DAY 1: INTRODUCTION & FOUNDATIONS OF BLOCKCHAIN

INTRODUCTIONS

Dr. Victoria Lemieux
v.Lemieux@ubc.ca

Blockchain @UBC

Professor of Archival Science, UBC School of Information and Founder & Co-Lead of Blockchain@UBC

- **Education & Qualifications**
  - *Certified Information Systems Security Professional*
  - *PhD (Archival Studies) UCL*
  - *MAS (Archival Studies) UBC*
  - *BA Hons (History) UofT*
- **Research in blockchain**
  - *Risks to and protection of the availability of trustworthy records*
  - *Authenticity of blockchain/DLT records*
- **Teaching**
  - *Blockchain for Information Professionals*
  - *IT Security, Information Assurance and Risk Management*

Dr. Tim Weingartner
tim.weingaertner@hslu.ch

HSLU Hochschule Luzern

- Professor at the School of Information Technology at the Lucerne University of Applied Sciences and Arts, Switzerland.
- Focuses on Blockchain technology and Smart Contracts.
- As a representative in the Smart-up Program, he supports the promotion of young start-ups from the Lucerne University of Applied Sciences and Arts.
- He played a major role in setting up the Central Switzerland Innovation Park in Rotkreuz. Under the thematic focus "Building Excellence", the park deals with the Digital Transformation in the construction industry.
- Before joining the university, Tim worked in the Swiss financial industry for more than 15 years.

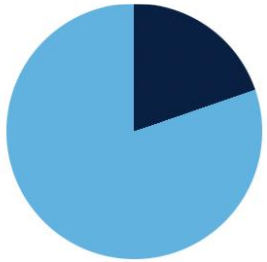
1. OVERVIEW OF UBC

ABOUT UBC

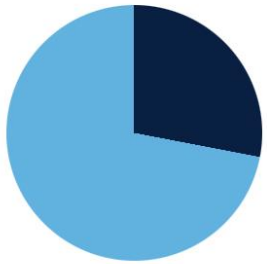
Students on our campuses

- 59,150 Vancouver students
- 11,748 Okanagan students
- 16,611 degrees granted in 2024
- 70,898 total UBC students
- 2,500 Indigenous students
- 5,762 students in UBC Extended Learning, with 8,346 enrolments

International Students

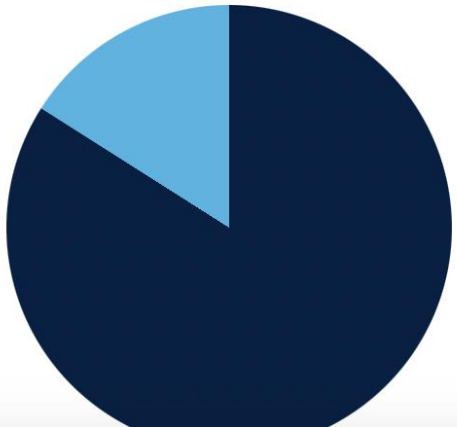


- 19.7% of Okanagan students are international



- 27.7% of Vancouver students are international

Enriched learning experiences



- 84% of undergraduate students participate by the time they graduate *National Survey of Student Engagement (2023)*

2. OVERVIEW OF BLOCKCHAIN@UBC

1. OVERVIEW OF THE COURSE

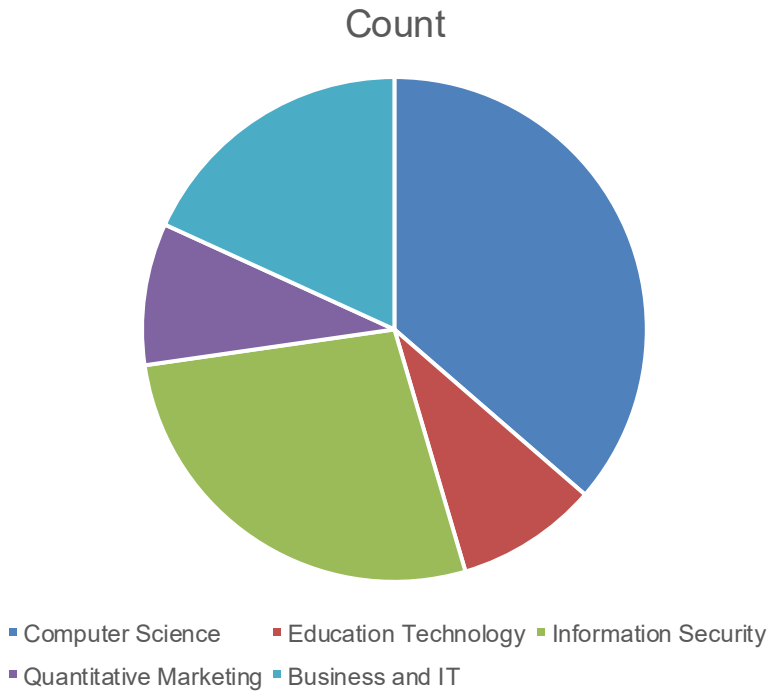
ABOUT THE SUMMER INSTITUTE

- Established in 2017 (this is the 9tth annual summer institute) as a way for students and faculty to learn about blockchain technology in an ‘open learning format’, acknowledging that everyone could contribute some knowledge about blockchain and also has something to learn
- From the outset, we incorporated a ‘Blockathon for Social Good’ based on a different theme each year. This year’s theme is ‘Blockchain + Responsible AI’.

https://youtu.be/Z7k5PVbG_dc

OUR MULTIDISCIPLINARY TRADITION

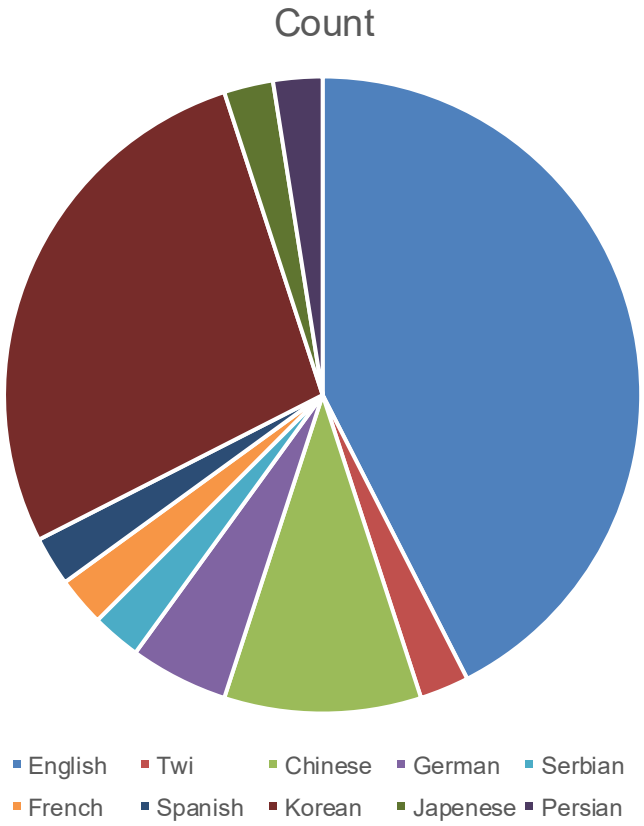
- Multidisciplinary in nature, incorporating ideas from archival and information science, engineering, computer science, business, economics, law, and more!



Please complete our student survey

NOT ONLY MULTIDISPLINARY, BUT INTERNATIONAL

- In 2019, Prof, Tim Weingartner joined us for the first time and our collaboration with HSLU was born.
- In 2022, we held our first summer institute at HSLU as a collaboration between UBC and HSLU
- In 2024, we were delighted to be joined by faculty and students from Sejong U. in Korea for the first time
- This year, we are delighted to welcome students from Zhejiang U. in China, participants from Ghana Communications Technology University, and from Sorbonne U. UAE as well!



FOCUS OF THE COURSE

What is possible? (**Design** focus)

- How can we design blockchain/DLT systems?
- What kinds of use cases and blockchain protocols are out there, and what can they do?
- What are the current opportunities, challenges, tradeoffs, in system design?

What steps should we take to make this a reality? (**Implementation** focus)

- How could we build the a solution?
- How could we overcome different barriers to adoption (e.g. cognitive, regulatory, operational, technological, etc.)

UBC iSchool

SUMMER INSTITUTE TOPICS AND LEARNING OUTCOMES

1. Appreciate different perspectives on blockchain/DLT, such as individuals, businesses, specific sectors and communities, and government.
2. Gain exposure to various blockchain/DLT use cases
3. Gain insights into different blockchain protocols, and their strengths and limitations for different use cases
4. Critically evaluate and compare blockchain/DLT solutions developed by others
5. Collaborate in multidisciplinary teams to design and present a Blockchain/DLT solution to address contemporary business, social, and/or environmental issues.

TYPES OF SESSIONS

1. **Introduction and orientation** (today)
2. **Protocol workshops:** Gaining exposure to specific blockchain protocols, and understanding their strengths and limitations (e.g., Bitcoin, Ethereum, Solana, Polygon, ICP, Oasis)
3. **Special topics sessions:** Learning about cutting edge research (e.g., BTS' 25) and topics necessary for successful blockchain adoption (e.g., governance, tokenomics)

3.Blockathon for Social Good: A five-day hackathon built into the course. Serves as part of our "final exam"

Blockchain @UBC

Sponsored by LAZAI

Summer Institute 2025 Schedule

UBC LIFE Building 2201, University of British Columbia, Vancouver

Date	Topic	9:00 - 11:30	11:30 - 12:30	13:00 - 15:30	17:00 - 19:30
Day 1 Mon, July 7th	**Introduction**	Introduction to Summer Institute Introduction to blockchain/DLT & use cases (DeFi, DePin, DeSci) Reveal teams (Dr. Victoria Lemieux, Dr. Chen Feng & Dr. Tim Weingärtner)	Lunch	Three Layer Model Three Layer Model Group Exercise (Dr. Victoria Lemieux) Team Building Campus Tour 15:45 - 17:00	
Day 2 Tues, July 8th	**Layer 1 Protocols**	Introduction to Bitcoin (Jarrett Vaughn)	Lunch	Introduction to Ethereum & Smart Contracts (Tim Weingärtner)	
Day 3 Wed, July 9th	**BTS '25**	Blockchain Technology Symposium (BTS '25) (Various Speakers)	Lunch	Blockchain Technology Symposium (BTS '25) (Various Speakers)	
Day 4 Thurs, July 10th	**BTS '25**	Blockchain Technology Symposium (BTS '25) (Various Speakers)	Lunch	Blockchain Technology Symposium (BTS '25) (Various Speakers)	
Day 5 Fri, July 11th	**Blockchain Protocols Overview**	Introduction to Ethereum & Smart Contracts cont'd (Dr. Tim Weingärtner)	Lunch	Overview of Solana (Solana Superteam) 13:00 - 14:15 Overview of Polygon (Ibrahim Tariq Javed) 14:30 - 15:30	
Sat, July 12th	Weekend	**Field Trip to Whistler**		**Field Trip to Whistler**	
Sun, July 13th	Weekend	Free day; activities on own		Free day; activities on own	
Day 6 Mon, July 14th	**Decentralized Federated ML/Intro to Decentralized Identity**	Decentralized Federated ML (Javier Arroyo Ferrer, ICP)	Lunch	Intro to Decentralized Identity (Matteo Cristino, Forkbomb)	**LazAI Reception**
Day 7 Tues, July 15th	**Decentralized Identity/ Intro to PontusX**	Decentralized Identity Use Cases: BC Government (Nancy Norris), Dr. Tim Weingärtner (HSLU), Prof. Jong-Hyouk Lee (Sejong University)	Lunch	PontusX Deep Dive (Thomas Komeda, PontusX)	
Day 8 Wed, July 16th	**Blockchain Governance/ Regulation & Tokenomics**	Blockchain Governance	Lunch	Tokenomics & Regulation (Virgo CX)	
Day 9 Thurs, July 17th	**Start of Blockathon**	Blockchain Governance (Trinh Nguyen) Intro to Blockathon	Lunch	Start of Blockathon	
Day 10 Fri, July 18th	**Blockathon**	Blockathon	Lunch	Blockathon	**Social Event at the Swiss Consulate 17:30 -19:30**
Day 11 Sat, July 19th	**Blockathon**	Blockathon	Lunch	Blockathon Final Presentations & Judging	**Announcement of Blockathon Winner & Post-Block Social**

Discord

Join the Summer Institute 2025 **Discord** server using this QR code! Get updates, ask questions, and connect with fellow students.
The most up-to-date schedule will be on blockchain.ubc.ca, with updates communicated through the Discord server.

blockchain.ubc.ca Blockchain@UBC @blockchainubc @blockchainubc @blockchainubc

UBC iSchool

COURSE RESOURCES

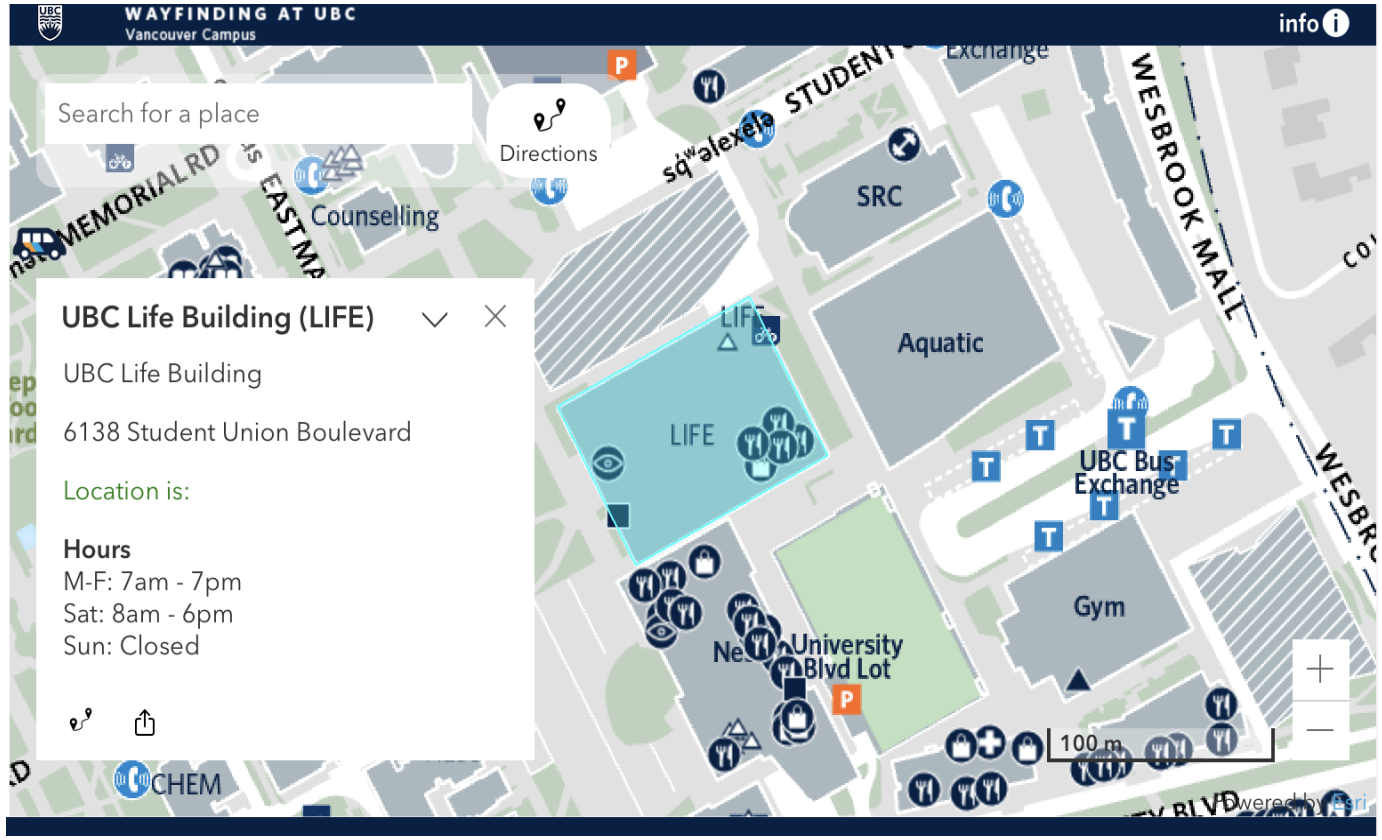
- **Shared Google Drive:**
  - Course schedule
  - Readings
  - Slides (published after the workshop)
  - Session recordings
  - Additional background information for use in workshops where relevant

Blockchain@UBC 2025 Google Drive

UBC iSchool

LOCATION

- All Classroom activities will take place in [UBC LIFE Building 2201](), University of British Columbia, Vancouver, Canada



bitly

Campus Wayfinding Map

UBC iSchool

AGENDA FOR TODAY

Morning (9:00-11:30)

1. Introductions & overview of the course
2. Introduction to blockchain technology

Lunch (11:30-13:00)

Afternoon (13:00-15:30)

1. The ‘Three Layer Modell’
2. Team Reveal & Icebreaker Activity

Late Afternoon/Evening (15:30-17:00)

1. Teams Self-Guided Tour of UBC Campus

Lunch Options

UBC iSchool

OUR RESPONSIBILITIES IN THIS COURSE

Guide you through a mix of concepts, examples, and exercises for an integrated learning experience

Ensure that you have the tools to learn from our facilitators and from one another

Help you find answers to your questions, even if these are not readily available

Help you to work effectively in multidisciplinary teams

UBC iSchool

WHAT WE NEED FROM YOU

COMMIT YOUR TIME AND ATTENTION

BE CURIOUS & THINK CRITICALLY

BE SUPPORTIVE, COURTEOUS & RESPECTFUL

UBC STUDENT ASSESSMENT

- As the program is listed as an upper-level undergraduate and graduate course at UBC, you must complete the assignments outlined in the syllabus to receive credit. we are aware that the program is intensive, so the deadlines for submitting the assignments are at least a week after the program is completed. please see the syllabus for specific deadlines.

- The assignment submission portal has been set up on canvas, as well as grading rubrics. as UBC students, you will submit your assignments via canvas, while students from other universities will submit by following the instructions of their own universities.

- There are recommended readings. however, we understand that you may not have time to read carefully during the course.

If anything is unclear or you are concerned about not being able to meet the assignment deadlines , please reach out to Dr. Lemieux (sooner rather than later)

CHECKING IN…AND BREAK

2. INTRODUCTION TO BLOCKCHAIN

Agenda

1. **Fundamentals.** *What is blockchain? What can it do?*

1. **Basic applications.** *How is blockchain enhancing existing processes?*

1. **Transformative applications.** *How can blockchain enable profoundly new ways of doing things?*

We have a lot to cover this morning, and you may feel lost at times

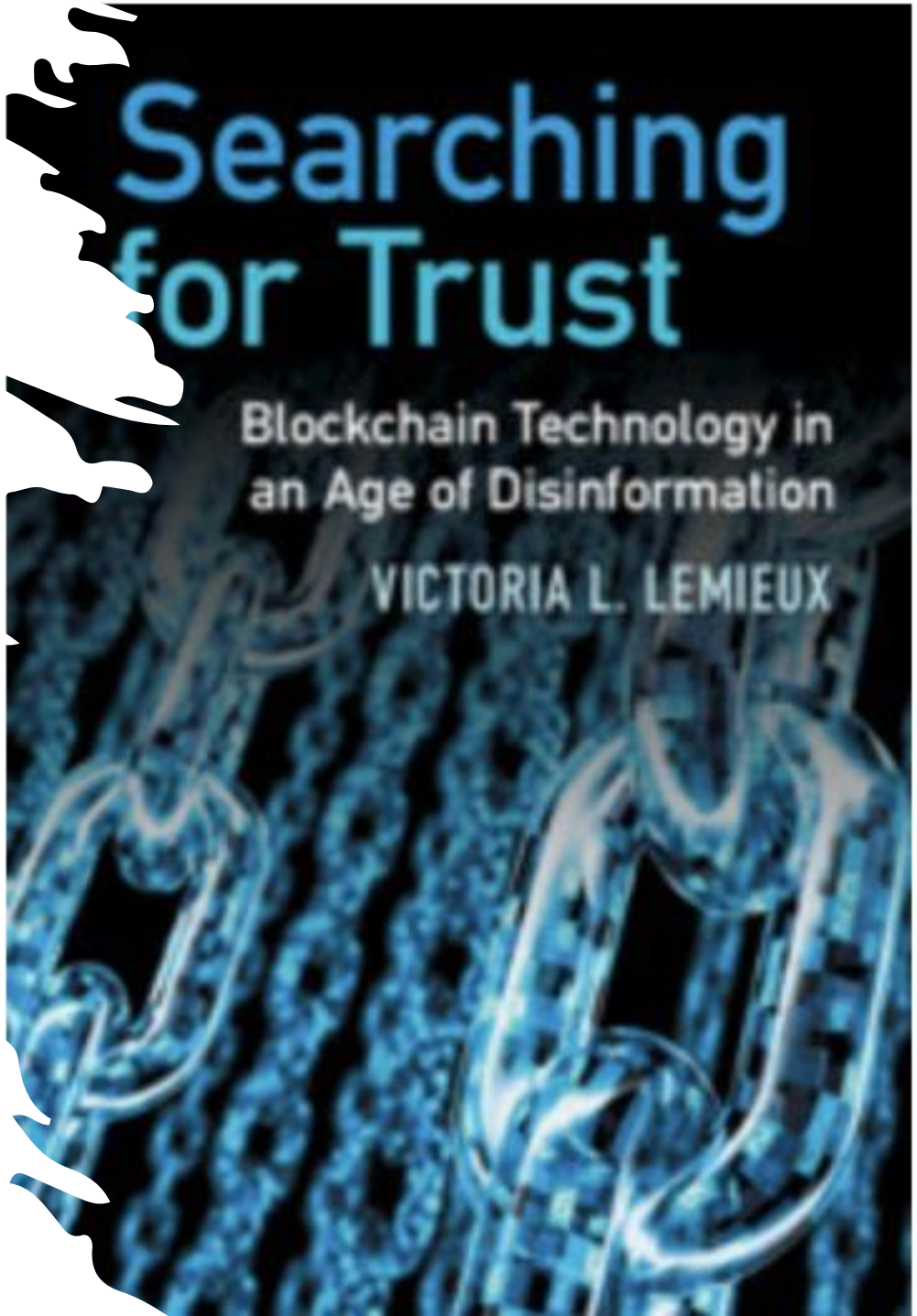
For some of you, these concepts are novel and challenging. It’s fine if you don’t grasp them all right away

Feel free to ask questions at any time

1. Fundamentals

What is blockchain?

INTRODUCTORY VIDEO



SO WHAT IS BLOCKCHAIN?

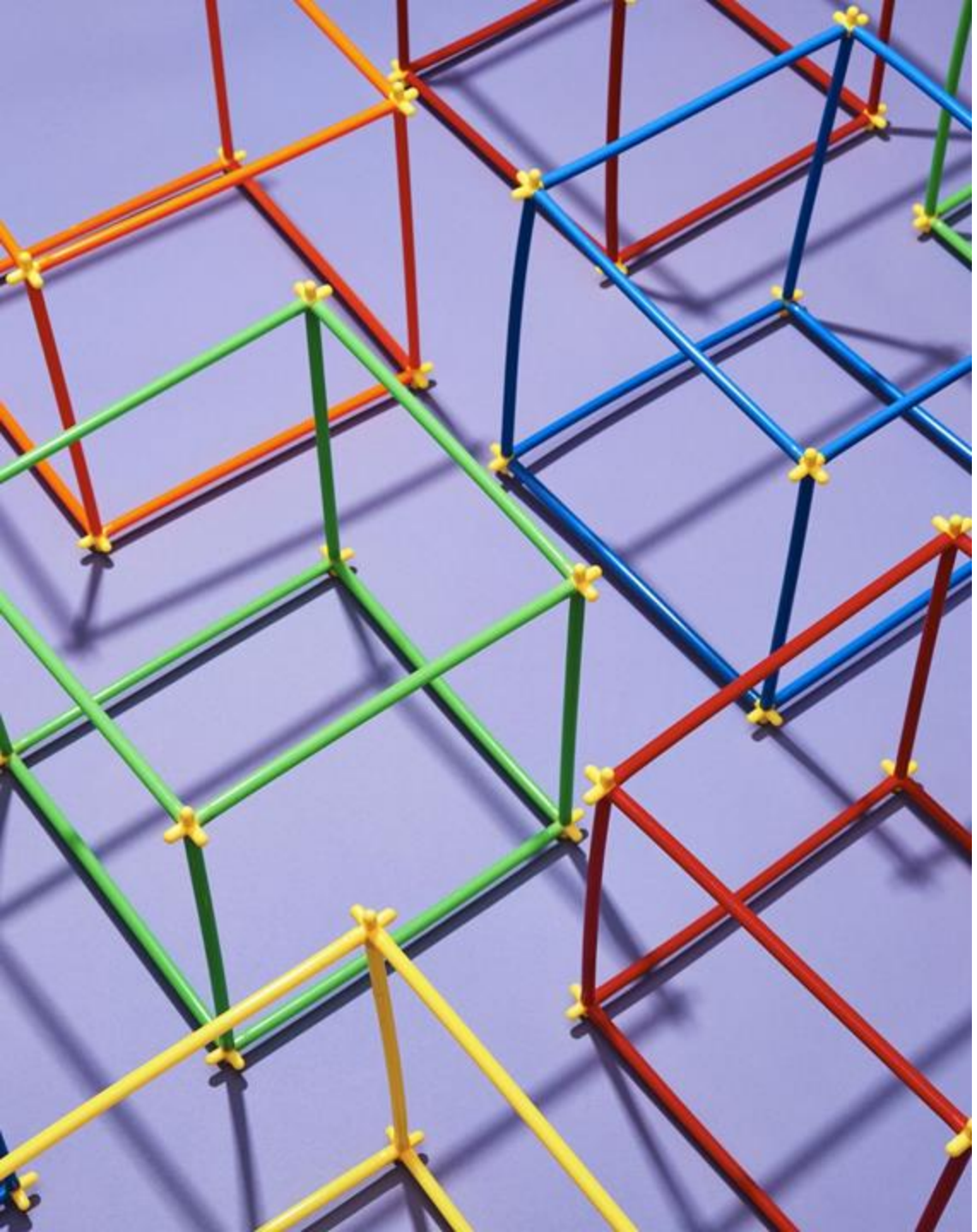
A DIGITAL LEDGER THAT…

- Records something of value
- Is distributed
- Harnesses the network to process transactions
- Uses cryptography to make records secure and immutable

Some blockchains have:

- Digital tokens that represent assets
- Different types of permissions
- Smart contracts

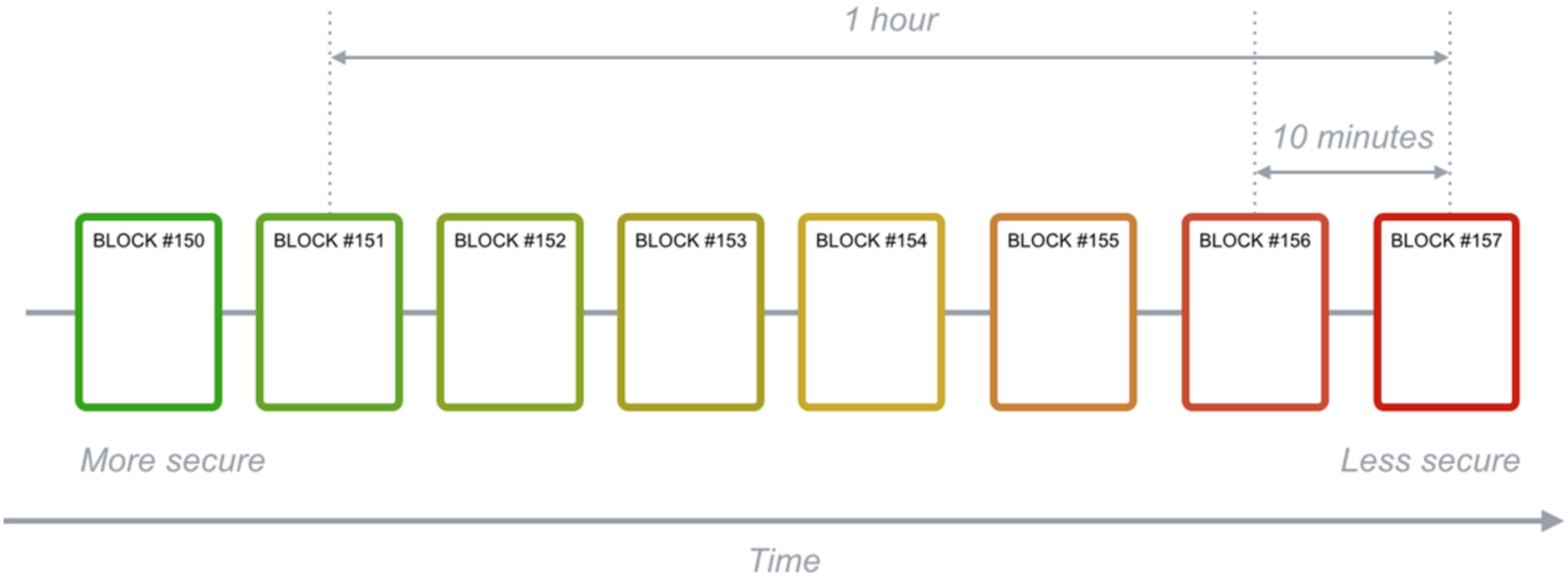
Key components & concepts of blockchain solutions



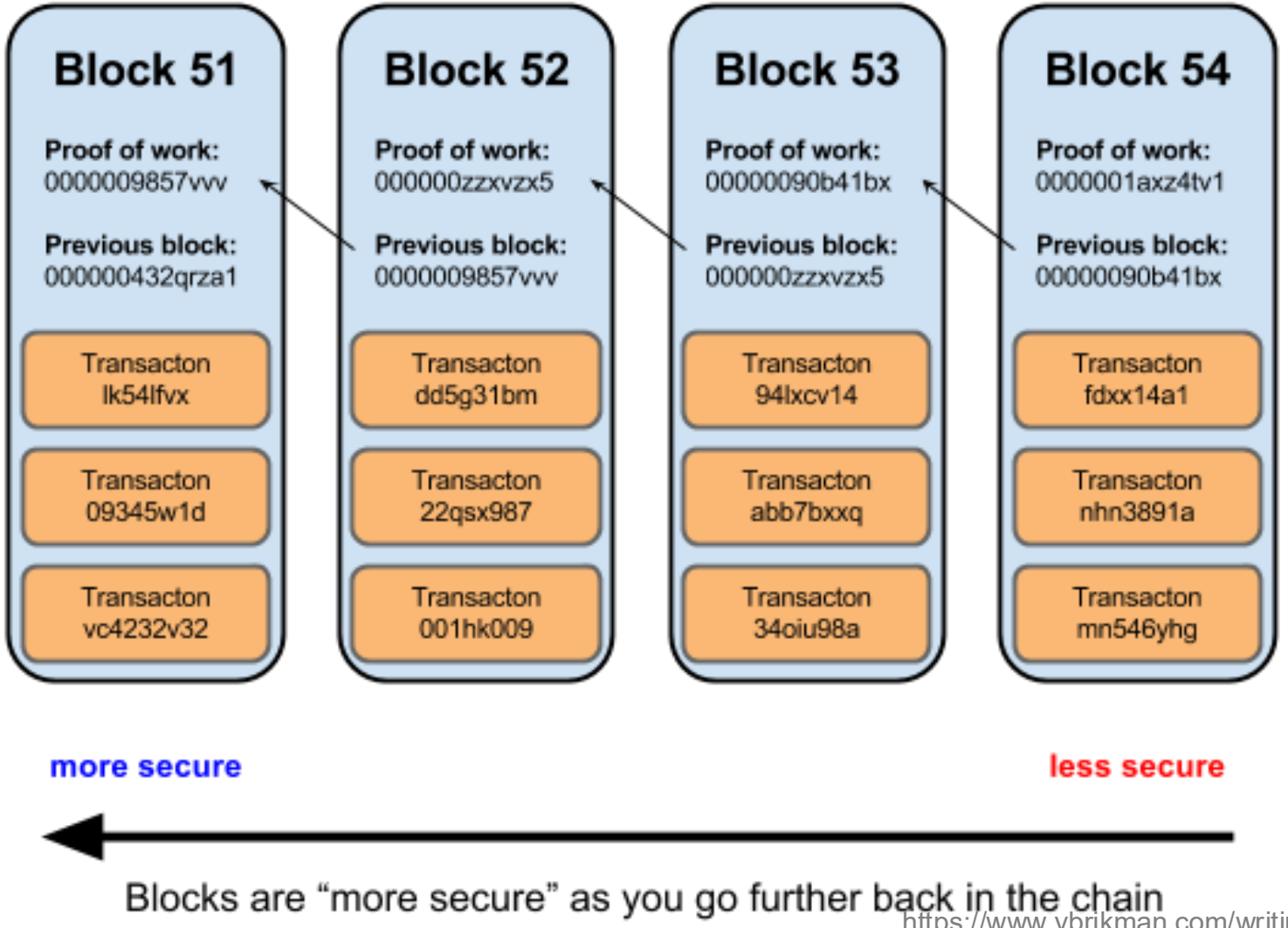
BLOCKS . . . The ‘building blocks’ of blockchains

- Each block in the blockchain is like a detailed invoice or bill of charges that contains a list or, in the case of some blockchains, a digest of transactions.
- Blockchain transactions are the equivalent of transfers of units of value, which appear as ledger entries that track the accumulation of value in an ‘account’ and its movement between accounts.
- Not all distributed digital ledgers use block data structures (e.g., IOTA and Nano use Directed Acyclic Graph data structures (DAGs)

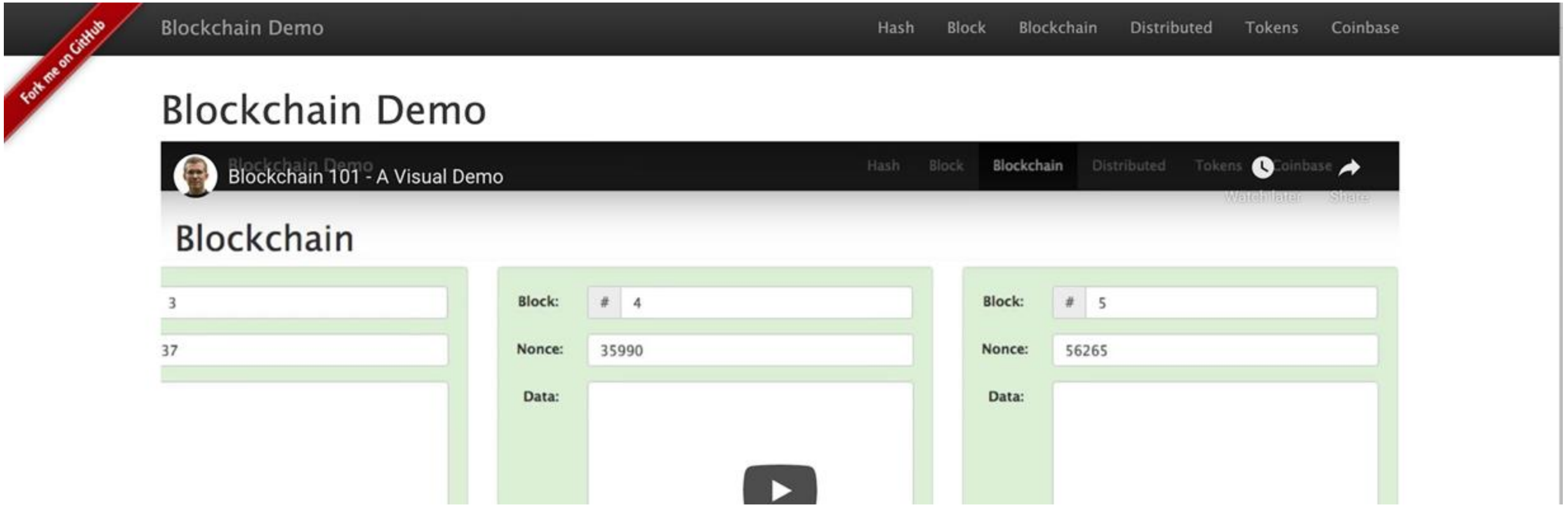
New data is added in blocks, which link together to make a CHAIN



CRYPTOGRAPHY links the blocks together helps makes the ledger 'immutable'



https://www.ybrikman.com/writing/2014/04/24/bitcoin-by-analogy/

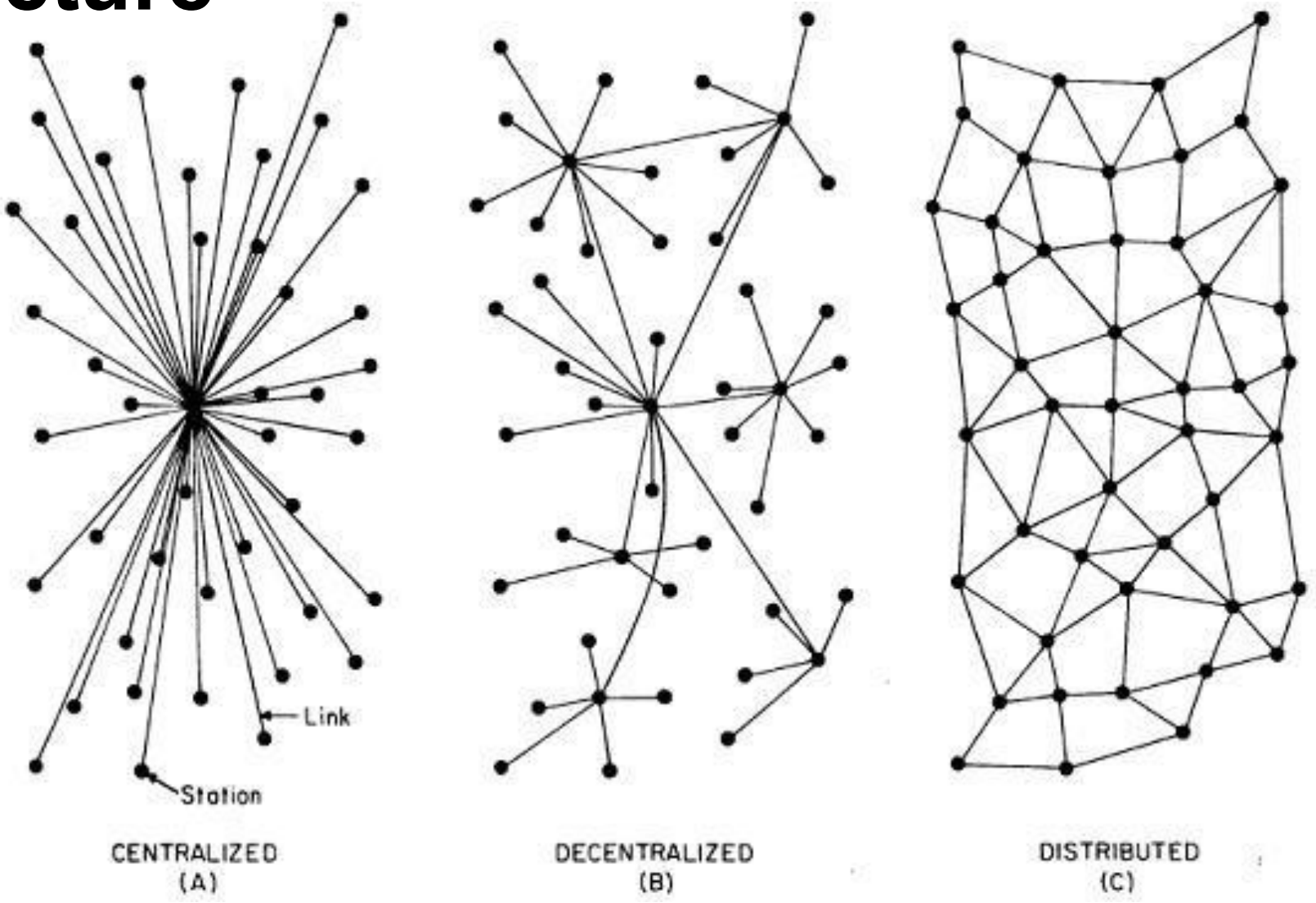


Live Blockchain LEDGER Demo in a Browser

https://andersbrownworth.com/blockchain/

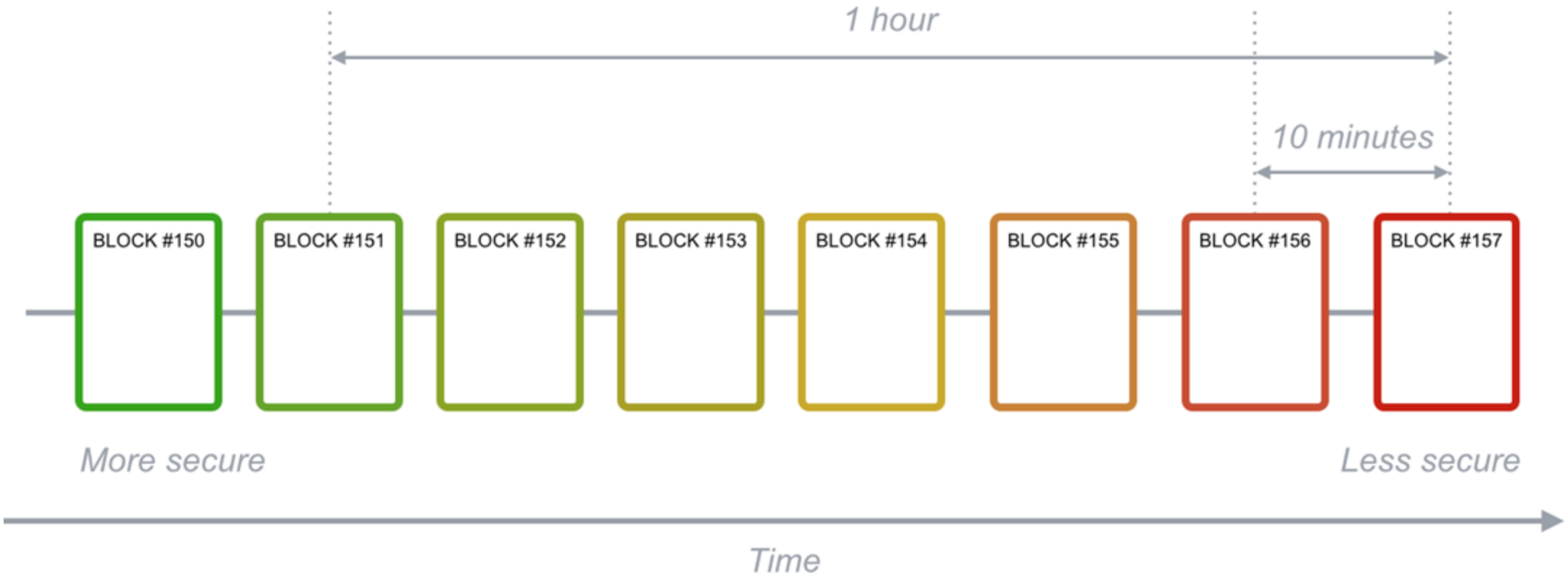
A DISTRIBUTED network structure

Baran (1964)



All nodes in the network have the same copy of the ledger, which enhances TRUST

Consensus: how the network agrees on the state of the ledger



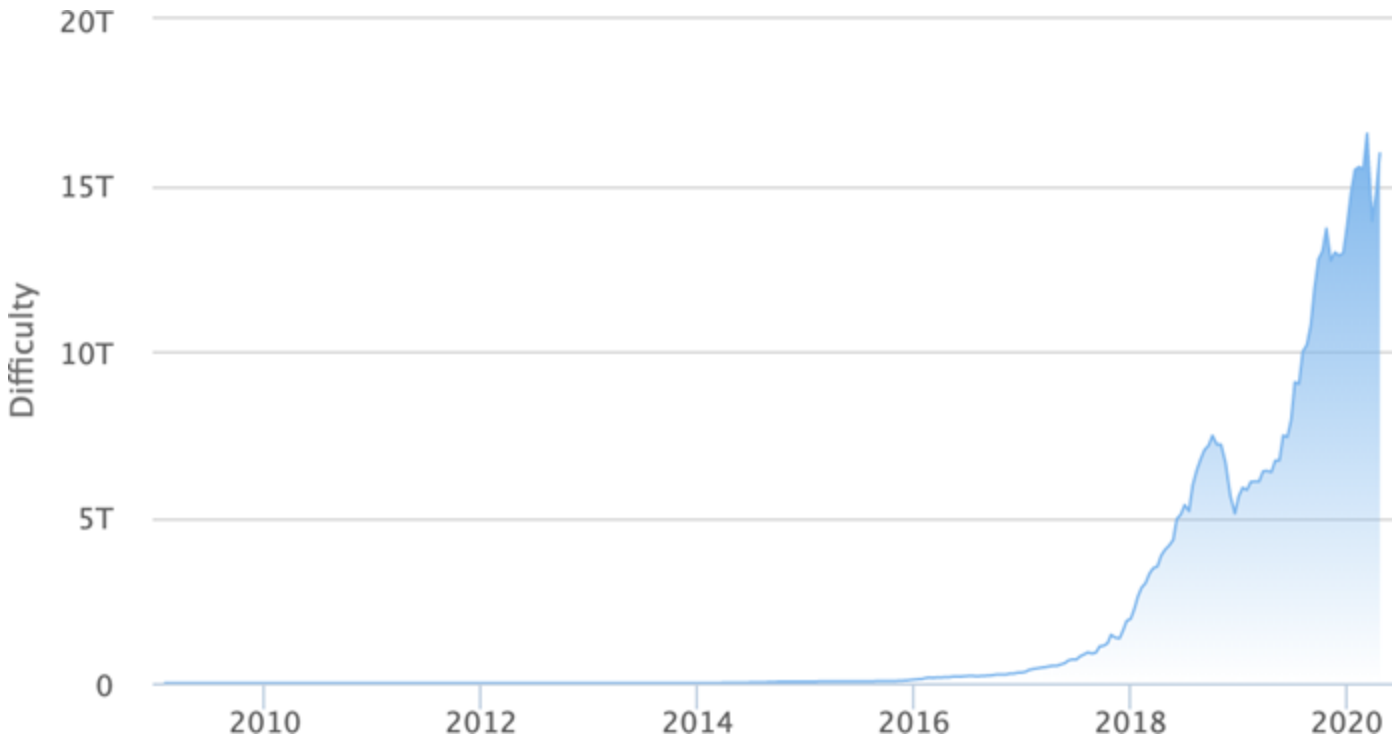
Common Consensus Mechanisms:

Proof of Work
Proof of Stake
Practical Byzantine Fault Tolerance (PBFT)

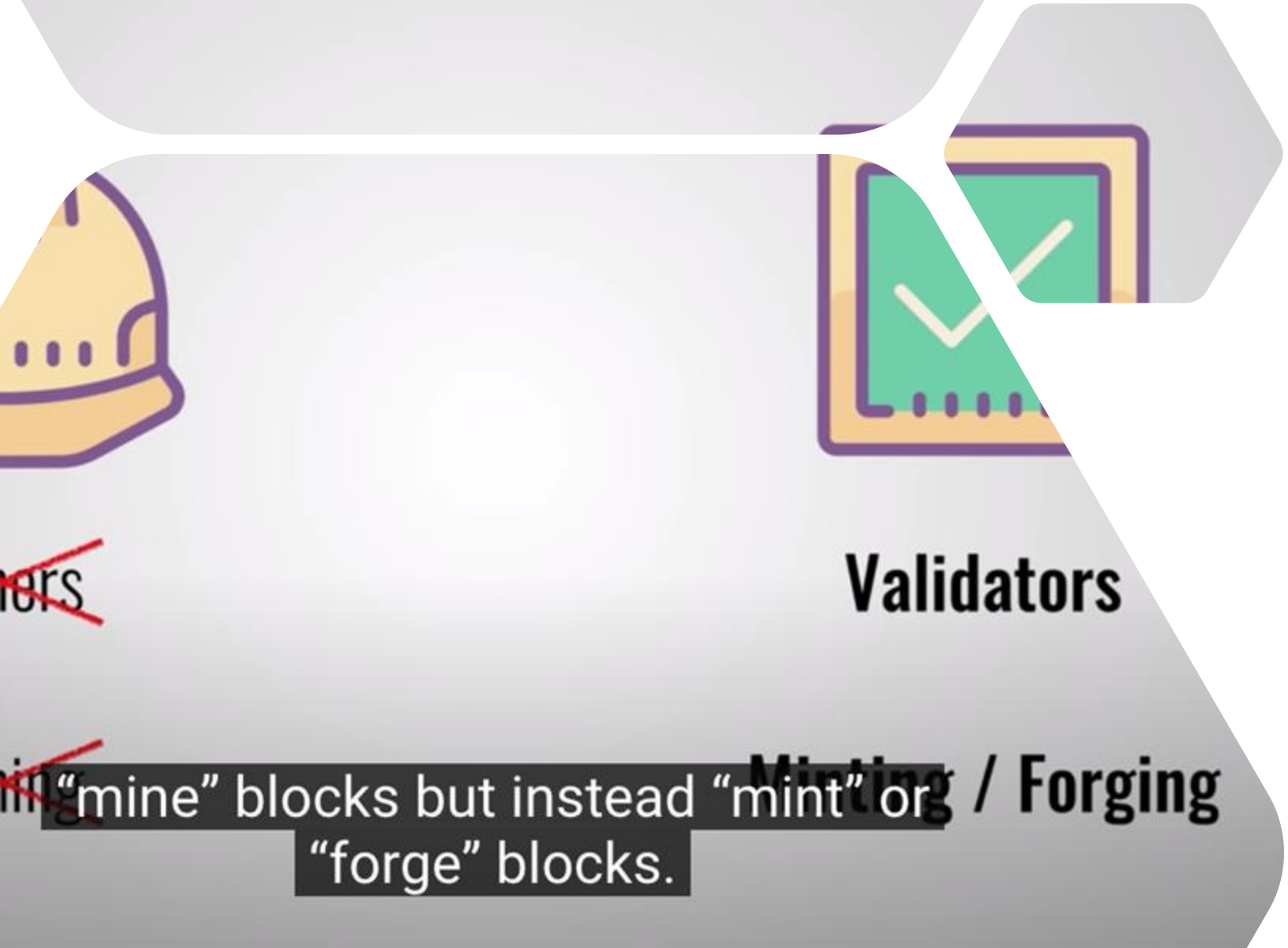
Mining on the Bitcoin network: “Proof or work”

Mining: a simple explanation

Bitcoin mining difficulty over time



The mining difficulty in Bitcoin's Proof of Work protocol increases as the blockchain grows to maintain a consistent block creation rate of approximately one block every 10 minutes, despite rising computational power. As more miners join the network and the total hash rate increases, the protocol adjusts the difficulty every 2,016 blocks (~2 weeks) to ensure blocks aren’t mined too quickly, preserving the security and predictability of the system.

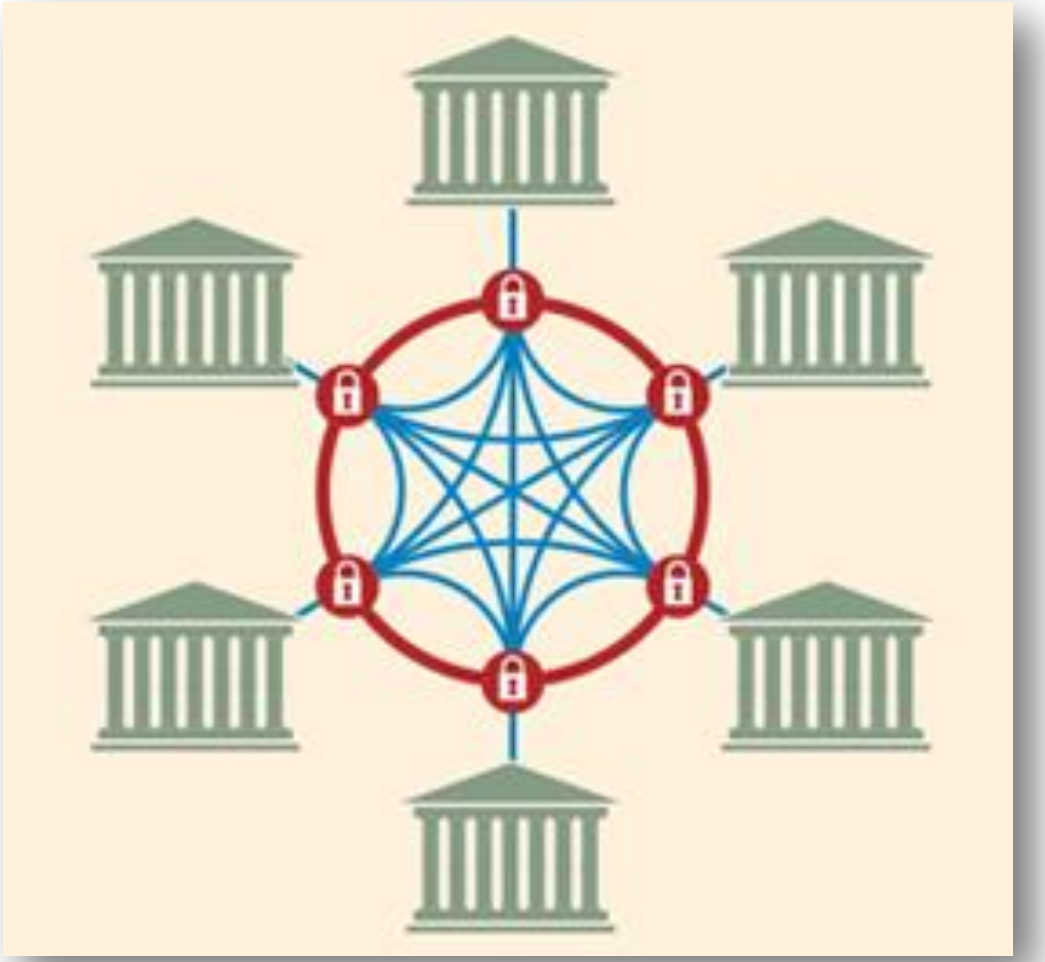


Proof of Stake

- https://www.youtube.com/watch?v=M3EFi_POhps

Public vs. Permissioned Blockchains

Public blockchain

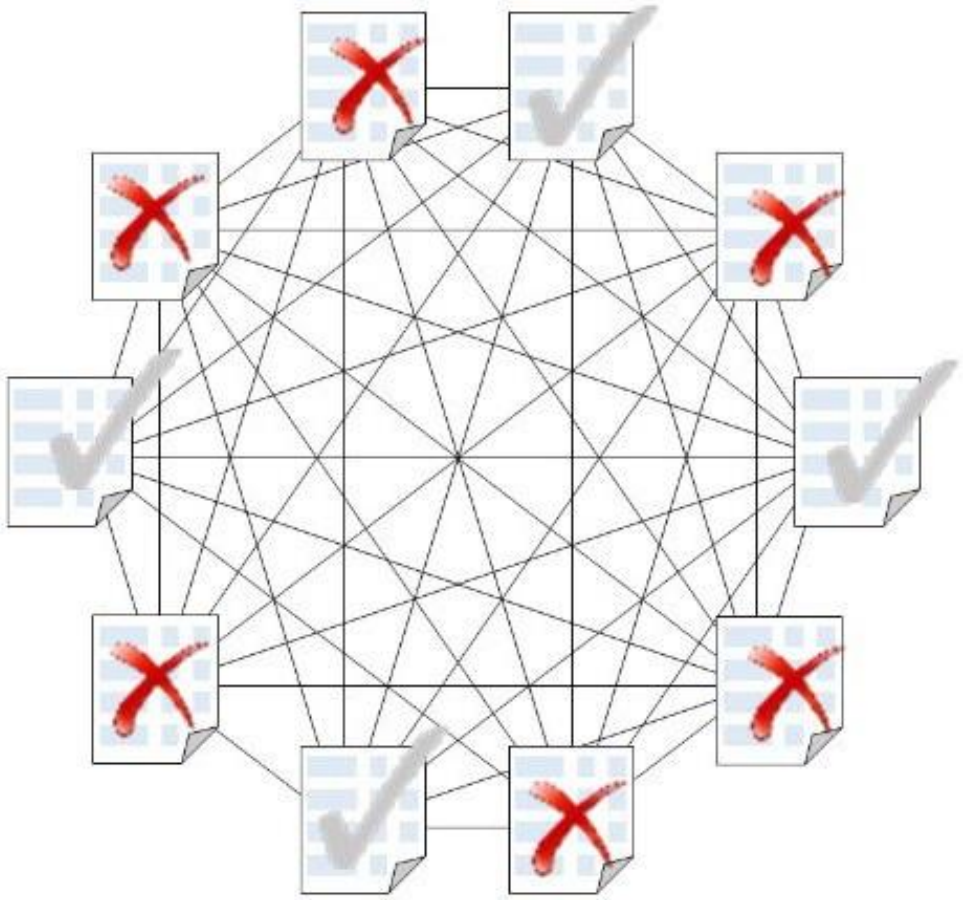


Permissioned blockchain

Source: Financial Times

Different types of permission

- Permission to join
- Permission to write transactions
- Permission to read all transactions
- Permission to read certain transactions (e.g. only those transactions they're involved in)



ETHEREUM

- Public, open-source blockchain
- First to enable smart contracts
- Designed for decentralized applications (“dApps”)
- Has it’s own cryptocurrency (Ether)
- Consensus mechanism is Proof of Work (PoW), with plans to change to Proof of Stake (PoS)

HYPERLEDGER

- Open source project to build *permissioned blockchains*
- Designed for industrial applications
  - E.g. supply chain solutions
- Developed by the Linux Foundation and used heavily by IBM
- Does not have its own cryptocurrency
- Consensus mechanism can change based on the application but commonly uses Practical Byzantine Fault Tolerance (PBFT)

Consensus in permissioned blockchain networks

- Users are known (e.g. supply chain)
- Consensus protocols are customizable
- Consume less energy to achieve consensus
- Relatively easier to corrupt (due to smaller number of nodes), so trust between users is needed

Summary of basic features

- A distributed, digital ledger that securely records something of value
- Both digital (e.g. Bitcoin) and *real-world assets* (e.g. mangoes) can be recorded on the ledger
- Provides a single source of 'truth'
- Enables the exchange of ownership between parties on the ledger *without the need for trusted third parties*

BANK OF AMERICA

- This transfer is designed to be immutable (legitimate and indisputable)

https://abcnews.go.com/Business/bank-america-sued-foreclosing-wrong-homes/story?id=9637897

Smart contracts and digital tokens

Smart contracts execute “if-then” statements

Blockchain for the individual user

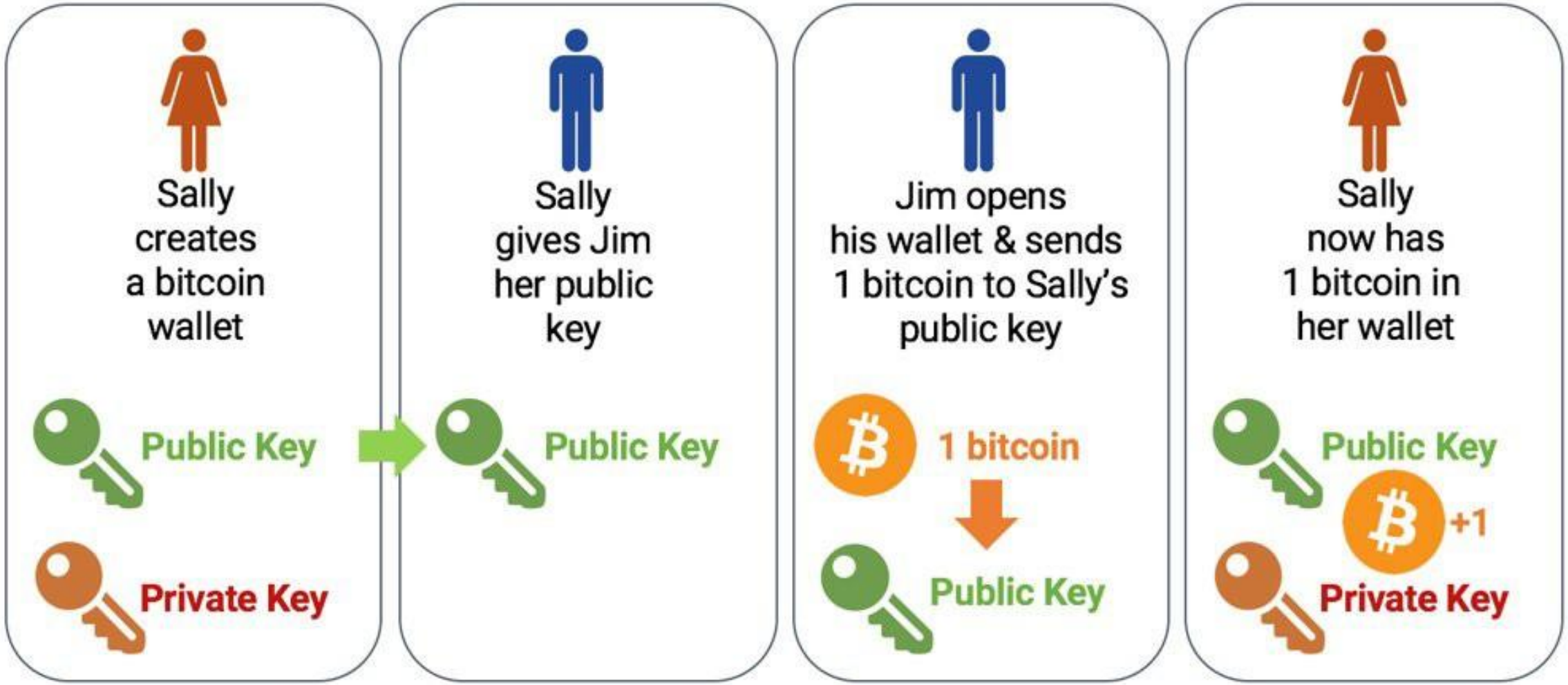
Use a “wallet” to access, send and receive value

Wallets have a “public key” and a “private key”

Private key allows you to look inside and take value out

Public key allows people to find your wallet and put value in

Digital Signatures



https://stansberrypacific.com/asia-wealth-investment-daily/become-blockchain-expert-4-minutes-read-2/

QUADRIGACX

Quadriga Fintech Solutions was the owner and operator of QuadrigaCX, which was believed to be Canada's largest cryptocurrency exchange. In 2019 the exchange ceased operations and the company filed for bankruptcy with C$215.7 million in liabilities and about C$28 million in assets.

The company's CEO and founder, Gerald William Cotten (born 11 May 1988), died in 2018 after traveling to India. Up to C$250 million (US$190 million) in cryptocurrency owed to 115,000 customers was missing or could not be accessed because only Cotten held the password to off-line cold wallets.

https://www.youtube.com/watch?v=vW2BPQ15OSw

Celsius

Our website is currently being updated. Related to the previously stated pause on withdrawals, Swap, and transfers between accounts, some of our products and services are temporarily unavailable. For more information, see our blog


Not Your Keys,
Not Your Bitcoin
Beginners Guide To Private Keys

Digital Tokens

Tokens can represent basically *any assets* that can be recorded and traded on the blockchain ledger

- Currencies (e.g. Bitcoin)
- Commodities
- Property
- Artwork
- Loyalty points
- Share certificates

Tokenization

The process of converting rights to real-world assets to digital tokens on a blockchain

1 to 1 1 to Many

E.g. Land registry

E.g. Fragmented property ownership

TRUMPCOIN

shitcoin

bananacoin

PotCoin

Don’t believe the hype…

PUTiN COiN

The world's first 100% honest Ethereum ICO.

You're going to give some random person on the internet money, and they're going to take it and go buy stuff with it. Probably electronics, to be honest. Maybe even a big-screen television.

Seriously, don't buy these tokens.

Crowdsale Statistics

Ether contributed

310.445

I had a feeling someone would waste their money.

Contributions in USD

$43539

Enough to buy 36 televisions!

Tokens issued

3965716.097

Including 591.000 bonus tokens!

Line Goes Up: The Problem with NFTS

https://www.youtube.com/watch?v=YQ_xWvX1n9g

NFTS – SNL

https://www.youtube.com/watch?v=mrNOYudaMAc

SUMMARY OF PART 1: BLOCKCHAIN IS A DIGITAL LEDGER THAT…

Records something of value

Is Distributed

Is designed to be Immutable

Is secured using cryptography & decentralization

Has coded rules (consensus mechanisms) for how the ledger can be updated

Some blockchains have:

- Digital tokens that represent assets
- Public/permissioned access and complete/limited transparency
- Smart contracts

ORGANIZATIONAL REASONS FOR BLOCKCHAIN

When blockchain is useful

- When transacting parties have misaligned goals and incentives that causes mistrust
- When there is a lack of transparency
- When actors can't be trusted not to cheat

Blockchain-based solutions make the most sense at the *interorganizational level*

When blockchain is less useful

- When a single actor can be trusted to maintain records and facilitate transactions (e.g. IT and accounting departments in a company)

Blockchain-based solutions are often unnecessary *within a single organization*

Applications

How blockchain can enhance existing processes

OVERVIEW OF BLOCKCHAIN USE CASES (BASED ON ISO TR 3242:2022)

— Data Provenance

Data Accountability (EC)

Property Records Management (IN)

Student Records Management (IN)

Education Certificate Provenance (SG)

Self-Sovereign Identity (SSID) (CY)

Content Timestamp Verification (NL)

— Fintech

Accounts Receivable (CN)

Interbank Loan Reconciliation (CN)

Organised CHIT Funds (IN)

Pension Process Optimisation (CN)

Transparent Securitisation (IT)

Decentralized Charity Platform (KR)

— Supply Chain

International Trade Transparency (SG)

Maritime Bills of Lading (IL)

Franchised Pharma Supply Management (CN)

Anti-counterfeit Pharma (IN)

IGP Traceability (IT)

Universal Farm Compliance (IE)

Intl. Waste Management System (NL)

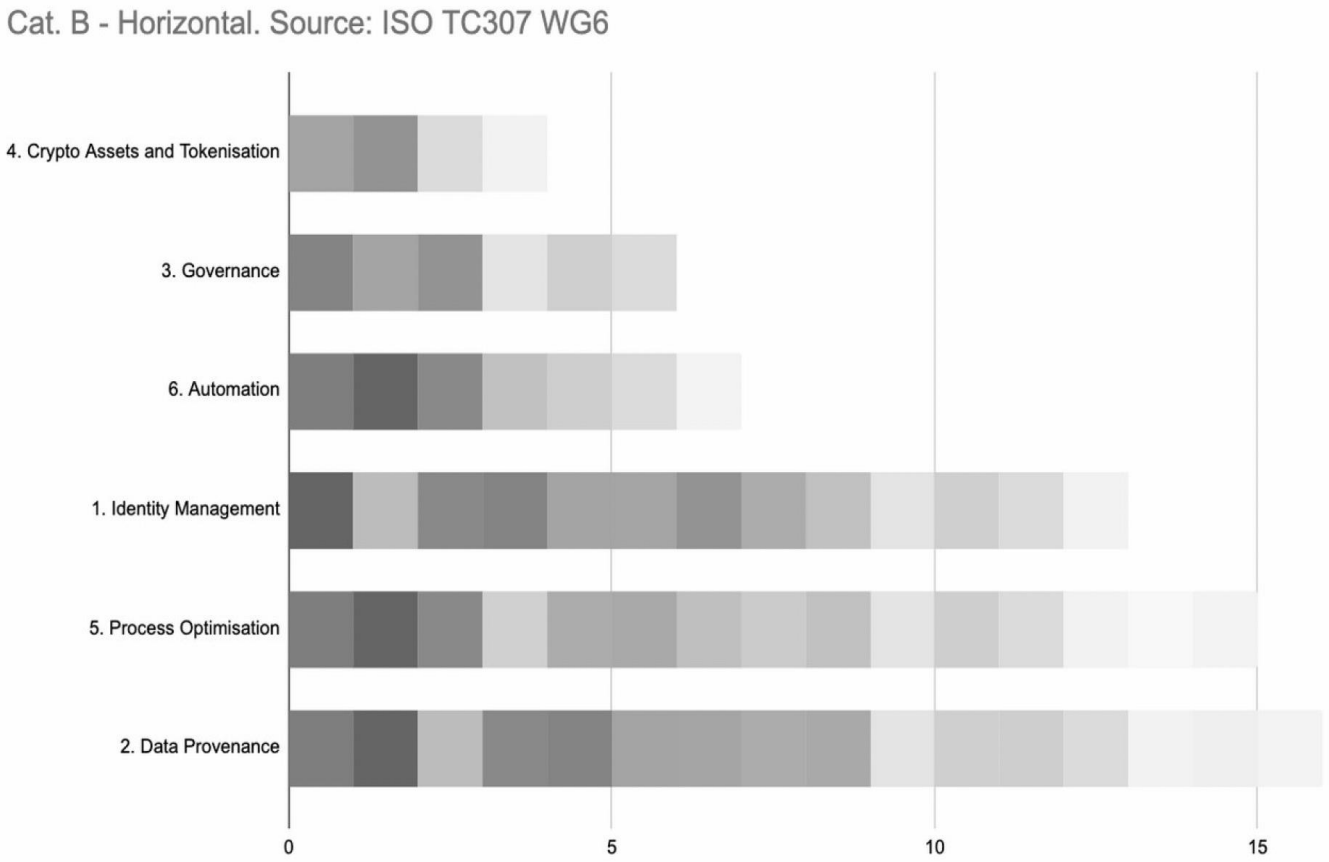
— Smart Energy

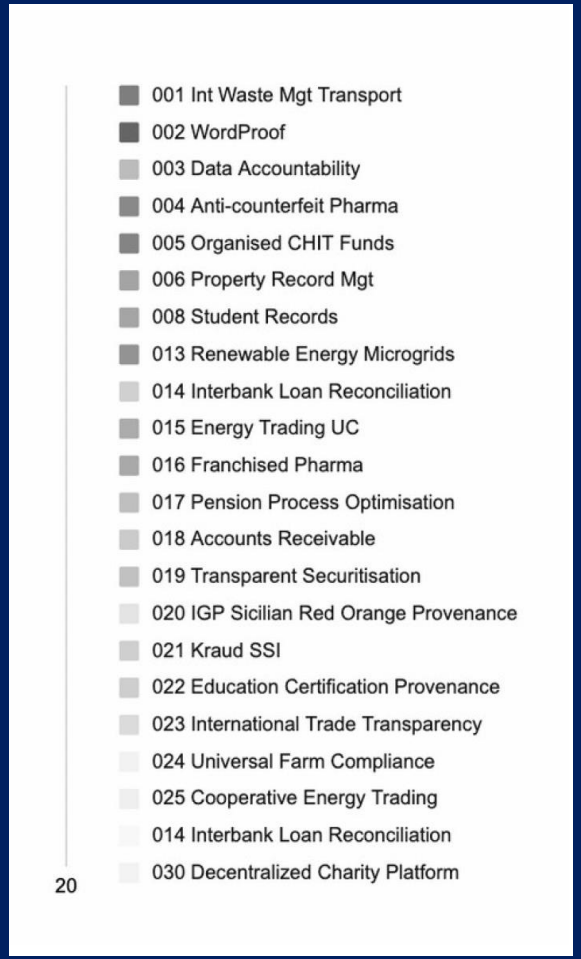
Cooperative Energy Trading (IE)

Energy Trading (IN)

Renewable Energy Prosumer Microgrids (ES)

USE CASE INSIGHTS – CROSS-SECTOR APPLICATIONS





PROPERTY RECORDS MANAGEMENT

The PRMS programme was initiated in 2017s with funding by the Ministry of Electronics and Information Technology (MeitY), Government of India. Further information:
Centre for Development of Advanced Computing (www.cdac.in) Telangana State Government

https://youtu.be/agLgwvPYhio?si=2wn8qVlUvVpZXnGg

INTERBANK RECONCILIATION AND SETTLEMENT

Today, the traditional reconciliation process between different banks often takes as long as T+1 or T+2 days. This long reconciliation time both creates inefficiencies and can lead to information asymmetry.

By enabling reconciliation with a distributed ledger, blockchain technology can streamline and reduce the
settlement period to T+0 days from the industry average of T+1 to T+2 days today.

This use case provides Interbank Loan Reconciliation and Settlement based on DLT, which is a live implementation in China.

The platform is a pioneering blockchain application for a "distributed business scenario", wherein a high level of interbank operational efficiency, process automation and system reliability are required to ensure cost efficiency and business continuity.

By enabling reconciliation with a distributed ledger, blockchain technology can streamline and reduce the settlement period to T+0 days from the industry average of T+1 to T+2 days today.

DECENTRALIZED AID PLATFORM

- **Challenge** is getting food to Syrian refugees in Jordan's refugee camps
- **Underlying issues** include:
  - High transaction costs
  - Too many intermediaries
  - High risk of cheating and fraud
- **Blockchain-based solution** is being used to:
  - Remove transaction costs
  - Send aid directly to individuals
  - Integrate with biometric scanning to prevent fraud
  - Provide greater privacy for individuals
  - *Create an immutable digital identity for each individual*

WFP

United Natio

World Foo

Programm

TRACEABILITY OF AGRICULTURAL FOOD PRODUCTS

This use case represents a strategic solution in the IGP Red Oranges supply chain management through a smart traceability solution based on the blockchain technology.

The solution provided by the Red Orange Upgrading Green Economy (ROUGE) provides the certified and unchangeable history of the product.

ROUGE supports the fight to fraud and forgery and guarantees transparency of transactions, security and Resilience within the supply chain.

SUMMARY OF TRANSFORMATIVE APPLICATIONS: BLOCKCHAIN COULD DISRUPT EXISTING WAYS OF DOING THINGS BY…

1. Enabling distributed organizations with no central authority

- Circumventing intermediaries (e.g. companies, banks, governments)
- Enabling new governance structures

2. Enabling individual data ownership and control

- Can allow individuals to take data with them across platforms

3. Creating new assets and markets

- New digital assets (e.g. utility tokens, cryptocurrencies)
- Tokenization, fragmentation, and recombination of real-world assets

What we've covered

1. Fundamentals: What is blockchain?
2. Applications: How blockchain enhances existing ways of organizing
3. Disruptive opportunities: How blockchain enables new ways of organizing

BLOCKCHAIN + AI

OPEN ACCESS PEER-REVIEWED CHAPTER

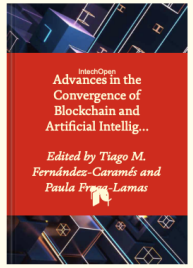
Blockchain-Empowered Mobile Edge Intelligence, Machine Learning and Secure Data Sharing

WRITTEN BY

Yao Du, Shuxiao Miao, Zitian Tong, Victoria Lemieux and Zehua Wang

Reviewed: 14 February 2021 , Published: 12 March 2021

DOI: 10.5772/intechopen.96618



FROM THE EDITED VOLUME

Advances in the Convergence of Blockchain and Artificial Intelligence

Edited by Tiago M. Fernández-Caramés and Paula Fraga-Lamas

Book Details | Order Print

https://www.intechopen.com/chapters/75695

LLM Knowledge Survey

UBC iSchool

AGENDA FOR TODAY

Morning (9:00-11:30)

1. Introductions & overview of the course
2. Introduction to blockchain technology

Lunch (11:30-13:00)

Afternoon (13:00-15:30)

1. The ‘Three Layer Modell’
2. Team Reveal & Icebreaker Activity

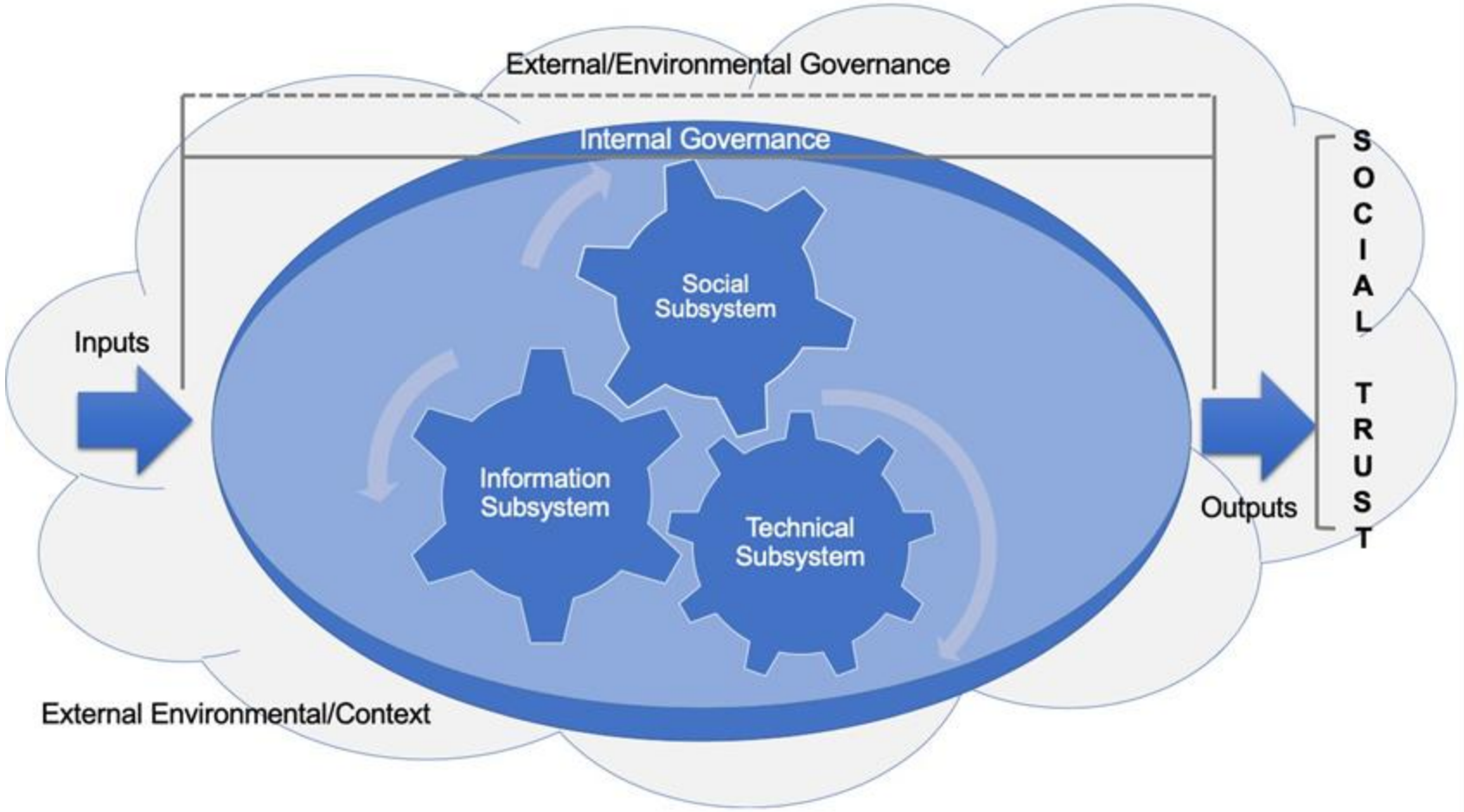
Late Afternoon/Evening (15:30-17:00)

1. Teams Self-Guided Tour of UBC Campus

Lunch Options

The Three Layer Model

A framework for designing and analyzing blockchain/DLT systems



1:30

2. FRAMEWORK FOR DESIGNING AND ANALYZING BLOCKCHAIN SYSTEMS

LEARNING GOALS

- Understand the development of and theoretical ideas underpinning the high-level Three Layer conceptual model of blockchain and distributed ledger systems and be able to discuss its merits relative to other approaches to the design of blockchain and distributed ledger systems

- Explain the “layers” of the Three Layer conceptual model as a multidisciplinary design space, the interactions among the layers and how they relate to the question-led design framework accompanying the model

- Understand and be able to apply the question-led design framework to a design case study.

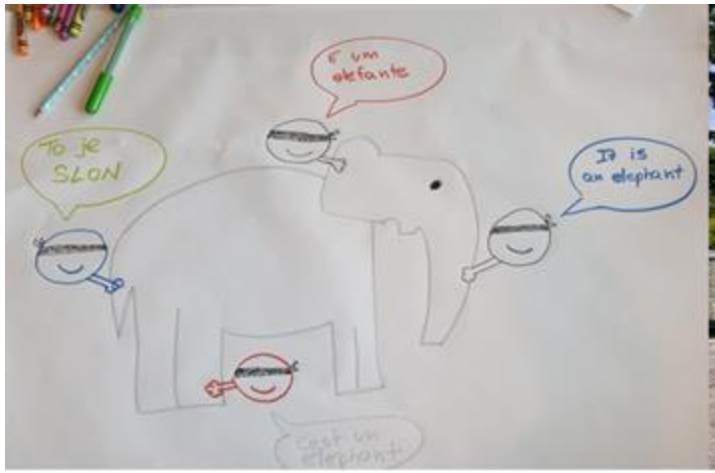
MOTIVATION FOR THE THREE LAYER MODEL

- We need to design effective blockchain/DLT solutions that achieve desirable outcomes. But how?
- The technology is still under theorized and not well understood.
- We need to better understand and consider **the trade-offs** among different characteristics and capabilities in the design of our blockchain/DLT solutions.
  - Existing models for blockchain system design fall short
- Failing to consider the trade-offs comprehensively can produce sub-optimal designs with negative unintended consequences.

WHAT TRADE-OFFS SHOULD WE CONSIDER IN THE DESIGN OF BLOCKCHAIN/DLT SOLUTIONS?

- Discussions of trade-offs in the blockchain/DLT literature are largely conceptualized in terms of the tension that exists among technical features (see, e.g., Kiayias and Panagiotakos, 2015 or Vitalik Buterin's Blockchain Trilemma of Decentralization, Scalability and Security).
- When conceptualization broadens, the focus is usually unidimensional (e.g., governance or ethical design).
- Kannegeisser et al (2019) expand this to considerations of trade-offs among six properties: security, performance, usability, development flexibility, level of anonymity, and institutionalization, drawn from a systematic analysis of extant literature on blockchain and DLT.
- The three layer model views trade offs as not just technical, or even socio-technical, but as *socio-informational-technical* (hence the three layers).

HISTORY AND DEVELOPMENT OF THE THREE LAYER MODEL



The Truth Machine: Exploring the Social, Records and Technical Potential and Pitfalls of Blockchain and Distributed Ledger Technologies

June 10th, 2019 to June 13th, 2019

https://blockchain.pwias.ubc.ca/

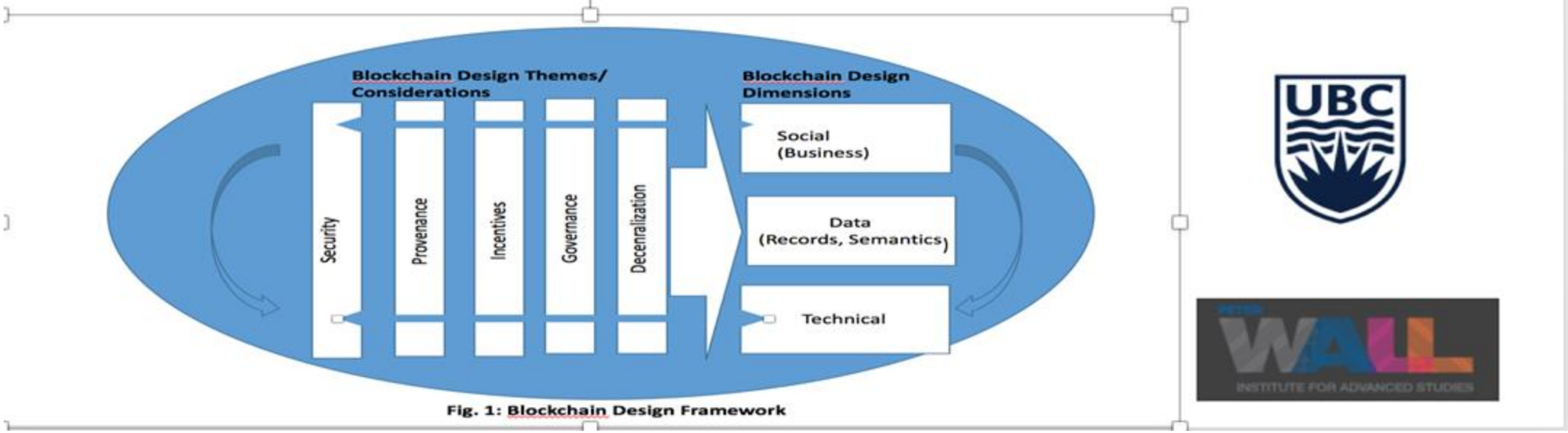


Fig. 1: Blockchain Design Framework

HISTORY AND DEVELOPMENT OF THE THREE LAYER MODEL

© 2021

Building Decentralized Trust

Multidisciplinary Perspectives on the Design of Blockchains and Distributed Ledgers

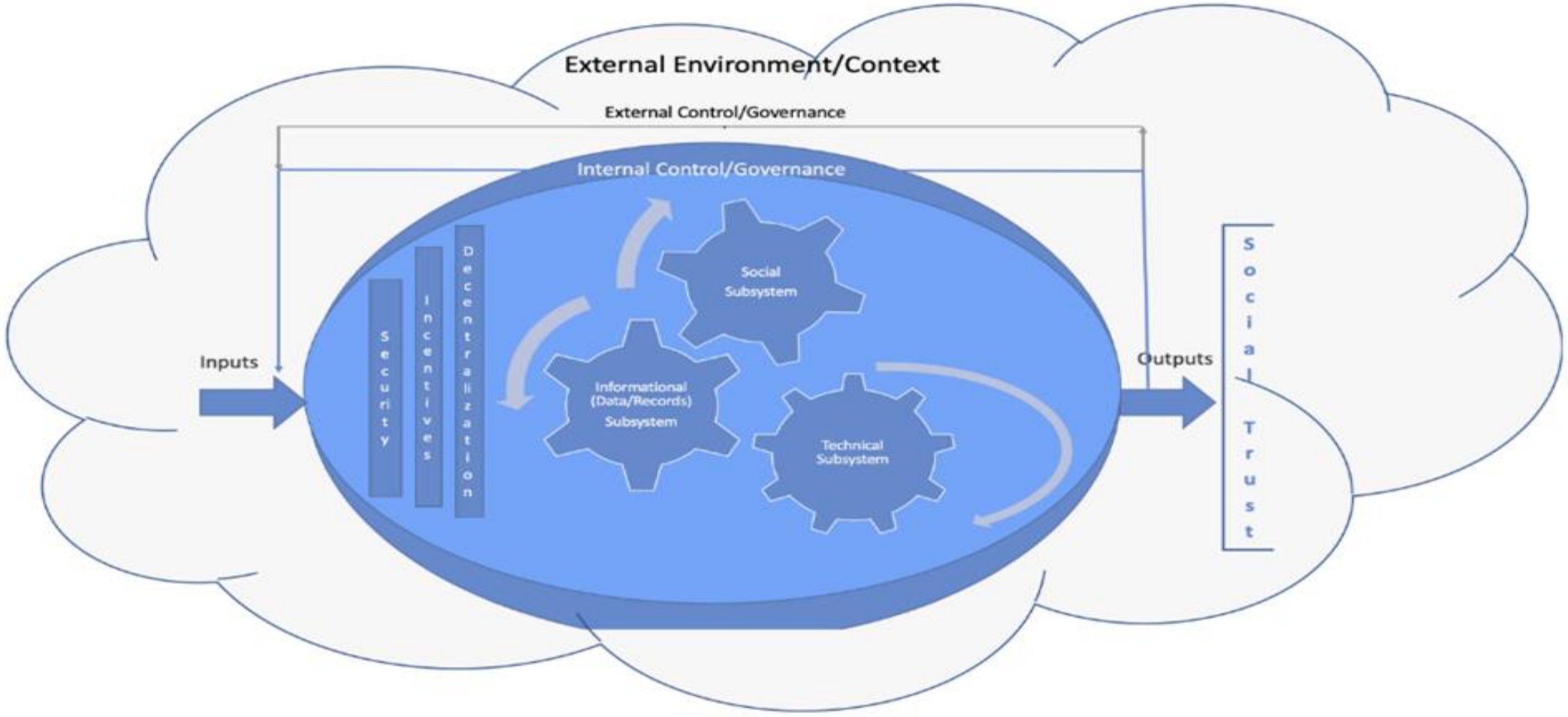
Editors: **Lemieux**, Victoria, **Feng**, Chen (Eds.)

Explores how blockchain can build trust in social, political and economic institutions

OVERVIEW OF THE THREE LAYER MODEL

Let’s begin with a review of the foundations of blockchains we discussed in the first part of the morning . . .

OVERVIEW OF THE THREE LAYER MODEL

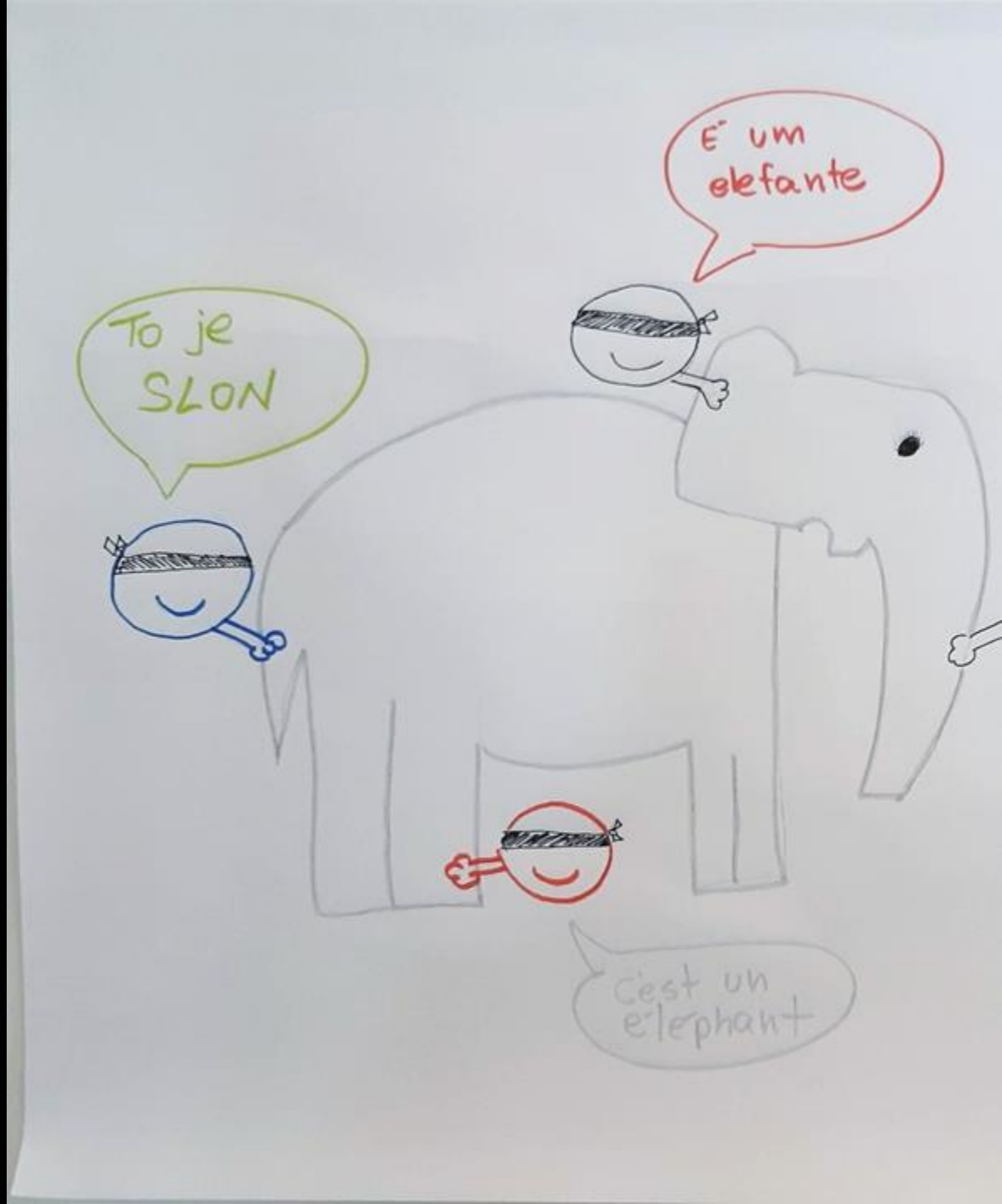


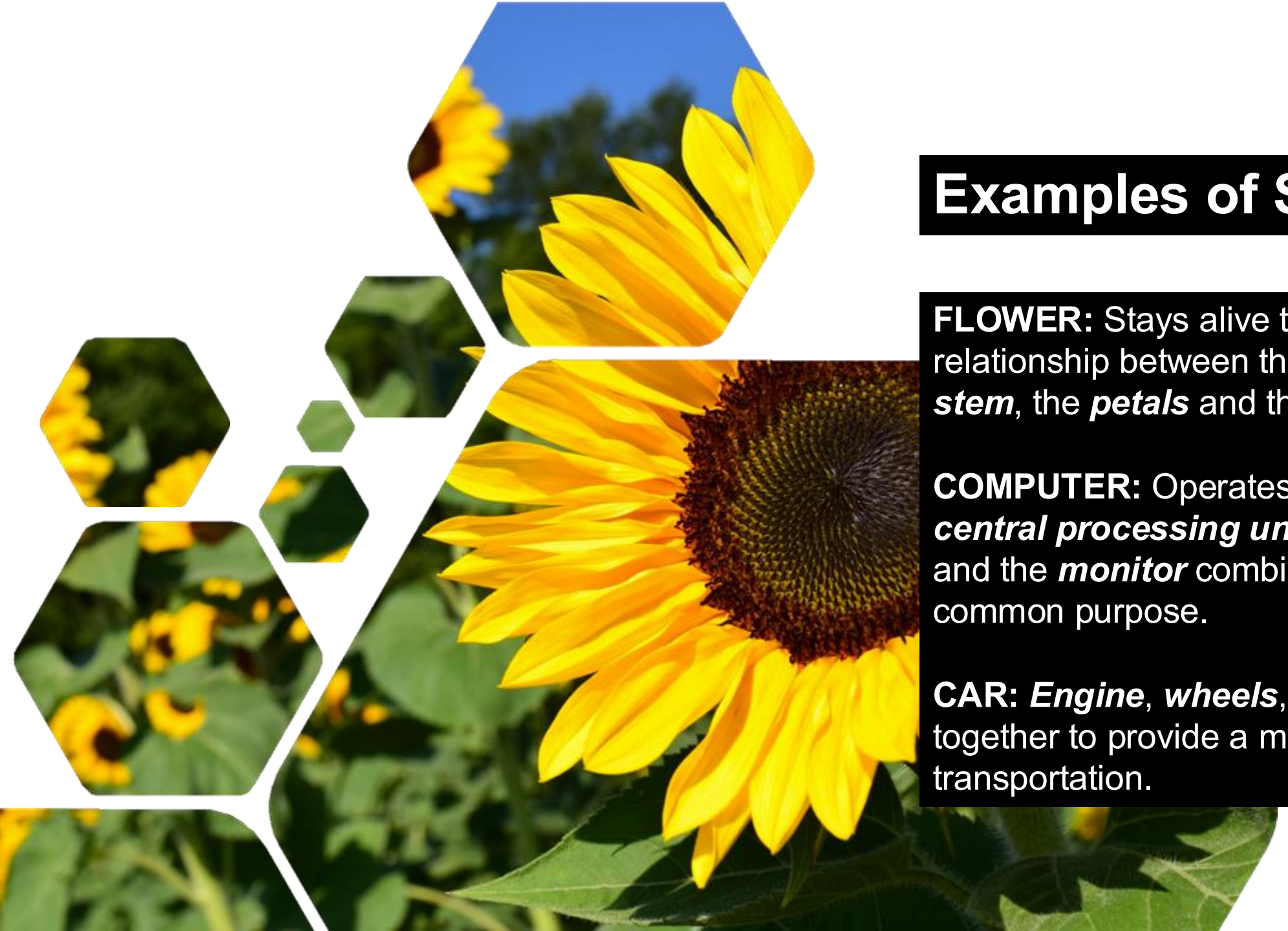
What Is a System?

System: A perceived whole whose elements ‘hang together’ because they continually affect each other over time and operate toward a common purpose. Systems consist of subsystems or functions, processes, activities and tasks.

Systems Thinking

‘Systems thinking’ is the process of thinking **holistically** and in terms of **inter-relationships** between these objects or phenomena, rather than seeing them as unrelated entities.





Examples of Systems

FLOWER: Stays alive through the relationship between the ***roots*** and the ***stem***, the ***petals*** and the ***seeds***.

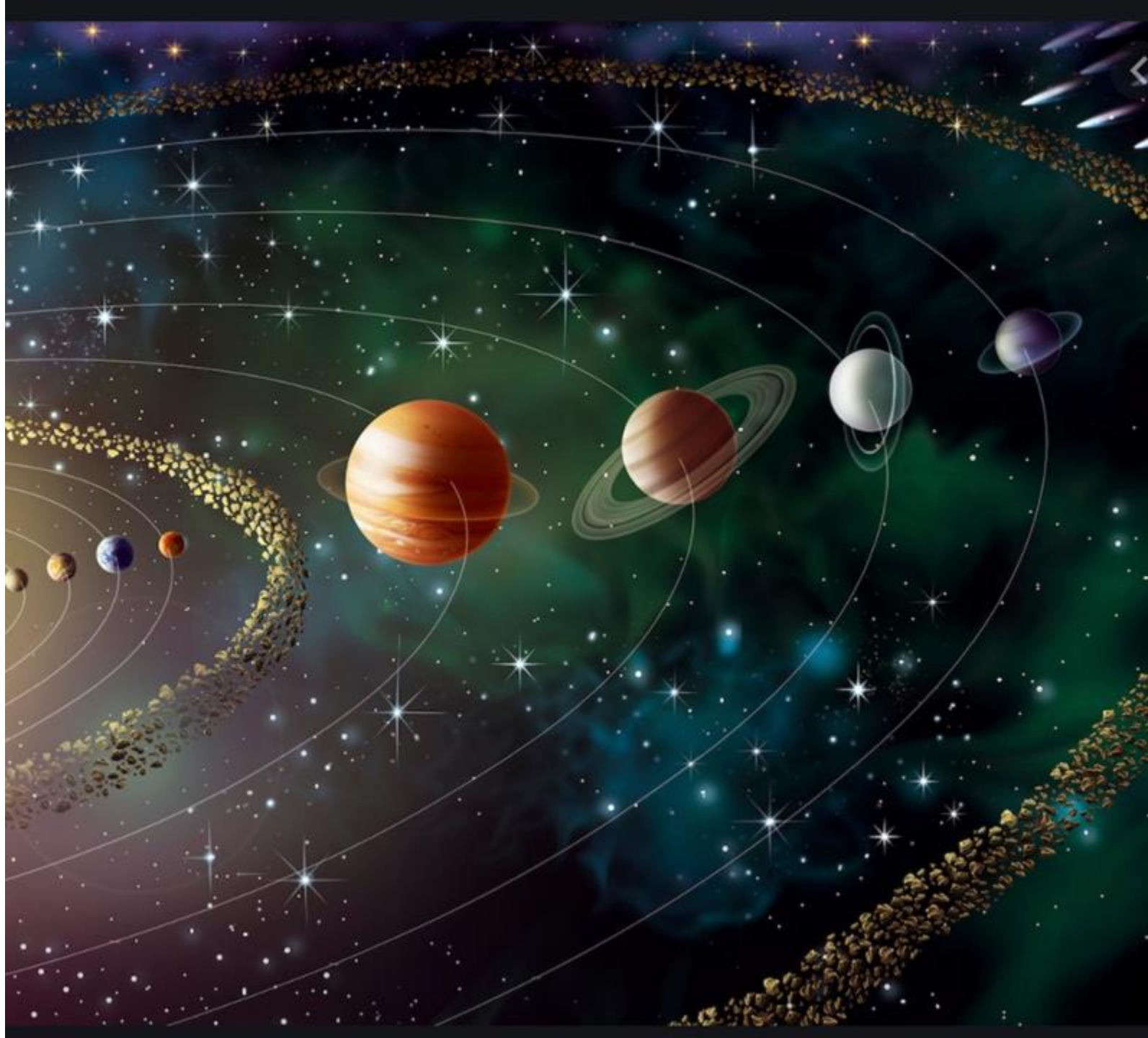
COMPUTER: Operates because the ***central processing unit***, the ***keyboard*** and the ***monitor*** combine toward a common purpose.

CAR: ***Engine***, ***wheels***, and ***chassis*** work together to provide a means of transportation.

Scale of Systems

Large: Solar system

Smaller: Human circulatory system



The Functions (Purpose) of a System

- Systems have functions.
- Function: The means by which THE system fulfils its purpose.
  - E.g. Circulatory System
  - Function: to carry blood through the body
  - Specialized parts: heart, the arteries, the veins.
- The heart is a major component of this system with its own unique. Its function is the pumping of blood through the body.
- The heart also has its own specialized structural components or parts: the aorta, the pulmonary artery, theleft atrium, the left ventricle, the right ventricle and the right atrium.

SUBSYSTEMS

Systems often contain subsystems

E.g. The earth is a subsystem of the Solar System, but can also be viewed as a system in its own right

When the earth is viewed as a system, the ocean can be considered a sub-system of the earth.

So which is the "system"? It depends on what is being examined.

If our focus is the earth, then that is the system.

If the ocean were being analysed, its relationship to the earth would be recognised but the main focus would be on the ocean.

Activities, Transactions, Processes

A system fulfills its purpose via undertaking **activities** (collectivities of which are called functions).

Activities are comprised of **many acts** that may span across an organizational structure, or even (nowadays) integrate several organizations that work together.

A **transaction** is an **act or several interconnected acts** in which more than one person is involved and by which the relations of those persons are altered (Duranti, *New Uses for an Old Science*, Pt. 2) or the smallest unit of a work process consisting of an exchange between two or more persons or systems (ISO 26122)

Business (or work) process: **one or more sequences of transactions** required to produce an outcome that complies with governing rules (ISO 26122).

A **sequence** is a **series of transactions** connected by the requirement that undertaking a later transaction **is dependent** on **completing earlier transactions** (ISO 26122).

ADVANTAGES OF A SYSTEMS APPROACH TO BLOCKCHAIN DESIGN

- Allows us to understand how design components (“subsystems”) are dynamically interacting with other components
- Allows us to evaluate systems holistically, and identify blind spots, hidden assumptions, and unexpected outcomes.
- Provides a foundation to dive deeper into different subsystems

THE THREE LAYERS

Social: Encompasses the social actors, and the social, political, and economic implications of these tools and platforms.

Informational: Focuses on the ledger itself as an ”immutable” store of transactional data.

Technical: Understood, even as there remain novel technical challenges to be overcome, being those technical components that implement blockchain and distributed ledger systems.

Each can be thought of as different abstraction layers

UBC iSchool

THE THREE LAYER MODEL IN DETAIL - TRUST

- Satoshi Nakamoto was the pseudonymous creator of Bitcoin, which gave rise to blockchain, Bitcoin's underlying technology
- In his own words, Nakamoto stated his reasons for creating Bitcoin (and Blockchain):

Commerce on the Internet has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments. While the system works well enough for most transactions, it still suffers from the ***inherent weaknesses of the trust based model****. Completely non-reversible transactions are not really possible, since financial institutions cannot avoid mediating disputes. The cost of mediation increases transaction costs, limiting the minimum practical transaction size and cutting off the possibility for small casual transactions, and there is a broader cost in the loss of ability to make non-reversible payments for non-reversible services. With the possibility of reversal,* ***the need for trust spreads****. Merchants must be wary of their customers, hassling them for more information than they would otherwise need. A certain percentage of fraud is accepted as unavoidable. These costs and payment uncertainties can be avoided in person by using physical currency, but no mechanism exists to make payments over a communications channel* ***without a trusted party*** *(Nakamoto, 2008a, p. 1).*

- Therefore, Blockchain was created to solve the problem of TRUST, without relying on a trusted intermediary (which is often not very trustworthy) . . . In other words TRUSTLESS TRUST

UNDERSTANDING AND THEORIZING KEY BLOCKCHAIN AND DISTRIBUTED LEDGER PROPERTIES, CAPABILITIES AND OUTCOMES USING THE THREE LAYER CONCEPTUAL MODEL

- Governance
- Incentives
- Security
- Decentralization
- Provenance tracking
- Temporality

DEEPER UNDERSTANDING ABOUT KEY ASPECTS OF BLOCKCHAINS/DLTS

- **Governance:**
  - A Blockchain/DLT control mechanism
  - Internal
  - External
- **Incentives:** a type of "actuator" that operates on the "logic" or set of instructions for processing information possessed of all system components.
- **Security:** Design of DLT systems not only involves the commonly mentioned trade-off between security and scalability (see, for example, Gountia, 2019) but also trade-offs among different security properties, i.e., confidentiality versus transparency, or data integrity vs. privacy. Equally, there may be trade-offs within the same security property as applied at different layers or levels of abstraction within the same layer, e.g., bit-wise data integrity may be in tension with the consequential integrity needed for records.

UBC iSchool

DEEPER UNDERSTANDING ABOUT KEY ASPECTS OF BLOCKCHAINS/DLTS

- **Decentralization:** The architecture of each sub-system/layer of a DLT system can be centralized or decentralized to varying degrees to affect the operation of the system as a whole.
    - to make assertions about the relationship between the design of decentralized sub-system components and the effects of those designs requires much more theoretical and empirical research on a social theory of change in relation to blockchain/DLT systems.
- **Provenance tracking:** a functional capability rather than an inherent property of a DLT system, its sub-systems, or components.
- **Temporality:** Blockchain/DLT systems, however, are not static and their properties and capabilities may not be entirely predictable.

A QUESTION-LED DESIGN FRAMEWORK BASED UPON THE THREE LAYER CONCEPTUAL MODEL – SYSTEM LEVEL

System Goal

- What is the stated purpose of the DLT system?
- How does the stated purpose support social trust?
- What problem(s) should this system solve?
- What use cases is the system designed to support?

System Constraints

- What behaviors must the system be designed not to tolerate?
- What is the system's space of permissible actions?

System Capabilities

- What capabilities must the system possess in order to achieve its goal within prescribed constraints?

A QUESTION-LED DESIGN FRAMEWORK BASED UPON THE THREE LAYER CONCEPTUAL MODEL – SYSTEM LEVEL

Environment

- Is the environment in which the DLT system operates relatively homogeneous or is it more heterogenous?
- What assumptions about the environment does the DLT system make in its design/operation?
- What aspects of the environment does the system rely upon? At what points and for what purposes are these relied upon?
- How aligned with all aspects of the environment is the DLT system?
- What elements from the environment influence or constrain designers of the DLT system?
- What elements from the environment influence or constrain system actors or actants?

A QUESTION-LED DESIGN FRAMEWORK BASED UPON THE THREE LAYER CONCEPTUAL MODEL – SYSTEM LEVEL

Temporality

- What known future changes will the system have to be able to respond to?
- What mechanisms need to be put in place to assure the longevity of the system?
- Could future events bring about consequences where the platform ought to be completely replace or cease operation?
- How will the governance sub-system address actors/actants' changing relationships to the system over time?
- How will risk factors be addressed, including those that lie unknown in the future and that may present existential or systematic risk?
- How has/does power shift among social actors over time?

UBC iSchool

A QUESTION-LED DESIGN FRAMEWORK BASED UPON THE THREE LAYER CONCEPTUAL MODEL – SUB-SYSTEM LEVEL

Social Sub-System

- Who are the social actors in the DLT? How are they identified/represented? How are their identities regulated?
- How does the DLT system empower or constrain their agency? What types of actions of social actors are forbidden, encouraged, or tolerated?
- Where is power located among social actors?
- What values are important to the social actors in this system?
- What expectations do we have of the behavior of the social actors?
- What actions will or might they take? How are these actions expected to impact upon others?
- When is the consent, permission, and authority of social actors needed, granted, or assumed?
- Will some social actors act on behalf of others? On what (moral, legal?) ground do they implement the will of others? Which others?
- How do social actors need to exercise (or do they exercise) discretion when conflict arises?

UBC iSchool

A QUESTION-LED DESIGN FRAMEWORK BASED UPON THE THREE LAYER CONCEPTUAL MODEL – SUB-SYSTEM LEVEL

Informational Sub-System

- How does the ledger serve to support social trust in the context of the DLT system?
- What data is captured/flows through the system to support the system goal? What records are generated to support the system goal, either on ledger or off ledger?
- How are the data/records actants in the system identified and how are their identities regulated?
- What data and/or records must the system store? (What are the legal or regulatory obligations?)
- What data and/or records must not be stored in the system? (For purposes of privacy, financial risk management, or corporate policy.)
- Are there data and/or records that require special consideration? For example, are there data and/ or records containing personally identifiable information that requires special treatment under law?
- Are there data and/or records that must not be kept indefinitely?
- Where are records stored? How are they propagated across networks? How are the intellectual components of the record assembled?

UBC iSchool

A QUESTION-LED DESIGN FRAMEWORK BASED UPON THE THREE LAYER CONCEPTUAL MODEL – SUB-SYSTEM LEVEL

Technical Sub-System

- What are physical actants in the DLT system (e.g., sensors, vehicles)?
- How are the technical actants in the system identified and how are their identities regulated?
- How do the physical actants serve to support social trust in the context of the DLT system?
- What capabilities and properties do they require to support the system goal?
- What is the system architecture?
- What is the network architecture/topography?
- What social actors control the physical actants in the DLT system?
- How do these social actors empower or constrain the activity of physical actants?
- What level of authority/authorization do the physical actants have?

UBC iSchool

A QUESTION-LED DESIGN FRAMEWORK BASED UPON THE THREE LAYER CONCEPTUAL MODEL – SUB-SYSTEM LEVEL

Governance Sub-System

- How much reliance will there be on internal or self-regulating governance versus external governance under normal operating conditions? Under abnormal operating conditions?
- How will consensus decisions be made among technical, informational, and social actants/actors?
- What incentives are or will need to be put in place so that the consensus mechanism operates in a manner that supports the goal of the system?
- How should decision management rights and decision control rights be allocated among various interacting components (where social, informational, or technical)?
- How will disagreement about those decisions be resolved?

FURTHER READING

- Lemieux, V.L., Searching for Trust: Blockchain Technology in an Age of Disinformation. Cambridge University Press, Cambridge, forthcoming April 2022.
- Lemieux, V. L., Bravo, M.: Introduction: Theorizing from multidisciplinary perspectives on the design of blockchain and distributed ledger systems (Part 1). In: Lemieux, V., Feng, C. (eds.), Building Decentralized Trust: Multidisciplinary Perspectives on the Design of Blockchains and Distributed Ledgers. Springer, Heidelberg (2021).
- Lemieux, V. L., Feng, C..: Conclusion: Theorizing from multidisciplinary perspectives on the design of blockchain and distributed ledger systems (Part 2). In: Lemieux, V., Feng, C. (eds.), Building Decentralized Trust: Multidisciplinary Perspectives on the Design of Blockchains and Distributed Ledgers. Springer, Heidelberg (2021).
- Palmer, C. K., Rowell, C., & Lemieux, V. L. (2021). Multidisciplinary Blockchain Research and Design: A Case Study in Moving from Theory to Pedagogy to Practice. In Diversity, Divergence, Dialogue: 16th International Conference, iConference 2021, Beijing, China, March 17–31, 2021, Proceedings, Part I 16 (pp. 587-602). Springer International Publishing.

ADVANTAGES OF USING THE THREE LAYER MODEL

- Created a common conceptual framework and language for multidisciplinary, problem-oriented design space.
- Able to ‘see’ the possible cross-over, knock on effects of design choices (i.e., mobilized ‘systems thinking’ in a design context)
- By utilizing the Question-led Framework to anchor our scope discussions, design team could more clearly delineate necessary requirements for an immediate prototype in contrast to long-term design goals for the full system (these latter aspirations were recorded for later reference).
- Helped identify the previously “unknown unknowns.”
- Framing of technical questions led to exploration of novel technical capabilities, e.g., integration with IoT.

LIMITATIONS OF THE THREE LAYER MODEL

- Questions are high-level and complex, and require time to learn and understand
- Still requires more broad-based empirical validation and reproducibility
- Applicability to other technologies, e.g., AI, remains to be seen

TEAM REVEAL

Team 1	Team 2	Team 3	Team 4	Team 5	Team 6
Juyeon Weon	Soonhong Kwon	AHMED ANTWI-BOAMPONG	Hongyan Sun	DAESUNG HWANG	Feng Haozhe
Kwon Yonghyun	Dr. Emmanuel Freeman	pyongjoo kim	Dasol Kim	Dowon Jang	Kim Junsik
Yasna Ahmad	Gwangjin Lee	Mingzhe Xue	Zhiyu Zhao	Joel Traber	Wooyoung Son
Nayoung Kong	minhee song	Mia Maric	JEHYEOK PARK	Michaela Jordache	LEE JIWON
ZHANG Jingyi	YAXI LI	Kaiyung Cao	Jeongwoo Seo	JI-HO LEE	Minjae Lee
JaeWookLee	Leyao Tan	Shun Yan Lee	Mariam Natalie Solis	Hong Yutong	Jean-Michel Carrel

ICEBREAKER ACTIVITY

2:30

2. APPLYING THE FRAMEWORK

Case Study – Swear (Background)

- Artificial intelligence (AI) has rapidly developed in the past two years
- Despite AI's immense potential to revolutionize industries and economies, scientists have warned of its risks
- This case study focuses on a key AI-related challenge that we are facing: deepfakes.
- Counterfeit images and videos are eroding the visual grounds for establishing belief in truth claims. Seeing is no longer believing.
- Blockchains are said to have capabilities that can defend against deepfakes. In this case study we will take a closer look at the Swear solution through the lens of the Three Layer Model, as a means of critically assessing the solution design and its application.

Case Study - Swear

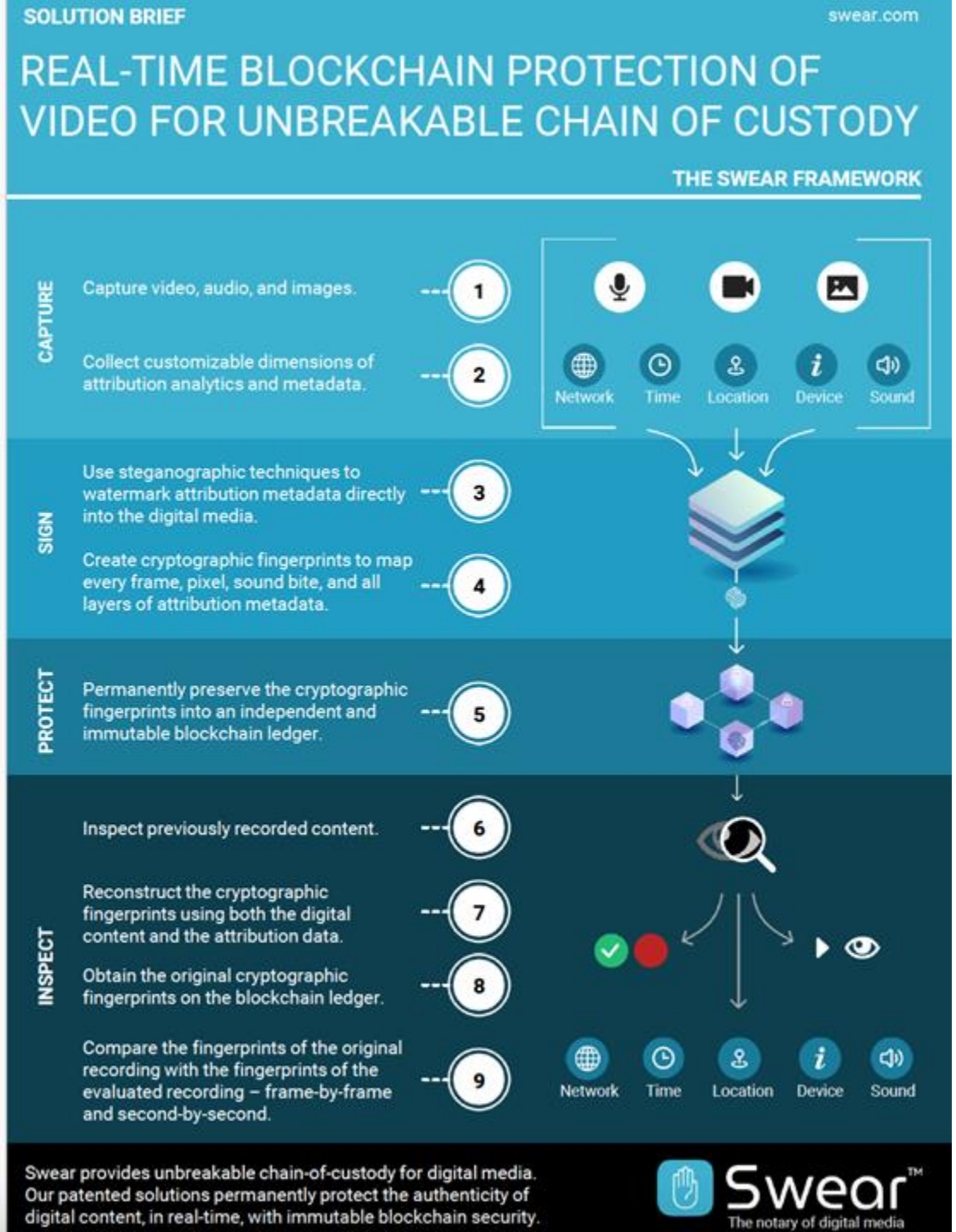
https://www.youtube.com/watch?v=AKWNA8XUWrw

Disclaimer

I have no relationship with this company and do not endorse its solution. The solution is being discussed for illustrative purposes only.

Swear Architecture & Workflow (https://swear.com/a/)

- Mobile App for video capture
- Supported formats: D1, 960H, HD-SDI, AHD,
HD-TVI, HD-CVI, IP, 4k
- Codecs: H.264, AVI, AVCHD H.265 (HVEC)
- Compatible with DVR and NVR
- Web3.0 Blockchain secures the fingerprints, establishing an immutable chain-of-custody.
- Digital media authenticity verified continuously and in real-time.
- identification of media manipulation at the pixel level.
- Integrates into existing surveillance systems.



CASE STUDY ANALYSIS . . .NEXT STEPS

- Review & discuss the Swear solution using the Three Layer Model. Look to classify features and capabilities of the solution according to the Three Layer Model; look for interconnections and interactions between each 'layer' of the model i.e., how does ledger enhance trust? Who are the social actors and institutions? What type of blockchain is used, and how is consensus formed?

QUESTIONS & ANSWERS

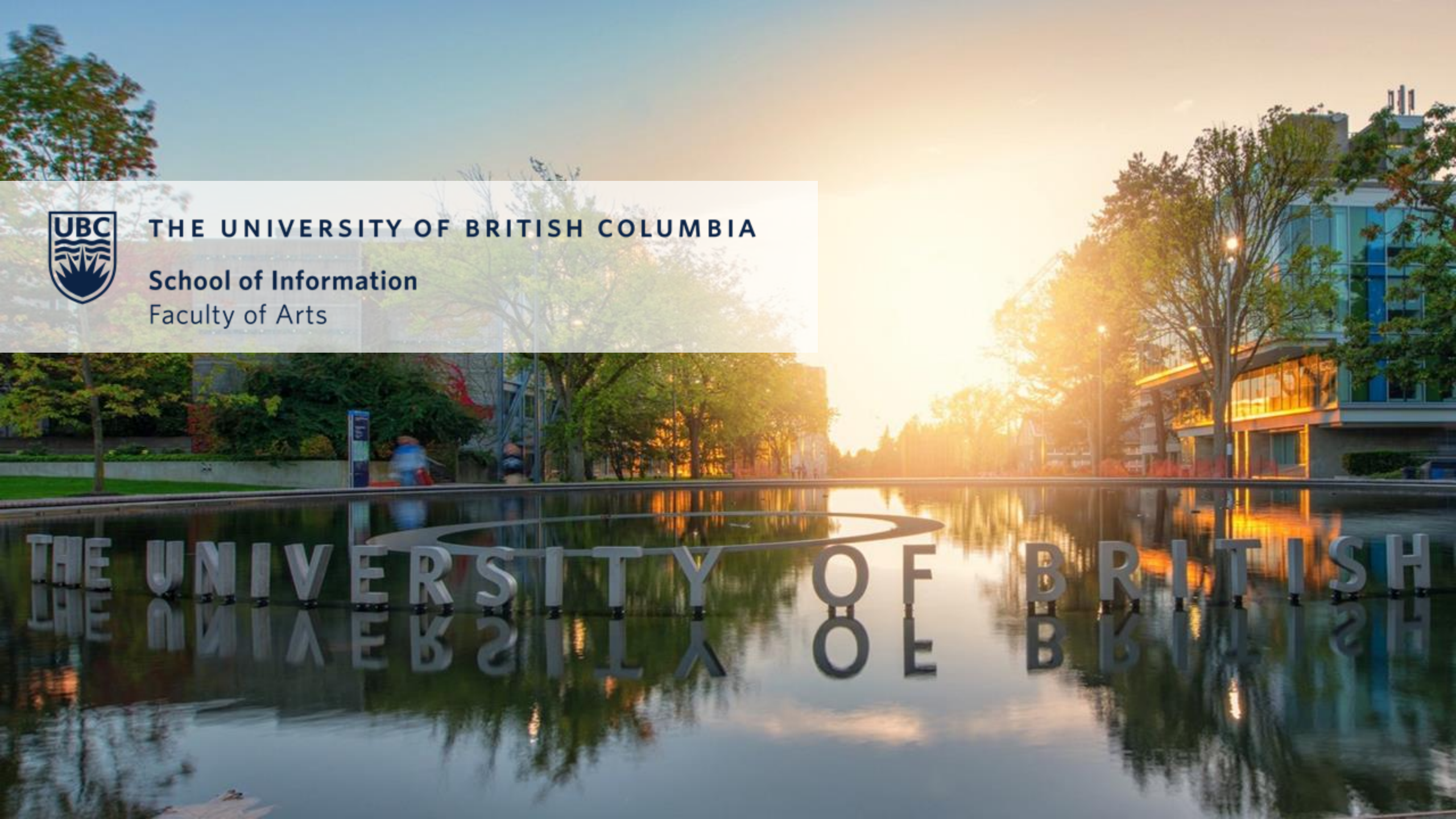
TEAM REVEAL & ICEBREAKER ACTIVITIES

TEAMS SELF-GUIDED TOUR OF UBC

TEAMS SELF-GUIDED TOUR OF UBC (Note: Moved to Tuesday 15:30-17:00)

- In the Google Doc Folder, you will find a document called UBC Self-Guided Walking Tour and a Wayfinding Map of UBC
- Teams should go to as many locations as they can visit until 17:00
- At each location, take a team ‘selfie’ as proof that you have visited the location and upload it to the Google Doc Folder for your Team
- We will put together a souvenir Blockchain@UBC 2025 poster using these photos

BEFORE YOU HEAD OUT FOR YOUR TEAM SELF-GUIDED TOUR WE WILL HAVE A GROUP PHOTO ON THE STEPS OF THE LIFE BUILDING


THE UNIVERSITY OF BRITISH COLUMBIA
School of Information
Faculty of Arts
THE UNIVERSITY OF BRITISH