



BLOCKCHAIN AS A SECURITY BRICK FOR SOFTWARE APPLICATIONS

WHO'S WHO



- Head of Life-Insurance & Post-Trade Software Development
- 18+ years experience : System Engineer, DBA , DATA Architect , Software Dev Manager & Blockchain Enthusiast since 2014

- My articles:

 <https://www.linkedin.com/in/sbelhadj/>

 <https://medium.com/@sbelhadj>

AGENDA

- Blockchain Definition (Technical/Conceptual)
- Blockchain or How to clone Physical transaction to Digital transaction
- Distributed Database vs Distributed Ledger
- Blockchain & Internet OF VALUE
- Blockchain Security Design
- Blockchain Security for IOT
- ICO Dapp demo

[HTTPS://WWW.LINKEDIN.COM/IN/SBELHADJ/](https://www.linkedin.com/in/sbelhadj/)

12/5/2020

3

BLOCKCHAIN DEFINITION (TECHNICAL)

- ✓ **Append-only** Distributed Database (Ledger) shared between multiple non-trusting writers without the need for a Trusted Central Authority.
- ✓ The data integrity of the Ledger is guaranteed by a **Distributed Consensus Algorithm**.

BLOCKCHAIN SOLUTIONS

3 BASIC COMPONENTS

:

1. A **data model** that captures the current state of the ledger.
2. A **language of transactions** that changes the ledger state.
3. A **protocol** used to build consensus among participants around which transactions will be accepted, and in what order, by the ledger.

BLOCKCHAIN OR HOW TO CLONE PHYSICAL TRANSACTION TO DIGITAL TRANSACTION

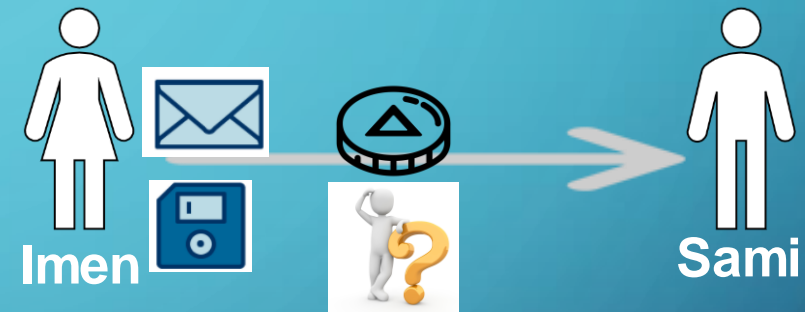
Physical Transaction



- ✓ Easily Verifiable.
- ✓ No need for a third-party to validate the transaction.
- ✓ Imen does not have the money anymore and Sami has it in his hands.
- ✓ Instant transfer of the asset

[HTTPS://WWW.LINKEDIN.COM/IN/SBELHADJ/](https://www.linkedin.com/in/sbelhadj/)

Digital Transaction



- ✓ What if the third trusted party duplicates the asset?
- ✓ He can even add to his account whenever he wants.
- ✓ He can impose high commissions
- ✓ What If his service is hacked : service unavailable (SPOF)
- ✓ The end user does not have the means to check by himself

BLOCKCHAIN OR HOW TO CLONE PHYSICAL TRANSACTION TO DIGITAL TRANSACTION

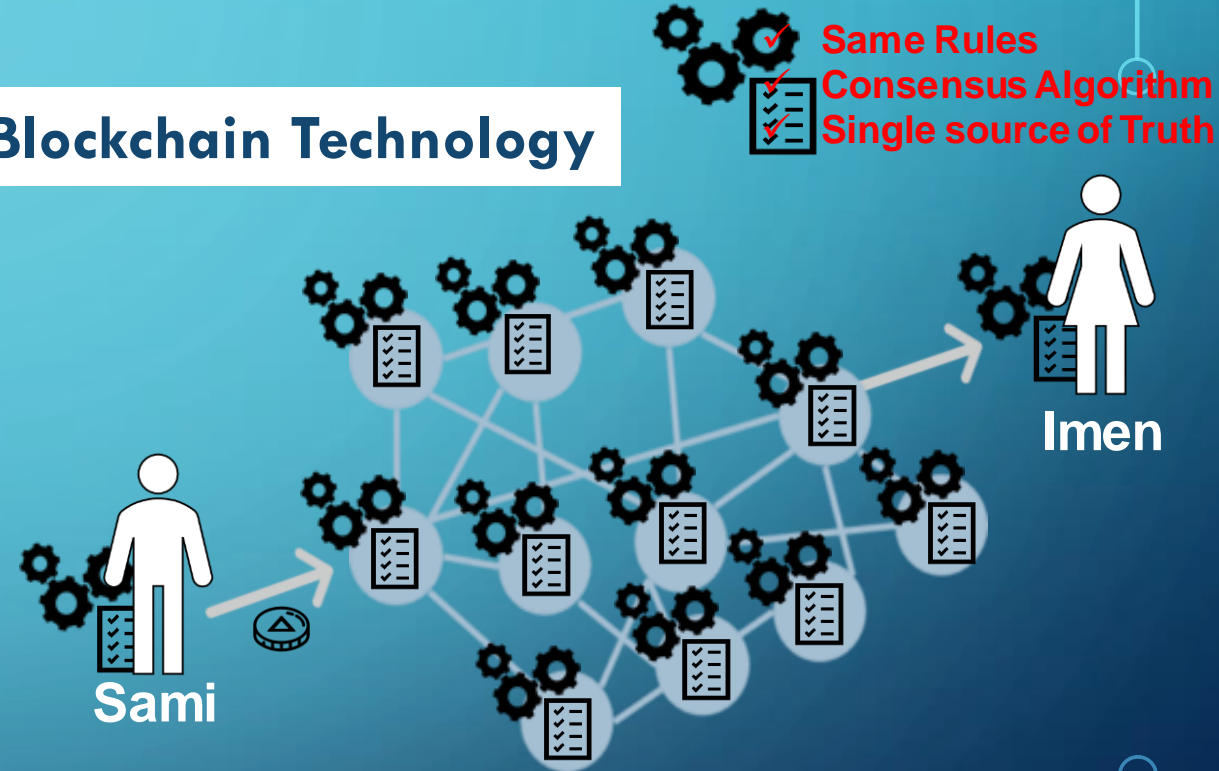
Trusted third-party



- ✓ What if the third trusted party duplicates the asset?
- ✓ He can even add to his account whenever he wants.
- ✓ He can request high fees
- ✓ What If his service is hacked : service unavailable (SPOF)
- ✓ The end user does not have the means to check by himself

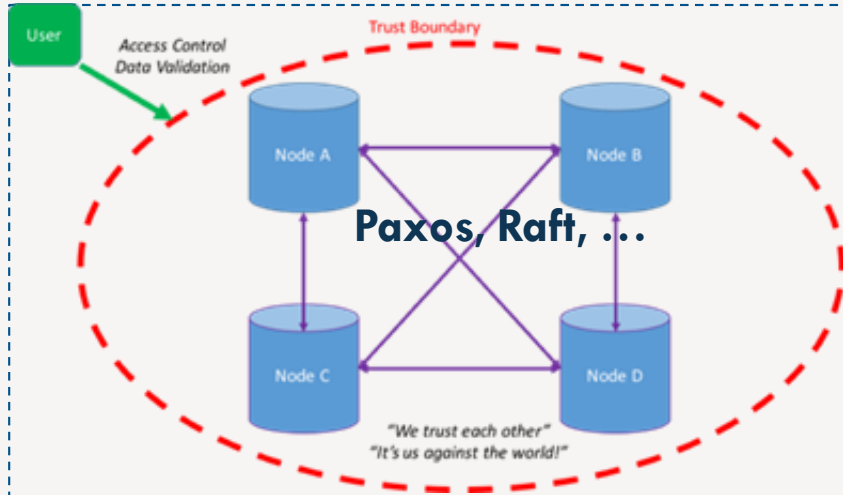
[HTTPS://WWW.LINKEDIN.COM/IN/SBELHADJ/](https://www.linkedin.com/in/sbelhadj/)

Blockchain Technology



- ✓ The Ledger is no longer owned by a single entity
- ✓ Validation and verification of the Ledger is no longer a monopoly
- ✓ Consensus rules guarantee the security of the Ledger
- ✓ The end-user can even participate in maintaining the Ledger (the purest version of the BC)
- ✓ Actors are incentivized to act "ethically"

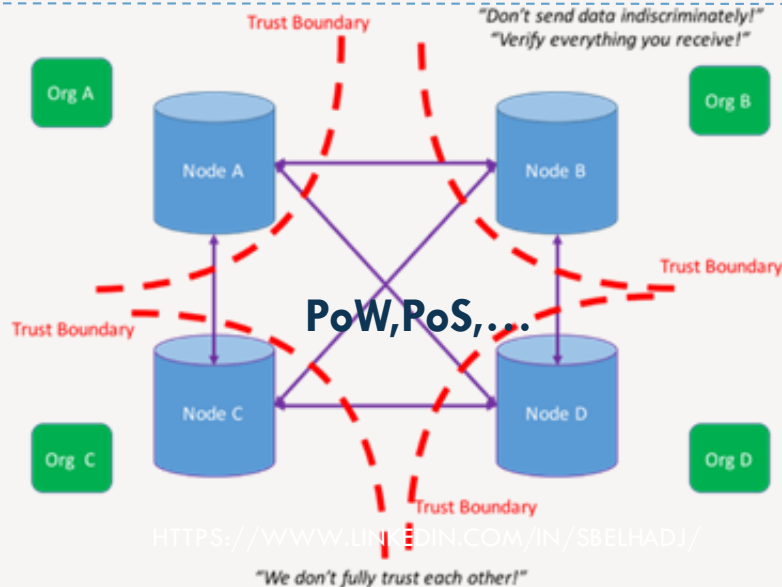
DISTRIBUTED DATABASE VS DISTRIBUTED LEDGER



Distributed Database

*Nodes of a distributed database **trust** each other and collaborate with each other to present a consistent, secure truth to the rest of the world.*

It's All About the Trust Boundary!!!



Distributed Ledger (Blockchain)

*Nodes of a distributed ledger (Blockchain) **can not trust** each other and so must independently **verify** data they receive from each other and only share data they are happy to be broadly shared.*

[HTTPS://WWW.LINKEDIN.COM/IN/SBELHADJ/](https://www.linkedin.com/in/SBELHADJ/)

12/5/2020

BLOCKCHAIN DEFINITION (CONCEPTUAL)

Blockchain is a **paradigm shift** in the way we approach designing economic systems involving **multiple peers** with **divergent interests** (~zero-sum game) but find it profitable to be part of the same system.

The traits of such systems are :

✓ **Decentralized** , governed by rules but without rulers : **Protocols** instead of **Platforms**.

✓ **Trust** is derived from the network not from hierarchy (Trustless).

✓ Transactions are secured by **Cryptography**.

BIG SHIFT IN BUSINESS MODELS DESIGNS

Business models are increasingly based on the reduction of intermediaries

Platform Economy



[HTTPS://WWW.LINKEDIN.COM/IN/SBELHADJ/](https://www.linkedin.com/in/sbelhadj/)

2010

Sharing Economy



UBER

KICKSTARTER

2015

P2P Economy

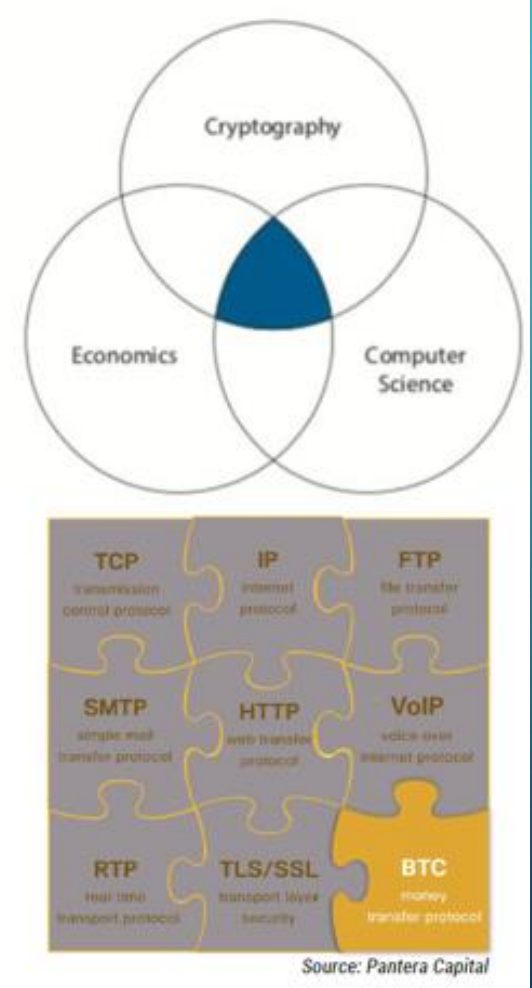


12/5/2020

10

BLOCKCHAIN & INTERNET OF VALUE

THE INTERNET Innovation in Information Transfer	THE BLOCKCHAIN Innovation in Value Transfer
Application Universe: <i>Streaming video and music, data sharing, cloud computing</i>	Application Universe: <i>Smart contracts, distributed computing, tokenization</i>
Killer App: Email	Killer App: Bitcoin
Network: ISPs, Routers	Network: Miners, Nodes, Staking, etc.
Protocols: TCP/IP, HTTP, DNS, FTP	Protocols: Bitcoin, Ethereum, IPFS, Blockstack



- Blockchain is the last Brick in the Internet protocol that allowed Internet to move

Value between peers

[HTTPS://WWW.LINKEDIN.COM/IN/SBELHADJ/](https://www.linkedin.com/in/sbelhadj/)

12/5/2020

11

EMBEDDED SECURITY IN BLOCKCHAIN DESIGN

- Internet was designed without security as a priority → Only a resilient network!!
- Blockchain protocol was designed with security EMBEDDED in its CORE (BFT in practice, identification , encrypted transactions,)
- Internet security was implemented at the Application protocol Level.
- Blockchain security is implemented at the low level protocol layer.

DAPPS SECURITY REQUIREMENTS

- **Identification & Authentication** → Cryptographic identity
- **Data Integrity** → Encrypted transactions coupled to Common Consensus mechanism
- **Data Confidentiality** → Zero-knowledge proof / Homomorphic encryption
- **Data Ownership/Control** → Distribution of Data

BLOCKCHAIN SECURITY FOR IOT

- The Distributed character of IOT networks makes it a good candidate for Blockchain technology
- **Blockchain**, which is most familiar for **bitcoin** and Ethereum, offers an intriguing solution for **IoT security**. **Blockchain** contains strong protections against data tampering, locking access to Internet of Things devices, and allowing compromised devices in an **IoT** network to be shut down.

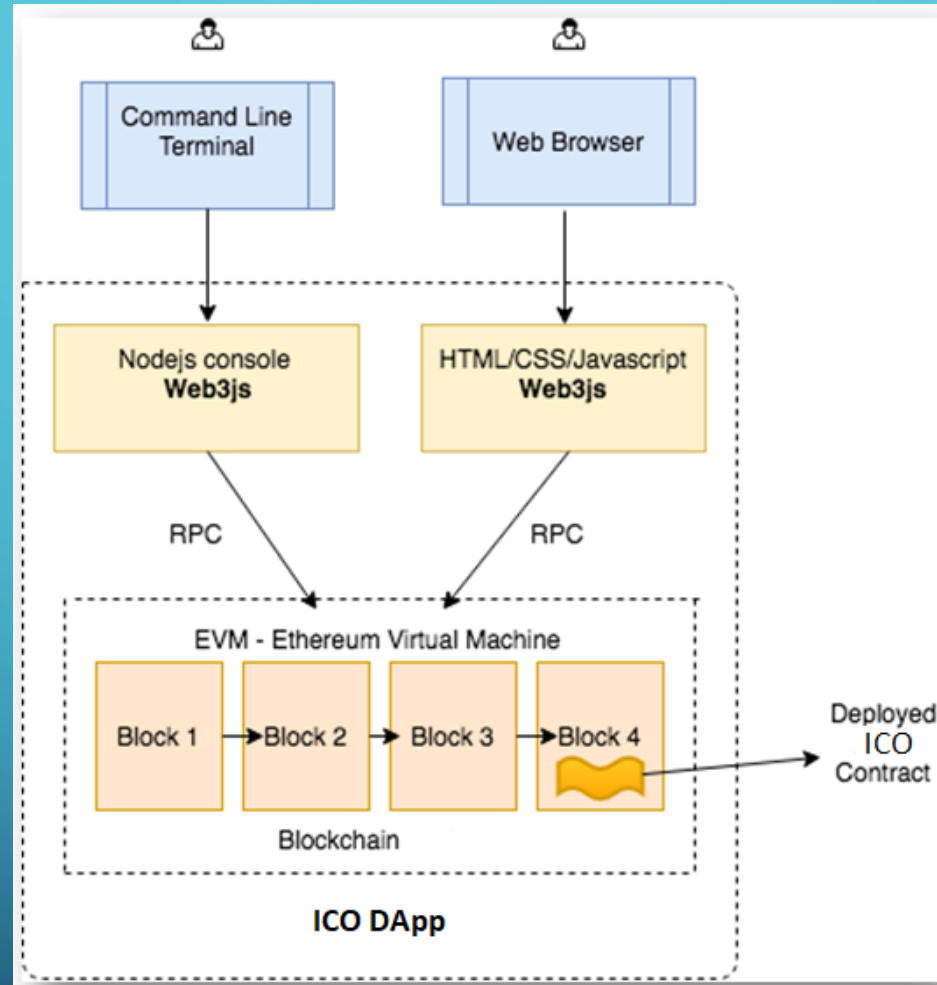
ICO DAPP DEMO

[HTTPS://WWW.LINKEDIN.COM/IN/SBELHADJ/](https://www.linkedin.com/in/sbelhadj/)

12/5/2020

15

DApp reference Architecture



Steps

Step 1 : Setting up the environment

Step 2 : Writing the Smart Contracts

Step 3 : Compiling and deploying(migrating) the Smart Contracts

Step 4 : Testing the Smart Contracts

Step 5 : Creating the Front-end

Step 6: Using the DApp

Creating the Front-end

A Simple ICO DApp for TDS

Token Stats

Tokens For Sale	100000000
Tokens Sold	11120
Price Per Token	1000 tokens = 1 Ether
Balance in the ICO Onwner address	109.04398641060000001 Ether

Purchase TDS Tokens

10000

Buy

Ethers for buying TDS tokens

Buy

TDSicoContract contract address:

0x14d758d923e920955c731fadcc86aa6918a3d1cf

TDSicoToken contract address:

0x3db003f0ec696a411667f655203ba2cb84d80416

Investors

Investor	TDS Tokens
0x00b1b8f1b9ee8b1f83027c045d02b9899dc9beea	120
0xad925a28bd049462c16163fbab3fa3b2769766fb	1000
0x00a329c0648769a73afac7f9381e08fb43dbea72	10000

Events

Transaction Hash :0x20b100723b928833d56989a74d2793b4a57a85482bd58a1814b29c1a0b7acdee
From:0x00
To:0x00a329c0648769a73afac7f9381e08fb43dbea72
TDS Tokens: 10000

Lookup Investor Info

Enter the investor address

Lookup

HTTPS:

12/5/2020

18

Step 6 : Interacting with the DApp

A Simple ICO DApp for TDS

Token Stats

Tokens For Sale	100000000
Tokens Sold	1430
Price Per Token	1000 tokens = 1 Ether
Balance in the ICO Onwer address	8.1808317130000003 Ether

Purchase TDS Tokens

Purchase order has been submitted. Please wait.

2000

Buy

Ethers for buying TDS tokens

Buy

Investors

	TDS Tokens
9766fb	1100
c9beea	200
62ab4	130

MetaMask Notification

CONFIRM TRANSACTION

Investor 4
Bc1ABB...2ab4
8.180 ETH
3665.34 USD

2dAE2e...589E

Amount
2.000 ETH
896.08 USD

Gas Limit
131785 UNITS

Gas Price
20 GWEI

Max Transaction Fee
0.002635 ETH
1.18 USD

Max Total
2.002 ETH
897.26 USD

Data included: 4 bytes

RESET SUBMIT REJECT

[HTTPS://WWW.LINKEDIN.COM/IN/SBELHADJ/](https://www.linkedin.com/in/sbelhadj/)

TDSicoContract contract