

unic.ac.cy/iff

Blockchain 101

Prof. Soulla Louca

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

louca.s@unic.ac.cy



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

✓ М н₀

Multicultural Learning Environment Hosts students <u>from all over the</u>

world, in a multicultural learning environment

Erasmus University Charter

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

Global Education Centre

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

Our Research

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

Community Involvement

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





IFF at a Glance

The Institute For the Future (IFF) is a cross-disciplinary research institute at the University of Nicosia (UNIC) founded to explore the hypothesis that exponential technologies will cause rapidly accelerating societal change over the coming decades.



IFF at a glance

IFF

Building a Society of Trust

Apps to improve quality of life, boost competitiveness & employment, to fight hunger (via blockchain-based supply chains, to fight human trafficking, to provide cybersecurity, for socioeconomic growth....

The Future

Thought Leadership & Building Trust



Academic Programs

Professional Training



societal future. Exploring novel apps across multiple domains <u>Community</u> <u>Building</u>

Decentralized University Network

Decentralized

M Competitions

Chapters

Foundational technologies Blockchain, Artificial Intelligence, Intelligence Augmentation, IoT, VR/AR, Autonomous Vehicles



Activity timeline





IFF in numbers

- Largest student community in the world
 - 40,000 MOOC participants from 90+ countries.
 - 550+ MSc students and graduates from 76 countries, including USA (19%), UK (6%), Canada (5%), South Africa (4%), Brazil (3%), India (2%) and Australia (2%).

• Accelerating research track record:

- €5m in competitive European Commission research grants since 2017.
- Member of the Austrian Blockchain Center (€17m consortium, funded by the Austrian government)

- Respected business & academic community organizer:
 - Three annual Decentralized conferences with speakers including: Llew Claasen (*Director*, *Bitcoin Foundation*), Roger Ver (*CEO*, *Bitcoin.com*), Eva Kaili (*MEP*), Garrick Hileman (*Head of Research at Blockchain.com & Cambridge University*), etc.
 - Growing base of local Decentralized chapters: Nicosia, New York City, Mexico City, California, Amsterdam, Nigeria, Malta, Dubai, London, Thessaloniki, Brussels, Tokyo.
- Strong team and partners:
 - 8 full-time faculty and 15 affiliate faculty members within UNIC
 - 30+ resident and visiting researchers
 - 40+ university and industry partners
 - One commercial spin-off



Leaders in blockchain research

Project	Budget	Funding by	Duration	IFF role
DLT4ALL	€1m	EC (Erasmus+)	3 years	Coordinator
EUNOMIA	€2.4m	EC (H2020)	3 years	Partner
BLOCKPOOL.EU	€1.5m	EC (H2020)	2 years	Partner
ABC	€17m	Austrian govt	4 years	Partner
PARITY	7.2m	EC(H2020)	3.5 years	Partner
Direct industry funding	€1m	Ripple, trade.io, PumaPay, etc.	Various	Main/sole partner





Leaders in blockchain education

The Global Universities Embracing Cryptocurrency

#1 University of Nicosia

#2 University of Cumbria
#3 Simon Fraser University
#4 MIT
#5 New York University
#6 Duke University
#7 McGill University
#8 Pompeu Fabra University
#9 Imperial College

Source: Coindesk, 2015

Top 5 University Bitcoin Courses

#1 University of Nicosia

#2 New York University#3 Stanford University#4 Princeton#5 Duke University

Source: The Merkle, 2017





Education

- 1. Massive Online Open Course (MOOC)
- 2. MSc in Digital Currency
- 3. Blockchain Professional Certificates
- 4. Blockchain Training Series

The Massive Online Open Course (MOOC) Introduction to Digital Currencies

The first MOOC on cryptocurrency with currently more than 40,000 enrolled students from over 85 countries, with a majority of students from:





Academic Programs

Master's in Digital Currency & Blockchain Technologies

- The World's First Master's Degree in Blockchain
 - Taught by Leading Faculty and Practitioners
 - 600+ Students Enrolled Since 2014
 - Over €300,000 in Scholarships Annually
- The program focusses on the fundamentals of blockchain technology
- It includes smart contracts and the associated architectures such as Ethereum
- It aims to prepare students on the possible impact of these technologies on various applications including those based on Artificial Intelligence, Machine Learning and Internet of Things.

Master's in Computer Science with Concentration on Blockchain Technologies

- The program focusses on the fundamentals of blockchain technology
- It includes smart contracts and the associated architectures such as Ethereum
- It aims to prepare students on the possible impact of these technologies on various applications including those based on Artificial Intelligence, Machine Learning and Internet of Things.



Blockchain Professional Certificates

leading the way in professional education

Certificate Courses:



Security Token Strategy

- Applied Forecasting: Improving the Accuracy and Value of Your Predictions
- Blockchain and Energy
- Blockchain and Cryptocurrencies

Become A Certified:

Blockchain Financial Analyst

6-week course: Open Financial Systems6-week course: Regulation and Digital Currencies6-week course: Blockchain Technology and Applications

Blockchain Business Analyst

6-week course: Regulation and Digital Currencies6-week course: Principles of Disruptive Innovation6-week course: Emerging Topics and Practical Considerationsin Blockchains

Blockchain Developer

6-week course: Blockchain Technology and Applications6-week course: Cryptographic Systems Security6-week course: Digital Currency Programming



Leaders in blockchain/AI community engagement

Decentralized 2019

30 Oct - 1 Nov 2019 Athens, Greece

- Europe's premier annual blockchain conference since 2017
- Bringing industry & academia together
- Pre- and post-conference events (**Decentralized Training Series**)
- Bottom-up community engagement (Decentralized Chapters)

M4 Conference 10-11 December 2018 Tribeca Rooftop, New York City

- Based on the results of the annual forecasting M-Competition
- 200+ research teams; 100,000 real-life time series analyzed
- In collaboration with NYU & Nassim
- Sponsored by Amazon and Uber
- NEXT YEAR M5...... STAY TUNED.....



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





f Dr Charis Savvides



Dr Ifigenia Georgiou Dr Ioannis Katakis



Dr Konstantinos

Karasavvas



Jeff Bandman



Valentinos Theofilou

Irene Patrikios



Nick Assimenos

Sokratis Mina



Elena Kontemeniotis



Maria Charalambous





Kristina Arapidou



Antonis Inglezakis



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



Introduction to Blockchain



The Evolution of Money and Beyond



https://steemit.com/steemit/@cryptomoni/6-stages-of-history-and-evolution-of-money

- **1. Barter** (no money)
- 2. Commodities / Precious metals (money from nature)
- **3. Printed money /coins** (money from institutions direct)
- 4. **Plastic money** (money from institutions indirect)
- 5. Cryptocurrencies/Network money (money as apps: borderless & unmediated) → Bitcoin



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.

Bitcoin is a <u>private</u>, <u>decentralized</u>, <u>digital cryptocurrency</u>

- Decentralized: No issuing party; units are issued algorithmically
- Digital: Fully electronic; with no underlying peg to assets
- Cryptocurrency: Anti-counterfeiting through cryptography





Some of Blockchain's Applications

Various Industries and Fields

Financial Services		Maritime and		
	E-marketing	Shipping	ID	
Accounting and Auditing	L-marketing	Governance		
	Retail and Supply		Digital scarcity	
Digital Rights Management	Management	Energy Management		
	Human Resource		Security	
Property Ownership	Management	Crowdfunding and Capital Raising		
	Education sector		Gamac	
	& digital CV		Games	





A Ledger

to

'e

ants

transact directly with each other

and

stores the history and state

of these transactions



Ledgers Rule our World

We take centralized ledgers (with trusted record-keepers) for granted because we have never before had a practical alternative







 If we let any untrusted party enter transactions in an important traditional ledger, chaos is likely to ensue (would you, for example, let strangers keep track of your checking account balance?)

 A trusted party is in charge of all ledgers of importance in modern society, whether it is Citibank for your bank account, or your local land registry office for the title deeds for your house



Blockchains change ledgers

- A successful decentralized ledger that allowed parties that did not know or trust each other to transact together would have a wide range of advantages. In fact, it practically sounds like a fairy tale in traditional terms:
 - Invulnerable to censorship and exclusion
 - Invulnerable to malfeasance by record-keepers
 - Invulnerable to loss of records





Bob wants to buy a suite from Sally's online clothes' Shop. He needs to pay Sally in advance.

Sally will send the goods to Bob once she has received the money ... or a proper proof that she will receive it.



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

Bob (Buyer)





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.

As a consequence → High transaction fees that WE pay



Other problems of this centralized process:

- *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;

UNIC | Institute For the Future

 Unfairness - The bank actually owns the accounts and funds can be garnished, even frozen completely or being cut...;





- **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;





Main idea: No central record of transactions;

- Many copies of the ledger are distributed around the world;
- Each owner of each copy records every transaction.

To buy something (or carry out any transaction) I give the shop details, the shop asks all the bookkeepers if am good for the money, the bookkeepers all check their records to see if I have enough – if I do, they tell the shop, and then all update their records to show the movement of money.

So, there's no way a forged transaction can make it in - if I try to alter a ledger, it wont match all of the other copies and it gets rejected. Oh, and one of them at random will be given a reward of some newly created cryptocurrency.



https://steemit.com/ledger/@crypt0k/centralized-anddecentralized-ledgers-do-you-know-the-difference



Solution behind Bitcoin: Blockchain

Some Definitions

<u>Hashing</u> - applying an algorithm to generate a value for some string of text using a mathematical function

- Every time you apply a hash to some data, you get the same hash value
- Hashes are one-way. If you have the data, you can find the hash. But, if you have the hash, you can't figure out the data
- Useful for verifying data



Mining -the way new Bitcoins are created

Miners publish blocks on the blockchain – As a reward for publishing blocks, they get to keep Bitcoins.

- **50** for the first 4 years, and halving every four years
- Miners also get transaction fees
- Race to find a conforming hash every 10 minutes
- miners try to solve a proof-of-work problem
- The first one to solve the problem publishes a "block" on the "blockchain" that includes all transactions from the last 10 minutes
- Reward is halved every 210,000 blocks (~every 4 years)
- ■Around year 2045 99.95% last one 2140 → 21 M



- A shared, time-stamped, appendonly, immutable, cryptographically secured ledger of any type of transactions;
 - Shared: blockchains do not make much sense unless two or more parties (or systems) are involved.
 - □ **Time-stamped:** transactions are stored in chronological order.
 - Append-only: you can only add new transactions to a blockchain.
 - Immutable: Once written, a transaction cannot be erased or altered.
 - Cryptographically-secured: advanced cryptography enables all the above

Centralized vs distributed ledgers





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 <u>by the network participants</u> and recorded in chronological order (in a sequence of "blocks");
- Transactions are protected by one-way cryptographic functions → secure;







Source: The process of the blockchain technology (KPMG)





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



Smart Contracts - 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);

Applications running on blockchains executing certain conditions



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



Smart contracts

A **smart contract** is a contractual agreement that is

implemented using software.



Unlike a traditional contract where parties may seek remedial action through the legal

system, a smart contract is self-enforced (possibly also self-

executed), depending on whether specific conditions, that

are monitored through software, are met.

"Smart contracts -automated programs that transfer digital assets within the block-chain upon certain triggering conditions."

-Joshua Fairfield

"The term smart contract can be so confusing. Really it is just a self-executing piece of code on a distributed ledger."

-Primavera De Filippi



Smart Contracts

- Automatically enforce power equality of all parties involved
- Protect an individual's rights by enforcing reasonable expectations for the signee
- Eliminate the possibility of any signatory defaulting on their obligations
- Enhance governance due to transparency and auditability
- Eliminate gatekeepers and expensive intermediaries
- ✓ Facilitate trustless and predictable transactions
- ✓ Reduce the possibility of human error
- Remove paper shuffling and time-consuming tasks such as updating registers





Smart Contracts Challenges

- **Caution**: Must not be designed so carelessly that new complexity is introduced.
- Dangers: It could prove very awkward, if not impossible, to unwind a feral smart contract given the technology challenge for judges and arbitrators and any jurisdictional maze.
- * **<u>Challenge</u>**: Getting the technology right and making it very very easy to use is the challenge.
- ✓ SMART CONTRACTS MUST BE SIMPLE TO UNDERSTAND AND EXECUTE!





Blockchain-based Use Cases





UNIC Institute For the Future

https://medium.com/fluree/blockchain-for-2018-and-beyond-a-growing-list-of-blockchain-use-cases-37db7c19fb99

unic.ac.cy/iff

Blockchain in Supply Chain (case of food)









https://ilsi.org/food-supply-chain-small/



Blockchain in Supply Chain

Blockchain & Supply Chain Challenges

- Tracking and traceability;
- Lack of transparency;
- Environmental incidents that cannot be easily tracked;



Counterfeit products, forced labor and poor conditions in factories are just some of the challenges in supply chain;

Characteristics of data on Blockchain:

- Immutable,
- Transparent &
- Traceable

→ Records stored on the blockchain are immune to modification and deletion, =>

- enhance trust in supply chain transactions
- help streamline administrative processes and reduce costs (reduced paperwork and administrative costs)



Blockchain in Supply Chain

Benefits of blockchain in supply chain

- Saves time from days to instants =>financial transactions are performed faster than in the traditional financial systems
- Streamlines administrative processes and reduces costs (from overheads and intermediaries)
- Increases trust through shared processes and record keeping
- Reduces risk tampering, fraud and cybercrime
- Enables traceability of environmental and other incidents
- Empower the consumer and the retailer



Use Cases

In Food Industry – IBM, Dole, <u>Driscoll's</u>, Kroger, McCormick and Company, <u>Nestlé</u>, Tyson Foods, <u>Unilever</u> and Walmart.

- Use the technology to trace contaminated food (400,000 deaths every year)
- Usually it takes weeks to identify the precise point of contamination, causing:
 - further illness,
 - lost revenue and
 - wasted product.



<u>Source : https://appdevelopermagazine.com/5467/2017/8/23/ibm-announces-blockchain-integration-with-bigbox-food-supply-chains/</u>

Source:

http://www.sustainablebrands.com/news_and_views/startups/sustainable_brands/ibm_ha rnesses_blockchain_technology_improve_supply_chain

Blockchain in Agriculture and Livestock

- Agricultural supply chain:
 - characterised by a large-scale non-transparent and non-communicating network consisting of many actors, processes, products and data;
 - Inefficient;
 - Suppliers and retailers are disconnected;
 - Lack of transparency;

→

- Difficult to track and trace the origin of products
 - not a fair price for producers
 - counterfeit products
 - forced labor
 - **T** Etc....
- Food crises and scandals (e.g. mad cow disease) have increased the need for greater supply chain transparency and data integration.
- These days, the public is increasingly embracing the need for transparency in food products and farming techniques.

Source: <u>https://iisdenino.it/blockchain-for-agriculture-and-food.html</u>

Blockchain based identification

Estonia & Bitnation

- As of May of 2015 Estonia has offered the option to have your ID on the blockchain, enabling people to notarize their documents remotely.
- Its designed to offer more convenient, secure and faster access to services requiring ID verification at a lower cost.
- It removes the location dependence and makes any documents signed with the ID globally recognized.

Blockchain Fighting Human Trafficking

• Problem

- No id
- ~40 M people trapped
- 1 of 3 known victims of human trafficking are children under the age of 5 (ID2020)

Goal

- To create an open source, self sovereign, blockchain based id system;
- To be used to address the human rights crimes aggravated by lack of legal identification.
- The system will enable authorities to track down both criminals and victims of human rights violations.
- Moldova to participate in project

Blockchain Fighting Human Trafficking

UN & World Identity Network (WIN)

Aim

- To prevent child trafficking;
 - Part of the project "Blockchain for Humanity"

Focus

- To provide identification for undocumented children and minors;
- Besides the children with no birth certificates (~50% for children 5<), there are more than 600 million children under the age of 14 worldwide;
- They live in the world's poorest countries and are 'invisible' to governments and development agencies, owing to lack of documentation and identification;

Use case – Certificates/Fake Diplomas

- THE SCHOOL OF YOUR CHOICE Fake? Lost? ON THE AUTHORITY OF THE COUNCIL OF THE FACULTY OF ARTS AND SCIENCE. AND IN COMPORATIVE WITH THE STATUTES OF THE SCHOOL CITY Theft? THE CHANCELLOR OF THE UNIVERSITY HAS CONFERRED ON YOUR NAME HERE Modified? THE DEGREE OF Costs? YOUR DEGREE AND MAJOR GIVEN IN THE CITY OF YOUR CITY, YOUR COUNTRY IN THE YEAR DAY AND MONTH Paper Work? Slow Dissemination? E.F. Meion Exponen PRESEDENT " BIGBTRAR
- Ultimately, these problems result in expensive and time-consuming issuance and verification processes by several parties. Recovery of lost or modified certificates can be impossible at times

Potential of Blockchain Solutions

Ease of Publication & Distribution

- Immutable Records Digital fingerprints (hashes) of the individual certificates issued, are placed permanently in a blockchain transaction
- Reduced time to issue Certificates
- Costs of re-issuing certificates in the case the hard copy is lost are minimal
- Independent validation Ease and instant authentication by interested parties (e.g. employers) even if the application used or the institution's website no longer exists. Operational costs minimized
- Universities and issuing authorities protect their brand names from being tarnished
- Employers can examine job applications more efficiently, ensuring that a candidate employee is presenting true information, without long waiting times or processing costs
- Permissionless blockchain looks more ideal (e.g. the Bitcoin Blockchain)

Block.co more local use cases

 Company formation certificates

- Clean criminal record certificates

- Non-bankruptcy certificate
- Civil wedding certificates

Other use cases for Certificates

- Insurance Industry Insurance policy certificates, claims certificates and cover notes.
- **Cyber security** Timestamped certificates of audits conducted, with all relevant information contained on a decentralized and secure blockchain, thus inaugurating added confidence in the cyber security of that entity.
- **Procurement (Valuable Goods)** Verifying the origin, quality as well as the whole supply chain for valuable goods such as art items. It can provide the consumer with verified information provided by the issuers of the certificate, on the origin, traceability, quality processes, while reducing waste, increasing productivity, sustainability and preventing errors in the production and distribution chain.
- **Professional Training Bodies** Maintain an easily verifiable record of members of institutes and professional bodies i.e. Medical, Legal, Accounting

Blockchain in Energy

Enables peer-to-peer (P2P) energy trading;

- Buy+sell locally generated reneable energy over P2P network with real-time prices
- Aggregation of microgrids to virtual power plants n
- **Flexible and reliable demand/response**
- Payments via cryptocurrencies and digitize contracts
- Transparent, trusted, secured and efficient data management

N

Blockchain in Fintech

- Cryptocurrencies new forms of money
- Money that is programmable and active money for machines
- Money transacted in nano-quantities leading to m2m commerce

Markets that rely on the following mechanisms:

- Intermediation
- Clearing and settlement
- Recording and information keeping
- Rating, recommendation, voting
- Databases
- Distributed storage, authentication, anonymization
- Incentive schemes (rewarding / punishing)
- Transaction traceability
- Refereeing, arbitration
- Notarization

Will be disrupted Banking/finance is right in the epicenter!

Potential Areas of Application in Fintech

https://www.cbinsights.com/research/report/fintech-trends-q1-2019/

Challenges

- Technology maturity;
- Regulatory framework;
- Consumer protection;
- Standards to use blockchain on an industrial scale are still not in place;
- Replacing existing infrastructure time and investment;

Concluding Remarks

Coupled with:

- AI, IoT, machine learning, quantum computing, etc, allows for social good.
- Areas of interest:
 - Human trafficking
 - Enable a healthier global environment
 - Buying enviormental firendly goods stop treating workers poorly, use of cultivation methods that do not affect adversely the environment, use of renewable energy blockchain-based systems....
 - Better healtchare systems
 - •

Social consequences will be vast

"It is not the strongest of the species that survives, nor the most intelligent that survives. It is the one that is the most adaptable to change"

Charles Darwin

Institute For the Future

blockchain.initiative.

Thank You!

