```
++++++[>++++++++++++<-]>.
>++++++++++[>++++++++++<-
]>+.
+++++++.
.
+++.
>++++[>++++++++++++<-]>.
<+++[><-]>.
<<<<<+++[>++++++<-]>.
>>.
+++.
.
.
>>+.
```

SUPER HOW?

⩾ Beginners Guide to the Galaxy of Blockchains

Linas Būtėnas,
2022-08-10, Vilnius

1

```
----[----
>+<]>++.[---
>+<]>+..[++>-
--<]>--.---[-
>++++<]>-
.+.-----.+++.--
-------.----.[---
>+<]>----.+[--
-->+<]>+++.--
-[->++++<]>-
.+.+[-
>+++<]>++.--
[--->+<]>---
.++.[----
>+<]>+++.---
[->++++<]>.-
---.--.--------.[-
-->+<]>.+[-
>+++<]>.---
.++++++++++
+++.----------
--.
```

⩾ Once Upon a Time...

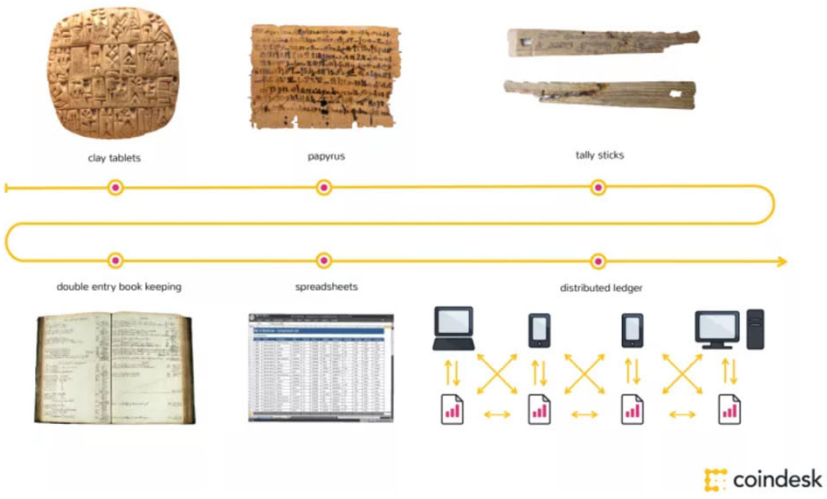
2

> Need for trust

- The value exchange is possible then trust is present

3

> Distributed ledger



4

> Digital Economy

- 1997 Don Tapscott – **DIGITAL ECONOMY**
  (The Age of Networked Intelligence)
- Web 2.0: **DIGITIZED INTANGIBLE GOODS**
  (Digitized intangible goods, Zero marginal cost intangible goods)
- 2006 Don Tapscott - **WIKINOMICS**
  (How Mass Collaboration Changes Everything)

https://en.wikipedia.org/wiki/Don_Tapscott

5

> When has it started??

Bitcoin (₿) - a decentralized digital currency, without a central bank or single administrator, that can be sent from user to user on the peer-to-peer bitcoin network without the need for intermediaries.

Invented in 2008 by an unknown person or group of people using the name **Satoshi Nakamoto**.

ASYMMETRIC CRYPTOGRAPHY – 50-year-old technology (invented in 1970-1973)

NETWORK INFRASTRUCTURE – ICT and cyber security

BLOCKCHAIN – distributed ledger data structure

2008 – 2009 Financial crisis led by Institutional Banks

6

> Crypto Economy

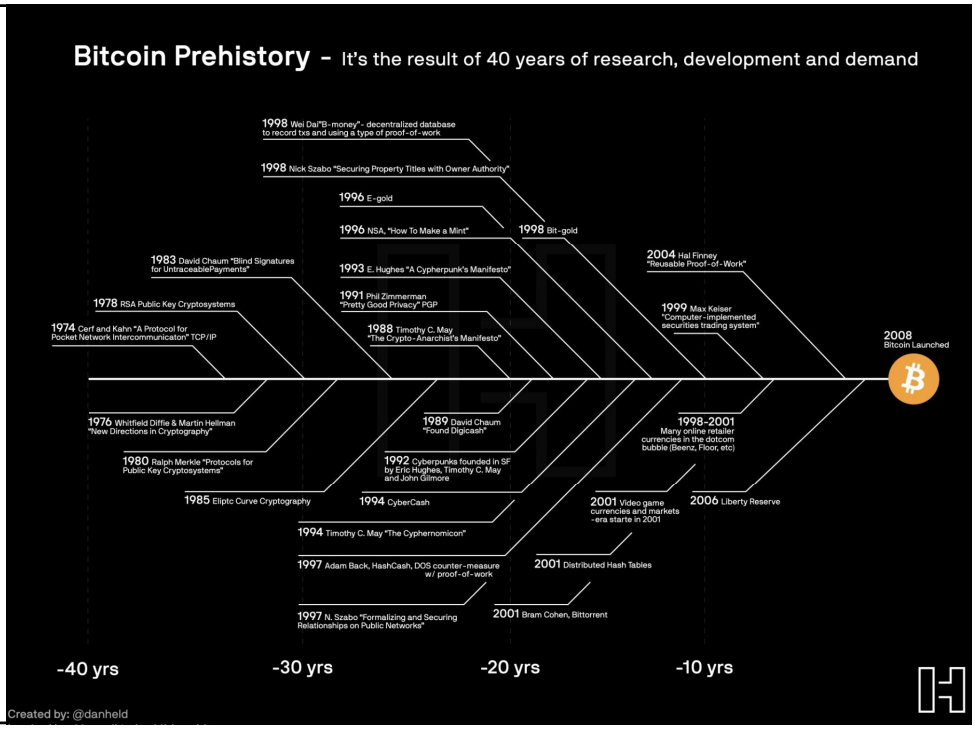
CRYPTO ECONOMY – economy based on cryptographical and decentralized infrastructures

- 2016 Don Tapscott – **BLOCKCHAIN REVOLUTION**
- **TRUST PROTOCOL**, social, virtual commerce
- Decentralised autonomous organisations (DAO)
- Self-sovereign Digital Identity
- Web 3.0: **TOKENISED ASSETS** (goods)

https://en.wikipedia.org/wiki/Don_Tapscott

7

> It has long history before...



8

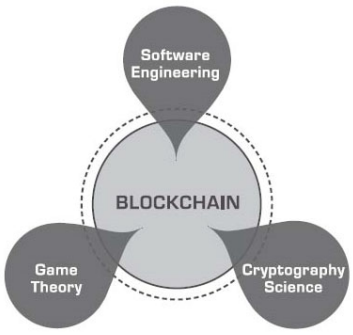
Where are we heading?

Web 1.0	Web 2.0	Web 3.0
Read-only web	Read-write web	Read-write-execute web
The first stage of the internet	The second stage of the internet	The third stage of the internet
The purpose is information sharing	It is about interaction	It aims at immersion
The content was owned	Shared content	Content will be collectively owned and shared
More of a simple and passive web	More of a social Web	It is a semantic web
Focuses on connecting information	Focuses on connecting people	Revolves around connecting knowledge
Static websites	Introduction of web applications	Web-based intelligent functionalities and applications
No or little interaction between server and user	Better interaction between server and user	Designed to deliver a personalized web experience to the users
Technologies related to Web 1.0 include Web and File Servers, HTML, and Portals	Associated technologies include Ajax, JavaScript, CSS, and HTML5	Technologies related to Web 3.0 include Blockchain, AI, decentralized protocols

9

The technological revolution

- **Block contains:**
  1. Data (transactions, smart-contracts, etc.)
  2. Previous block hash
  3. Block hash
- **Chain features:**
  1. Consensus mechanism (PoW, PoS, etc.)
  2. Incentives - Rewards to miners/validators
  3. Block time - Difficulty (10 min., 2 min, etc.)



Game theory is 'the study of mathematical models of conflict and cooperation between intelligent rational decision-makers."

https://andersbrownworth.com/blockchain/hash

10

Token

A *token* is an IOU

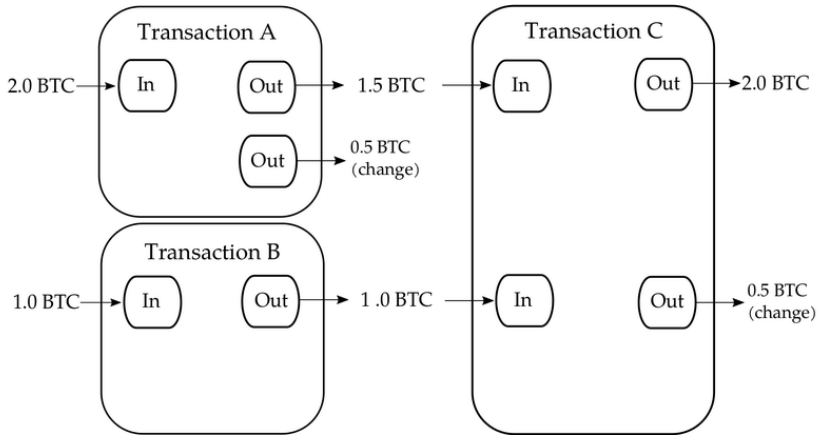
- A poker chip, concert ticket, stock certificate, bond, coat-check token,
- Dinner reservation, driver's license, passport, airline ticket, etc.

A dollar bill is a token, but a dollar is not

A digital token: 1HieAFgpQdrVLN8GPFMfG8yMcDxDsrXiLN

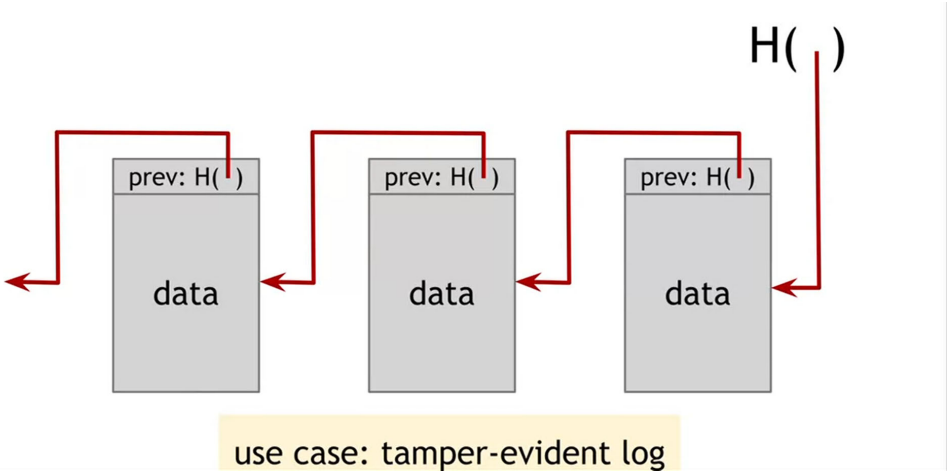
11

Blockchain Transaction – UTXO



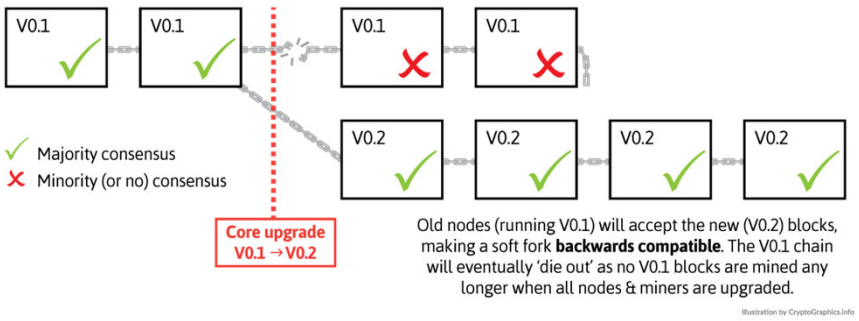
12

Blockchain block sequence



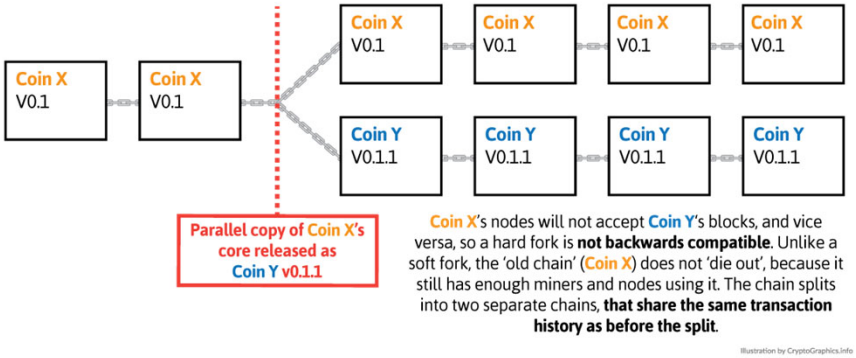
13

Blockchain consensus



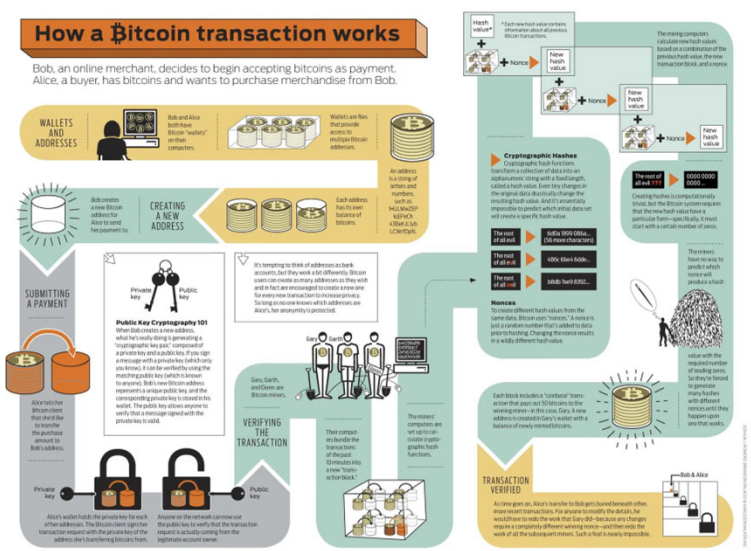
14

➢ Blockchain hard fork



15

➢ How Bitcoin netwok works?



16

How secure is Bitcoin wallet?

3.1 Public/Private Key Pair

A *private key* is a random 256-bit integer k. To derive the public key $\underline{A}$ from it, the following steps are taken:

$$H(k) = (h_0, h_1, \ldots, h_{511}) \quad (1)$$

$$a = 2^{254} + \sum_{3 \le i \le 253} 2^i h_i \quad (2)$$

$$A = aB \quad (3)$$

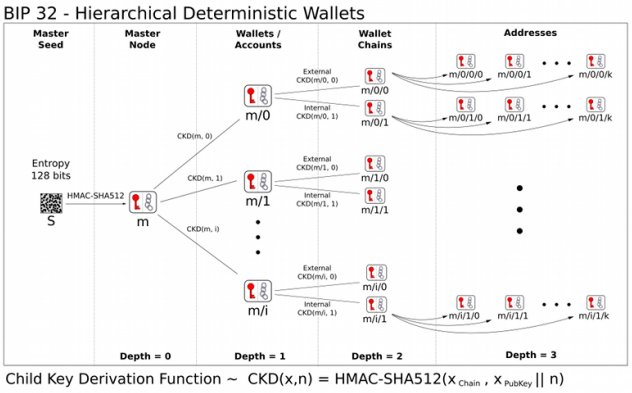
Since A is a group element, it can be encoded into a 256-bit integer $\underline{A}$, which serves as the public key.

- **How secure is SHA256:**
  - https://www.youtube.com/watch?v=S9JGmA5_unY&t=2s

17

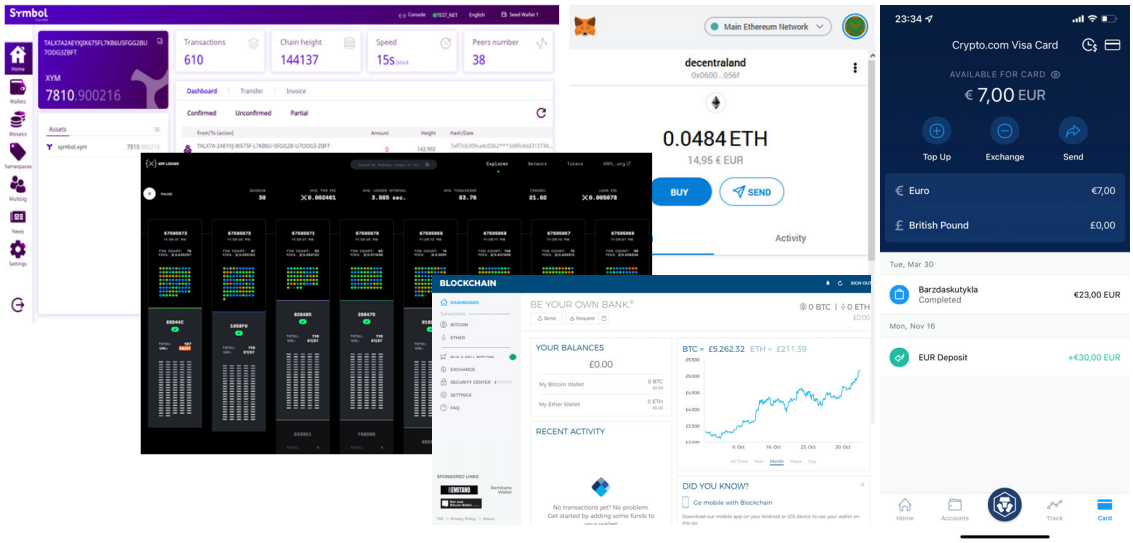
HD wallet

- **HD – Hierarchical Deterministic**
- https://medium.com/@harshagoli/hd-wallets-explained-from-high-level-to-nuts-and-bolts-9a41545f5b0



18

Wallets, Explorers and other



19

Some interaction

- https://brainwalletx.github.io/
- Bitcoin paper wallet
  - Be aware of scammers!!!
- https://www.blockchain.com/
- Bitcoin genesis block
  - https://www.blockchain.com/btc/block/000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f
- https://bitcoincore.org/

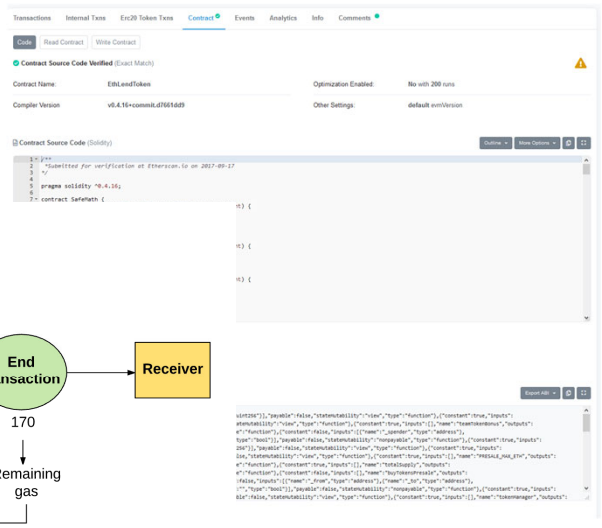
20

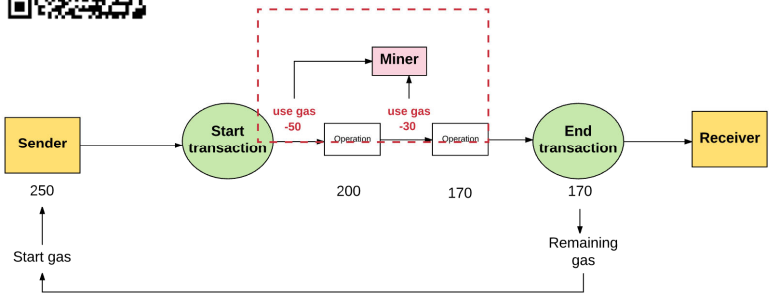
> Some interaction

- Blockchain block & mempool situation
  - https://mempool.space/
- Address generation
  - https://iancoleman.io/

21

> Smart Contracts, Chaincodes, etc.





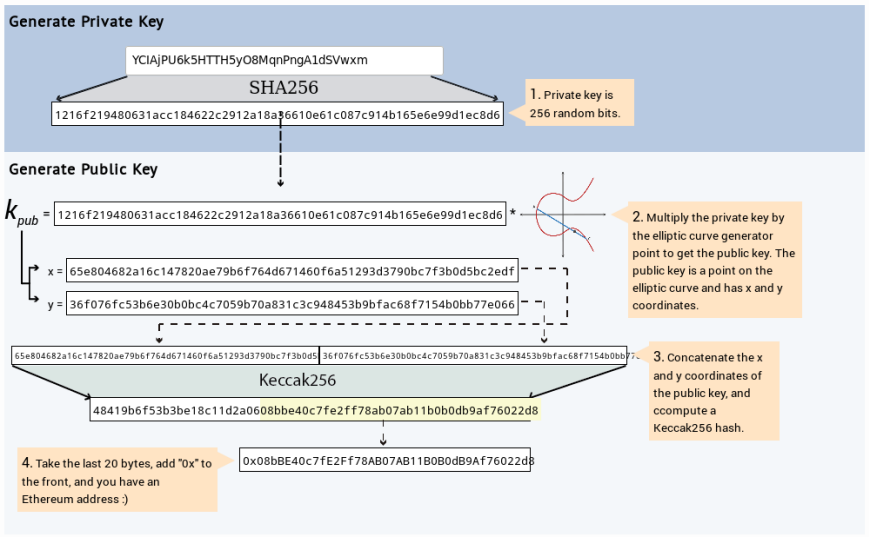
22

Ethereum

- Ethereum blockchain statistics
  - https://ethstats.net/
- Ethereum zero address
  - https://etherscan.io/address/0x0000000000000000000000000000000000000000

23

Ethereum wallet address



24

```
+[-------
>++<]>.+.++++++++.+[
---->+<]>++.-[---
>++<]>-
.++++++++++.[----
>+<]>+++.-[--->++<]>-
.++++++++++.+[----
>+<]>+++.++[-
>+++<]>+.--.[--->+<]>-
--..----------.+++++.----
---.-[--->+<]>--.---[-----
>++<]>.----------.----
.++++++++++.++[-----
>++<]>.-----------.+[---
-->+<]>.-----------
.++++++++++++.-[-
>+++++<]>.
```

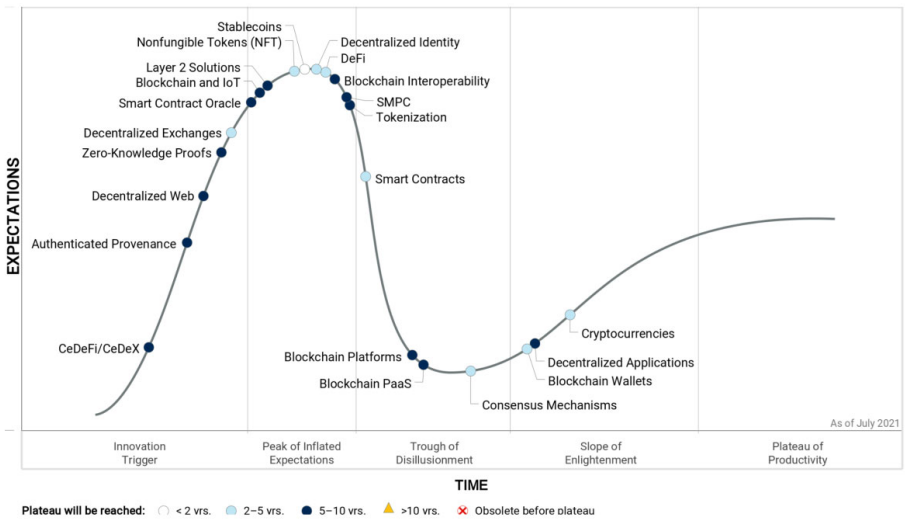
> Point Of No Return...

25

[S]

> Blockchain Technology Cycle 2021

```
++++[++++>---
<]>.+[--
>+++<]>++.----
---.-[++>-----
<]>.++++.+++[-
>+++<]>.++++
+++++++++.[--
>+++++<]>+++
.+++++[-
>+++<]>.-.------
---.
```



Source: Gartner (July 2021)

26

> Key adoption drivers

++++[+
+++>---
<]>.+[--
>+++<]
>++.----
---.-
[++>----
-

- **Mainstream adoption of Bitcoin**, including El Salvador's adoption of Bitcoin as legal tender in June 2021 and Central African Republic in April 2022
- Payment network, banking and social network adoption of distributed ledger technologies (DLTs) for money movement, with the expected deployment of **central bank digital currencies (CBDCs)** being a key influencer.
- **Decentralized finance (DeFi)** applications offer substantially greater financial rewards than traditional finance. Centralized firms like hedge funds already take advantage of this.
- Tokenization of assets, including **explosive growth of NFTs and DeFi tokens**, and the promise of tokens linked to physical assets in the future.
- Blockchains such as Binance, Polygon, Avalanche and Solana offering viable **cost-effective alternatives to Ethereum chain transactions**.
- Monumental **progress in blockchain interoperability**, including gateways and abstraction middleware, already used today by DeFi applications.
- Blockchain **migration from the proof-of-work (POW) consensus** method (still used for Bitcoin) **to more energy-efficient consensus methods such as proof of stake (PoS)**. The ongoing upgrade of Ethereum leads this trend.

27

> Still existing challenges

++++[++++>---
<]>.+[--
>+++<]>++.----
---.-[++>-----
<]>.++++.+++[-
>+++<]>.++++
+++++++++.[--
>+++++<]>+++
.+++++[-
>+++<]>.-.------
---.

- **Adoption of permissioned blockchains and DLTs is moving much more slowly**. Some use cases — especially around supply chain and authenticated provenance — are benefiting from ledger technology. However, most users are stuck trying to align use cases to the technology.
- **Lack of global regulations and accounting standards** for most enterprises to adopt cryptocurrency.
- **User experience and interfaces** in most of DeFi applications are not designed for ordinary user

28

```
++++++[>+++
++++++++<-
]>.
>+++++++++
+[>++++++++
++<-]>+.
+++++++.
.
+++.
>++++[>++++
+++++++<-]>.
<+++[><-]>.
<<<<<+++[>+
++++<-]>.
>>.
+++.
.
.
>>+.
```

To Happily Ever After...

```
++++[++++>---
<]>.+[--
>+++<]>++.-------.-
[++>-----
<]>.++++.+++[-
>+++<]>.++++++++
+++++.[--
>++++++<]>+++.+++
++[->+++<]>.-.------
---.
```

"Remember „ATOMIC" and you know what Blockchain offers"

Programmable:

+ Assets
+ Trust
+ Ownership
+ Money
+ Identity
+ Contract

++++[++++>---
<]>.+[--
>+++<]>++.-------.-
[++>-----
<]>.++++.+++[-
>+++<]>.++++++++
+++++.[--
>+++++<]>+++.+++
++[->+++<]>.-.------
---.

> Blockchain features

+ Transparency
+ Security
+ Traceability
+ Immutability

31

++++[++++>---
<]>.+[--
>+++<]>++.----
---.-[++>-----
<]>.++++.+++[-
>+++<]>.++++
+++++++++.[--
>+++++<]>+++
.+++++[-
>+++<]>.-.------
---.

> Blockchain unique benefits

+ Decentralised consensus
+ Self governance
+ Censorship resistance

32

++++[++++>
---<]>.+[--
>+++<]>++.
-------.-[++>-

<]>.++++.++
+[-
>+++<]>.++
+++++++++
++.[--
>++++++<]>+
++.+++++[-
>+++<]>.-.--
-------.

➢ Blockchain Myths

+ Cryptocurrencies and Blockchain is harmful for Ecology
+ Blockchain and Cryptocurrencies are used only by Tech-anarchists and Marginals
+ Cryptocurrencies are best for money laundering and terrorist financing
+ Tokens and Cryptocurrencies are stored in Wallets
+ Where is underlying value of Cryptocurrencies?

33

++++[++++>
---<]>.+[--
>+++<]>++.
-------.-[++>-

<]>.++++.++
+[-
>+++<]>.++
+++++++++
++.[--
>++++++<]>+
++.+++++[-
>+++<]>.-.--
-------.

➢ Few Tips and Tricks

+ You need to think "decentralised" and sometimes totally reshape the business model
+ Tokenonomics consists of two words – Token and Economy
+ Sometimes you will need to sacrifice something to achieve "greater good"
+ Not all business models need blockchain

34

++++[++++>---
<]>.+[--
>+++<]>++.----
---.-[++>-----
<]>.++++.+++[-
>+++<]>.++++
+++++++++.[--
>+++++<]>+++
.+++++[-
>+++<]>.-.------
---.

➢ What's next?

We project that by 2023, 35% of enterprise blockchain applications will integrate with decentralized applications and services.

The rewards are simply too high to ignore, and are far greater than the costs.

Source: Gartner (July 2021)

747513

35

+[------>++<]>-
.------------
.++++++.++.-----
-.[--->+<]>-.-[---
>++<]>-
.+++++.-------
.++++++++++.
----------.-
.+++++.----
.+++++++++.++
++++.

➢ „Any Sufficiently Advanced Technology is Indistinguishable from Magic“

ARTHUR C. CLARKE

www.superhow.com

36

37

> Systhemical decentralisation

- **DATA MANIPULATION** (Cambridge Analytica, Facebook, etc.)
- **TRUST ISSUES** (Governments, Politics, Inequality, etc.)
- **DATA MISUSE & LOSS** (Banks, Google, Clinical trials, etc.)
- **SINGLE POINT OF FAILURE** (central data bases, registers, etc.)
- **DIGITAL IDENTITY** (SIM Swapping, identification problems, KYC, etc.)
- **TECHNOLOGICAL PROGRESS** (decentralised consensus, trustless protocols, decentralised applications, etc.)

38

Tripple vs double-entry

++++[++++>---
<]>.+[--
>+++<]>++.----
---.-[++>-----
<]>.++++.+++[-
>+++<]>.++++
+++++++++.[--
>+++++<]>+++
.+++++[-
>+++<]>.-.------
---.

Alice account

Debit	Credit
	$100

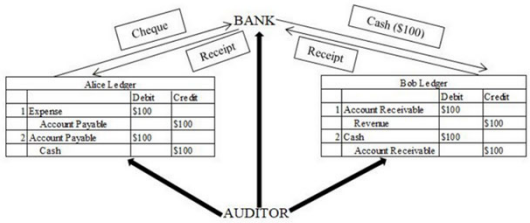
Bob account

Debit	Credit
$100	

Public Ledger
(Digital Receipt)

Alice	Bob
$100	$100
Out	In
Signature	Signature

A Simple Example of Triple-Entry Accounting



A Payment Transaction between Alice and Bob in a Double-Entry Accounting System

39

Merkle Tree

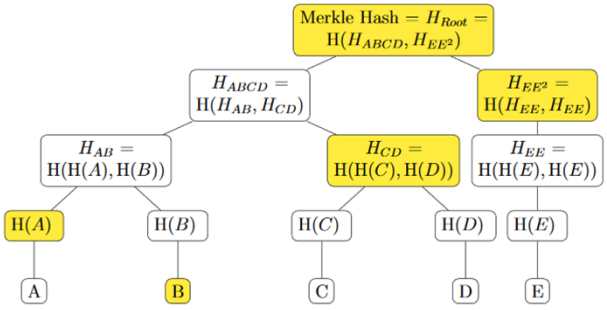
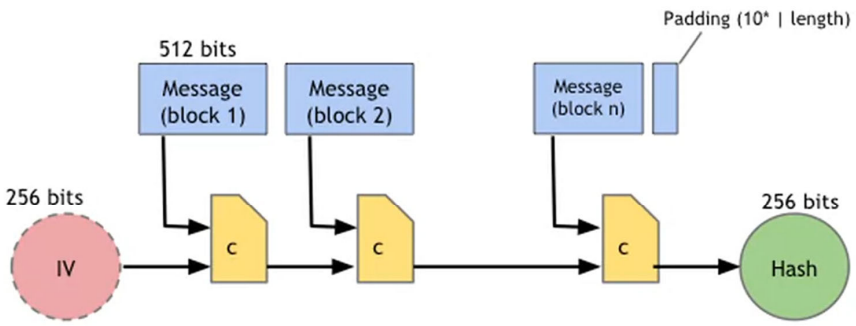


Figure 2: Merkle proof required for proving existence of B in the tree

40

> SHA256



Theorem: If c is collision-free, then SHA-256 is collision-free.

41