gbf
Attorneys-at-law

Privacy by Blockchain

Big Chance, Big Risk or Big Fail?

Marco Novoselac

8 November 2019

The Blockchain

The Blockchain

The biggest invention since emergence of internet.

The Blockchain

Every industry acting as a middleman between producers and customers of immaterial or digital goods and services is vulnerable to being replaced.

The Blockchain – Main Components

- **Distributed ledger or database**, shared across a public or private computing network
- Each computer («**node**») in the network holds a copy of the ledger -> no single point of failure
- Most pieces of information are mathematically encrypted and added as a new data-«**block**» to the **chain** of historical records
- Various **consensus protocols** used to validate a new block with other participants («**miners**») before added to chain -> no fraud or double spending
- **No central authority** needed

The Blockchain

- Big **machinery**
- **Complex** technical construct
- Consists of a variety of **mathematical concepts** and **principles of software engineering** and computer science optimised and adopted to one another

The Blockchain – Concepts & Principles

- **Peer to peer system**: users can interact directly
- **Cryptographical hashing functions**: small computer programs that transform any kind of data into number of fixed lengths, regardless of size of input data (digital equivalent to fingerprints)
- **Cryptography** (asymmetric): protect data from being accessed by unauthorized people; **encrypted data** = cypher text
- **Digital signatures**: protecting ownership
- **Merkle trees**: contain the data
- **Computational puzzles**: making the data immutable

The Blockchain – Concepts & Principles

- **Data storage**: append-only (data can not be changed) protecting data from manipulation and forgery
- **Network architecture**: distributed ledgers - gossip style information forwarding through network
- **Blockchain-algorithm**: defines how miners are rewarded
- **Distributed consensus methods**: agreement among the nodes of the blockchain-system on each state/final state (version of truth/reality) of the data records

Variety of these concepts and technologies can be used and are still in the **area of active research**

The Blockchain - Properties

- Highly available
- Censorship proof
- Reliable
- Open
- Pseudonymous
- Secure
- Resilient
- Consistent
- Integer

The Blockchain - Limitations

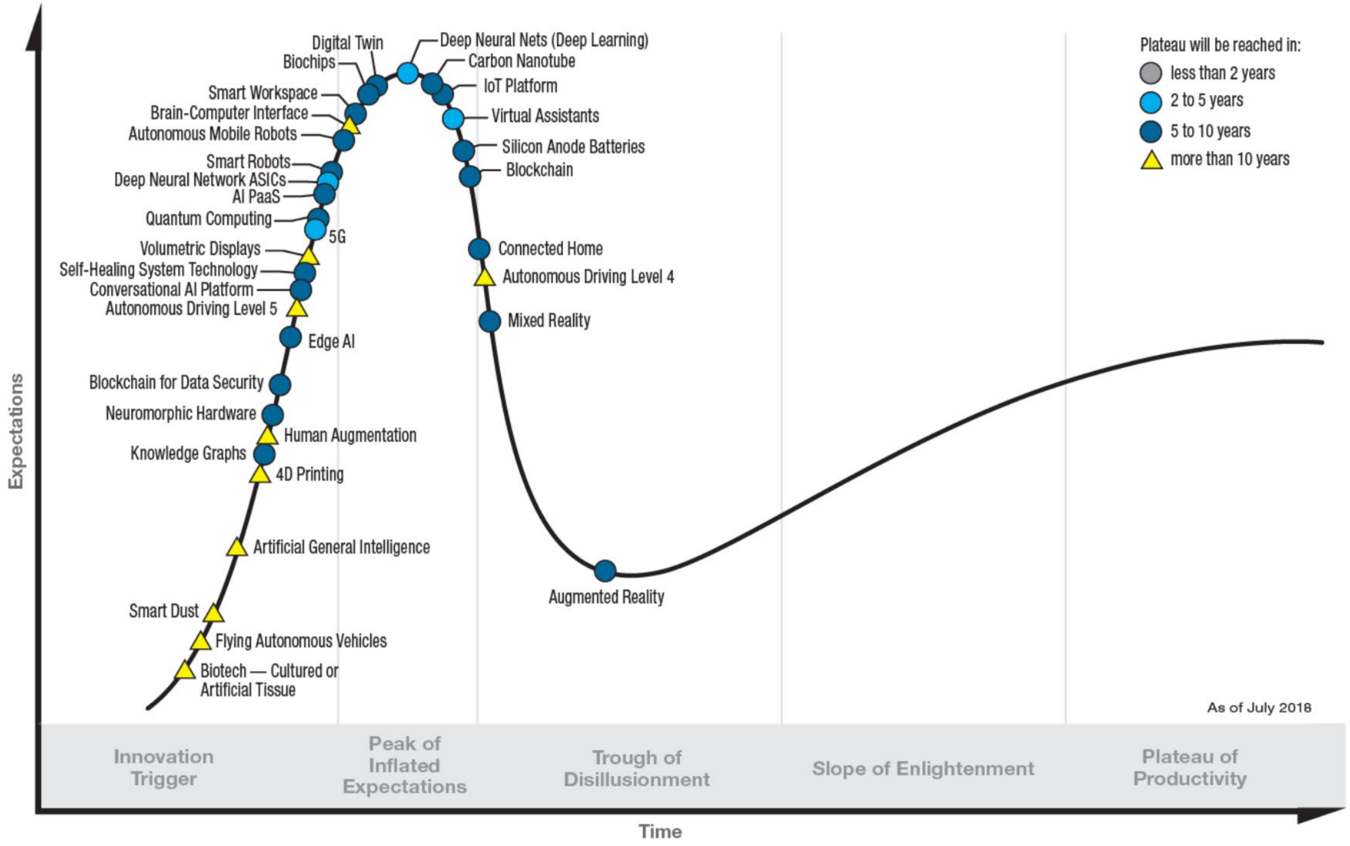
- Lack of **user acceptance**: fundamental functioning not understood
- Lack of **legal acceptance**: incorporation of a new approach of managing ownership in the legal system
- **Overhyped technology**; no better than a glorified excel spreadsheet or database
- **Centralisation in mining** (computational power) -> security risk
- As efficient as a lame hippo with a hangover (very **slow** and **inefficient**)

The Blockchain – new versions

- **Public & Permissionless**: everyone can read, create transactions and write
- **Public & Permissioned**: read access, right to create transactions everyone, write access limited group
- **Private & Permissioned**: read and write access, right to create transactions limited -> most attention from **business side** (consortiums of leading companies of certain sector or industry) -> realizing gains of standardization, automation, process streamlining and **cost reduction**

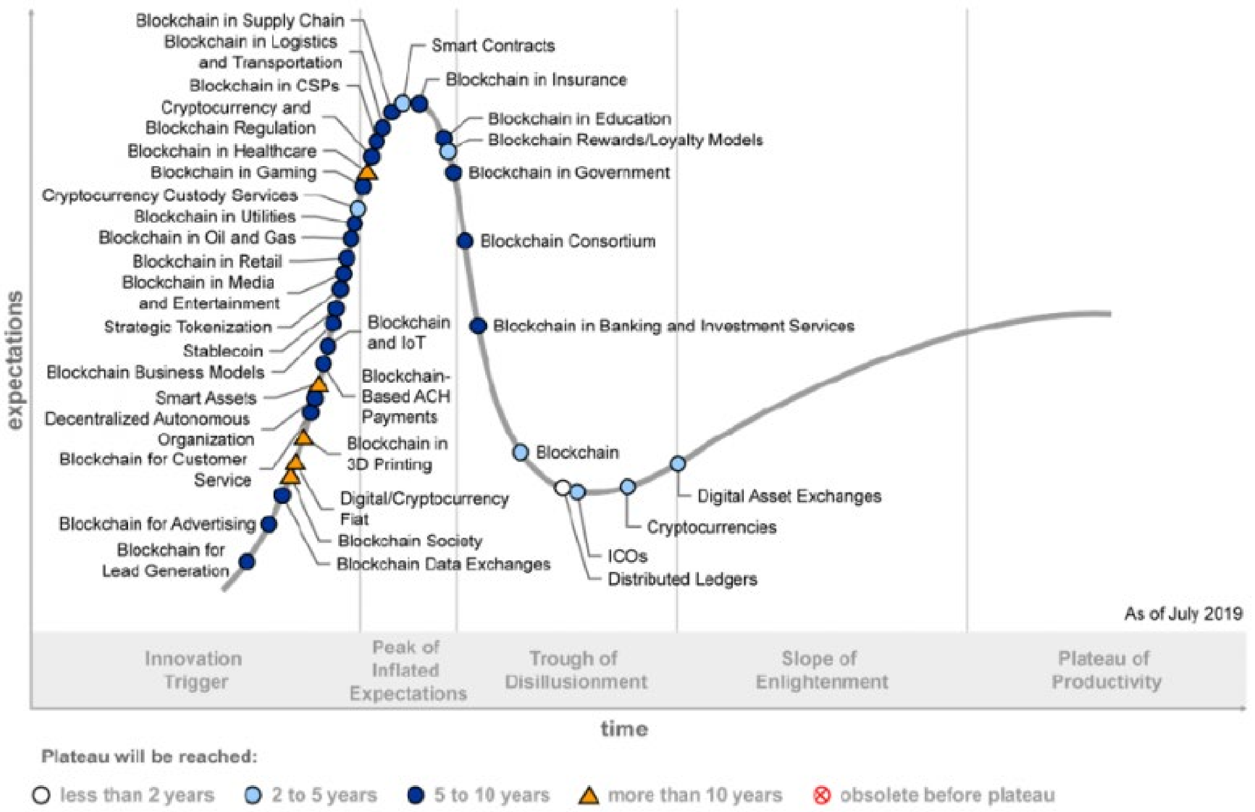
Hype Cycle

Hype Cycle for Emerging Technologies, 2018

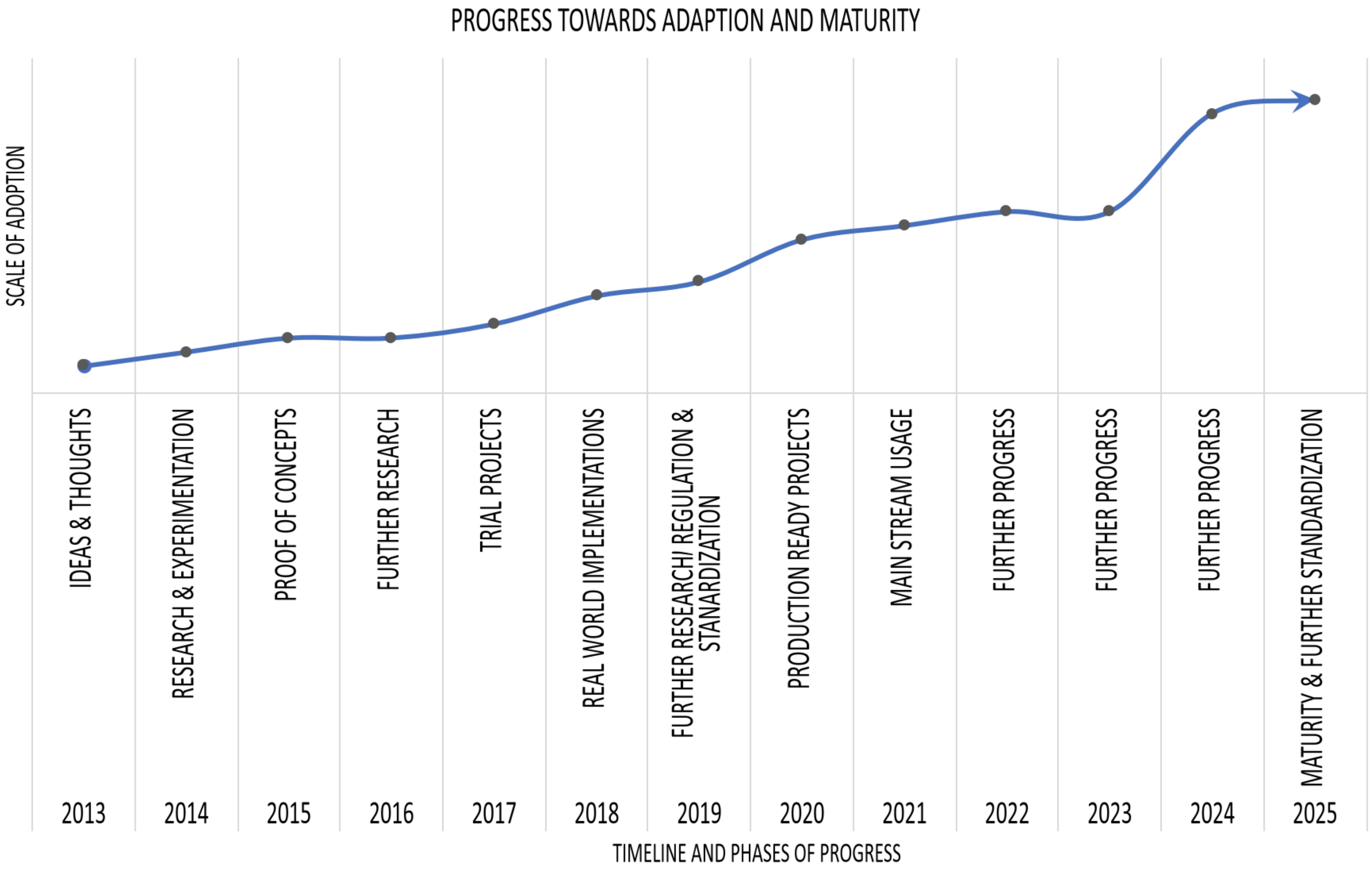


Hype Cycle

Hype Cycle for Blockchain Business, 2019



Source: Gartner
ID: 390391


PROGRESS TOWARDS ADAPTION AND MATURITY
SCALE OF ADOPTION
IDEAS & THOUGHTS
RESEARCH & EXPERIMENTATION
PROOF OF CONCEPTS
FURTHER RESEARCH
TRIAL PROJECTS
REAL WORLD IMPLEMENTATIONS
FURTHER RESEARCH/ REGULATION & STANARDIZATION
PRODUCTION READY PROJECTS
MAIN STREAM USAGE
FURTHER PROGRESS
FURTHER PROGRESS
FURTHER PROGRESS
MATURITY & FURTHER STANDARDIZATION
2013
2014
2015
2016
2017
2018
2019
2020
2021
2022
2023
2024
2025
TIMELINE AND PHASES OF PROGRESS

1994

A computer scientist and inventor described a software he was about to develop:

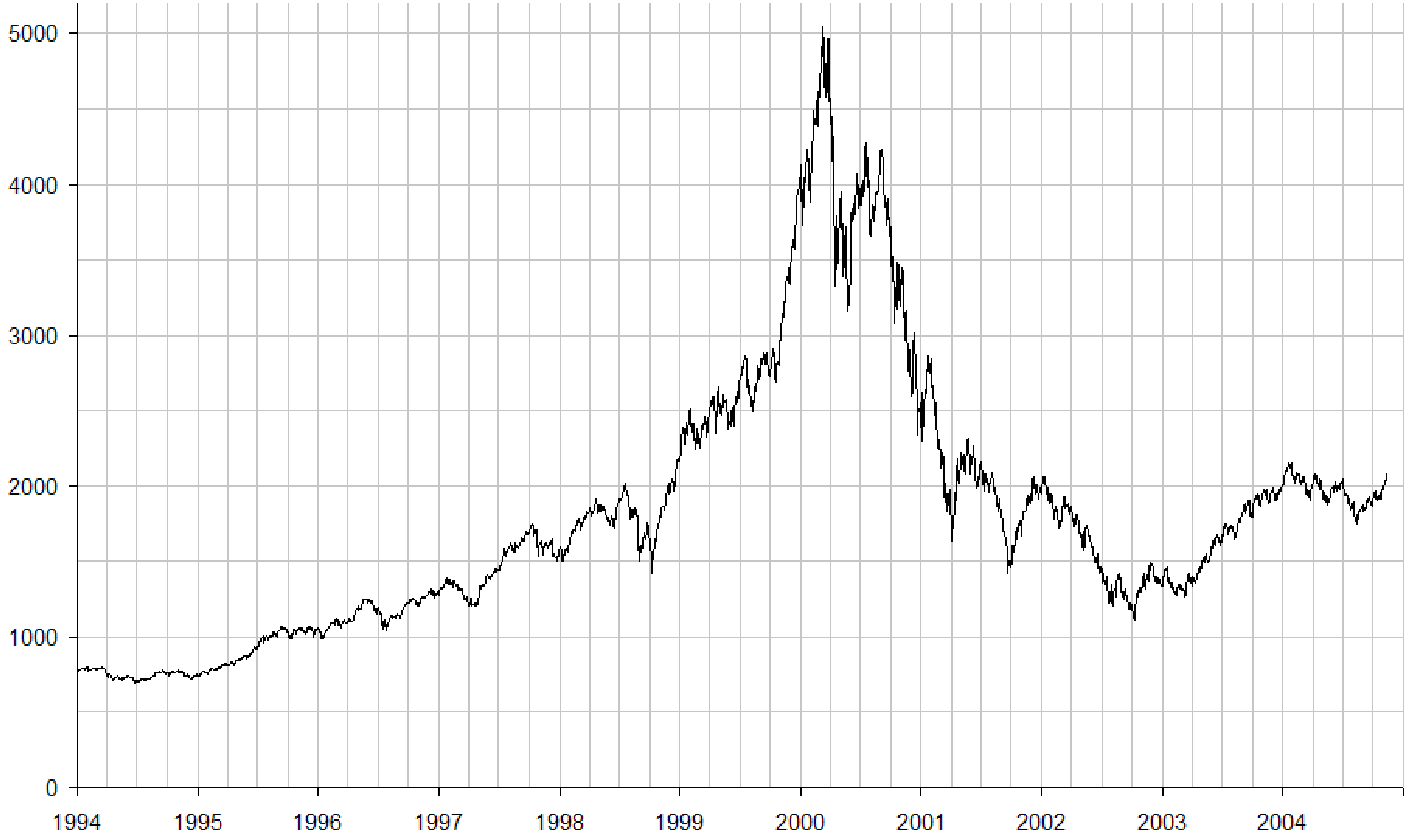
- **Decentralisation**: No central authority and no single point of failure
- **Openess**: System will be developed in full view of everyone, encouraging maximum participation and experimentation
- **Nondiscrimination**: Everyone free to choose his own way to connect to the system
- **Universality**: All the computers involved communicate with each other regardless of their hardware or location
- **Consensus**: System and its users will comply with standards that are created through a transparent participatory process based on consensus

The Internet

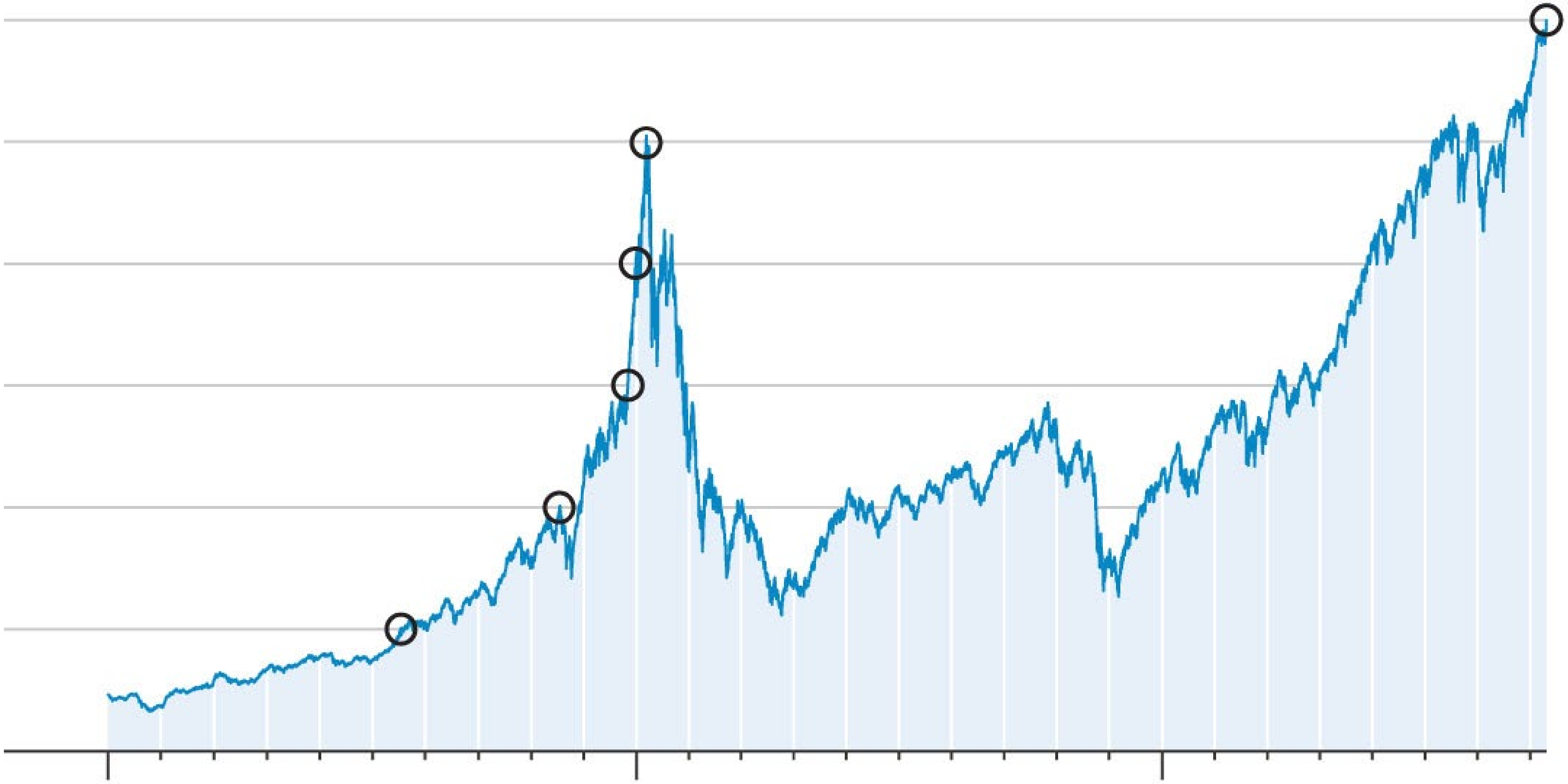
The Internet – early days

- Establishment of the **internet** and **mobile phone** as well as the development of **handheld computers** led to euphoric mood in the field of digital technology
- Large number of new companies (**startups**)
- Fine granularity and **diversity**
- **Upend existing social order** through distribution of communication tools, replacing existing centralized organisations
- **Era of freedom**: free haven, anonymous, beyond territorial jurisdiction

The Dotcom Bubble



The Dotcom Bubble



The Internet today

- **Concentration** and Centralisation
- Important internet hubs controled by few large organisations (**platform economy**)
- Governements and companies transformed internet ultimate apparatus for **political and social control** by monitoring speech, identifying dissidents and disseminating propaganda
- **Information warfare**
- **Monitoring-capitalism**
- **Data-Dysphoria**: unease over ways and means of data creation, dissemination and preservation

GDPR

- European General Data Protection Regulation
- In force since **25. Mai 2018**
- GDPR developed in the context of a world where business models based on **collecting user's personal data** in exchange of gratis services, and then monetize knowledge and analytics extracted from it
- GDPR aims at solving the problem **data misuse** by providing legal grounds for making such **businesses accountable** for how they process and exploit the data and to **give** citizens **back** the **control** of their personal data

GDPR - Material Scope

- Scope of GDPR applies only if **personal Data** is involved
- Art 4 (1) GDPR: “**personal data**” means any information relating to an identified or identifiable natural person

GDPR - Material Scope

- **Absolute approach**:
  - Data personal as long as **any third party worldwide**
  - holds **identifying information**, which could be used to identify a person (regardless of the likelihood of attribution)
- **Relative approach**:
  - Identifing information must be **sufficiently accessible**

GDPR - Material Scope

- **European Court of Justice** ruled that dynamic IP addresses may constitute “personal data” even where only a third party (in this case an internet service provider) has the additional data necessary to identify the individual – if:
  - possibility to combine the data with additional data constitues a “**means likely reasonably to be used to identify**” the individual
  - **additional data only considered** if identification of the data subject is **legally and practically possible**
  - **without disproportionate effort** in terms of time, cost and man-power

  ⇒ **Relative Approach**

GDPR - Core Principles

- Personal data shall be:
  - processed **lawfully** and **transparently**
  - collected for **specified** and not processed for **incompatible purposes**
  - **adequate** and **not excessive (in relation to purpose)**
  - **accurate** and **up to date**
  - stored **no longer** than necessary
  - processed in a manner that ensures appropriate **security**

GDPR - Lawfulness of processing

- Processing shall be lawful only if and to the extent that at least one of the following applies:
  - the data subject has **given consent** to the processing of his or her personal data for one or more specific purposes
  - processing necessary in order to protect the **vital interests of the data subject** or of another natural person
  - processing necessary for the performance of a task carried out in the **public interest** or in the exercise of official authority vested in the controller
  - processing necessary for the purposes of the **legitimate interests** pursued by the controller or by a third party

GDPR - Rights

- **Erasure** of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without **undue delay** where personal data have been **unlawfully processed**
- Right to **rectification/amendment**

Blockchain <–> GDPR

- GDPR aims to regulate world of **centralised data processing and storage**, blockchain wants to challenge it by providing a system of decetralised data collection, storage and processing
- GDPR focuses on entities which have the ability to actively **control** the data-flow of an IT-System

Blockchain in the light of GDPR

- Personal Data?
- Responsible person?
- Consent?
- Rights?

Blockchain <-> Personal Data?

- Blockchain handles no names, adresses or e-mail Ids, only **hashes, encryption keys, cypher text** -> personal data?
- If the data controller is able, by the **means at his disposal** or available to him, to attribute the data in question to a specific person, the information/data is personal
- But: if **disproportionate** amount of time, cost and effort necessary – not personal data

⇒ **Depending on Blockchain-structure and data stored**

Blockchain <–> Responsibility

- Art 4 (7) GDPR: controller means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the **purposes and means** of the **processing** of personal data
- Possible person in charge:
  - programmer of the blockchain
  - participant who makes a transaction
  - miner, which checks new blocks before recording and appends them to the blockchain
  - participant acting as a node

⇒ **Public & permissionless blockchain: No responsible entity - no control over the purpose and means of processing; GDPR does not fit**

Blockchain <–> Consent

- 4 (11) GDPR: consent of the data subject means any freely given, specific, **informed** and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data
- In the case of public blockchains: data subject does not know who the person responsible is and to which countries the data is transmitted, since the operators of the nodes are not necessarily known

⇒ **GDPR does not fit**

Blockchain <–> Right to Erasure

- Data on blockchain **immutable**
- Right to erasure **is not absolute**
- GDPR 17 (1): “personal data are no longer **necessary for the purposes** for which they were collected or otherwise processed"
- The law derived from Art 7 and 8 of the **Charter of Fundamental Rights of the European Union**
- Fundamental rights can be restricted by the rights of third parties, with particular reference to **freedom of expression** and information and **freedom to conduct a business**

Blockchain <–> Right to Erasure

- If **existence of the entire blockchain endangered** by the request for deletion, because the deletion would make the continued operation of the nodes impossible -> balancing of interests in favour of the responsible node operators
- The balancing of interests should also take into account whether a person concerned was **aware of the immutability** of the blockchain before it was used

⇒ **Legal uncertainty and not enforceable on public permissionless blockchain**

Technical options

- **Permissioned private blockchains**
- Create data with encryption and decryption keys and **delete the decryption key** in case of deletion
- Provide the owner of the data with **specific private keys** that enable read access - control is then with the owner
- **Hashing-out**: personal data in a referenced encrypted database off-chain; pointer and hash in blockchain - hash serves as proof that data not changed; if deletion request -> entry in database deleted and pointer goes nowhere
- Address obfuscation, non-reversible transformation of personal information, homomorphic encryption, peppered hashes, ring signatures

Outlook - Prognosis

- **Turning point**
- **Knowing** what a system does with our data – identify risks
- Self-hosting of one's personal data in a secure peer to peer system – **data self sovereignty** – controll back in the hands of individuals
- **Anonymous digital identity**

Summary

- GDPR **outdated** with regard to (permissionless) blockchain applications – cannot account for the technology's characteristic features
- Permissionless Blockchain more of a **no man's land** under data protection law, a data protection-free pace
- **Legal system** incorporated every new technology
- **Legal uncertainty** - depending on how case law evolves
- **Factual uncertainty**: how will blockchain technology develop – overestimating short term effects - ignoring long term impacts
- **Conclusion: Blockchain (peer-to-peer and cryptography) is a big chance for privacy -> brings back control over data**

Thank you for your attention!

Marco Novoselac
Partner
Attorney-at-law, Notary of the Canton of Solothurn,
EMBL-HSG (Business Law)
novoselac@gbf-legal.ch

gbf
Attorneys-at-law

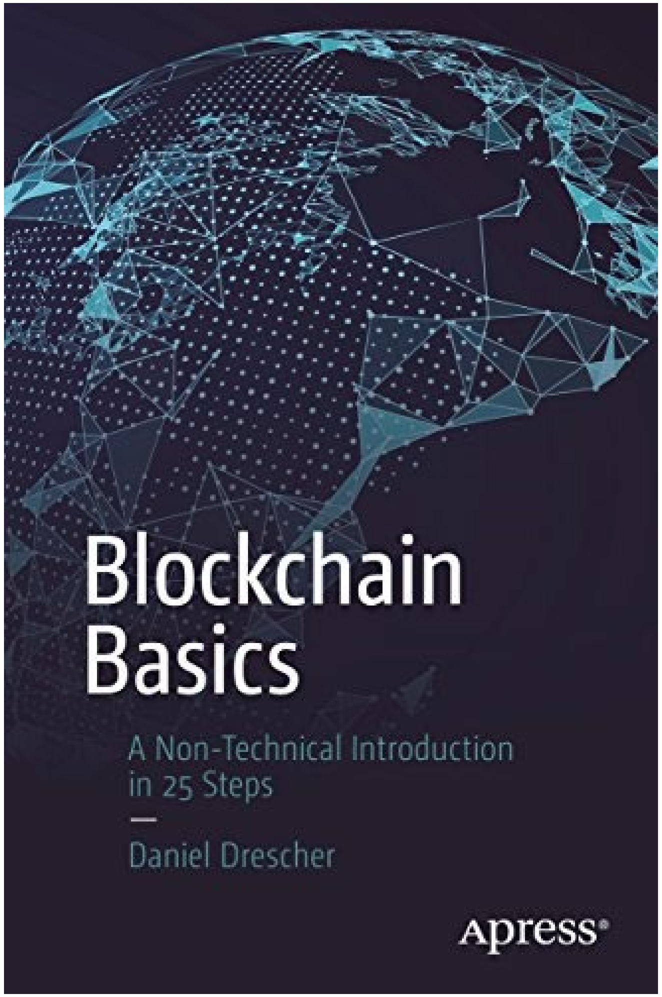
P.O. Box 1661
Hegibachstrasse 47
8032 Zurich
Switzerland

T +41 43 500 48 50
F +41 43 500 48 60

P.O. Box 1911
Route de Pré-Bois 20
1215 Geneva Airport
Switzerland

T +41 22 533 48 50
F +41 22 533 48 54

contact@gbf-legal.ch
www.gbf-legal.ch



Blockchain Basics

A Non-Technical Introduction in 25 Steps

—

Daniel Drescher

Apress®