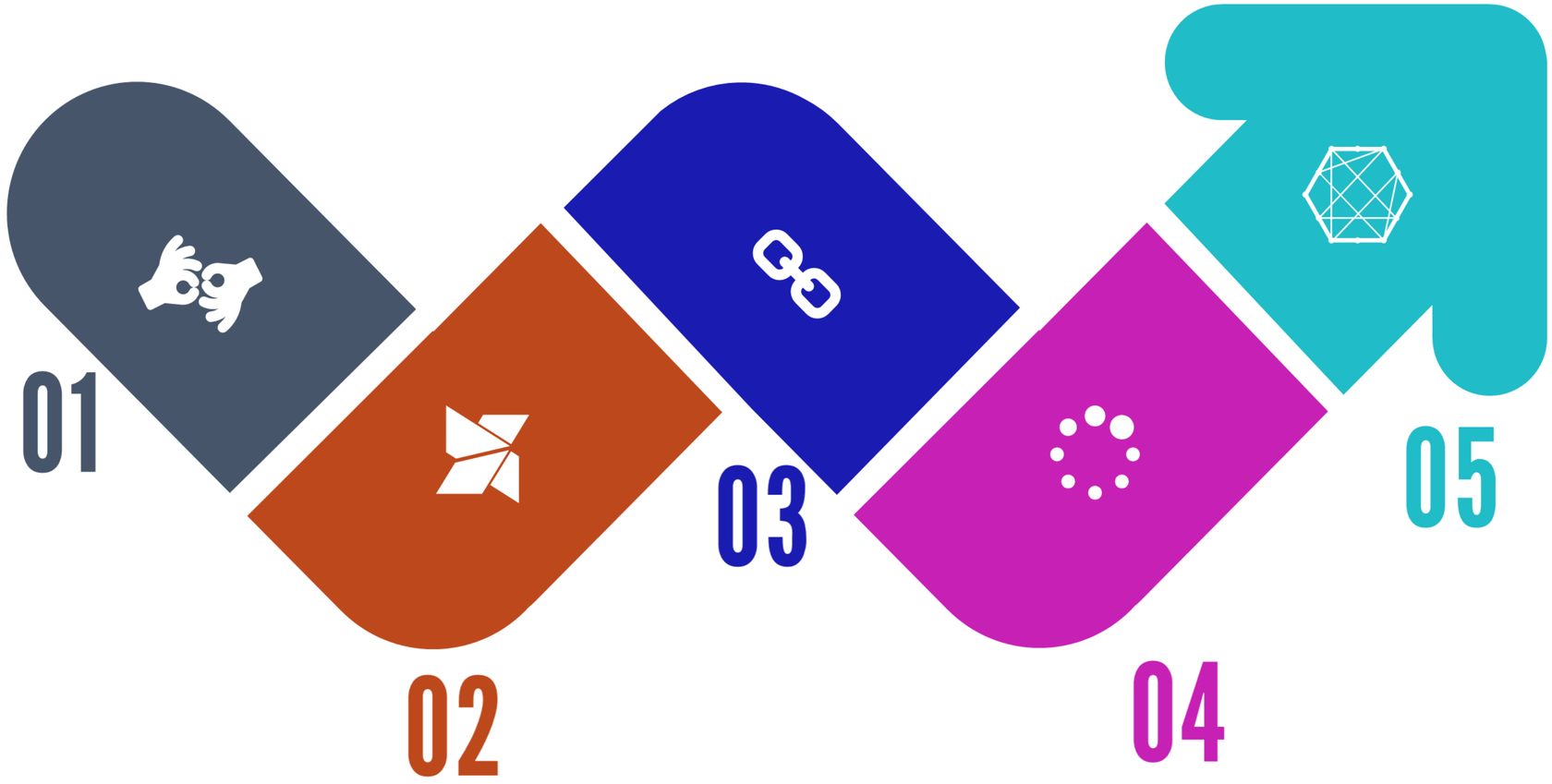
THIRDEYE BLOCKCHAIN FOCUS

Leveraging with Mangozteen



BLOCKCHAIN JOURNEY WITH TE

5 Phase approach



01 Assessment: Use case

02 Evaluation: Feasibility

03 Build: MVE

04 Onboard: Partners

05 Operate

ENGAGEMENT MODEL WHICH CAN BE MONETIZED

Enabling businesses and clients