University of BATNA 2
Department of Computer Science

Blockchain Fundamentals

Mr. A.Dekhinet

http://staff.univ-batna2.dz/dekhinet-Abdelhamid

Master 1 Distributed Information Systems Engineering and Security - 2021/2022

University of BATNA 2

Department of Computer Science

Chapter 1

Introduction to the Blockchain

Master 1 Distributed Information Systems Engineering and Security - 2021/2022

Blockchain origin

- Blockchain was proposed by a person (or a group of person) using the pseudo name **Satoshi Nakamoto** in 2008. It was originaly designed to serve as a public transaction ledger (سجل المعاملات) to track digital currency (Cryptocurrency) : Bitcoin

- So, the Blockchain technology was originally dedicated for the Bitcoin, but blockchain is now being a general purpose technology. The generalization is materialized by the definition and the use of programming language, such Solidity, Python, …

Blockchain origin

The proposal of **Satoshi Nakamoto** was the subject of a paper entitled :

“Bitcoin : A Peer-to-Peer Electronic Cash“

The paper can be downloaded from the address :

https://bitcoin.org/bitcoin.pdf

Blockchain origin

In this paper the author wrote

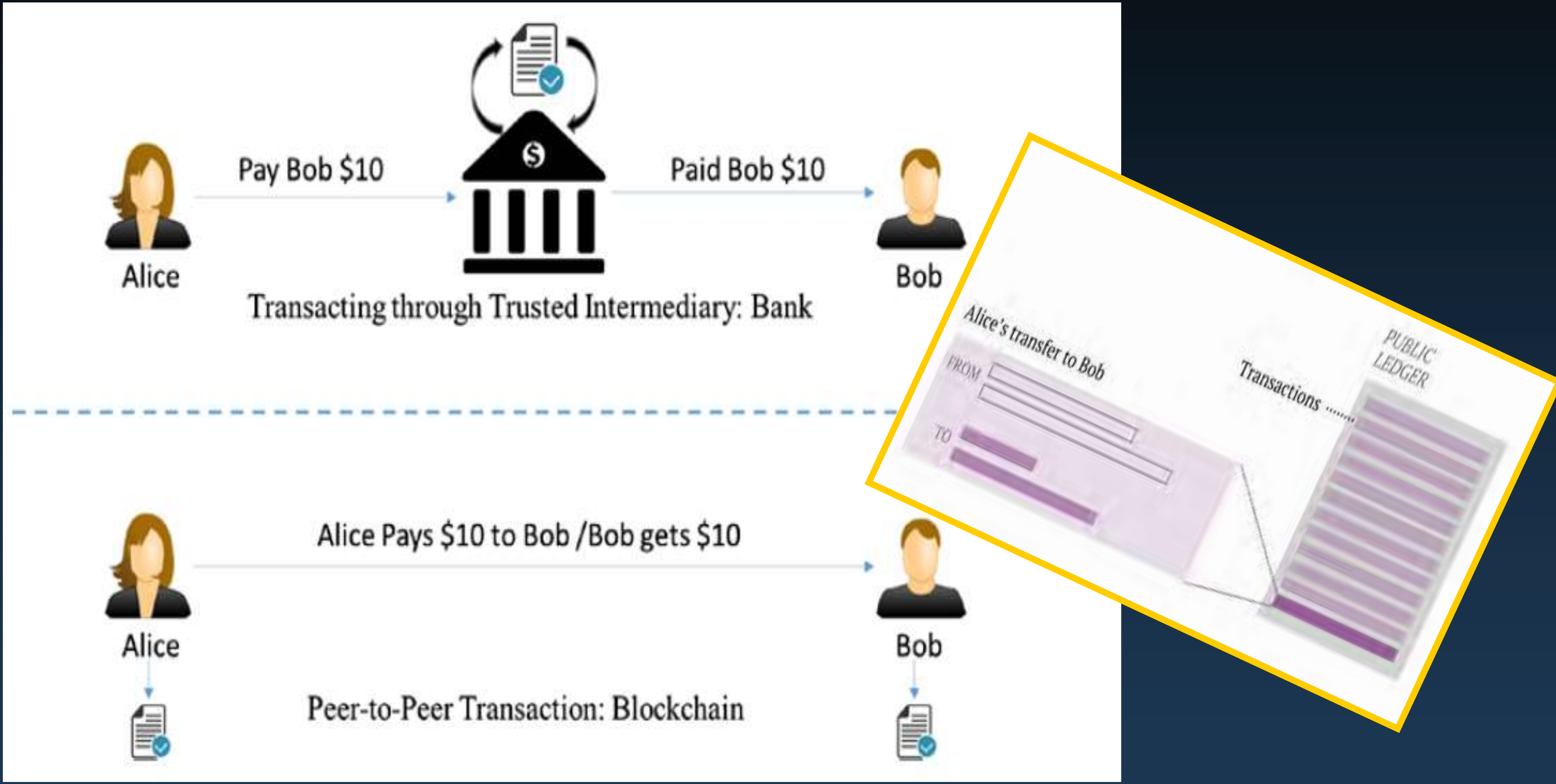
……………………

What is needed is an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party.

……………………

We propose a solution to the double-spending problem using a peer-to-peer distributed timestamp server to generate computational proof of the chronological order of transactions

Peer-To-Peer operation


Alice
Pay Bob $10
Paid Bob $10
Bob
Transacting through Trusted Intermediary: Bank
Alice
Alice Pays $10 to Bob /Bob gets $10
Bob
Peer-to-Peer Transaction: Blockchain
Alice's transfer to Bob
FROM
TO
Transactions ....
PUBLIC LEDGER

Transaction through a third party vs. peer-to-peer transaction

Blockchain foundations

- The blockchain technology is , mainly, founded on two well-established systems in computer science :

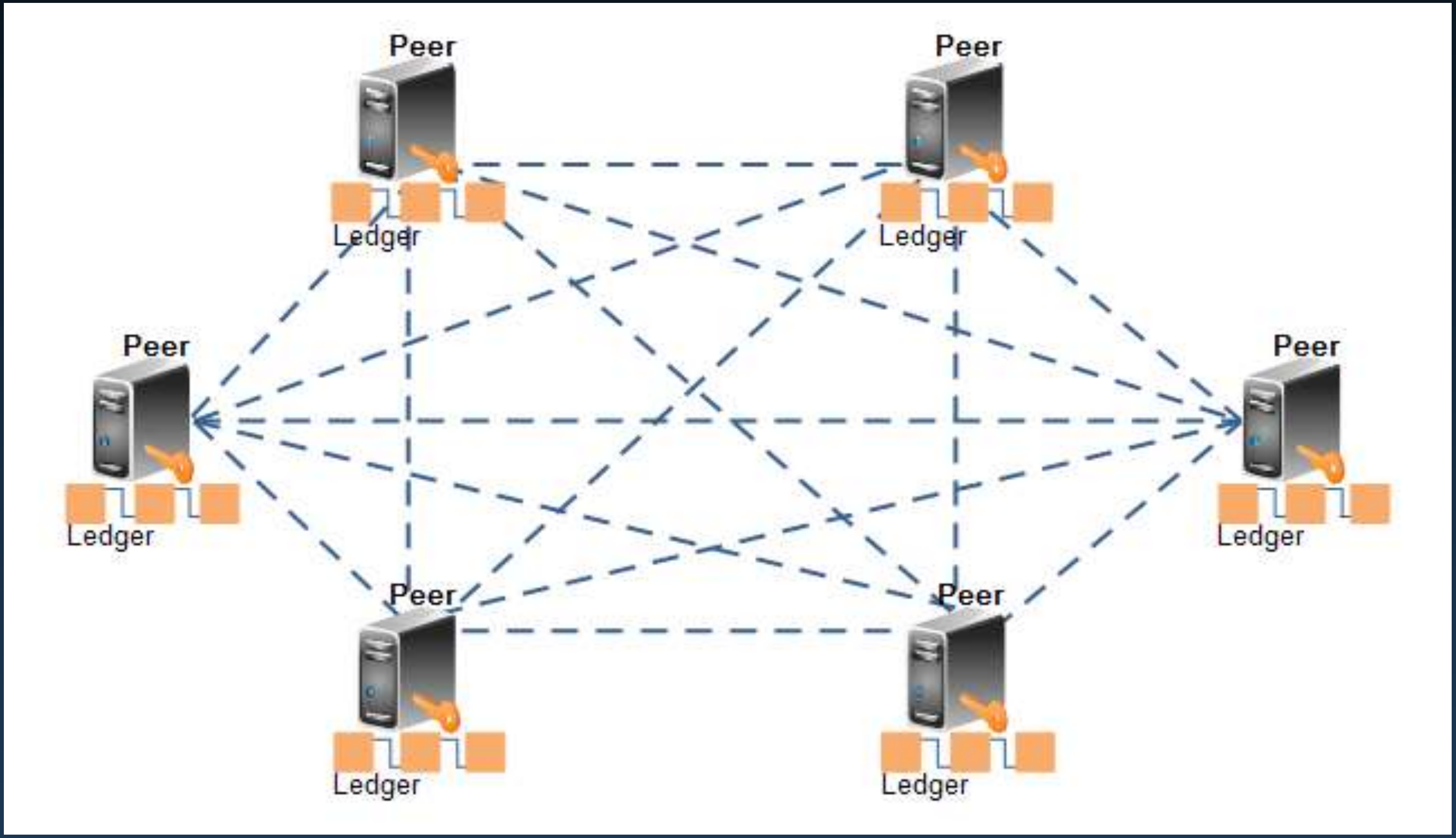
  Distributed system : Peer-To-Peer
  Security system : Cryptosystem
  (Cryptographie, Hashing)

- The two systems constitute the core of any blockchain platform. Many platforms was built since the emerging of this technology : Ethereum, Aion, Hyperledger Fabric, …

- A comprehensive list of platforms can be find in :

  https://www.technoduet.com/

Peer-To-Peer Network



Peer-To-Peer Model, Peer = Blockchain Ledger

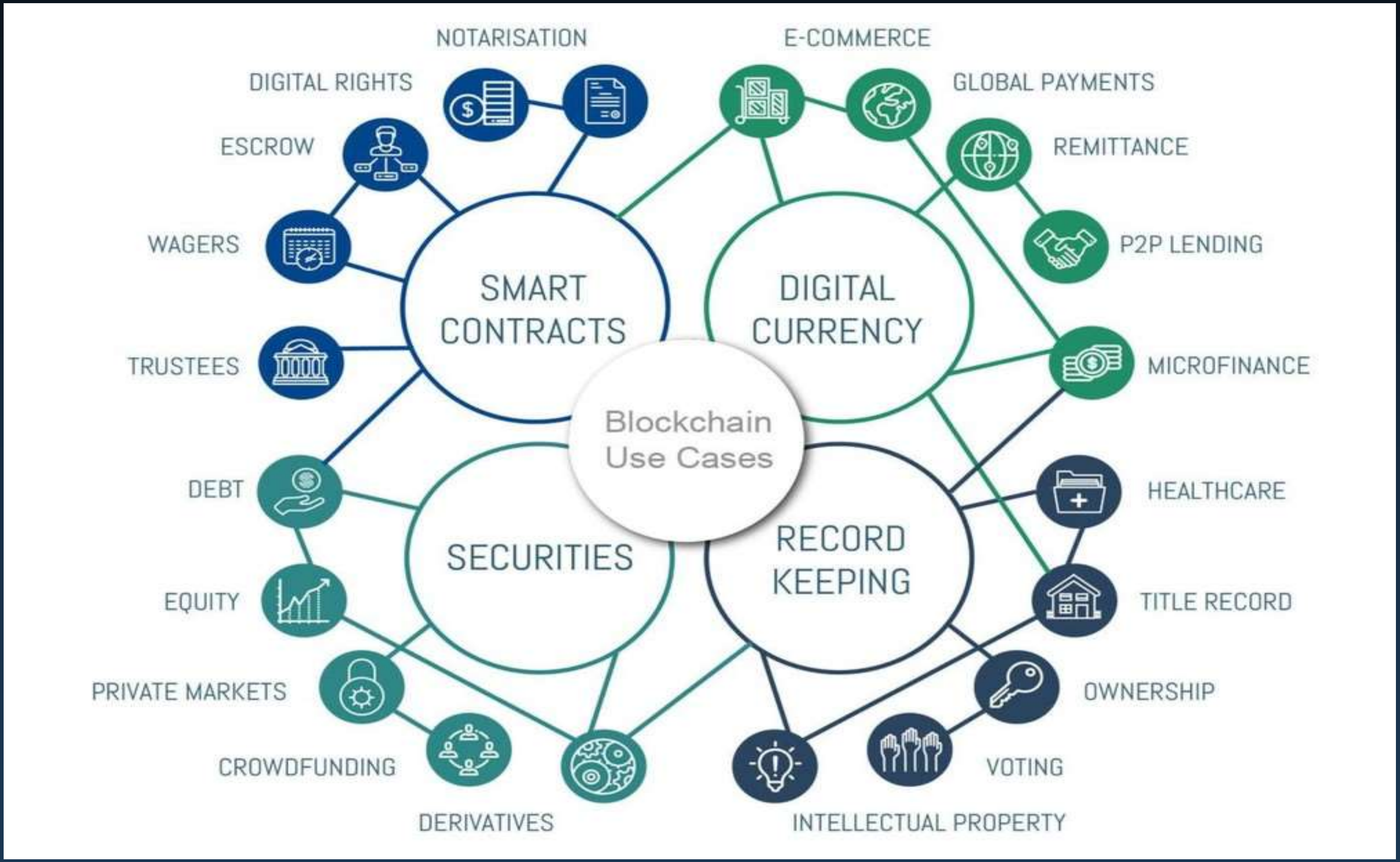
Cryptography

- Cryptography is the science of encryption whose objective is to preserve the confidentiality, the integrity, the Non-repudiation and the authenticity.

- According to encryption methods used, Cryptosystem can be :
  - Symmetric cryptosystem
  - Asymmetric cryptosystem (Public-key Cryptosystem)
  - Hash function cryptosystem

- Blockchain uses principally Hash function and Asymmetric cryptosystem.

Blockchain application



Some application areas of Blockchain