

Blockchain: From Theory to Practice

Nikolas Markou MSc, MEng
CTO Electi Consulting

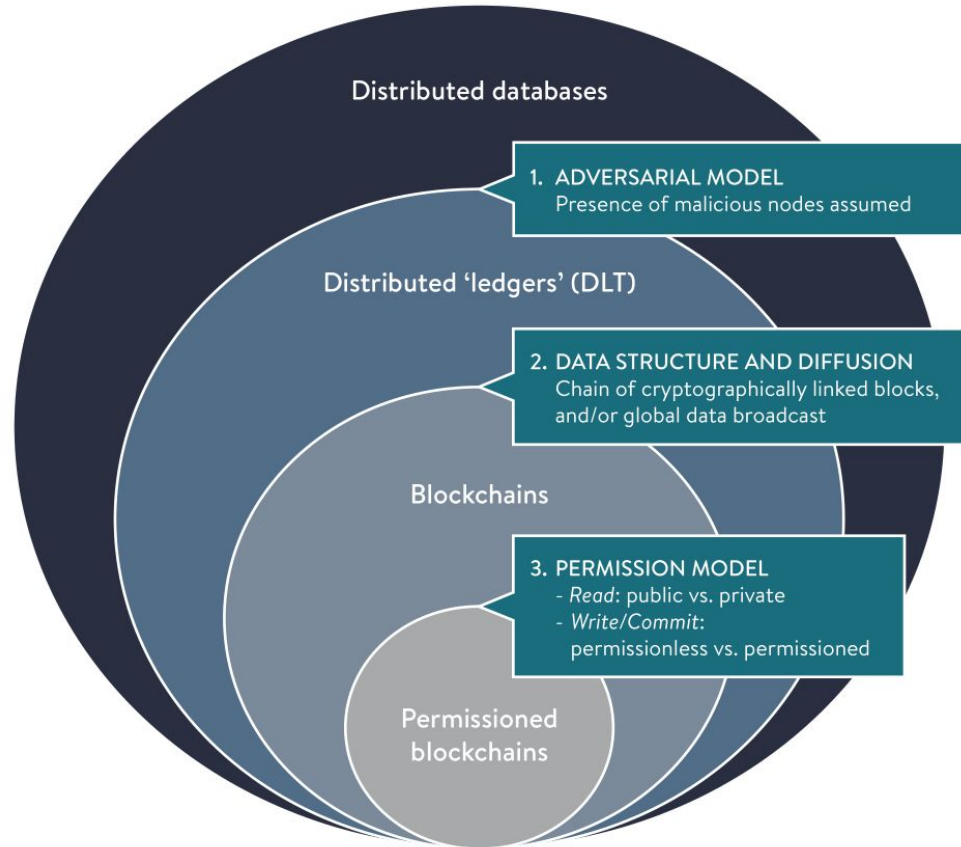
Overview

- What is a Blockchain ?
- Theory: Elements of Blockchain
- Practise: Problems in paradise

What is a Blockchain ?

Distributed Ledger Technology (DLT) has established itself as an umbrella term to designate multi-party systems that operate in an environment with no central operator or authority, despite parties who may be unreliable or malicious.

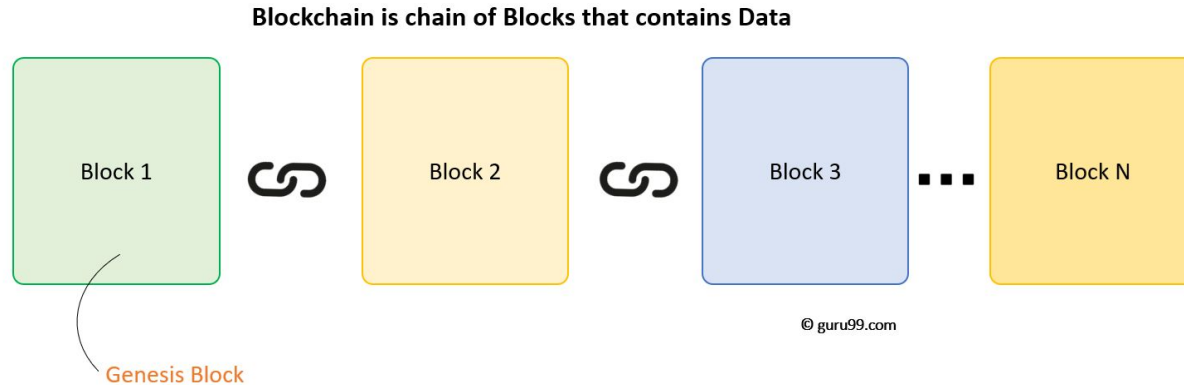
Blockchain technology is often considered a specific subset of the broader DLT universe.



What is Blockchain ?

No magic here, a Blockchain is a **data structure** that is

- append only
- timestamped,
- data aggregated into fixed size blocks,
- with each block connected to the previous one using cryptographic hashing functions



What is Blockchain ?

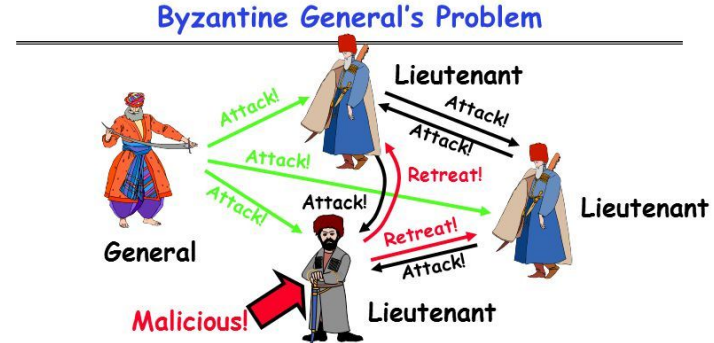
It doesn't have to be distributed BUT...

there is no point in setting such a structure for local computing/storage.

The computational overhead doesn't make sense.

What is Blockchain ? How it started ?

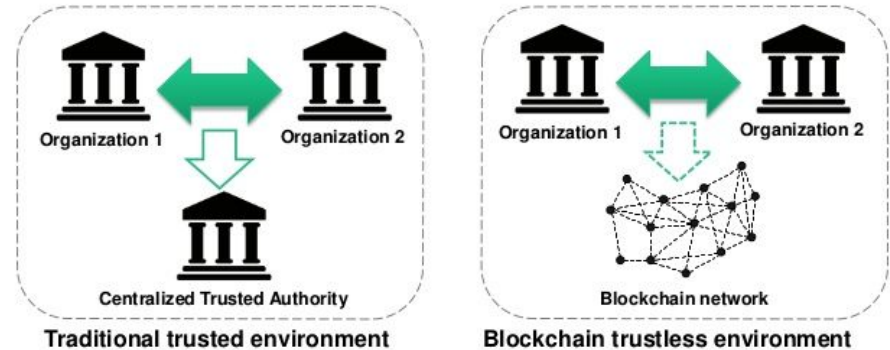
- The **Byzantine Generals Problem (BGP)** theorised by Lamport et al. (1982) described how distributed computer systems must handle **conflicting information** in an **adversarial environment**.



- **Byzantine General's Problem** (n players):
 - One General
 - $n-1$ Lieutenants
 - Some number of these (f) can be insane or malicious
- **The commanding general must send an order to his $n-1$ lieutenants such that:**
 - IC1: All loyal lieutenants obey the same order
 - IC2: If the commanding general is loyal, then all loyal lieutenants obey the order he sends

What is Blockchain ? The Bitcoin Solution

- The Bitcoin Blockchain (2008) gave a solid solution to the BGP and revitalized interest in the area.
- The conflicting information and malicious environment assumptions are key
- The Bitcoin Blockchain was created and it is still operating as a completely trustless environment



What is Blockchain ? The Bitcoin Solution

The Bitcoin network has been operating since 2008 with only a couple of mishaps.

GLOBAL BITCOIN NODES DISTRIBUTION

Reachable nodes as of Wed Jan 16 2019
15:55:02 GMT+0300 (Moscow Standard Time).

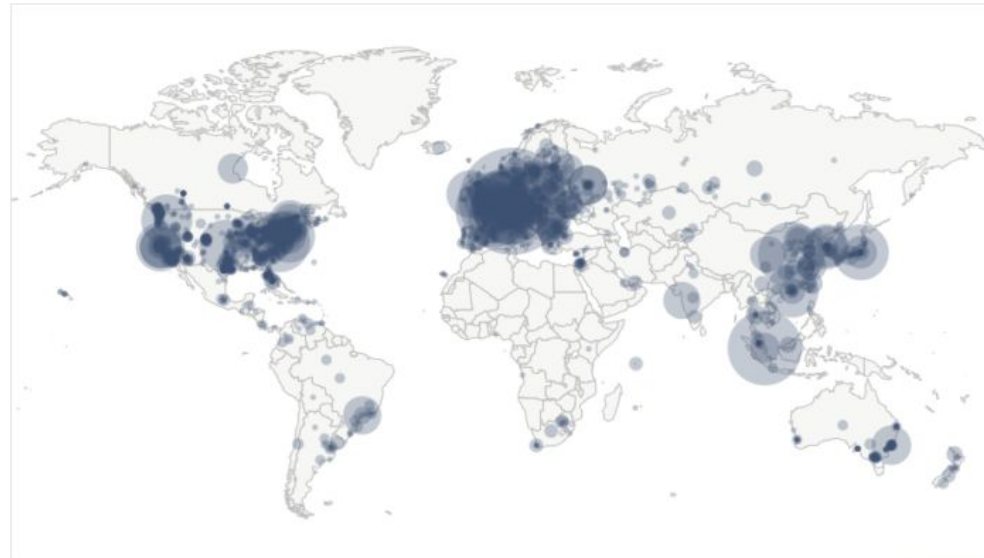
10214 NODES

24-hour charts »

Top 10 countries with their respective number of reachable nodes are as follow.

RANK	COUNTRY	NODES
1	United States	2490 (24.38%)
2	Germany	1931 (18.91%)
3	France	663 (6.49%)
4	Netherlands	484 (4.74%)
5	China	419 (4.10%)
6	Canada	390 (3.82%)
7	United Kingdom	350 (3.43%)
8	Singapore	316 (3.09%)
9	Russian Federation	267 (2.61%)
10	Japan	246 (2.41%)

[More \(100\) »](#)

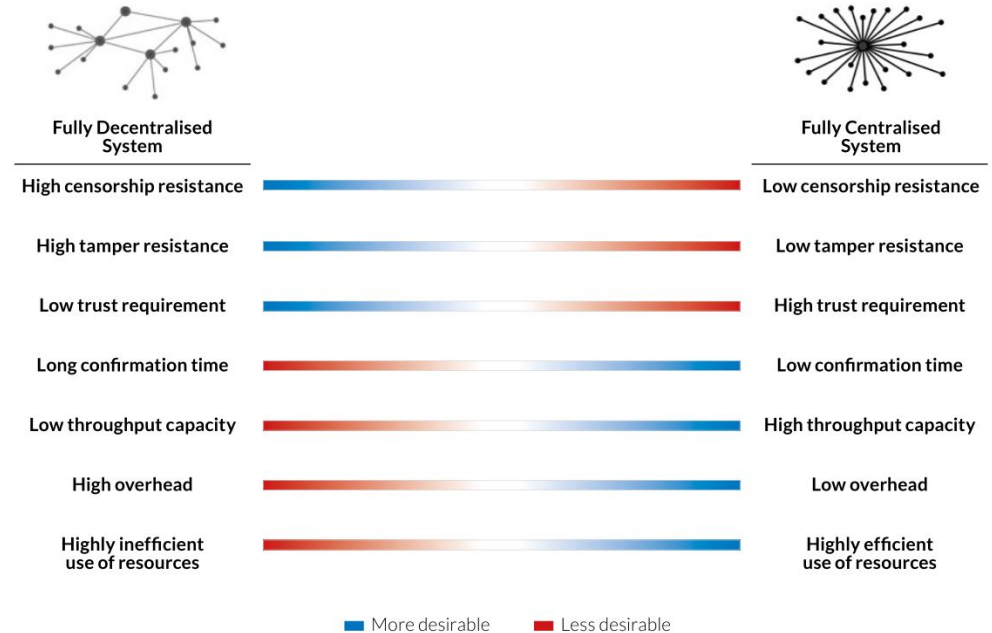


Map shows concentration of reachable Bitcoin nodes found in countries around the world.

[LIVE MAP](#)

What is Blockchain ?

- The Bitcoin creator made specific design decisions
- These decisions dictate how the Bitcoin Blockchain will evolve.
- If we relax or change the assumptions we get a plethora of different blockchains.



Elements of Blockchain

These design decisions are embedded into the Blockchain software.

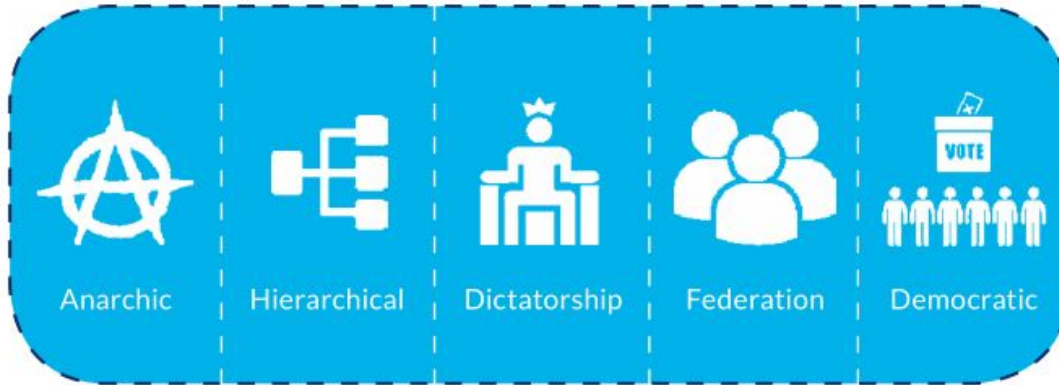
The Bitcoin network was iteratively created by the consensus of several teams across the world and many of the design decisions were not clearly mapped.

Later DLT/Blockchain designers make a conscious effort to address several of these in writing.

We can break down a Blockchain Network and understand the core

Elements of Blockchain / Governance

GOVERNANCE



Potential implications on:

- Decision-making
- Ruleset
- Sustainability/antifragility
- Perceived legitimacy
- Transparency
- Outsider access
- Efficiency and coordination

Elements of Blockchain / Network Access

NETWORK ACCESS



Potential implications on:

- Diversity of network participants
- Choice of consensus mechanism
- Trust requirements

Elements of Blockchain / Broadcast

BROADCAST



Potential implications on:

- Privacy and confidentiality
- Scalability
- Complexity

Elements of Blockchain / Transaction Processing

TRANSACTION PROCESSING



Potential implications on:

- Transaction finality
- Participation
- System maintenance costs
- Degree of tamper resistance

Elements of Blockchain / Incentives

INCENTIVES



Potential implications on:

- Nature of consensus (secured by economic incentives vs. secured by contractual agreements)
- Security

Elements of Blockchain / Reference




REFERENCE



Potential implications on:

- Enforcement

Elements of Blockchain / Comparison

			
GOVERNANCE	Anarchic	✓	
	Hierarchical		✓
	Dictatorship		✓
	Federation		
NETWORK ACCESS	Open	✓	✓
	Semi-open		
	Closed		
TRANSACTION PROCESSING	Decentralised	✓	✓
	Semi-centralised		✓
	Centralised		
INCENTIVES	Intrinsic	✓	✓
	Extrinsic		✓
REFERENCE	Endogenous	✓	
	Hybrid		✓
	Exogenous		✓

Elements of Blockchain

A Blockchain Network is a complex software system comprising of three layers:

- Protocol: set of software-defined rules that determine how the system operates
- Network: interconnected actors and processes that implement the protocol
- Data: information flowing through the system that carries a specific meaning in relationship to the design and functions the system is intended to play for users

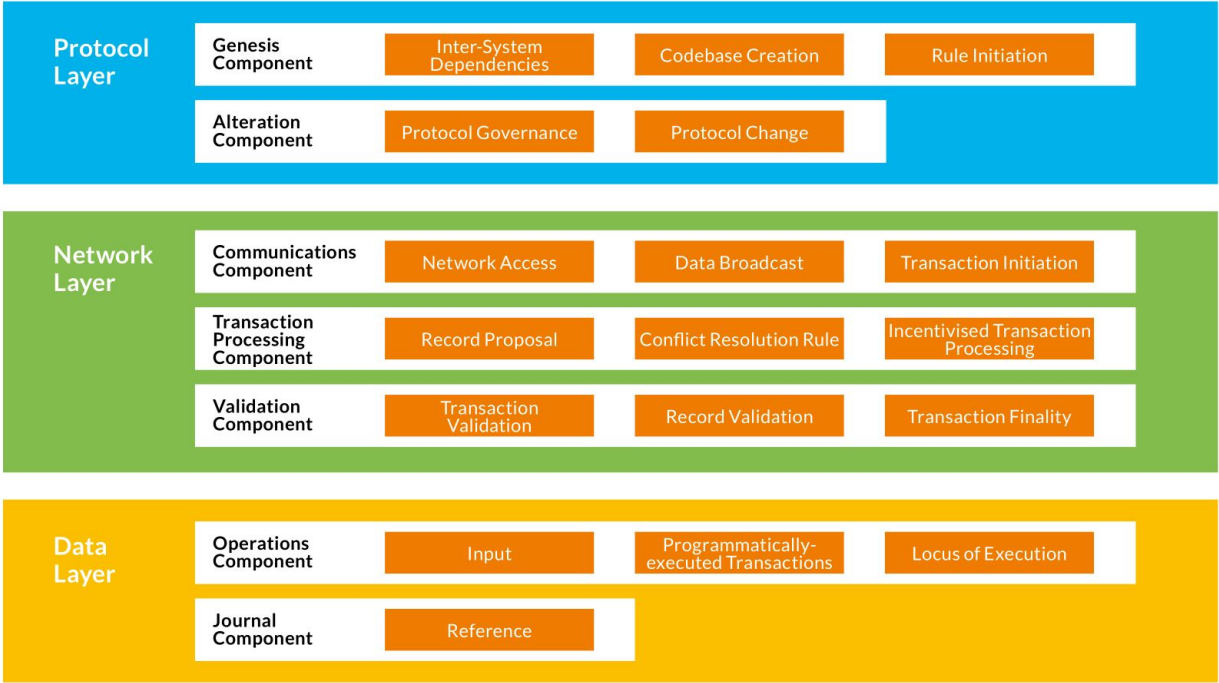
Elements of Blockchain

Each layer is composed of one or more components involved in the creation or operation of a DLT system.

A component is a logical set of related processes necessary for the functioning of the system.

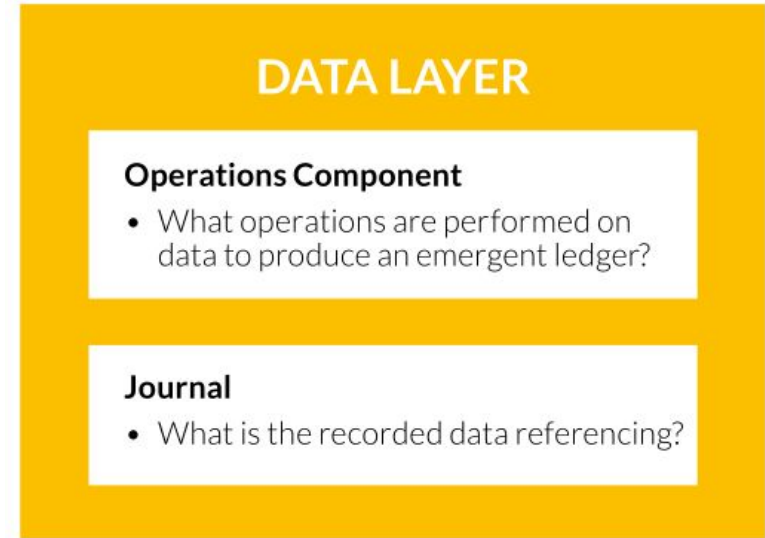
A process is a series of actions carried out by actors to achieve a specific objective or series of objectives involved in the successful operation of a component.

Elements of Blockchain / System Layers



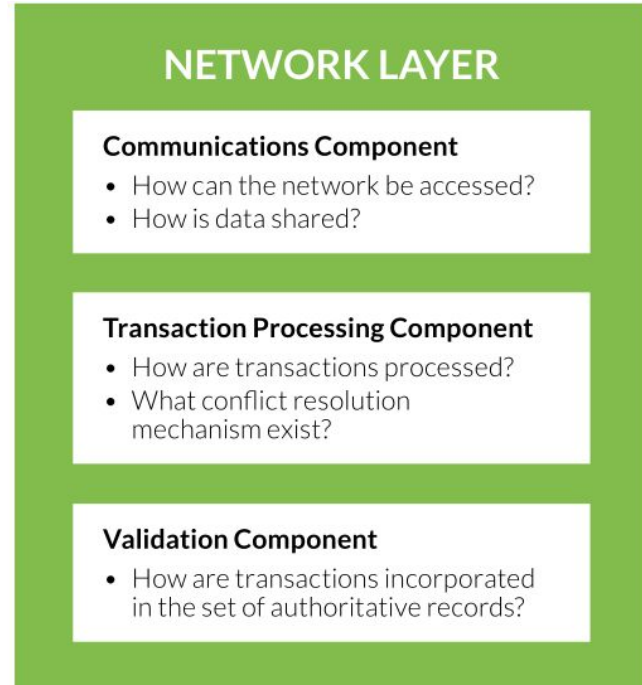
Elements of Blockchain / Data Layer

The data layer refers to the information processed and stored by the DLT system in the form of records. The data layer is at the core of the functionality the system delivers.



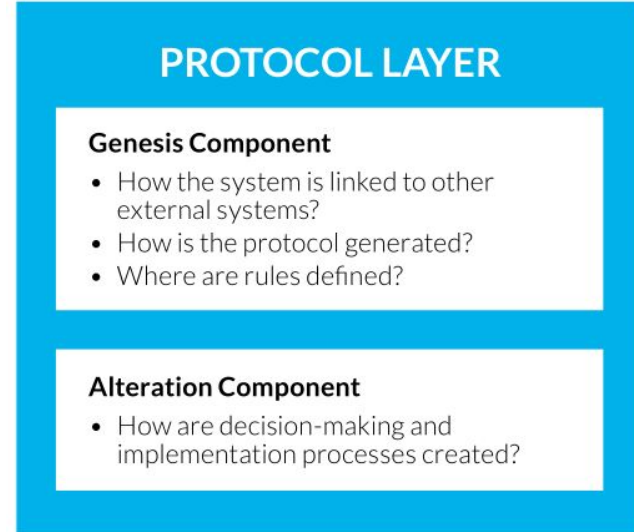
Elements of Blockchain / Network Layer

The network layer is comprised of interconnected actors that collectively store, share, and process data. The network layer is the practical implementation of the protocol rules, describing how participants access the system, how data is shared within the network, how the ledger is updated, and how participants verify the validity of transactions and records



Elements of Blockchain / Protocol Layer

The protocol layer is the foundation of the entire DLT system: it defines the set of formal rules that governs the system and codifies its architectural design. The protocol can be considered a set of 'constitutional' arrangements agreed upon by all system participants.



Elements of Blockchain / Actors



Elements of Blockchain / Actors / Developers

Developers write and review code that underlies the technological building blocks of a DLT system and its connected system(s). Developers may be professionally employed or participating as volunteer contributors.

- Protocol: maintaining the core protocol codebase (or an alternative implementation).
- Client: building the DLT client that provides an interface to the DLT system.
- Application: designing applications that run on top of the DLT system platform.
- External systems: creating infrastructure to enable protocols to function or interact with each other.

Elements of Blockchain / Actors / Admins

Administrators control access to the core codebase repository and can decide to add, remove and amend code to change system rules.

Administrators are often considerably involved in the governance process and may have absolute control over it.

Elements of Blockchain / Actors / Participants

The network consists of interconnected participants that communicate by passing messages among each other.

- Auditors: checking submitted transactions and records for validity, reporting invalid records to the network, and relaying valid transactions and records. Often called full/fully-validating nodes.
- Record Producers: producing and submitting sets of candidate records for potential inclusion into the ledger. Often called miners or validators.
- Lightweight Clients: querying auditors for data regarding specific transactions.
- End-users: indirect users of the system who require a gateway to access the system

Elements of Blockchain / Actors / Gateways

Gateways provide interfaces to the system by acting as a bridge between the system and the external world.

- Gatekeeper(s): granting participants access to the system.
- Oracles: transmitting external data to the system.
- Custodians: holding assets in custody.
- Exchanges: facilitating purchase/sale of digital assets.
- Issuers: issuing or redeeming tokens representing the assets recorded in the system.

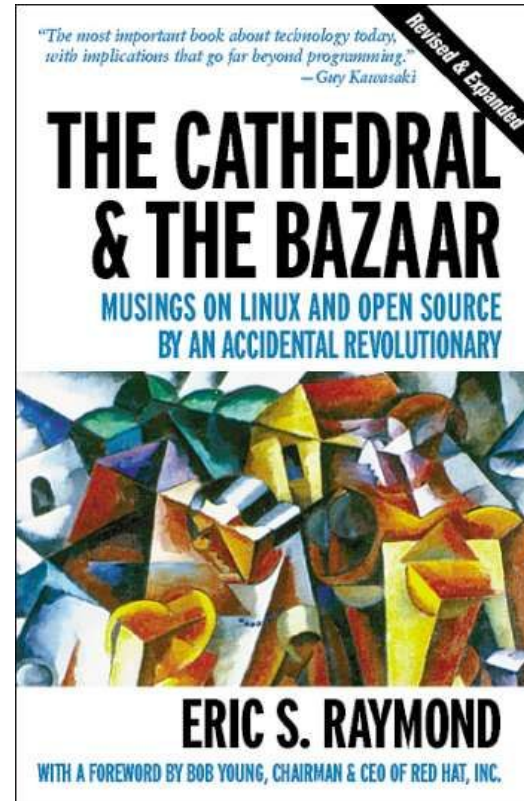
Practise

Ideally we would want to know all the above before we even start writing a single line of code.

However we rarely do.

Open Source Software is rarely a top down procedure but rather an iterative chaotic process.

This process was beautifully captured in the book “The Cathedral & the Bazaar”



Practise / Principles or Law

What happens in practise is that we have a set of principles coming from the founding team that tries to address all the above mentioned parts but cannot possible anticipate every eventuality.

In short there are a lot of problems in paradise which must be aware before we jump in.

Practise / Not enough nodes

On a lot of Blockchains the number of participants is too small.

This opens up the Blockchain for a 51% attack.

This makes those Blockchains unreliable for serious projects.

Name	Symbol	Market Cap	Algorithm	Hash Rate	1h Attack Cost	NiceHash-able
Bitcoin	BTC	\$69.09 B	SHA-256	46,134 PH/s	\$306,698	0%
Ethereum	ETH	\$14.07 B	Ethash	133 TH/s	\$75,151	4%
Litecoin	LTC	\$3.46 B	Script	265 TH/s	\$35,492	4%
BitcoinCashABC	BCH	\$2.36 B	SHA-256	1,439 PH/s	\$9,569	3%
BitcoinSV	BSV	\$1.18 B	SHA-256	701 PH/s	\$4,661	5%
Monero	XMR	\$859.73 M	CryptoNightR	251 MH/s	\$4,293	3%
Dash	DASH	\$786.88 M	X11	2 PH/s	\$3,146	36%
EthereumClassic	ETC	\$471.26 M	Ethash	8 TH/s	\$4,606	72%
Zcash	ZEC	\$302.30 M	Equihash	3 GH/s	\$15,248	5%
BitcoinGold	BTG	\$234.45 M	Zhash	3 MH/s	\$937	59%
Bytecoin	BCN	\$145.39 M	CryptoNight	266 MH/s	\$83	66%
Verge-Lyra2REv2	XVG	\$106.66 M	Lyra2REv2	6 TH/s	\$149	197%
Sia	SC	\$106.39 M	Sia	2 PH/s	?	0%
Ravencoin	RVN	\$69.81 M	X16R	7 TH/s	\$8,040	14%
Electroneum	ETN	\$61.45 M	CryptoNight	7 GH/s	\$2,092	3%
Metaverse	ETP	\$40.71 M	Ethash	640 GH/s	\$361	917%
Monacoin	MONA	\$33.63 M	Lyra2REv2	17 TH/s	\$408	72%

Practise / Centralization

Even though provisions were made, a lot of participants pooled their resources to get a better share on the incentivization scheme.

In addition to that large computing centers run ASIC's that pushed out a lot of people.



Practise / Governance

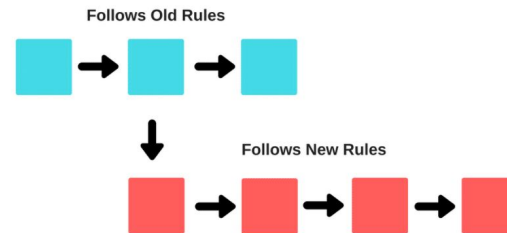
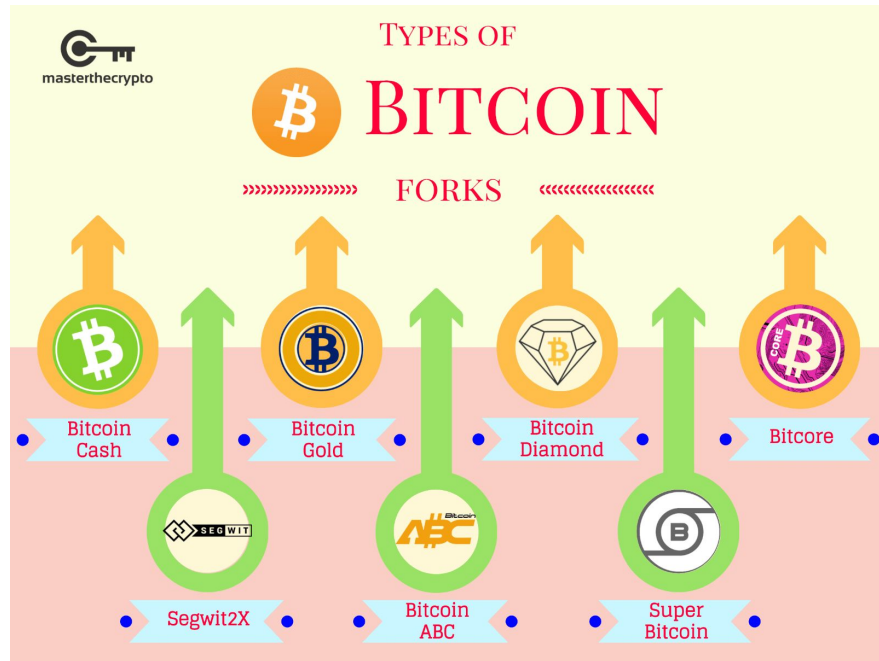
It is an iron law of software that :

SUCCESSFUL PROJECTS WILL EVOLVE

A lot of projects had a poorly thought out governance model.

When they attained some success they had trouble agreeing on the next steps.

This led to several hard and soft forks



The primary difference between a soft fork and hard fork is that it is not backward compatible

Practise / Greed

A lot of greed went into forking unnecessary projects and spreading resources too thinly.

Whereas most of these low quality projects with no business plan or team are destined to fail this will have a negative impact on serious projects



Practise / Power Consumption

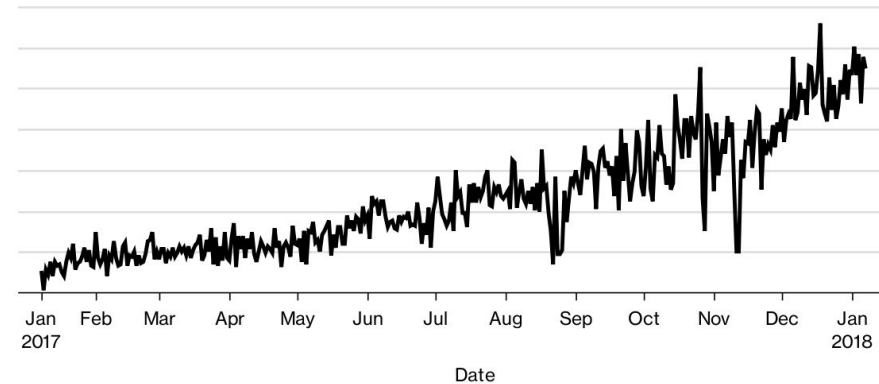
The consensus algorithm and the incentivization scheme of several blockchains need a lot of energy.

As it works now, the more people enter the scheme the harder the puzzle becomes to crack and the more power is used.

Bitcoin Power Consumption

Cryptocurrency's power needs have tripled and hit a record 43 GWh in December

■ Consumption per day (GWh/day)



Source: Bloomberg New Energy Finance

Bloombe

Practise / Smart Contract Troubles

We are all familiar with Software bugs.

This is also the case for all non-trivial smart contracts.

The non amendability of the blockchain makes it difficult to fix smart contracts already deployed.



Practise / Present State

Despite all these problems,

A lot of progress is happening.

- Adoption is high.
- Applications are being built on public and private blockchains.
- Issues like consensus and power consumption are being addressed
- Standardization of moving parts will make cross blockchain movement easier
- Application and efficiencies are being explored by governments all over the world.

Summary

- **Blockchain design decisions**
- **Blockchain layers**
- **Blockchain participants**
- **In practise a lot of problems exist no software is perfect**
- **A huge amount of progress is happening**

Thank you

Nikolas Markou MSc, MEng

CTO Electi Consulting