unic.ac.cy/iff

AI techniques to identify bitcoin trail

Prof. Soulla Louca

Director, Institute For the Future (IFF)
University of Nicosia

louca.s@unic.ac.cy


Voyage

Who we are

University of Nicosia

Institute For the Future & Blockchain Initiative

(IFF)

University of Nicosia

excellence.in.education.

The University of Nicosia is the culmination of an ongoing journey which began over 30 years ago. Today, the University of Nicosia is the leading university in Cyprus - in line with our enduring motto: “Excellence in Education”.

Unique Location

Located in Nicosia, the capital of Cyprus

Global Education Centre

At the cross-roads of three continents, the university has become a global education centre

Multicultural Learning Environment

Hosts students from all over the world, in a multicultural learning environment

Our Research

Involved in European and local research projects as partner as well as coordinating institution

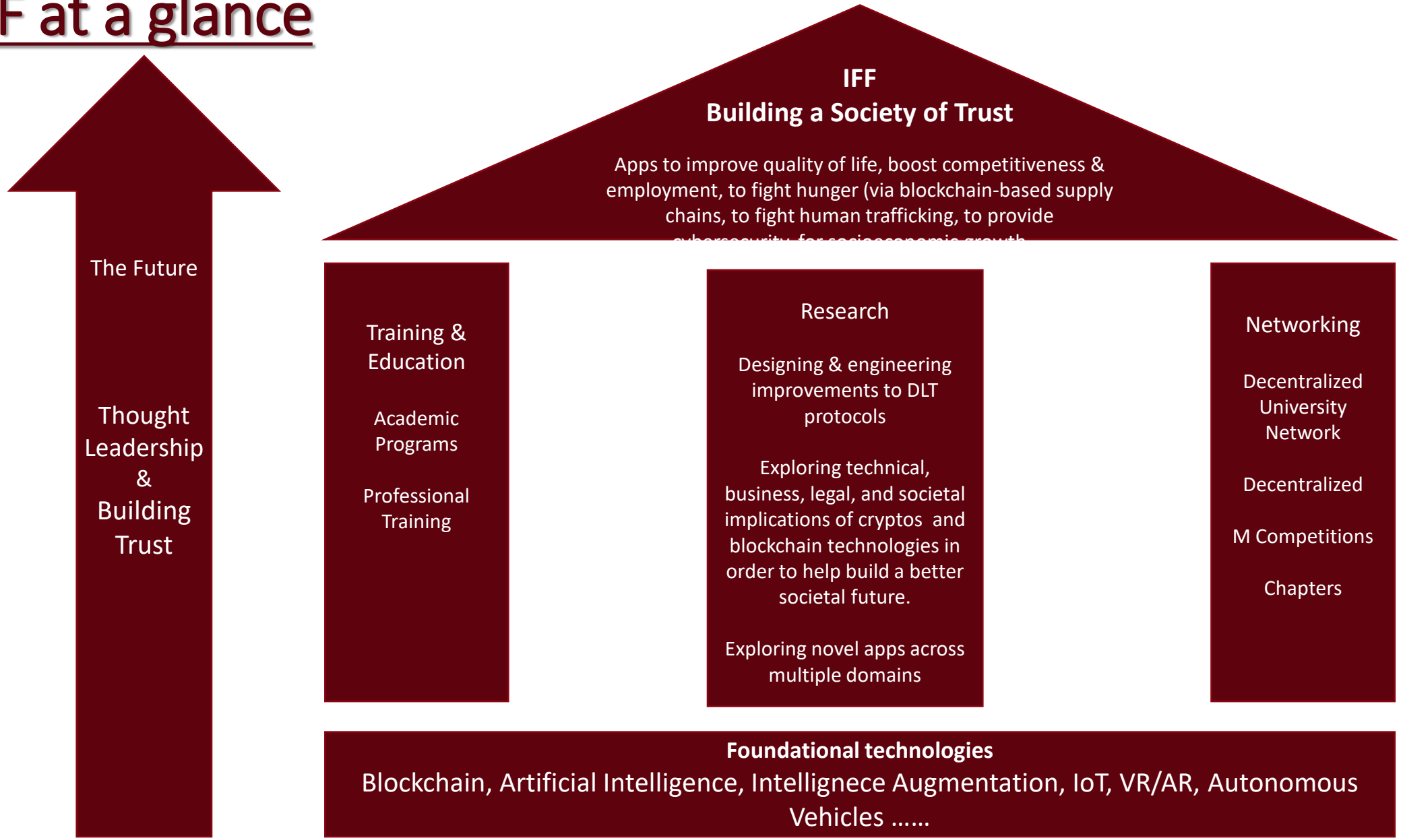
Erasmus University Charter

Erasmus University Charter and participant in the European Credit Transfer System (ECTS)

Community Involvement

Involved in the community (e.g. environmental protection and fighting world hunger)

IFF at a glance



Activity timeline

2013

- Bitcoin acceptance
  - **1st in the world**

2014

- Launch blockchain MOOC & MSc degree
  - **1st in the world**

2015

- Publish MOOC certificates on the blockchain
  - **1st in the world**

2016

- First MSc graduates
- Launch *Blockchain Research Center*

2017

- All UNIC Diplomas on the Blockchain
  - **1st in the world**
- Launch *Institute For the Future (IFF)*
- Decentralized 2017
  - 500+ attendees, 20 countries

2018

- "*Biggest Contributor in the Rise of Blockchain*" Award
- Decentralized 2018
  - 1,200+ attendees, 39 countries
- M4 competition & conference
  - 100,000 datasets, 200+ research teams
- Launch block.co

Our people: IFF Governing Board

Antonis Polemitis
UNIC CEO

Dimitris Drikakis
UNIC VP of
Global Partnerships

George Giaglis
IFF Director

Soulla Louca
IFF Director

Spyros Makridakis
IFF Director

Marinos Themistocleous
IFF Director

Our people: IFF Researchers & Staff


Dr Klitos Christodoulou


Dr Elias Iosif


Dr Charis Savvides


Dr Ifigenia Georgiou


Dr Ioannis Katakis


Dr Konstantinos Karasavvas


Dr Ariana Polyviou


Jeff Bandman

Andreas Vlachos


Kypros Stefanou


Valentinos Theofilou


Irene Patrikios


Nick Assimenos


Sokratis Mina


Elena Kontemeniotis


Maria Charalambous

Our people: Visiting Scholars

Andreas Antonopoulos

Prof Nassim Nicholas Taleb

Stefan Loesch

Adam Hayes

Dr Theodosis Mourouzis

Athanasios Leontaris

Apostolos Kourtis

Yiannis Menelaou

Mark Toohey

Blockchain & Cryptocurrencies

Setting the Scene

Blockchain -An Introduction

The Origin

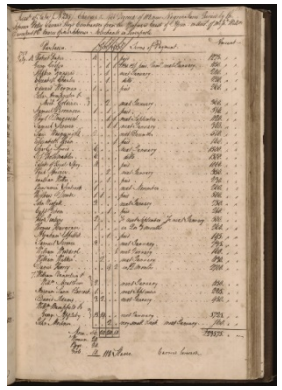
Blockchain was introduced, in 2008, as the technology underlying Bitcoin, the platform and cryptocurrency that has gained immense popularity due to the upward trend in the value of bitcoins.

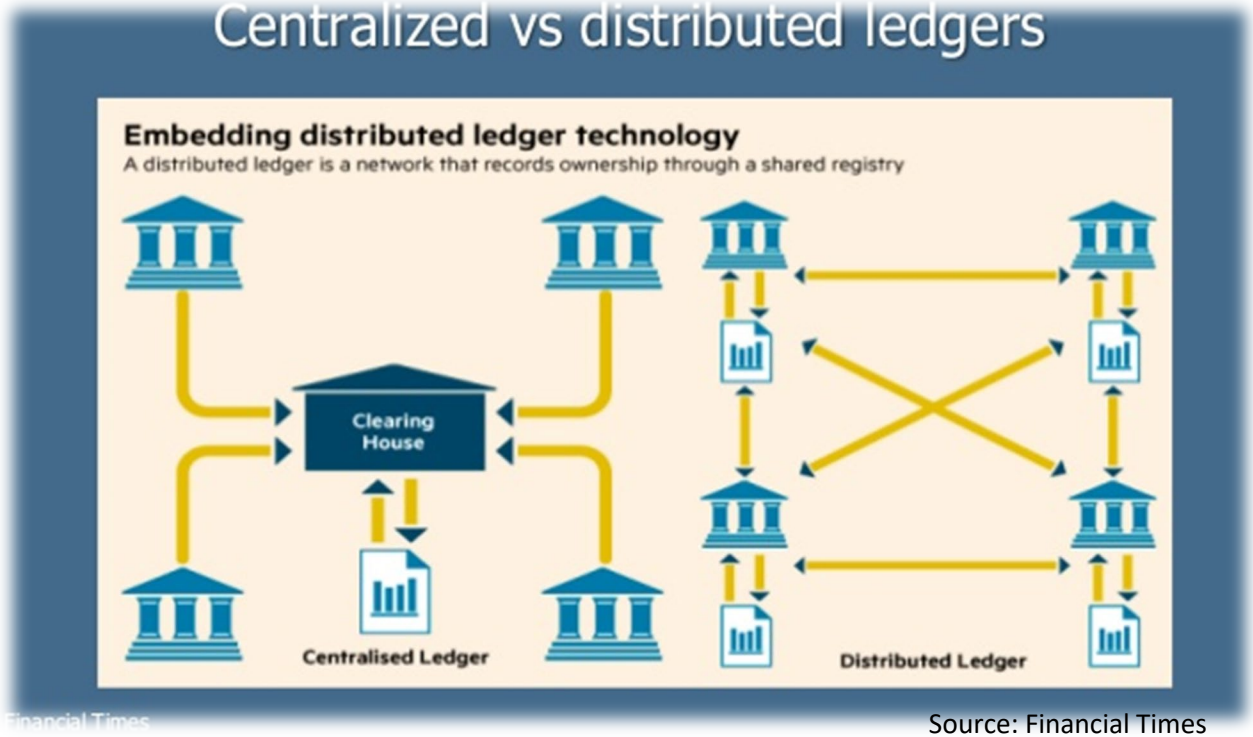
The Potential

Despite it being invented to support Bitcoin, important stakeholders from various industries recognized its potential and started exploring applications of the technology to either improve current practices, or create news one that were not possible until now.

Blockchain -An Introduction

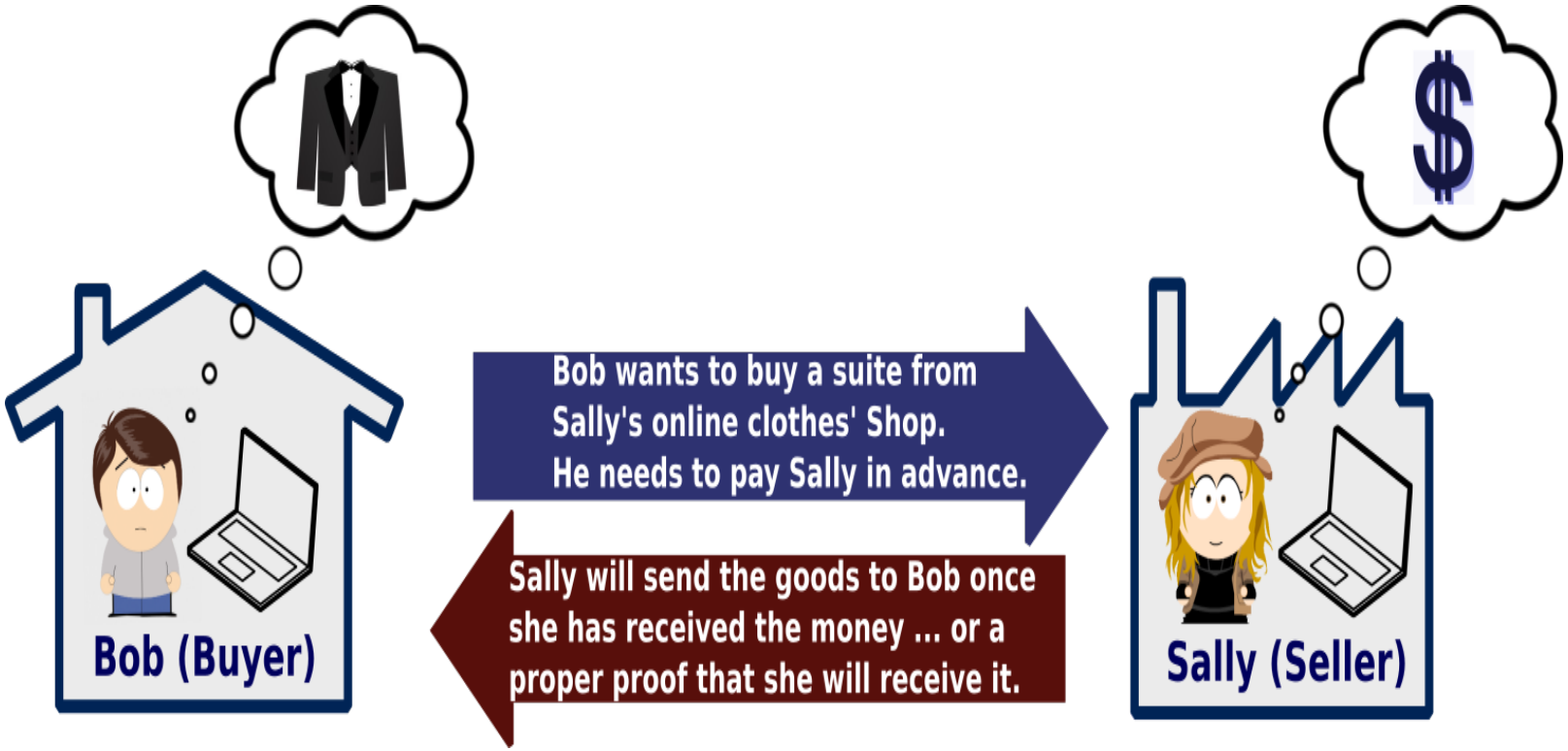
- A distributed ledger of any type of transactions;
  - Transactions – exchange of data that represent medical data, consumer details, product data….
  - A decentralized network for peer-to-peer transactions, **without the need for a central/trusted/third party;**
  - Once added to the rest of the chain, the records cannot be modified;
  - Transactions are timestamped





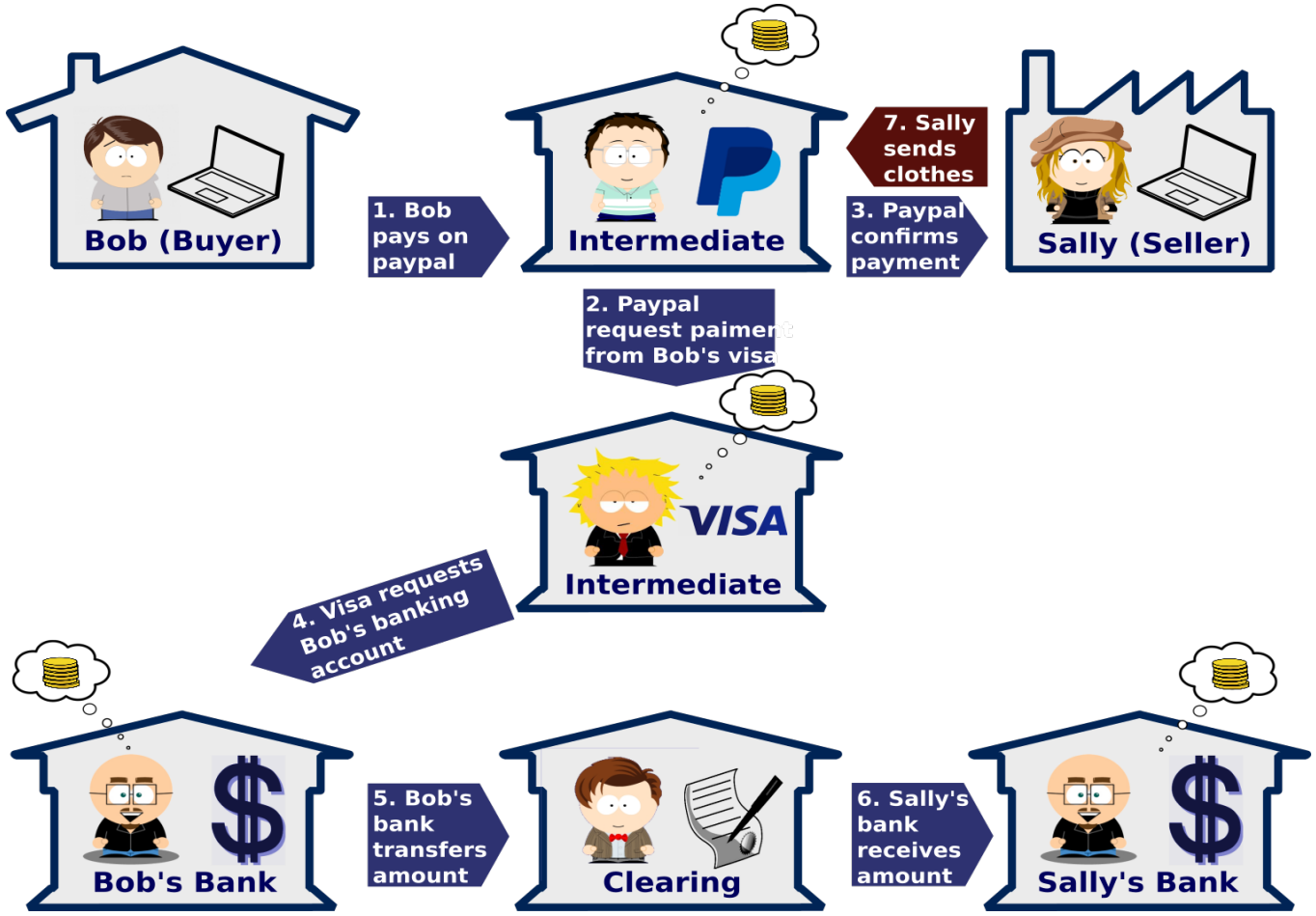
Source: Financial Times

Blockchain -An Introduction



Example (source: https://www.niceideas.ch/roller2/badtrash/entry/blockchain-explained-beta)

Blockchain -An Introduction



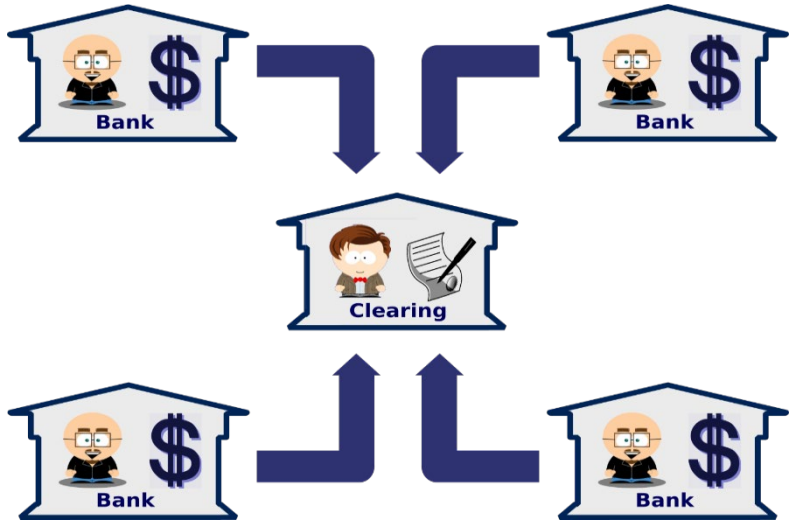
Problem: Lots of intermediaries ; (credit cards -e.g. Mastercard, Visa etc., Clearinghouses, Banks, etc.)

Reason for problem: Need to establish trust between two parties who do not know each other.

Blockchain -An Introduction

This centralized process causes problems such as:

- ***Inefficiency*** – Slow transaction settlements;
- ***High costs*** – Not only these third parties need to get paid, but potential disputes need additional costs to be covered for such as insurance provision;
- ***Lack of transparency*** - Not all stakeholders have access to information relevant to them;
- ***Fraud and errors*** – May lead to bad decision making and missed opportunities;
- ***Delays*** - in transactions;
- ***Unfairness*** - The bank actually owns the accounts and funds can be garnished, even frozen completely or being cut...;
- Etc. ...

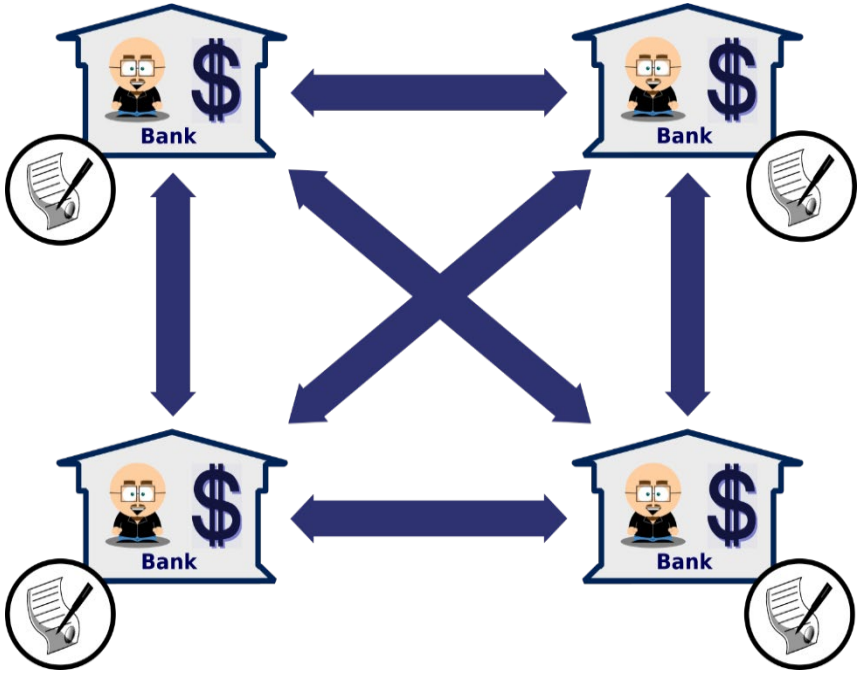


Blockchain -An Introduction

- **Blockchains** eliminate the need of the central ledger;
- Consist of blocks that hold batches of valid transactions;
- Can be open, verifying **anonymous (?)** actors in the network;

or

- they can be closed and require actors in the network to be identified;

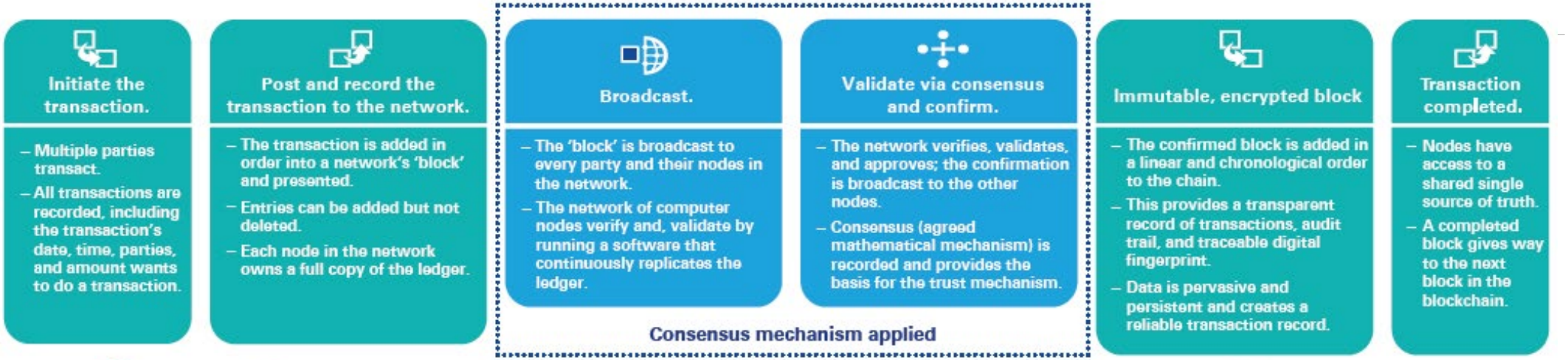


Blockchain -An Introduction

The Blocks

- Each block includes the hash of the prior block in the blockchain, linking the two. The linked blocks form a chain.
- Once a transaction/record is added to the of chain, they cannot be modified;
- Transactions are validated by the network participants and recorded in chronological order (in a sequence of "blocks");
- Transactions are protected by one-way cryptographic functions ➔ secure;

Blockchain -An Introduction



Source: **The process of the blockchain technology (KPMG)**

Blockchain -An Introduction

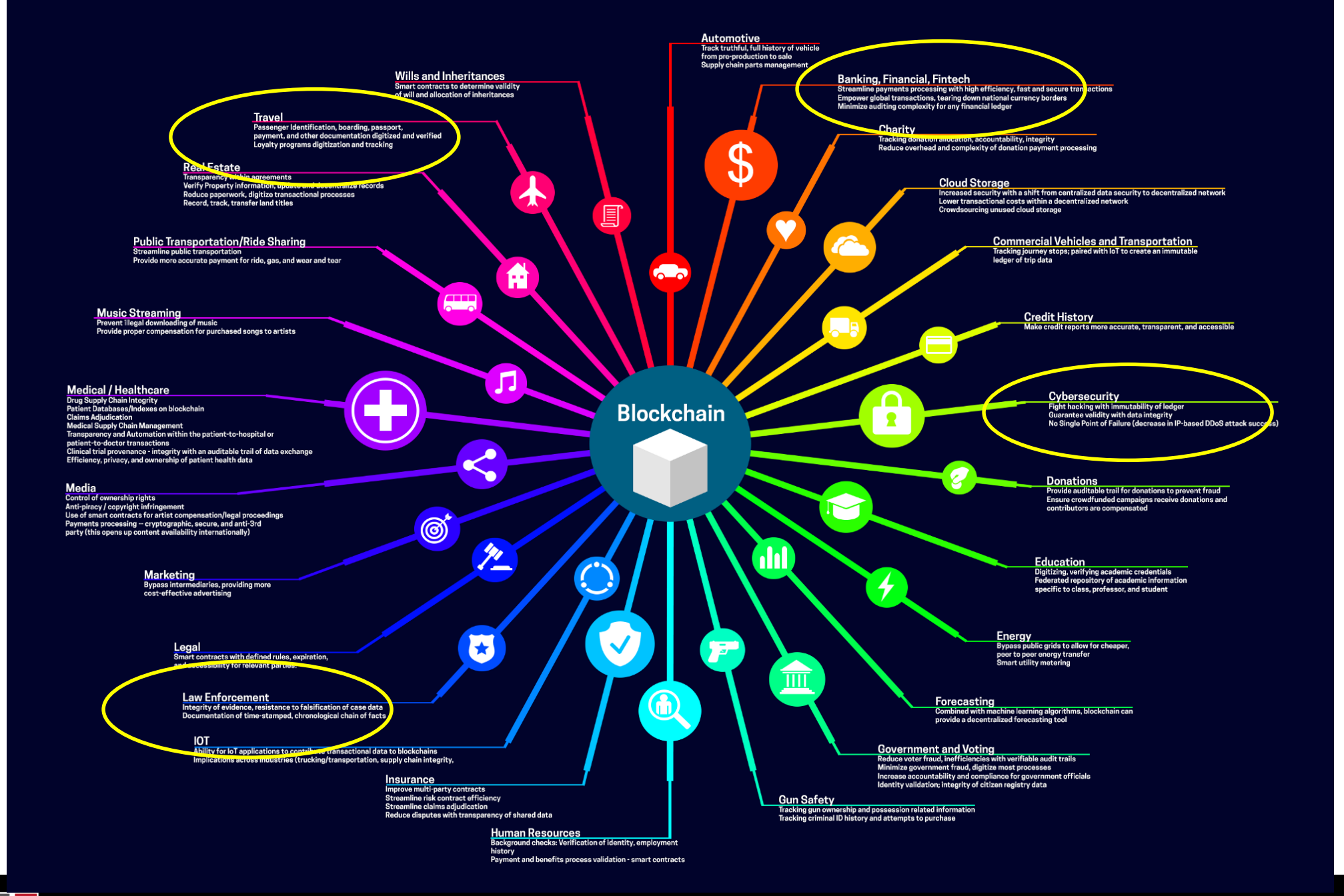
Source: https://www.i-scoop.eu/blockchain-distributed-ledger-technology/

Blockchain -An Introduction

Blockchain and Smart Contracts

- Blockchain can also be programmed; (such as if-else and if-then statements to ensure that certain conditions are met);
  - e.g., When a visa is overstayed the authorities are notified.
  - Or if someone tries to take employment outside of their visa terms, again the correct persons can be notified and action taken automatically.
  - Etc. ...

Source : http://blog.cryptoiq.ca/?p=380



A growing list of use cases

Blockchain & Human Trafficking

Blockchain is a: secure, decentralized, immutable, traceable database technology

- Blockchain by its self cannot end human trafficking
- BUT
  - It can prevent it in many cases;
  - it can make it easier to prosecute criminals of human trafficking;
  - It can make it easier to trace victims;
  - It can also make it easier to repatriated and reunite those affected by human trafficking;

Challenges in human trafficking where blockchain can assist

- Identification: 1.5B people, representing ⅕of the world's population, do not have proper legal identification (World Bank)

- Problem of the "invisible" children: children under the age of five and who do not possess a birth certificate are at "risk" and can fall into the hands of child traffickers. These children are often missed by social programs offered by governments or development agencies.

  - **Storing digital identities** on a blockchain provides a higher chance of catching traffickers;
  - **Securing identity data on an immutable ledger** will make trafficking attempts "more traceable and preventable";
  - **Can prevent the use of fake identification** documents to transport young people across borders for eventual forced participation in serious illicit activities including the sex trade, the illegal human organ trade, ….;

AI techniques to identify bitcoin trail

"Our challenge is that technology is taking slavery into a darker corner of the world where law enforcement techniques and capabilities are not as strong as they are offline," BUT "it can also be a fantastic tool for law enforcement";

Rob Wainwright – Head of Interpol

- **Integration of blockchain, AI, and machine learning:**
  - To enable algorithms for detecting suspicious transaction patterns;

Cryptocurrencies: Bitcoin

- ***Bitcoin is a <u>private</u>, <u>decentralized</u>, <u>digital</u> <u>cryptocurrency</u>***
  - **Decentralized**: No issuing party; units are issued algorithmically
  - **Digital**: Fully electronic; with no underlying peg to assets
  - **Cryptocurrency**: Anti-counterfeiting through cryptography

Can we deanonymize Bitcoin?

- **In a way, Yes we can!**
- **Is it possible to infer patterns from transactions?**
  - **Yes… Inferring spending patterns is one way to reveal personal facts with regards to the transacting entity.**
- **How does this happens in reality?**
  - Some people share their address publicly.
  - The exchange you bought your bitcoin from has both your identity and your addresses.
  - Merchants you pay can make the association.

Privacy on the Blockchain

- **Fact 1:** Bitcoin is *pseudonymous* and *fully traceable*.
  - Every transaction in Bitcoin maps inputs to outputs, allowing anyone to follow the flow of such transactions.
  - Bitcoin's transactions are tracked on the Blockchain permanently.

- **Fact 2:** If someone can elicit information that links your identity to your bitcoin address, they can learn a ton about you.

Why do we care?

- There is evidence that Bitcoin fuels Human Trafficking Markets

Facts & Figures

- At any given time in 2016, an estimated 40.3 million people are in modern slavery, including 24.9 million in forced labour and 15.4 million in forced marriage.
- It means there are 5.4 victims of modern slavery for every 1,000 people in the world.
- 1 in 4 victims of modern slavery are children.

http://www.ilo.org/global/topics/forced-labour/lang--en/index.htm

Why do we care?

Facts & Figures

- Bitcoins are untraceable digital currency.
- Bitcoin is appealing to human traffickers, drug pushers and arms dealers who operate in the illicit markets.
- Increase use of cryptocurrencies for money laundering
- Lack of transparency in bitcoin interactions
  - helped exploit the growing illicit markets
  - Challenge for law enforcement when trying to rescue trafficking victims and prosecute traffickers.

http://www.ilo.org/global/topics/forced-labour/lang--en/index.htm

However… traces on the Blockchain

- Reveal data from the address re-use
- From linking transactions with a single profile
- IP address reuse when transacting
  - This could provide a hit to people that someone is using multiple addresses

- Combining inputs from multiple transactions, revealing the contours of addresses you control.
- Using light clients, effectively revealing to a third party your full set of addresses.

Can we exploit data from the Blockchain to reveal Identities?

- ***Our Thesis:*** *Data from the Bitcoin Blockchain transactions could be leveraged to reveal data insight that could lead to Identity Discovery.*

- We argue that ownership of arbitrary data and identity discovery can be made possible by:
  - observing patterns from the data that are injected on the blockchain
  - and link such addresses to real entities.

Experiments: methodology and data

- **Methodology**
  - Step 1: Install Bitcoin blockchain
  - Step 2: Collect transactions recorded into the blockchain
  - Step 3: Extract metadata from collected transactions
  - Step 4: Compute features from extracted metadata
  - Step 5: Train AI algorithms using the features of Step 4
- **Experimental dataset**

Number of transactions	38985
Number of entities behind transactions	23

- **Purpose of extracted features**
  - To capture patterns in metadata & utilized for training AI algorithms

Experiments: experimental task & evaluation metric

- Experimental task
  - **Input:** a transaction made between two entities of unknown identity
    - Example: person X send crypto-currencies to person Y
  - **Output:** identify the entities involved in transactions
    - Example: identify X and Y
- Several AI algorithms used
- Evaluation metric
  - **Accuracy:** percentage of correct identifications
- Baseline performance
  - **Random guess:** no employment of AI
  - For comparison purposes: compare against AI

Experiments: evaluation results

- Summary of main results

Approach	Performance
Random guess	12.99% accuracy
AI algorithm	99.98% accuracy

- Excellent performance: 99.98% accuracy
  - Outperforms random guess (12.99% accuracy)
- This performance was verified through the use of various AI algorithms
  - From traditional AI approaches to recent state-of-the-art algorithms

Experiments: conclusions & future work

- **Conclusions**
  - Bitcoin blockchain are **pseudo-anonymous**
  - AI (as well as other algorithmic approaches) can be **utilized for discovering** the identity of entities involved in blockchain-based transactions
  - AI itself does not solve all challenges: to be used in combination with other sources of intelligence, e.g., human intelligence
- **Future work**
  - Integration with specific applications (e.g., illegal blockchain-based payments) in collaboration with appropriate authorities (e.g., Interpol)
- **Related publication**
  - *Klitos Christodoulou, Elias Iosif, Soulla Louca, and Marinos Themistocleous.* ***"Identity Discovery in Bitcoin Blockchain: Leveraging Transactions Metadata via Supervised Learning"****, International Conference on Big Data and Blockchain, Vancouver, Canada, August 23-25, 2019*

UNIVERSITY of NICOSIA

Institute For the Future

blockchain.initiative.

Thank You!

Other References

- https://humantraffickingsearch.org/bitcoin-fuels-the-human-trafficking-market/
- https://www.21cryptos.com/us-bill-to-study-impact-of-cryptocurrency-on-sex-and-drug-trafficking/
- https://www.ey.com/en_gl/banking-capital-markets/how-to-bring-cryptocurrencies-into-the-light
- https://www.unodc.org/unodc/en/drug-trafficking/crimjust/news/unodc-delivers-the-first-cryptocurrency-investigation-training-course-in-latin-america.html