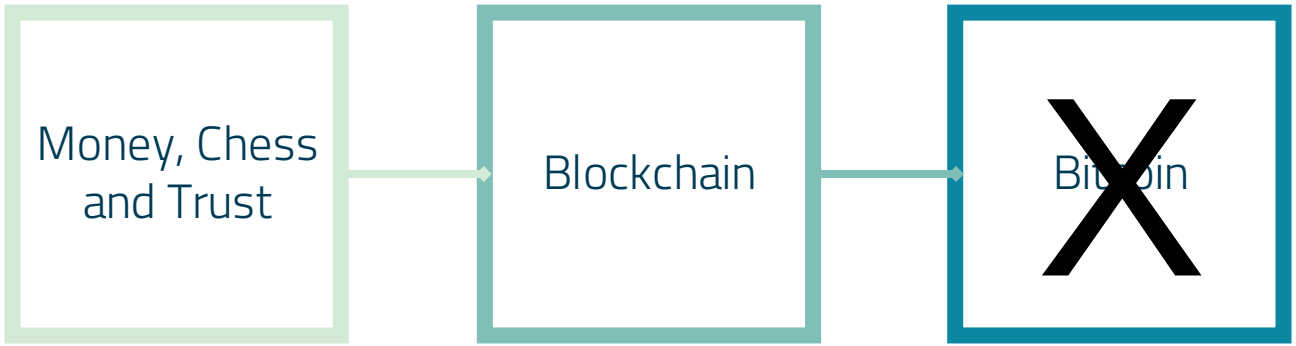
Blockchain

A Very Simple Introduction

Prof. Marco Comuzzi
Department of Industrial Engineering
Ulsan National Institute of Science and Technology (UNIST)
mcomuzzi@unist.ac.kr

bitcoin
ACCEPTED HERE

What's the plan for this lecture?



Marco Comuzzi mcomuzzi@unistac.kr

1.
MONEY, CHESS AND TRUST

Marco Comuzzi mcomuzzi@unistac.kr

Why shall we talk about money?

Understanding the design of different forms of money helps understanding what is blockchain

Mar

There used to be no money!

People exchanging goods/services that they believed have the same value

The fisherman and the butcher trust each other on the value of the meat and fish that they are exchanging

Marco Comuzzi mcomuzzi@unistac.kr

Commodity money

Coins made of precious metal used to exchange value.

Value of coins given by the value of the precious metal they are made of.

Everybody trusts the value of gold (scarce, hard to forge)

Where does the value of banknotes come from?

Money today

Money are notes/coins of intrinsic insignificant value.

Value is given to notes/coins by the state (government) that promises to accept these notes/coins from its citizens to pay taxes.

Let's sum up

Design

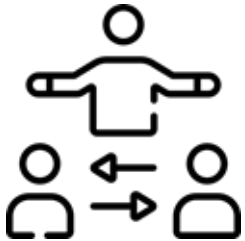
Money systems can be designed in different ways

Trust

Value of money is a matter of trust among agents exchanging goods and services

Intermediaries

Create the trust needed to give value to money
(ex. nation states)



Marco Comuzzi mcomuzzi@unistac.kr

Alice and Bob play chess on the Internet

They want to be able to disconnect and resume a game at any time

How can we design a system to support them?

How can such a system prevent that, while one player is offline, the other does not cheat?

Marco Comuzzi mcomuzzi@unistac.kr

A gaming platform!

Gaming Web site

A central server stores the state of all games

Players can disconnect and reconnect at any time, retrieve the state of their game, and keep playing

Good, but...

Web site is a single point of failure - what happens if the server is down?

Can the players trust the Web site?


TRUST

What if we could **design** a technology that

creates the **trust** needed by

a system and its users to operate well,

without the need for any **intermediary**?

Marco Comuzzi mcomuzzi@unistac.kr

Understand blockchain designing a “blockchain version” of the chess game

2.
BLOCKCHAIN

Creating trust in a trustless world

Marco Comuzzi mcomuzzi@unistac.kr

What is blockchain?

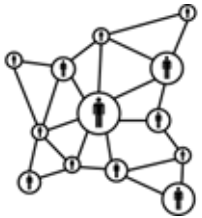
- The technology behind Bitcoin
- A technology that can create by design the trust required by a set of agents to exchange information and value
  - money, moves in a chess game,... anything!

OK, but … what is blockchain?

Network

A set of nodes (peers) connected to each other on the Internet

[peer-to-peer network]



Data structure

A database replicated on each node of the network

[distributed ledger]

Protocol

A set of rules for nodes to agree on the content of the database

[consensus mechanism]

Marco Comuzzi mcomuzzi@unistac.kr

Immutable database

Data can only be added to the database

Existing data **cannot** be modified

Existing data **cannot** be deleted

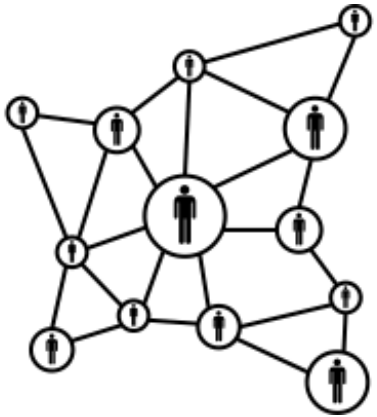
Marco Comuzzi mcomuzzi@unistac.kr

Now, let's play chess again … with blockchain

- Instead of using a gaming platform, let's try to use a blockchain platform
  - A network of nodes
  - An immutable database
  - A protocol for nodes to agree on the content of the database at any time

A network of nodes...easy

- Each player is a node
- No other intermediary node



Marco Comuzzi mcomuzzi@unistac.kr

An immutable database

- Records the initial state
  - Always the same for any game
- Records all the moves of both players

A protocol to agree on the content of the database

- Let Alice and Bob agree on the initial state of the game
- "To be recorded, a move proposed by a player must be approved by the other player"
- We may also call this a **"consensus mechanism"**

Marco Comuzzi mcomuzzi@unistac.kr

A protocol to agree on the content of the database – why?

- "To be recorded, a move proposed by a player must be approved by the other player"
- Players do not have any incentive to submit moves that violate the rules of chess
  - The other player will simply never approve them

Marco Comuzzi mcomuzzi@unistac.kr

Replaying all the moves any node can reconstruct the current state of the system

Fig. 3.6 – Distributed immutable ledger example in the BC4C system

Content of the ledger (transactions)

Transaction id	Transaction	Originator	Timestamp
0	Genesis of BC4C	BC4C	22-04-19 12:00:17
1	CreateNewGame[AliceCarol1, Carol]	Alice	22-04-20 09:00:03
2	CreateNewGame[BobCarol1, Carol]	Bob	22-04-20 09:00:45
3	ConfirmGameCreation[BobCarol1]	Carol	22-04-20 09:01:23
4	ConfirmGameCreation[AliceCarol1]	Carol	22-04-20 09:01:28
5	Move[BobCarol1, 1, pawn_h2, h3, false]	Bob	22-04-20 09:02:34
6	CreateNewGame[DaveAlice1, Alice]	Dave	22-04-20 09:02:48
7	Move[AliceCarol1, 1, pawn_d2, d4, false]	Alice	22-04-20 09:03:01
8	ConfirmMove[AliceCarol1, 1]	Carol	22-04-20 09:03:55
9	Move[AliceCarol, 2, pawn_a2, a3, false]	Carol	22-04-20 09:04:26

State of the System (games currently playing)

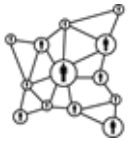
AliceCarol1

BobCarol1

Marco Comuzzi mcomuzzi@unistac.kr

What have we done?

- We have created a system to play chess…
  - … in which players can trust each other
  - … without the need for any intermediary
- Players can disconnect at any time and resume games
  - Replay all the moves stored in the database



Marco Comuzzi mcomuzzi@unistac.kr

Let's sum up … again

Trust

Effective collaboration among agents who want to play a game online (or more generally, exchange information and value) relies on trust among them

Intermediaries

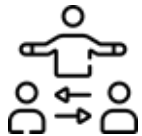
Can help to create trust, but they can also be a problem.

Are they reliable?

Can we trust them?

Design

Trust can be achieved to different levels by different design choices



Marco Comuzzi mcomuzzi@unistac.kr


HEY
WAIT A MINUTE
makeameme.org

You forgot to explain something ....

Immutable database

How can we really build a database that is immutable?

Identity of nodes

How can Bob trust that he is really playing with Alice, and not somebody else pretending to be her?

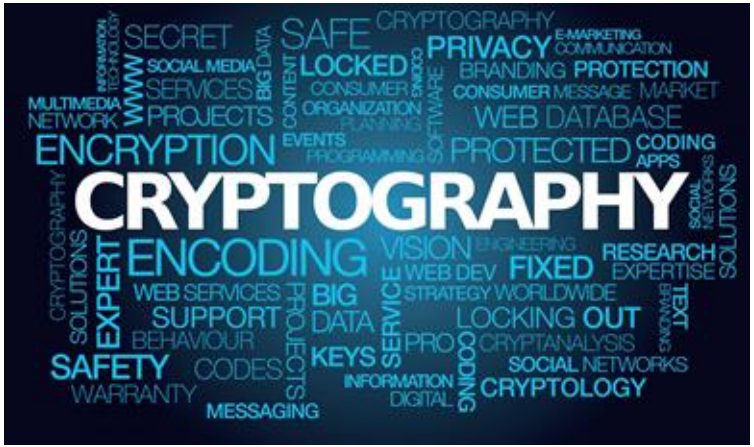
Additional “crypto” ingredients to the blockchain recipe

Cryptographic Hashing

To create an immutable database

Digital Signatures

To verify identity of users



Marco Comuzzi mcomuzzi@unistac.kr

Cryptographic hashing

Fixed output size

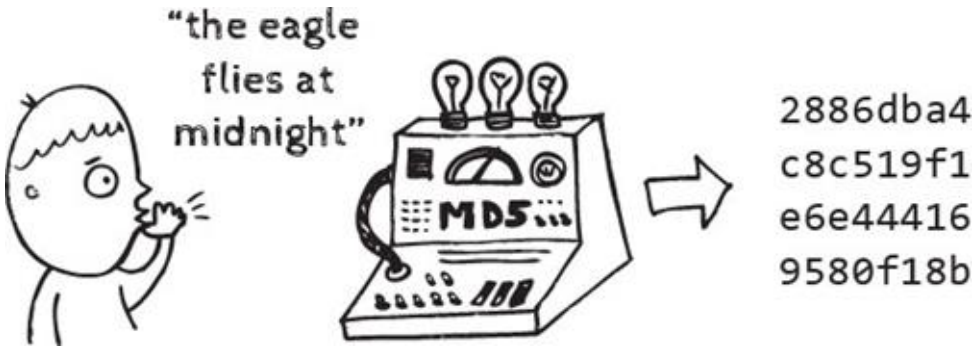
Size of hash is fixed, no matter how big or small is the input.

Unique output

Two different inputs never map to the same hash value

Impossible to invert

Given the hash, it is impossible to reconstruct the input



Marco Comuzzi mcomuzzi@unistac.kr

Hashing to build a **blockchain**

Information in the database is stored into blocks

A block contains the hash of the previous block

Forming an immutable chain of blocks

Marco Comuzzi mcomuzzi@unistac.kr

Identity of nodes

A gaming platform will ask all users to login with a username and password to identify themselves

What about identity verification in the blockchain version?

Managing identity of the players

Instead of logging in with username and password, every node will “digitally sign” all the messages (moves, etc.) sent to other nodes of the blockchain network

Marco Comuzzi mcomuzzi@unistac.kr

Digital signature

Extension of hashing that allows a person to sign a digital message

Allows to verify the identity of the signer

Prevents the signer to repudiate having sent the message

To sum up … what is blockchain?

Network

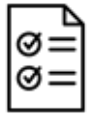
[peer-to-peer network]

Data structure

[distributed ledger]

Protocol

[consensus mechanism].



Hashing

[Immutability of ledger]

Digital signatures

[identity of nodes]

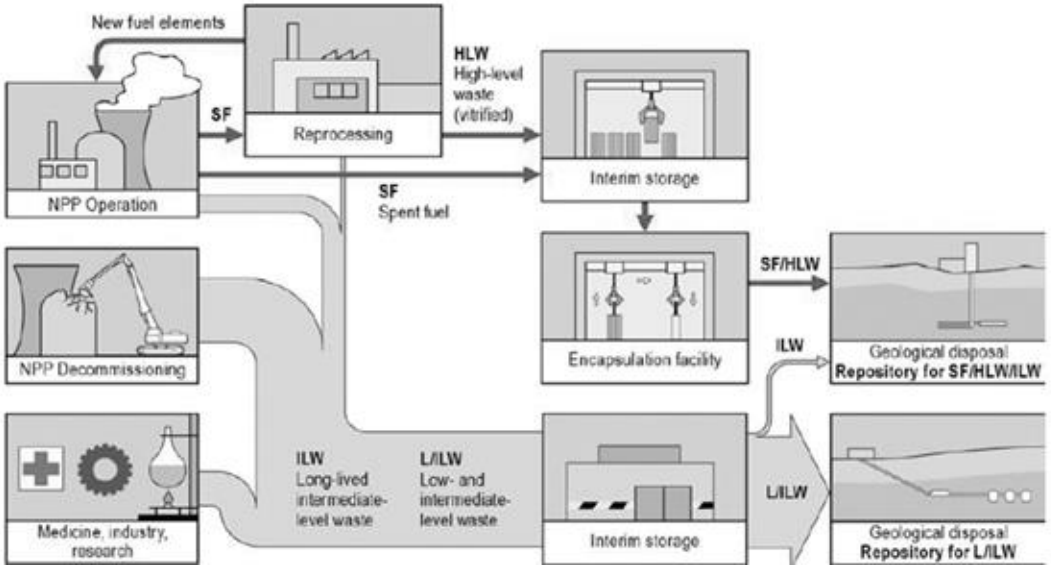
Marco Comuzzi mcomuzzi@unistac.kr

What are the applications of blockchain today?

Marco Comuzzi mcomuzzi@unistac.kr

Marco Comuzzi mcomuzzi@unistac.kr

Blockchain for radioactive waste management



Marco Comuzzi mcomuzzi@unistac.kr

THANKS!

https://sites.google.com/site/marcocomuzziphd

http://iel.unist.ac.kr/

You can find me at:

@dr_bsad

mcomuzzi@unist.ac.kr