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/ 12/5/2020
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 Concensys Algorithm.
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.
Imen does not have the money anymore and Sami has it in his hands.

- Instant transfer of the asset
- 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
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

✓ 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"
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!!!

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.
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  Sharing Economy  P2P Economy

2010 2015

PayPal, salesforce, Facebook, Funding Circle, Airbnb, Uber, Bitcoin, Ethereum

HTTPS://WWW.LINKEDIN.COM/IN/SBELHADJ/
Blockchain is the last Brick in the Internet protocol that allowed Internet to move value between peers.

HTTPS://WWW.LINKEDIN.COM/IN/SBELHADJ/
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.
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
Step 6: Interacting with the DApp

A Simple ICO DApp for TDS

Token Stats
Tokens For Sale: 10,000,000
Tokens Sold: 1,430
Price Per Token: 1,000 tokens = 1 Ether
Balance in the ICO Owner address: 8.18083171300000003 Ether

Investors

CONTRM TRANSACTION
Amount: 2.0000 ETH
Gas Limit: 131785
Gas Price: 20
Max Transaction Fee: 0.002635 ETH
Max Total: 2.002 ETH

TDSicoContract contract
HTTPS://WWW.LINKEDIN.COM/IN/SBELHADJ/