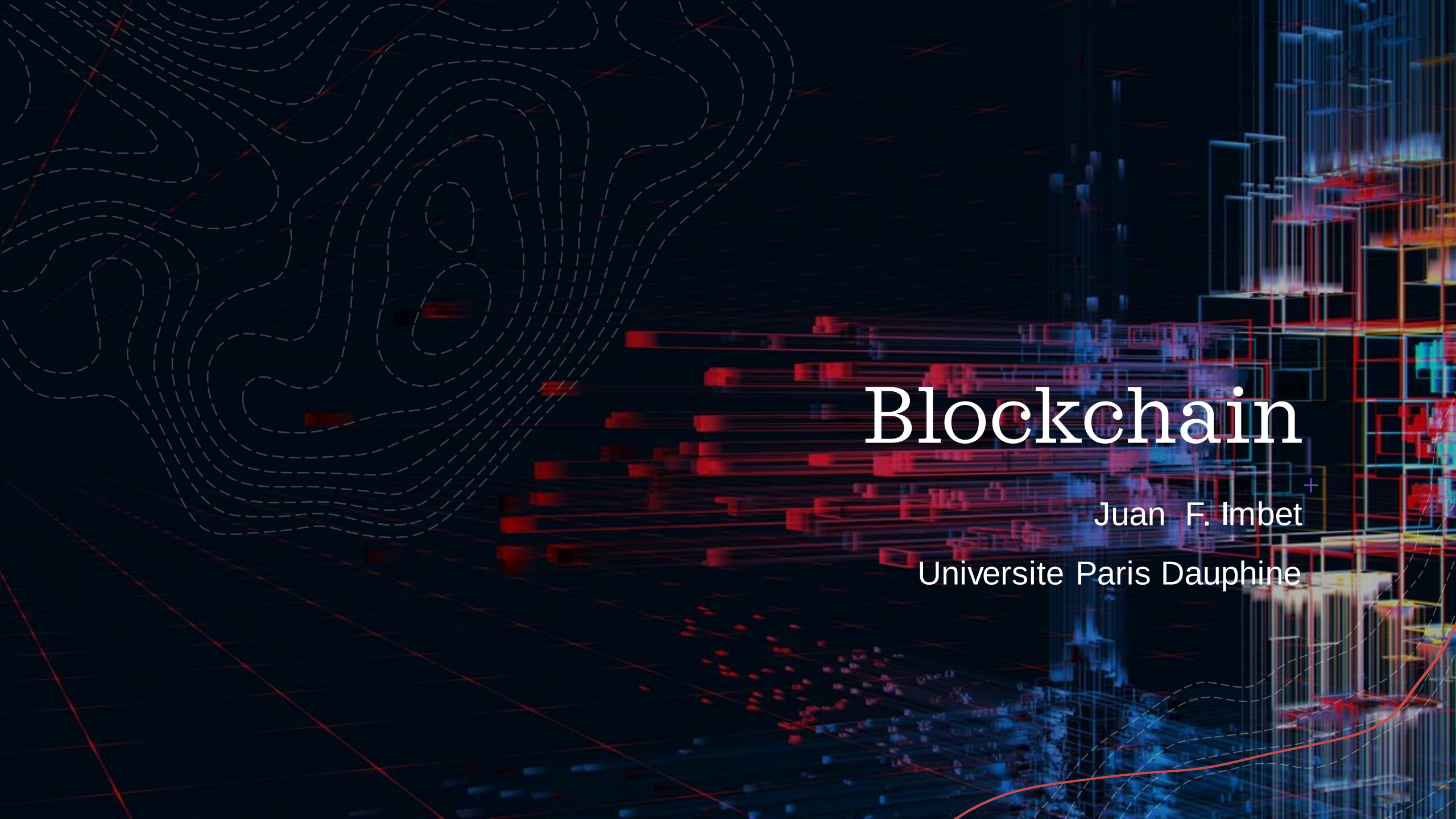


Blockchain

Juan F. Imbet

Universite Paris Dauphine

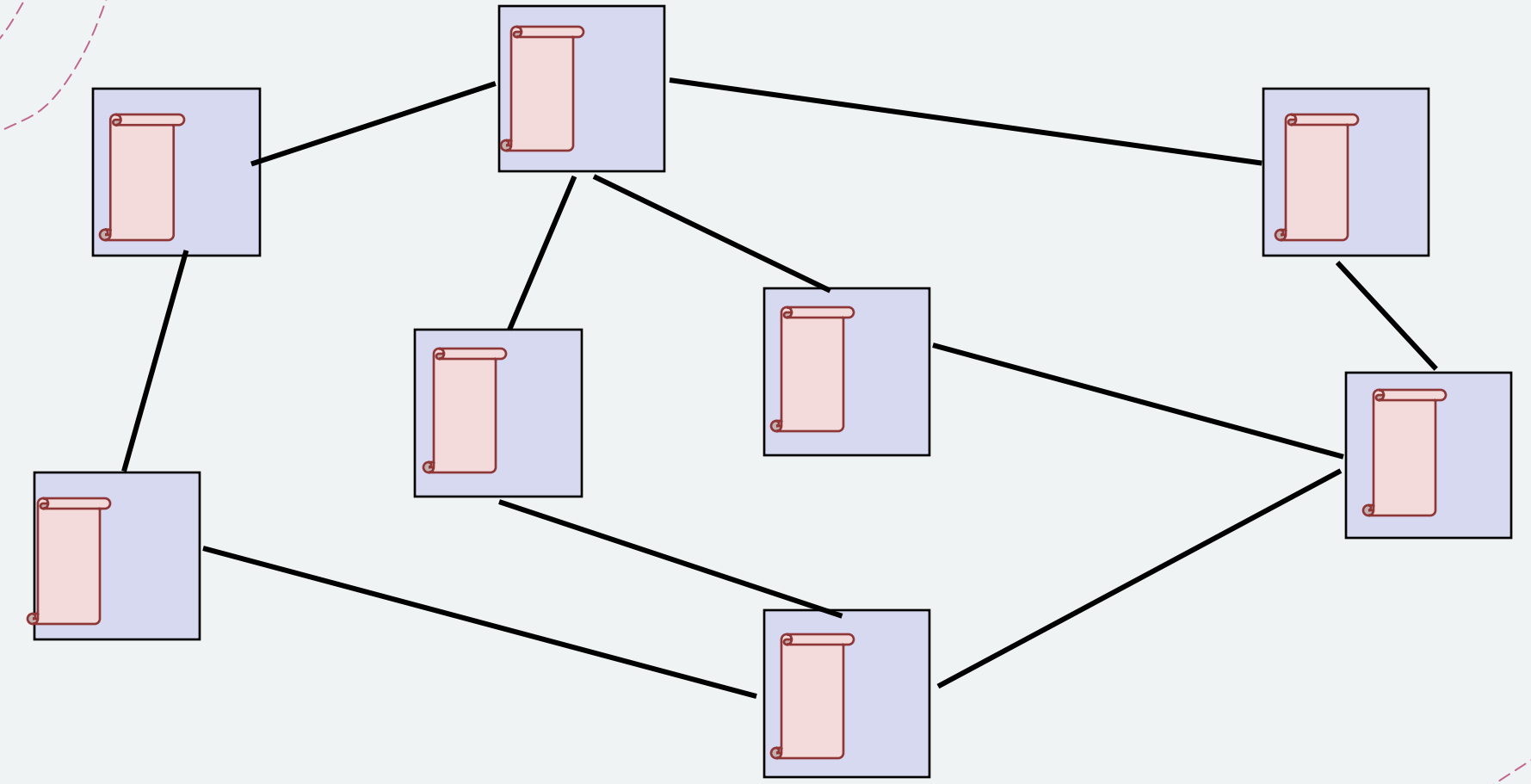
Agenda

+ Blockchain
+ Distributed Ledgers
+ Web 3.0
+ NFTs
+ Decentralised Finance

What is Blockchain?

- A blockchain is a shared **ledger** of transactions between parties in a network not controlled by a single central authority.
- You can think of a ledger like a record book: it records and stores all transactions between users in chronological order.
- Instead of one authority controlling this ledger (like a bank), an identical copy of the ledger is held by all users on the network, called **nodes.**

The blockchain in practice



Distributed:
All copies of one document are spread among users and they are constantly and automatically synchronised, hence identical at all times.

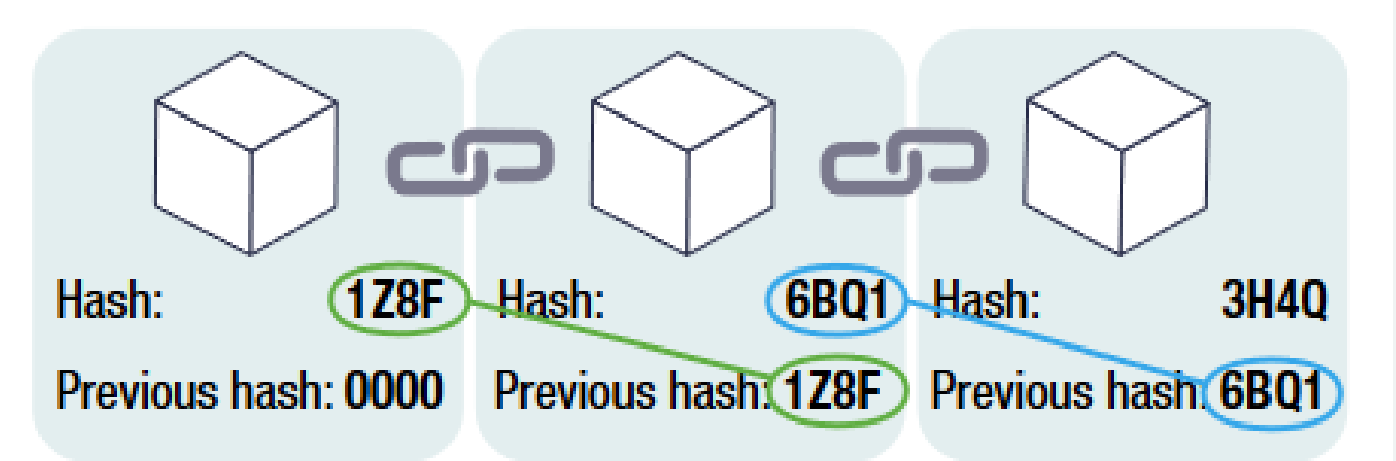
How does the ledger look like?

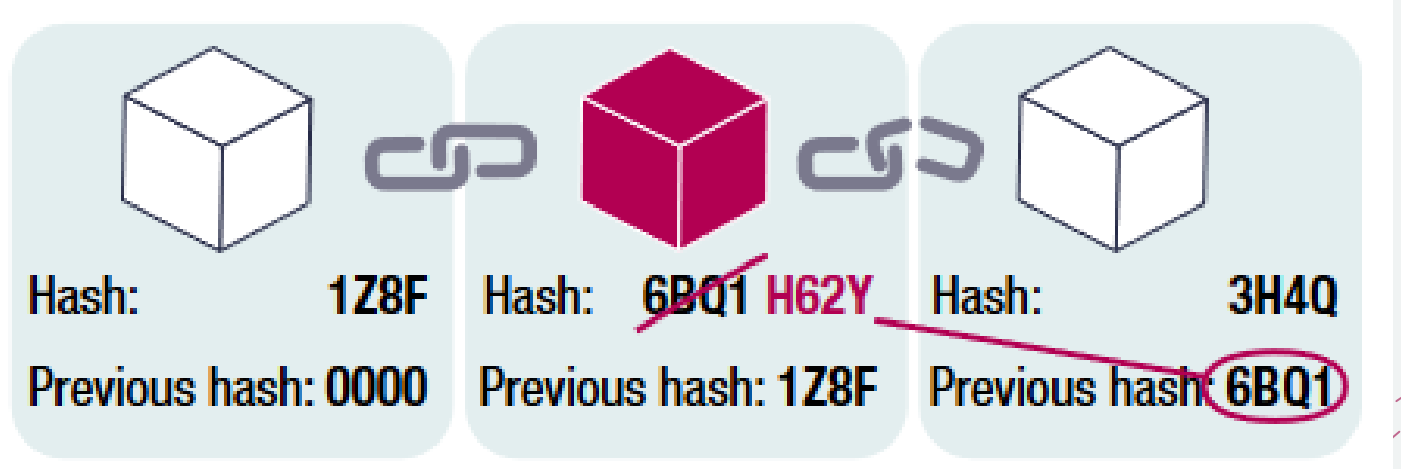
- The ledger is a list of all transactions that consist of a chain of blocks.
- A block is comprised of a group of transactions from the same time period, like a page from a record book.
- Blocks have a unique ID represented as the **hash** of its own code (or something that makes them unique).
- Along with its own hash, each block stores the hash of the block before it.

Ledger

- A hash is a unique string of letters and numbers created from text using a mathematical formula. Blocks are therefore “chained” together making the ledger (almost) immutable or unable to be changed. To add a block, it may first need to be mined and then approved by a number of notes through a consensus mechanism.

Example


Hash: 1Z8F
Previous hash: 0000
Hash: 6BQ1
Previous hash: 1Z8F
Hash: 3H4Q
Previous hash: 6BQ1


Hash: 1Z8F
Previous hash: 0000
Hash: 6BQ1 H62Y
Previous hash: 1Z8F
Hash: 3H4Q
Previous hash: 6BQ1

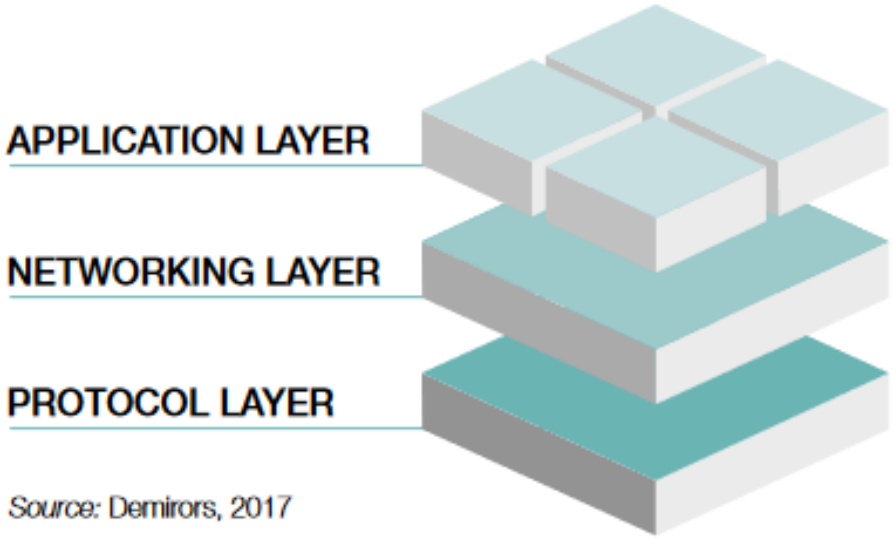
Different types of blockchain

			READ	WRITE	COMMIT	EXAMPLE
BLOCKCHAIN TYPES	OPEN	Public permissionless	Open to anyone	Anyone	Anyone	Bitcoin, Ethereum
		Public permissioned	Open to anyone	Authorised participants	All or subset of authorised participants	Supply chain ledger for retail brand viewable by public
	CLOSED	Consortium	Restricted to an authorised set of participants	Authorised participants	All or subset of authorised participants	Multiple banks operating a shared ledger
		Private permissioned "enterprise"	Fully private or restricted to a limited set of authorised nodes	Network operator only	Network operator only	External bank ledger shared between parent company and subsidiaries

The Layers of Blockchain

- Because blockchains work as a distributed database, they can also work as a distributed computing system.

The layers of blockchain



Source: Demirors, 2017

Blockchain is comprised of three layers that each add different components to its development. It is not necessary to get involved in the most technical layers in order to develop an application or use a blockchain application.

The **protocol layer** lays the foundational structure of the blockchain. It determines the computing language the blockchain will be coded in and any computational rules that will be used on the blockchain.

The **networking layer** is where the rules set up on the protocol layer are actually implemented.

The **application layer** is where networks and protocol are used to build applications that users interact with.

Blockchain: Distributed

- **Distributed:** The main ledger is maintained and held by all nodes in the network. No central authority holds or updates the ledger, rather each node independently constructs its own record by processing every block, deciding if its valid, and voting via the **consensus mechanism** on their conclusion.

Blockchain: Immutable

- In general, once a transaction is added to a blockchain ledger, it cannot be undone.
- The immutability is secured through its use of cryptography. In a centralised database, an authorised user can connect to the server to add or modify the data without the approval.

Agreed by consensus

- No block can be added to the ledger without approval from specified nodes in the network.
- Rules regarding how this consent is collected are called **consensus mechanisms.**
- Consensus protocols are crucial in ensuring that every block is valid and that all participants agree and maintain the same version of the ledger.

Misconceptions about blockchain

- **Pseudonymous:** Blockchain does not allow its users to be totally anonymous. User identities are anonymous but their accounts are not, as all of their transactions are visible to all other users.

Mining

- For some blockchains, in order to add blocks to the ledger, transfers must go through a mining process.
- Mining is a way of adding transaction records, via blocks, onto a public ledger.
- Miners are nodes in the network that ensure the transactions in the block are valid.
- Specifically, they ensure that senders have not already used the funds they want to send to receivers.
- Once miners finish the verification, they have to ask the network for **consent** to add the new block to the ledger.
- In order to do so, they have to follow the **consensus mechanisms** chosen for the platform.

Consensus

- Agreement among the nodes regarding the "state" of the ledger is essential for the function of the blockchain ledger.
- The bitcoin blockchain uses a consensus model called **Proof of Work,** which requires the miner to compete against other miners to create and broadcast blocks for approval.
- **Proof of work** (PoW) describes a system that requires a not-insignificant but feasible amount of effort in order to deter frivolous or malicious uses of computing power, such as sending spam emails or launching denial of service attacks.

Proof of Work at Bitcoin

- PoW requires nodes on a network to provide evidence that they have expended computational power (i.e. work) in order to achieve consensus in a decentralized manner and to prevent bad actors from overtaking the network
- The work itself is arbitrary. For Bitcoin, it involves iterations of SHA-256 hashing algorithms.
- Proof of work requires a computer to randomly engage in hashing functions until it arrives at an output with the correct minimum amount of leading zeroes. For example, the hash for block #660000, mined on December 4, 2020 is 00000000000000000008eddcaf078f12c69a439dde30dbb5aac3d9d94e9c18f6. The block reward for that successful hash was 6.25 BTC.

Digital Assets

- **Tokens:** Tokenization describes the process of transferring rights to a real world asset into a digital representation – or token – on the blockchain. Being in possession of that digital token then gives you the right to that asset and the ability to trade and track it digitally.

Types of digital assets

- **Payment tokens:** Commonly known as cryptocurrency, a payment token can be store of value and a unit of measurement.
- **Utility tokens:** A token that represents a right to a good or service, similar to a gift card.
- **Security tokens:** A token that provides equity or equity like investment in a company. The holder of the token has rights to the company's future profits.

Relevance

- In today's financial system, banks are an essential intermediary for financial transactions and transfers. They verify the identity of the sender, the ability of the sender to make a transfer (i.e. a sufficient account balance) and accuracy of the recipient's address. In this context, the bank acts as the only trusted third party.
- However given the bank stores all data on a single centralised ledger, it therefore creates a single point of failure, whereby hackers or malicious actors can direct all their efforts for cyberattacks or manipulation to this specific entity. These financial intermediaries also charge fees to process transactions. In the case of international remittances, these fees are significant compared to the overall value of the transaction.

Blockchain beyond finance

- Blockchain technology goes far beyond cryptocurrencies and tokens, and its usefulness as a wider economic and administrative tool is well worth exploring. The table below describes just a small sample of blockchain's potential to transform supply chains, healthcare and the energy sector.

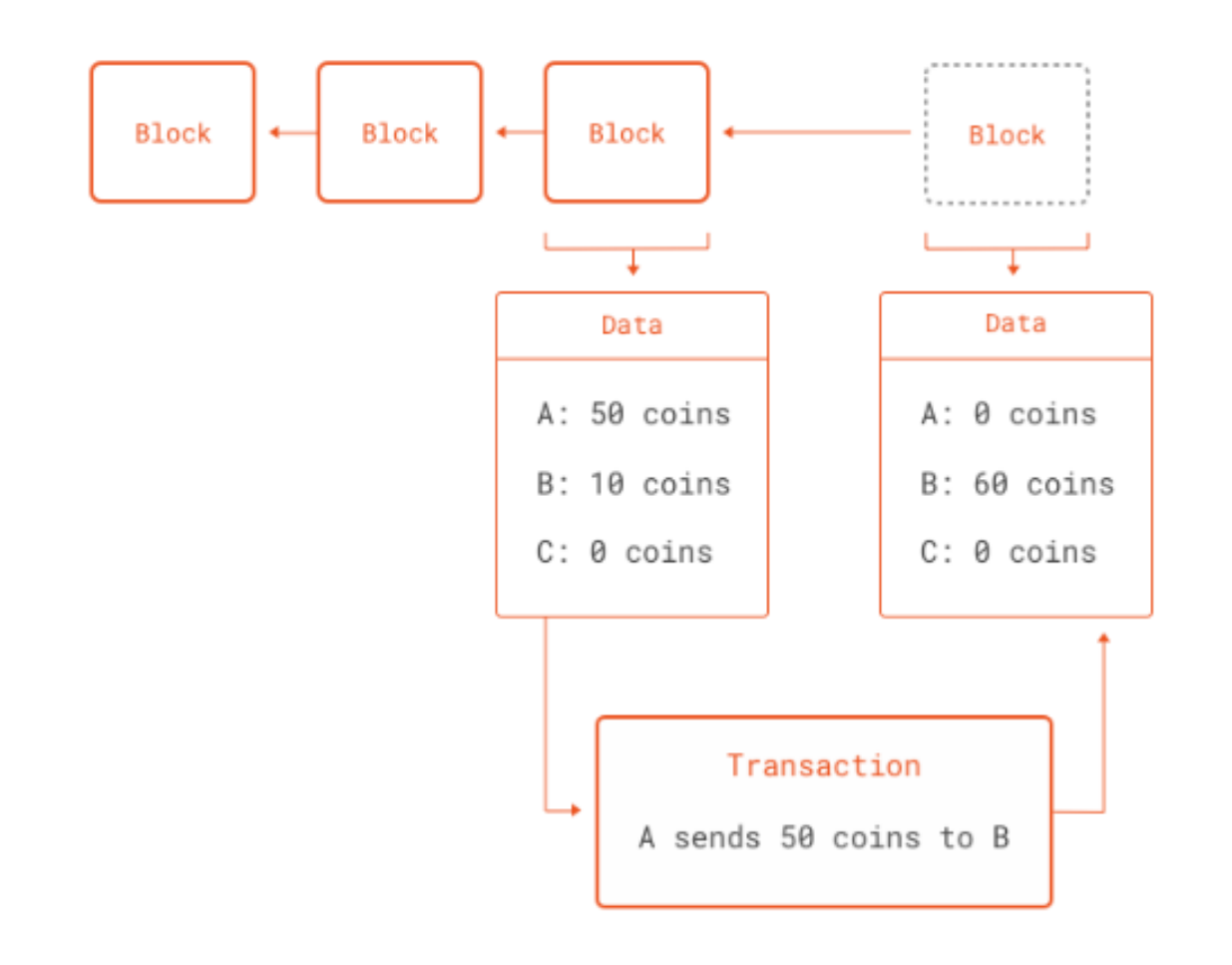
Policy area	Description	Potential benefits	Potential risks/Obstacles
Due diligence in supply chains	Blockchains allow multiple parties to access the same database to track and record and audit products as they move along the supply chain	**Enhanced transparency** A more transparent supply chain will help companies and consumers identify risks of adverse impacts (i.e. human rights abuse and financial crime), and on that basis, prioritise further efforts to prevent or mitigate such risks. **Sharing value of due diligence** Using blockchain technology to tokenise due diligence data (attaching a monetary value to access to the data), could potentially help fund due diligence efforts. **Financial inclusion** Blockchain technology can lead to greater integration of informal actors and SMEs in the formal supply chain by helping overcome cash flow barriers through self-executing smart contracts.	**Difficulty controlling data quality** Widely known as the "garbage in garbage out" issue where the information entered on the blockchain is only as good as its source. **Upfront costs and lack of access** In order to link the physical world to the digital, supply chain stakeholders have to invest in technology as well as facilitate access to and encourage uptake of the technology. **Fragmentation** Despite being created for very similar purposes, multiple blockchain initiatives have developed, operating on different platforms, identifying and collecting information differently, and with different governance structures.

Healthcare	Blockchain could be used to provide more robust patient healthcare information data management systems. Instead of information siloed in different data systems, patients and healthcare providers could choose what they share and with whom.	**Continuity of care** Information can be shared between different healthcare stakeholders and end users could find it easier to share information to new providers. **Cost effectiveness** Providing better data sharing between stakeholders can increase the ability of healthcare organisations to provide cost effective care and reduce clerical errors that are at best inefficient and at worst life threatening.	**Privacy rules** While some healthcare blockchain solutions will make only high level demographic information publicly viewable, it is conceivable that the combination of demographic data and geographic location could reveal sensitive information. **Data security** Given the information stored (or linked onto the blockchain) is highly sensitive, data security is a potential risk.
Energy	Blockchain can enable decentralised peer-to-peer electricity markets, allowing individuals and entities to balance supply and demand and trade electricity without going through a central entity.	**Lower transaction costs** Without intermediaries, costs can be significantly reduced along the electricity value chain. This could potentially lead to more competition and a broader range of options for consumers. **Facilitating distributed and low carbon electricity** Blockchain could reduce the complexity of managing systems with large numbers of small-scale renewable and distributed energy resources, accelerating their deployment.	**Scalability and technical performance** As is, several types of blockchain have difficulties scaling (for example, due to data volumes and transaction speeds). **Energy consumption** To reach scale in energy applications, blockchain technologies will have to develop less energy-intensive frameworks for processing transactions.

Ethereum: A Programmable Blockchain

- Although the concept of the blockchain was born out of the research into cryptocurrencies, they are much more powerful than just that.
- Blockchain essentially encodes one thing: state transitions. Whenever someone sends a coin in Bitcoin to someone else, the global state of the blockchain is changed.Moreover, it provides a crypographically secure way to performing these updates in the ledger.
- An interesting way to think of a blockchain is as a never-halting computation: new instructions and data are fetched from a pool, the pool of unconfirmed transactions. Each result is recorded in the blockchain, which forms the state of the computation. Any single snapshot of the blockchain is the state of the computation at that point.

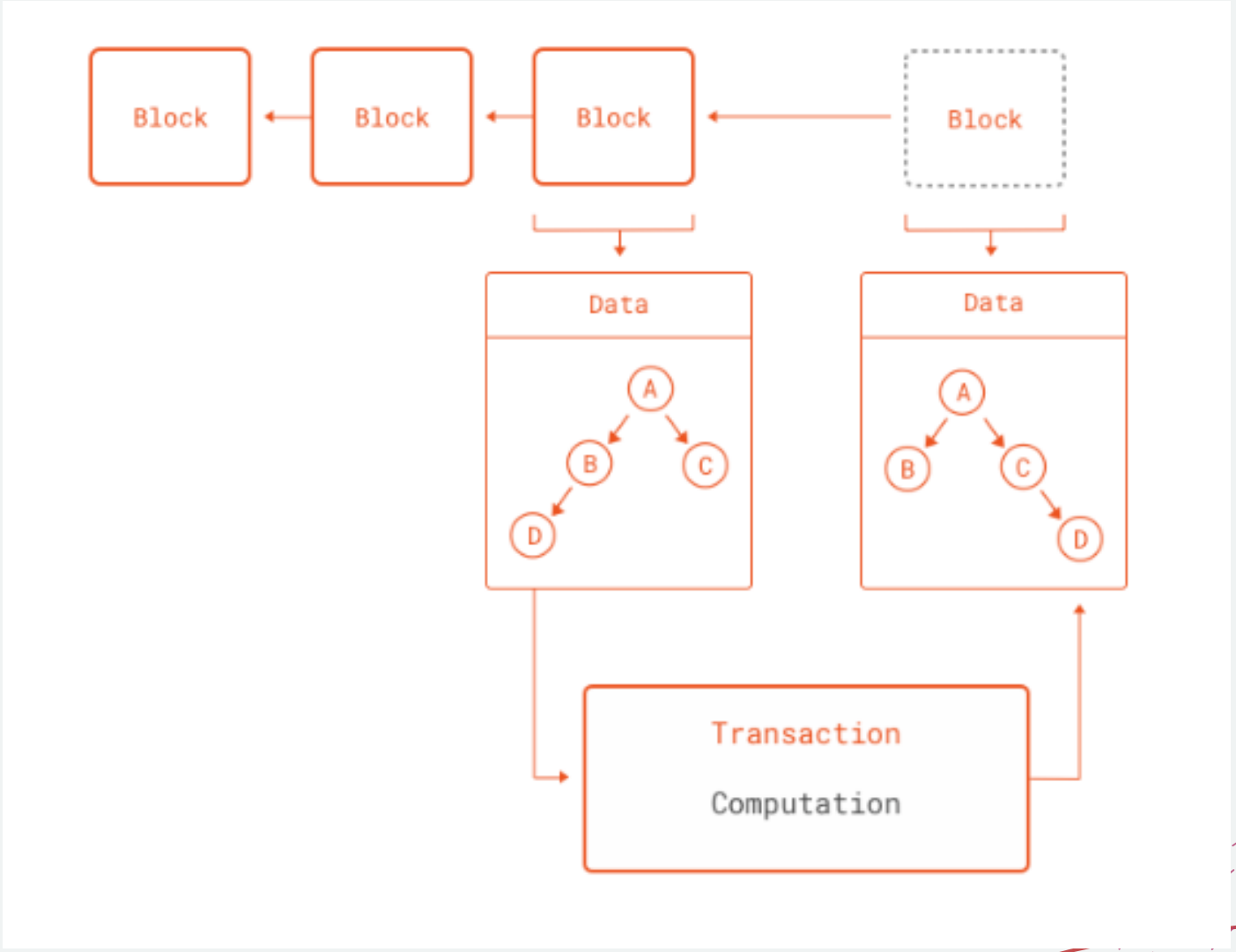
Transactions as computations



Blockchains and software

- All software systems deal in some way or another with state transitions. So what if we could generalize the state transitions inside a blockchain into any software we could think of.
- Blockchains deal with reaching consensus for decentralized computations, it does not matter what those computations are. And this is exactly what the Ethereum network brings to the table: a blockchain that can perform any computation as part of a transaction

Transactions as computations



Where distributed, secure computations make sense? Examples

- Secure deposits that get returned to the payer if conditions are met (or not).
- Money that cannot be spent unless a certain number of users agree to spending it.
- Money that can only be spent after producing external data that satisfies rules set in the scrip

Technicalities

- Since Ethereum as a blockchain is **Turing-complete**, many more applications are possible.
- A Turing-complete language is a language that, by definition, can perform any computation. In other words, if there is an algorithm for something, it can express it. Ethereum scripts, called **smart contracts**, can thus run any computation. Computations are run as part of a transaction. This means each node in the network must run computations. Any machine capable of running a Turing-complete language (i.e. a Turing machine) has one problem: **the halting problem**

Ether

- Although Ethereum brings general computatings to the blockchain, it still uses a "coin".
- Since computation is costly, and it is in fact rewarded by giving nodes that produce blocks ether, what better way to limit computations than by requiring ether for running them.
- Thus Ethereum solves the problem of denial of service attacks through malicious (or bugged) scripts that run forever. Every time a script is run, the user requesting the script to run must set a limit of ether to spend in it.

Smart Contracts

- Smart contracts are the key element of Ethereum. In them any algorithm can be encoded. Smart contracts can carry arbitrary state and can perform any arbitrary computations. They are even able to call other smart contracts. This gives the scripting facilities of Ethereum tremendous flexibility.
- When a block is created, in contrast to Bitcoin, Ethereum follows a different pattern for selecting which blocks get added to the valid blockchain.
- For consensus, Ethereum follows a protocol called GHOST, (Greedy Heaviest Observed Subtree).
- An important aspect of how smart contracts work in Ethereum is that they have their own address in the blockchain. In other words, contract code is not carried inside each transaction that makes use of it. This would quickly become unwieldy. Instead, a node can create a special transaction that assigns an address to a contract.

Apps using Ethereum (dapps)

+ **No Owners:** Once deployed to Ethreum, dapp code can't be taken down. And anyone can use the dapp's features. Even if the team behind the dapp disbanded you could still use it. Once on Ethereum, it stays there.
+ **Free from censorship:** No body can be blocked from using a dapp or submitting transactions. If Twitter was on Ethereum no one could block an account.
+ **Built-in payments:** Ethereum uses by default ETH payments.
+ **Open Source:** Most code is maintained and tested by large communities.
+ **Anonymous Login:** Your Ethereum wallet (account) is the login.
+ **Safer than current Web applications:** Protocols backed with stronger cryptography.
+ **No down time:** An app will only go down if Ethereum goes down.

How dapps work

- Dapps have their backend code (smart contracts) running on a decentralized network and not a centralized server. They use the Ethereum blockchain for data storage and smart contracts for their app logic.
- A smart contract is like a set of rules that live on-chain for all to see and run exactly according to those rules. Imagine a vending machine: if you supply it with enough funds and the right selection, you'll get the item you want. And like vending machines, smart contracts can hold funds much like your Ethereum account. This allows code to mediate agreements and transactions.

DeFi – Decentralized Finance: E.g. Financial Applications built on the Ethereum blockchain

Lending and borrowing

Aave
Lend your tokens to earn interest and withdraw any time.
Go

Compound
Lend your tokens to earn interest and withdraw any time.
Go

Oasis
Trade, borrow, and save with Dai, an Ethereum stablecoin.
Go

Token swaps

Uniswap
Swap tokens simply or provide tokens for % rewards.
Go

Matcha
Searches multiple exchanges to help find you the best prices.
Go

1inch
Helps you avoid high price slippage by aggregating best prices.
Go

Trading and prediction markets

Polymarket

Bet on outcomes. Trade on information markets.

Go

Augur

Bet on outcomes of sports, economics, and more world events.

Go

Loopring

Peer-to-peer trading platform built for speed.

Go

dYdX

Open short or leveraged positions with leverage up to 10x. Lending and borrowing available too.

Go

Investments

Token Sets

Crypto investment strategies that automatically rebalance.

Go

PoolTogether

A lottery you can't lose. Prizes every week.

Go

Index Coop

A crypto index fund that gives your portfolio exposure to top DeFi tokens.

Go

Payments

Tornado cash

Send anonymous transactions on Ethereum.

Go

Sablier

Stream money in real-time.

Go

Crowdfunding

Gitcoin Grants

Crowdfunding for Ethereum community projects with amplified contributions

Go

Insurance

Nexus Mutual

Coverage without the insurance company. Get protected against smart contract bugs and hacks.

Go

Etherisc

A decentralized insurance template anyone can use to create their own insurance coverage.

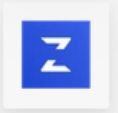
Go

Portfolios

Zapper

Track your portfolio and use a range of DeFi products from one interface.

Go



Zerion

Manage your portfolio and simply evaluate every single DeFi asset on the market.

Go

Rotki

Open source portfolio tracking, analytics, accounting and tax reporting tool that respects your privacy.

Go

Dapps and Web 3.0

- Web 1.0: Internet used for sharing information through the http protocol. Few information providers to a growing audience. Mostly static content.
- Web 2.0: Ability to let users share and modify data. Success for large tech companies e.g. Google, Amazon, Airbnb...
- Web 3.0: Internet applications running on a block-chain. Less reliance on large database and server providers. The front end of these applications are very similar to modern web applications (except authentication),while the backend uses smart-contracts as their "programming language", usually coded in a programming language called Solidity.

NFTs

- Non Fungible Tokens.
- Non-fungible tokens or NFTs are cryptographic assets on a blockchain with unique identification codes and metadata that distinguish them from each other. Unlike cryptocurrencies, they cannot be traded or exchanged at equivalency.
- NFTs can be used to represent real-world items like artwork and real-estate.
- "Tokenizing" these real-world tangible assets allows them to be bought, sold, and traded more efficiently while reducing the probability of fraud.
- NFTs can also be used to represent individuals' identities, property rights, and more.
- Much of the current market for NFTs is centered around collectibles, such as digital artwork, sports cards, and rarities.
- Applications outside finance, e.g. Passports, academic credentials, tickets, and voting (more secure than the current electronic voting).