Zereon Associates

ADVISORY | DIGITAL | INVESTMENTS

DISTRIBUTED LEDGER TECHNOLOGIES AND BLOCKCHAIN : A NON-SPECIALIST RIGOROUS INTRODUCTION

(A BRIEF SUMMARY FOR NON-SPECIALIZED AUDIENCES)

ZURICH, 2020

(DISCLAIMERS)

This summary document has been created by Zereon Associates GmbH ("ZA") during and after the online training "Digital Transformation: from AI and IOT to Cloud, Blockchain and Cybersecurity", Prof. Williams, J. and Sanchez, A., MIT-Emeritus, 2019. It is distributed for free and with "open source" spirit with no further counter-obligations whatsoever by the reader, except citation, document change protection and no occultation of authorship as described below. The document has been created voluntarily and is offered for non-technical divulgation and convenient reference, widespread technology awareness and ZA's general promotion purposes only, without any gainful commercial payment involved in cash or in kind by any party. After-the-fact advisory business by the author to future and current Clients derived from later discussions might be possible if interested parties so request.

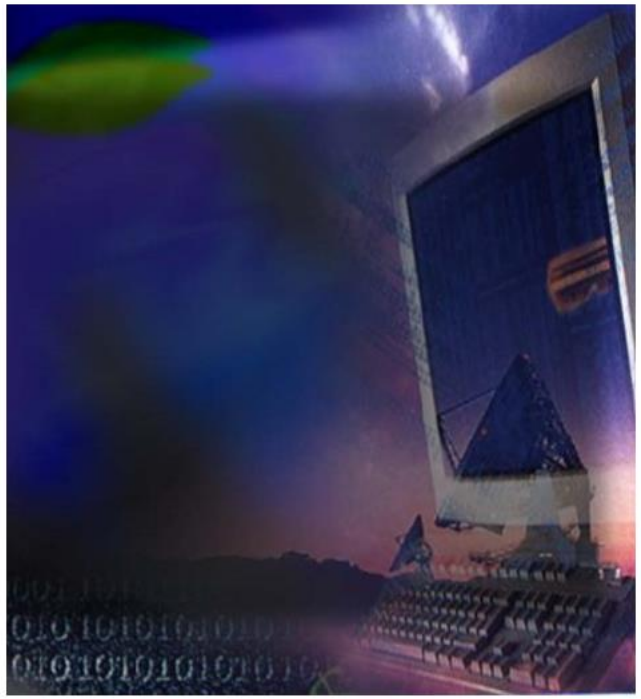
The document is based on 1) class notes and peer / professor discussions by Mario Ceron, MBA, ZA's Managing Partner & CEO, top-grade course alumnus (score 100/100) and document's author, 2) materials from the training course itself and 3) research by the author on 3rd party publicly available content. Even if mostly based on course materials and generated with rigorous professionalism intent, this summary work is unaffiliated directly with MIT, Emeritus and/or the course professors Dr. John Williams and Dr. Abel Sanchez, or the proprietors of the respective brands, technologies and tools mentioned herein, and unintended mistakes and/or omissions might occur.

Any kind of download, distribution, reading, interpretation, deployment or use, or lack thereof, of this document is voluntary, and additional professional advice is necessary and in fact strongly recommended for any real-life document content application - no responsibilities or damages of any kind can be accepted by ZA and/or Mr. Ceron whatsoever for the direct or indirect use of, or not use thereof, or any decision-making or investment of any size, or lack thereof, based on this document in full or in part. The document content is otherwise subject to all academic and technical recognitions, gratefulness and honors due to the Professors and to MIT and Emeritus as course creators, owners and distributors, as well as other due protections awarded by applicable laws. Likewise, due legal protections and recognitions apply to the proprietors of the respective brands, technologies and tools mentioned in the document as well; some logos were modified almost negligibly in the presentation for clarity.

Partial or total redistribution of this document is allowed, but only on condition of being completely for free and always citing both Zereon Associates GmbH AND MIT / Emeritus prominently. Suggestions and improvements are most welcome, but changes to the document itself, and/or occultation of authorship are not permitted without prior consultation with the author. Plagiarizing in full or in part is strictly forbidden. Please write to legal@zereonassociates.com for further legal comment and details, and to contact@zereonassociates.com for any technical clarification and/or content-related queries.

Zereon Associates
ADVISORY | DIGITAL | INVESTMENTS

CONTENTS

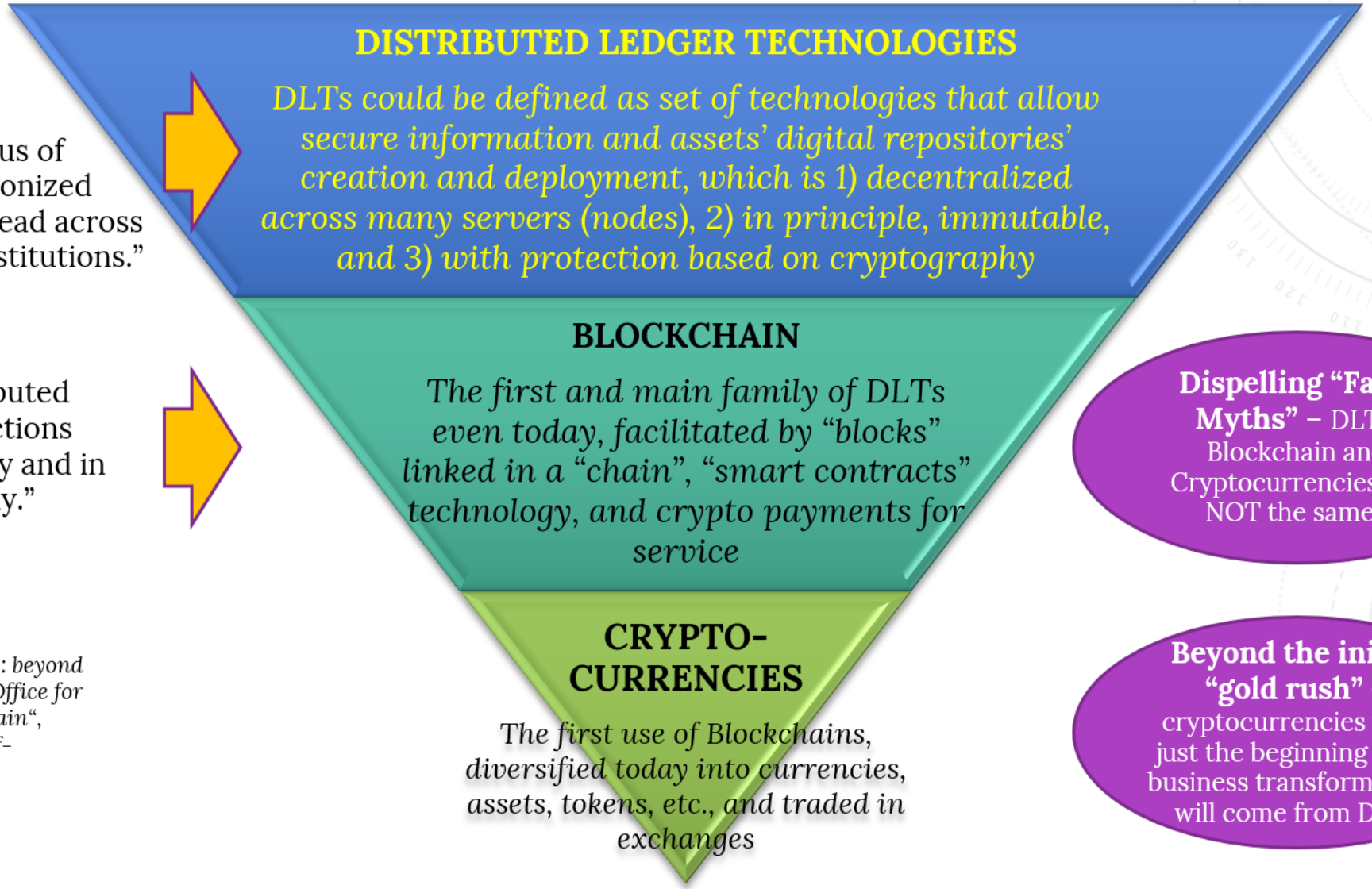


I. WHAT ARE DISTRIBUTED LEDGER TECHNOLOGIES AND WHAT IS BLOCKCHAIN ?

Zereon Associates
ADVISORY | DIGITAL | INVESTMENTS

"A **distributed ledger** (**shared ledger, distributed ledger technology, DLT**) is a consensus of replicated, shared, and synchronized digital data geographically spread across multiple sites, countries, or institutions."

"Blockchain is an open, distributed ledger that can record transactions between two parties efficiently and in a verifiable and permanent way."



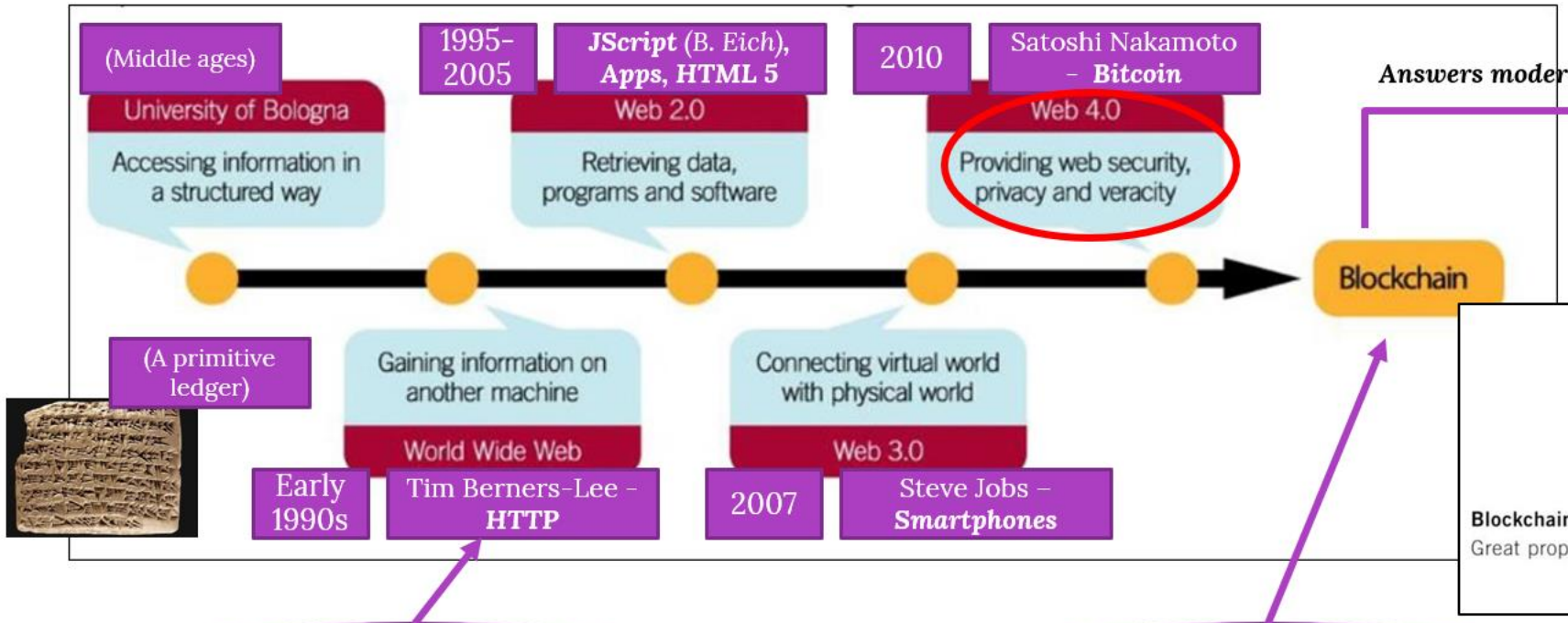
Dispelling "False Myths" – DLTs, Blockchain and Cryptocurrencies are NOT the same !

Beyond the initial "gold rush" – cryptocurrencies were just the beginning ; true business transformations will come from DLTs

Sources: "Distributed Ledger Technology: beyond block chain (Report)", UK Government, Office for Science, 2016; "The Truth About Blockchain", Iansiti, M.; Lakhani, K. R., HBR, 2017; self-elaboration.

II. THE EVOLUTION OF THE WEB TOWARDS DLT / BLOCKCHAIN

Zereon Associates
ADVISORY | DIGITAL | INVESTMENTS



Internet was NOT born with cybersecurity in mind, or to connect millions of devices and perform e-commerce - but to retrieve information from and inject content into remote computers !!

From the very beginning, the first DLTs (blockchain) were born with security, asset integrity and identity proof in mind

Source: "Digital Transformation: from AI and IOT to Cloud, Blockchain and Cybersecurity", Prof. Williams, J. and Sanchez, A., Course Materials MIT-Emeritus, 2019, and self-elaboration.

III. HOW BLOCKCHAIN WORKS – A) ENCRYPTION AND HASHES

Zereon Associates
ADVISORY | DIGITAL | INVESTMENTS

Basics of encryption via "hashes" – an example

H E L L O
↓ ↓ ↓ ↓ ↓
8 + 5 + 12 + 12 + 15 = 52

The hash function for HELLO could be 52

A message "hash" or ID obtained with a very simple algorithm: change the letters by alphabet number, then add the numbers

Real life hashes : very long and hexadecimal, generated with advanced math operations, difficult to generate and even harder to crack

The property of hashing

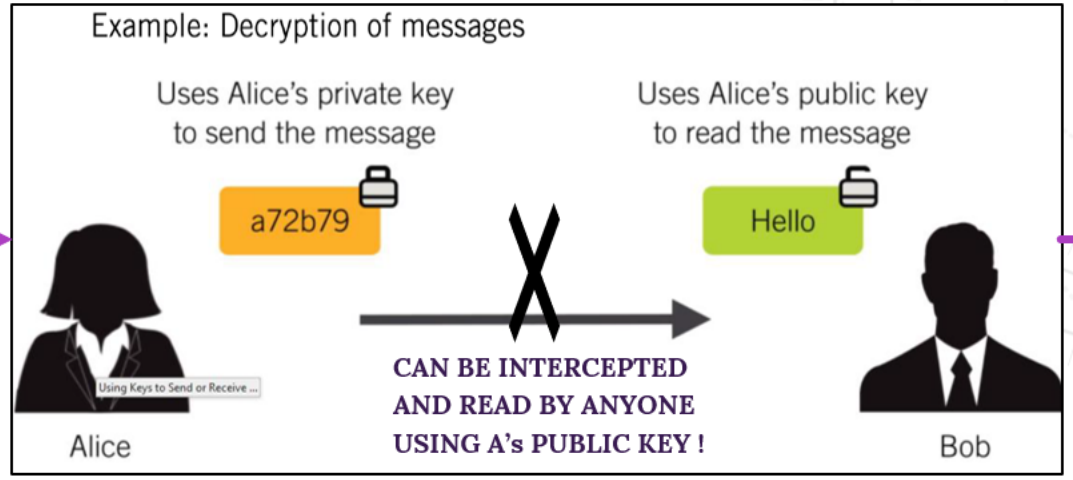
A small change in the input leads to a radically different hash sum

Input	Hash
000	8AEFB06C 426E07A0 A671A1E2 488B4858 D694A730
001	E193A01E CF8D30AD 0AFFEFD3 32CE934E 32FFCE72
010	47AB9979 443FB7ED 1C193D06 773333BA 7876094F

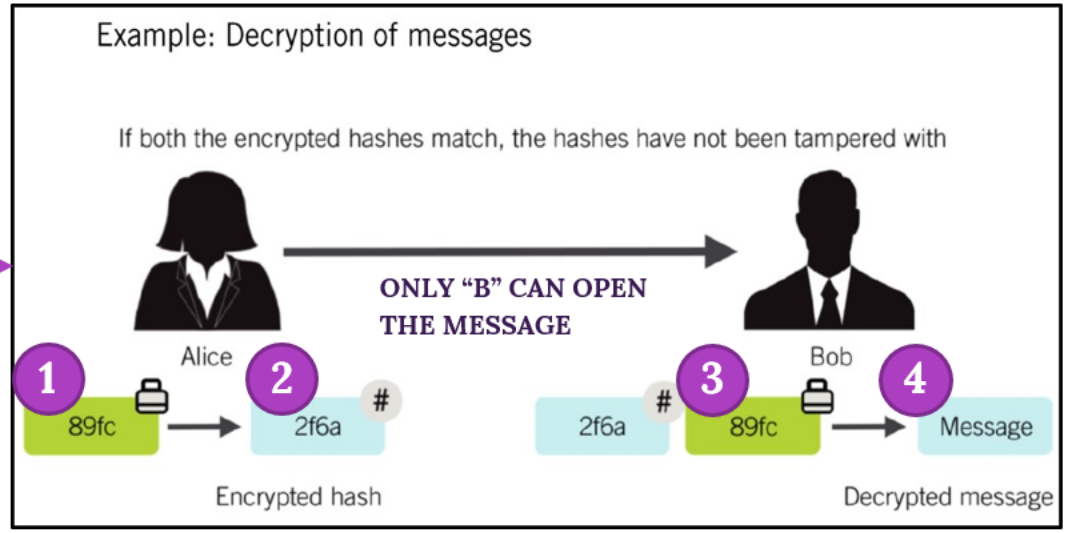
One cannot predict inputs based on the hashes provided

A hash is like a lock on a document

Basic idea of an encryption process



Reality of encryption processes



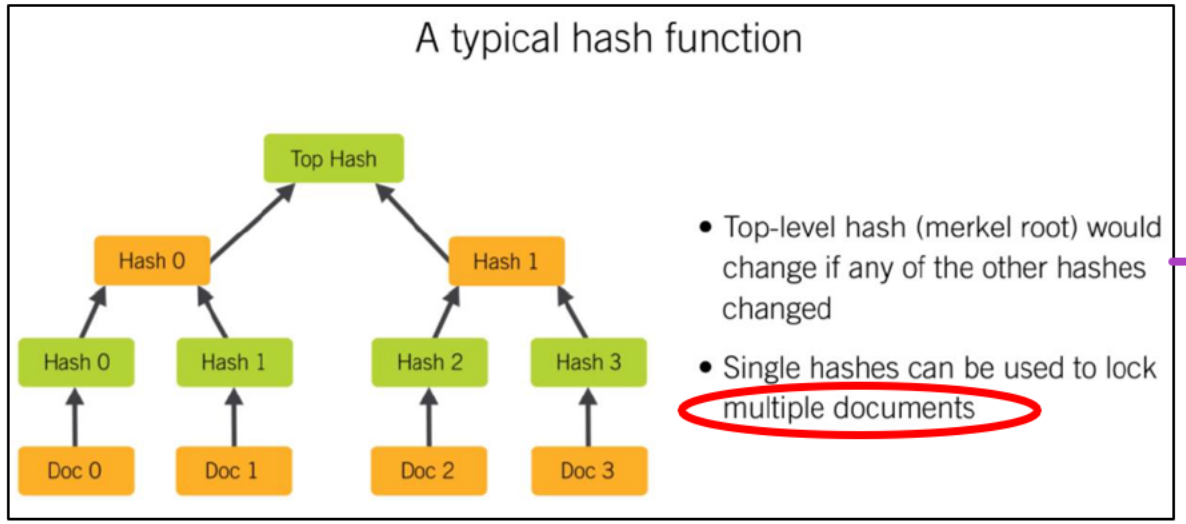
1. **A uses A's Private Key to lock the document and get a hash.**
2. **A creates a "hash of the hash" with B's Public key ("signs") and sends the package.**
3. **B uses B's Private Key to read that hash ("signature") and gets A's original hash.**
4. **B uses A's Public Key on the original hash to access the document.**

Source: "Digital Transformation: from AI and IOT to Cloud, Blockchain and Cybersecurity", Prof. Williams, J. and Sanchez, A., Course Materials MIT-Emeritus, 2019, and self-elaboration.

III. HOW BLOCKCHAIN WORKS – B) CREATING AND LINKING BLOCKS

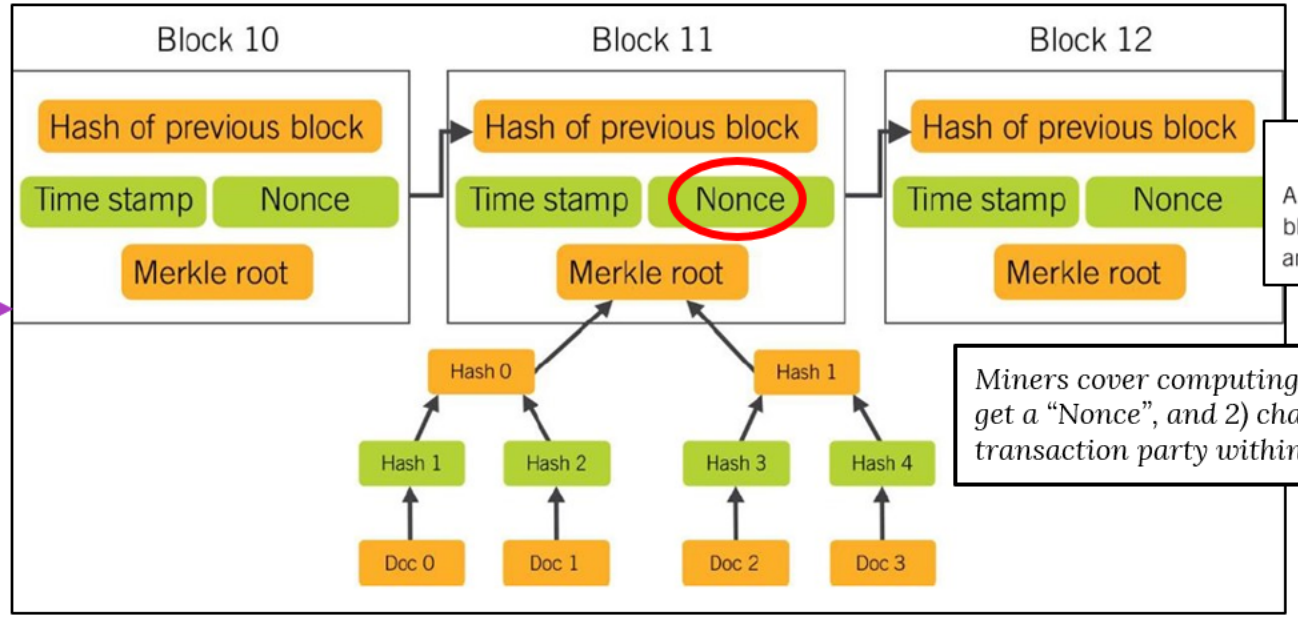
Zereon Associates
ADVISORY | DIGITAL | INVESTMENTS

Linking several docs / transactions together



- ✓ **Unique ID (hash of hashes), Top Hash, or "Merkle root" is the heading of the whole structure (called "Merkle tree")**
- ✓ **Includes several hashed transactions from different users.**
- ✓ **Not tampered with (public and private key successive encryptions).**
- ✓ **Creators authenticated via ID hashing process.**
- ✓ **Specific "blocks" or structures chosen, created and executed by decentralized, competitive "miners", depending on reward expected and computational cost required.**

How blocks are created and linked - **MINING**



Challenge for miners

A nonce value needs to be found such that the hash of the entire block (including hash of previous block, timestamp, Merkle root, and nonce) starts with a defined number of leading 0's

Miners cover computing cost and make money 1) by being the first to get a "Nonce", and 2) charging a small cryptocurrency amount to each transaction party within the block created (fees lower than classic DBs).

Source: "Digital Transformation: from AI and IOT to Cloud, Blockchain and Cybersecurity", Prof. Williams, J. and Sanchez, A., Course Materials MIT-Emeritus, 2019, and self-elaboration.

III. HOW BLOCKCHAIN WORKS – C) THE WHOLE PROCESS

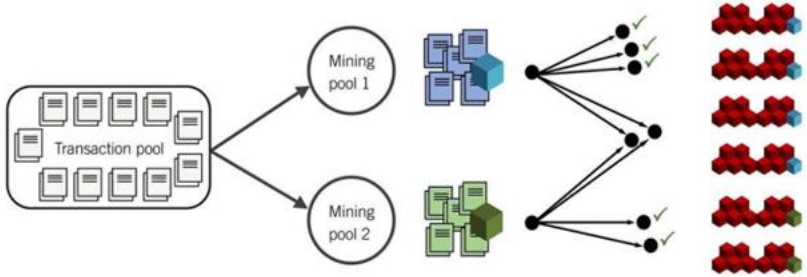
Zereon Associates
ADVISORY | DIGITAL | INVESTMENTS

A blockchain user proposes a transaction by communicating to one of the nodes → Nodes broadcast and rebroadcast the proposed transaction until every node has a copy → The proposed transaction is added to the transaction pool

Miners bundle the profitable transactions, solve the puzzle, and propose the next block → The winning miner broadcasts the proposed block to other users for validation → The validated block is added to the blockchain

(Mining – *see previous page*)

The two miners, from two different mining pools broadcast different blocks, leading to unsynchronized blockchains



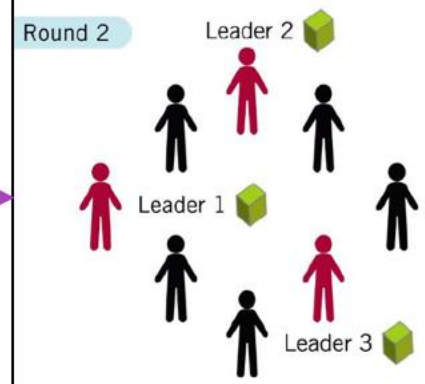
Conflicts are resolved by checking the timestamps and designating the later timestamp as an "orphaned block", not to be considered for synchronizing the network

Consensus: "Proof of Work" (PoW)

		Orphaned block		
466252	Timestamp	2017-05-13 20:41:14	Timestamp	2017-05-13 20:41:20
	Number Of Transactions	2100	Number Of Transactions	886
	Relayed By	BW.COM	Relayed By	BitFury

Issue 1: *PoW is becoming an expensive data mining algorithm →* ***Proof of Stake*** *(cheaper, faster)*

Steps in the Proof of Stake algorithm:



1. A number of leaders are chosen at random
2. The chosen leaders are ordered, which is called **sortition**
3. Leaders broadcast their blocks and proof of their leader status

Rule: All leaders follow **Leader 1** in the next round as long as the block is valid

4. New leaders are chosen, and based on the messages they received in the last round, they follow Leader 1 and choose the green block

(Other Consensus methods are being proposed, such as the Hyperledger blockchain Orderer Service).*

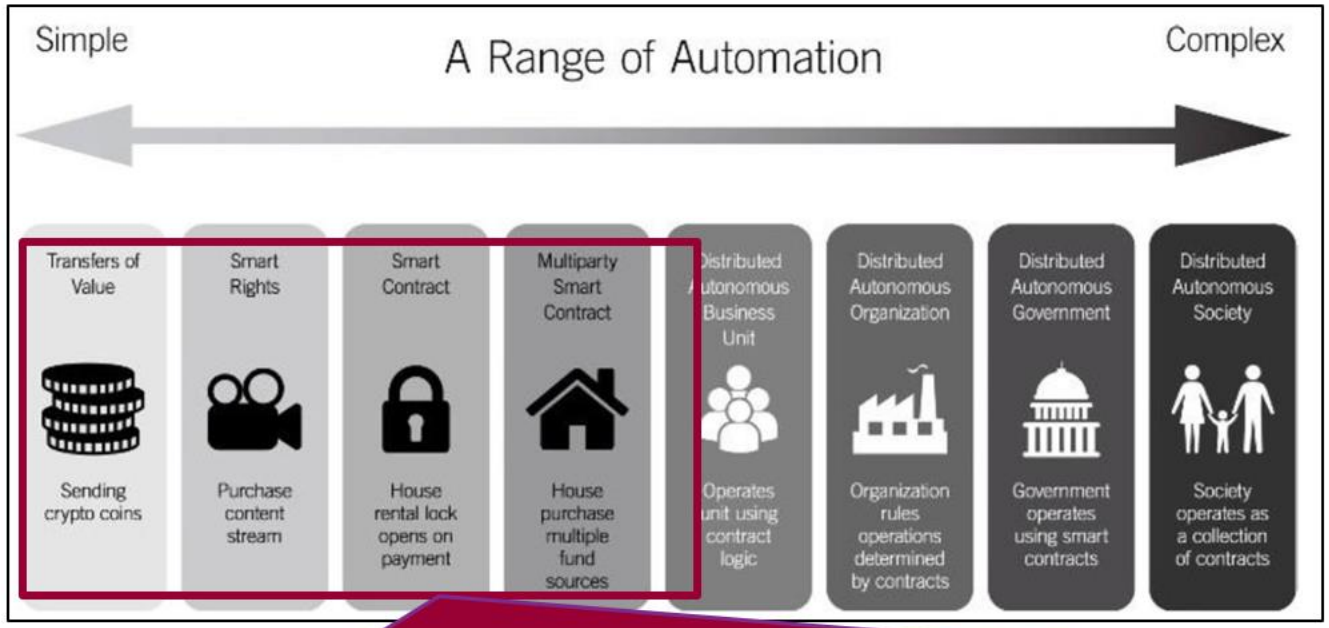
Issue 2: *How to speed up transactions*

Sidechains and **sharding** make blockchains run faster by consolidating transactions and putting only the consolidated transactions into the main blockchain

The **Cosmos architecture** runs a hierarchy of blockchains where small blockchains that do specific things, feed into larger blockchains, which further feed into even larger blockchains

Source: *"Digital Transformation: from AI and IOT to Cloud, Blockchain and Cybersecurity", Prof. Williams, J. and Sanchez, A., Course Materials MIT-Emeritus, 2019, and self-elaboration.*

IV. USE CASES – A) GENERAL STATUS



1st Generation - Currencies	2nd Generation - Contracts	3rd Generation - Digital services	4th Generation - Digital infrastructure
• Bitcoin • Bitcoin like	• Financial services • Crowdfunding • Prediction markets • Smart property • Development platforms • DApps	• DNS • Digital identity	• Government • Education • Health • Publishing *(and more)*

Many DLT use cases are already running in multiple industries, well beyond the original cryptocurrency use

Most DLTs are strictly blockchain-based (Bitcoin, Ethereum), but not all (Hyperledger, R3, etc.)

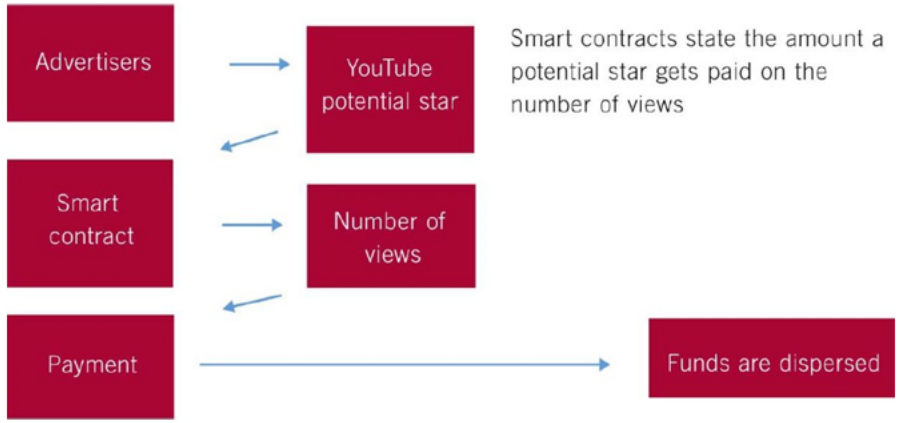
Trend towards private ("permissioned") DLTs created by company groups- full potential not deployed yet

Source: "Digital Transformation: from AI and IOT to Cloud, Blockchain and Cybersecurity", Prof. Williams, J. and Sanchez, A., Course Materials MIT-Emeritus, 2019, and self-elaboration.

IV. USE CASES – B) SOME EVOLVED EXAMPLES

Zereon Associates
ADVISORY | DIGITAL | INVESTMENTS

YouTube



IBM

Walmart

清華大學 Tsinghua University

- ✓ Major global food traceability and supply chain BC-based management consortium ("IBM's Food Trust").
- ✓ Enables companies to quickly track unsafe products back to their source and see where else they have been distributed, preventing illness, even saving lives, and reducing the time and cost of product recalls.
- ✓ For example, it allows time reduction to track a mango from the store back to its source from seven days to 2.2 seconds.
- ✓ Affiliates: founding members, plus Dole, Driscoll's, Kroger, Nestle, Tyson, Unilever and several others.

energy web

- ✓ World's first public, open-source, enterprise-grade blockchain tailored to the energy sector, located in Switzerland.
- ✓ Enables peer-to-peer generation and distribution, renewable energy certificate trading and operating effective demand-response energy programs, with transparency into how participant stakeholders conduct operations.
- ✓ Affiliates: utilities and grid operators in Belgium, France, Southeast Asia and Central America, plus at least one Fortune 500 global power company, and blockchain developers OLI Systems, FlexiDAO, Wirepas and Digital Virtues.

Bit Pesa

- ✓ First payments company based on blockchain to be recognized by the UK Financial Conduct Authority.
- ✓ Allows same-day payments to African company employees, distributors or suppliers into their local or international bank accounts, as well as accept payment from local customers in seven major African currencies.
- ✓ Â fee is charged that is a fraction of traditional payment transfers. This improves profitability for producers (often farmers) and everyone else in the supply chain.
- ✓ Mentioned in Wired, WSJ, Forbes, CNN, Fortune, etc.

Sources: "Digital Transformation: from AI and IOT to Cloud, Blockchain and Cybersecurity", Prof. Williams, J. and Sanchez, A., Course Materials MIT-Emeritus, 2019; "Energy sector gets first open-source, tailor-made blockchain", Maisch, M., PV Magazine Global, 2019; "Six Ways Blockchain is Being Used in Food and Agriculture Supply Chains", Noel, A., Medium.com / Cultivati, 2018.

V. DISTRIBUTED LEDGERS VERSUS TRADITIONAL DATABASES - 1

Zereon Associates
ADVISORY | DIGITAL | INVESTMENTS

DLTs / Blockchains = new type of database.

Traditional databases (SQL or NoSQL, ie relational or not relational DBs) → controlled by one single entity (centralized).

DLTs / blockchain → shared by a group of selected parties directly, no central administrator exists (* there may be technology infrastructure facilitators, however).

- **Traditional, centralized databases have a single point of failure and attack ("honey pot problem"), and data analytics is monetized by the owner of the platform only →** as opposed to distributed databases / DLTs which are secured by much larger redundancies, cryptography and consensus mechanisms, and in which the parties share the information.
- **Private ("permissioned") DLTs and blockchains →** allows for network members' exclusivity and administration over who can join and participate via an additional control layer built into DLT protocols.

Source: "Is Blockchain Better Than a Database ?", Yanowitz, J., Medium.com, 2018, and self-elaboration.

V. DISTRIBUTED LEDGERS VERSUS TRADITIONAL DATABASES - 2

Zereon Associates
ADVISORY | DIGITAL | INVESTMENTS

Qualities of DLTs / Blockchain		Qualities of Traditional DBs	
Security	An attack needs to bring down the whole network worldwide. Plus, very long hexadecimal hashes exist inside that contain many other nested, very long hexadecimal hashes – building those alone consumes staggering amounts of computing power; breaking them is almost impossible today even with quantum computing.	**Open to cyberattacks**	You only need to attack the "central authority" servers. Standard protection algorithms have more and more trouble to keep up with cheaper and more powerful attack and crack modes, even if assisted with AI.
Robustness with less Performance	For most DLTs, every node process every transaction, no individual node is crucial to the whole DB - this makes it very durable, even if slower comparatively. *(* Visa can handle 1,700 transactions per second; Etherscan ca. 20 - however, the tech is improving fast.)* If many nodes go down, the tech can catch up on missed transactions – safe copies reside in every node.	**Performance with less Robustness**	Traditional DBs may take less energy and time, whereas DLT requires computationally complex Signature Verification, Consensus Mechanisms and Redundancy. However, traditional DBs have the risk of "single point of failure" and have much more limited backups / disaster recovery.
Immutable Audit Trail	"Append only" system (Create / Read transactions, not Update / Delete) – immutable ledger. A user can only add more data and all previous data is permanently stored.	**Modification possible**	A traditional DB can be changed as key users have CRUD commands available (ie they can Update and Delete information) – and mistakes can be made.
Disinter-mediation	Data can be shared across a network of parties without needing a single master intermediary to authorize it, once the rules have been set.	**"Central authority"**	There is a "king of the data" that has omnipotent rights and power of authorization over all other users and often monetizes data analytics from the other parties.
Controlled Transparency	In DLT every node must have visibility into the single digital signatures via a hash / ID that uniquely identify each transaction's parties, and other details (but not the specific content).	**Opacity (if desired)**	The ID of the transacting parties and all other information can be faked or hidden.

Source: "Is Blockchain Better Than a Database ?", Yanowitz, J., Medium.com, 2018, and self-elaboration.

Zereon Associates
ADVISORY | DIGITAL | INVESTMENTS

THANK YOU !

ZEREON ASSOCIATES GMBH
Zurich, Switzerland
contact@zereonassociates.com
www.zereonassociates.com