

The multimedia blockchain: challenges and perspectives

Eric Paquet
16 October 2018



Blockchain-based technologies have the potential to resolve some of the current challenges:

- **Micropayment**-based pricing models
- **Monetization** options emerge for fragmented content
- Advertising more **targeted** as **media usage can be directly linked to the respective content items**
- **Copyright infringements and piracy** would be nearly impossible

Blockchain

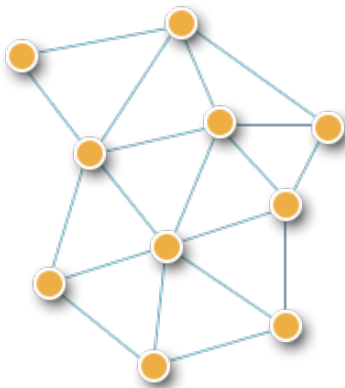
- “A blockchain is a digital, **immutable, distributed ledger** that **chronologically** records transactions in near real time. The **prerequisite** for each subsequent **transaction to be added** to the ledger is the respective **consensus of the network** participants (called nodes/miners), thereby creating a continuous mechanism of control regarding manipulation, errors, and data quality.” (blockchain institute)



Distributed

- **Identical copies** of all records are shared in the blockchain. Participants can independently verify information. Verification processes are **not dependent on a centralized authority**. If one node fails, the remaining ones can continue to operate ensuring availability and reliability.

Distributed



Centralized



Decentralized

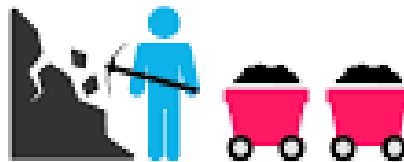


Consensus-based

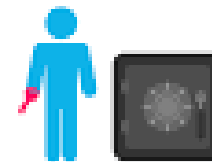
- Participants in the network collectively authenticate and approve transactions to the blockchain. There are different methods of reaching the consensus. Generally speaking, a majority of network participants **has to agree to the transaction's correctness, and rules can be tailored to circumstances.**



Proof of Work vs **Proof of Stake**



proof of work is a requirement to define an expensive computer calculation, also called mining



Proof of stake, the creator of a new block is chosen in a deterministic way, depending on its wealth, also defined as stake.

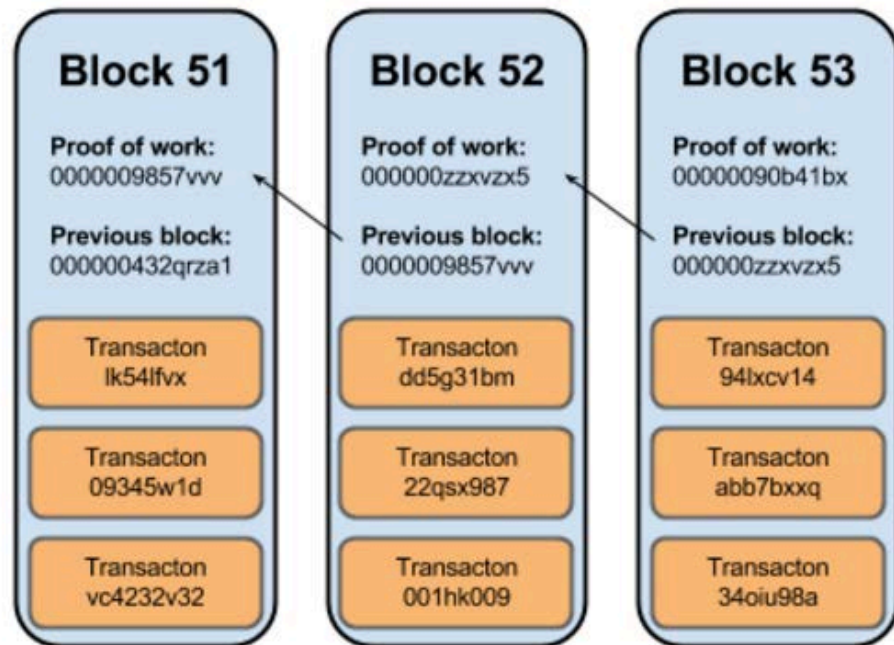
Chronologically updated

- The blockchain is **permanently timestamped**, each block points to and refers to the data stored in the previous block in the chain, so all blocks are linked to each other.



Cryptographically sealed

- Sealed in the chain, blocks can no longer be changed: the prevention of deletion, editing, or copying creates true digital assets.
- You cannot erase!



Smart contracts

- Smart contracts enable counterparties to **automate transaction tasks** that are typically performed manually and that require the involvement of **third-party intermediaries**. Smart contract technology can result in processes that are faster and more accurate and cost-efficient.
- Smart contracts cover a large number of contractual application areas that can profit from increased reliability, faster transaction processing, lower costs, and fewer manual process steps via intermediaries.

New pricing options for paid content

- As micro-payments become economically efficient and digital content is harder to copy illegally, new pricing opportunities arise
- Low-price content (<1 CAD) can efficiently be settled between seller and buyer
- Inclusive



Content bypassing aggregators/distributors

- Content consumption / usage is captured in Blockchain and a precise consumption-based analysis is possible
- Near real-time allocation of royalty payments (cryptocurrency)
- Alternative to imprecise estimates

Consumption of paid content without boundaries

- National / regional limitations of paid content subscriptions and digital right management (DRM) complexities will be decreased by the Blockchain
- True de facto but not entirely true in reality...
- Decreased complexity of rights management
- Direct linkage of consumption to individual / user through Blockchain authentication (**as long as they don't have many wallets!**)

New pricing options for paid content

- Transaction quantity is massive because a large quantity of historical data needs to be retained at the blockchain nodes, due to the number of transactions.
- **Common blockchain standards** still need to be agreed on.
- **Copyright tracking** becomes more accurate, as does allocation to media copyright holders and the subsequent **distribution of royalty payments**.
- **Efficiency increases**, since costly monitoring of contractual agreements and complex distribution of profits are not necessary.

Content bypassing aggregators

- Blockchain permits direct customer relationships between consumers and producers.
- Marketing performance and impact become more accurately measurable.
- Existing complex media and advertising ecosystems become simple and transparent.

Distribution of royalty payments

- **Common blockchain platform and interoperable blockchain standards** need to be agreed upon by the many relevant participants
- Near real-time and exact allocation and distribution of royalty payments according to usage, based on smart contracts - no more black boxes
- Cost efficiency – no costly tracking and monitoring systems for media usage required, as every consumption / usage will be tracked in the blockchain

Is a standard premature?

- After all...
 - Relatively new technology
 - Rapid development
 - Mostly industry driven
- But imagine mobiles without standards (e.g. 5G)
 - Apple to Apple only
 - Blackberry to Blackberry only
 - The Babel Tower!!!
- A standard is a process
 - The best that may be achieved today
 - Mobile: 1G, 2G, 3G, 4G, 5G ...
 - Many iterations will be required
 - It is an ongoing process

ISO/TC 307/JWG 4	Joint ISO/TC 307 - ISO/IEC JTC 1/SC 27 WG: Blockchain and distributed ledger technologies and IT Security techniques
ISO/TC 307/SG 2	Use cases
ISO/TC 307/SG 6	Governance of blockchain and distributed ledger technology systems
ISO/TC 307/SG 7	Interoperability of blockchain and distributed ledger technology systems
ISO/TC 307/WG 1	Foundations
ISO/TC 307/WG 2	Security, privacy and identity
ISO/TC 307/WG 3	Smart contracts and their applications

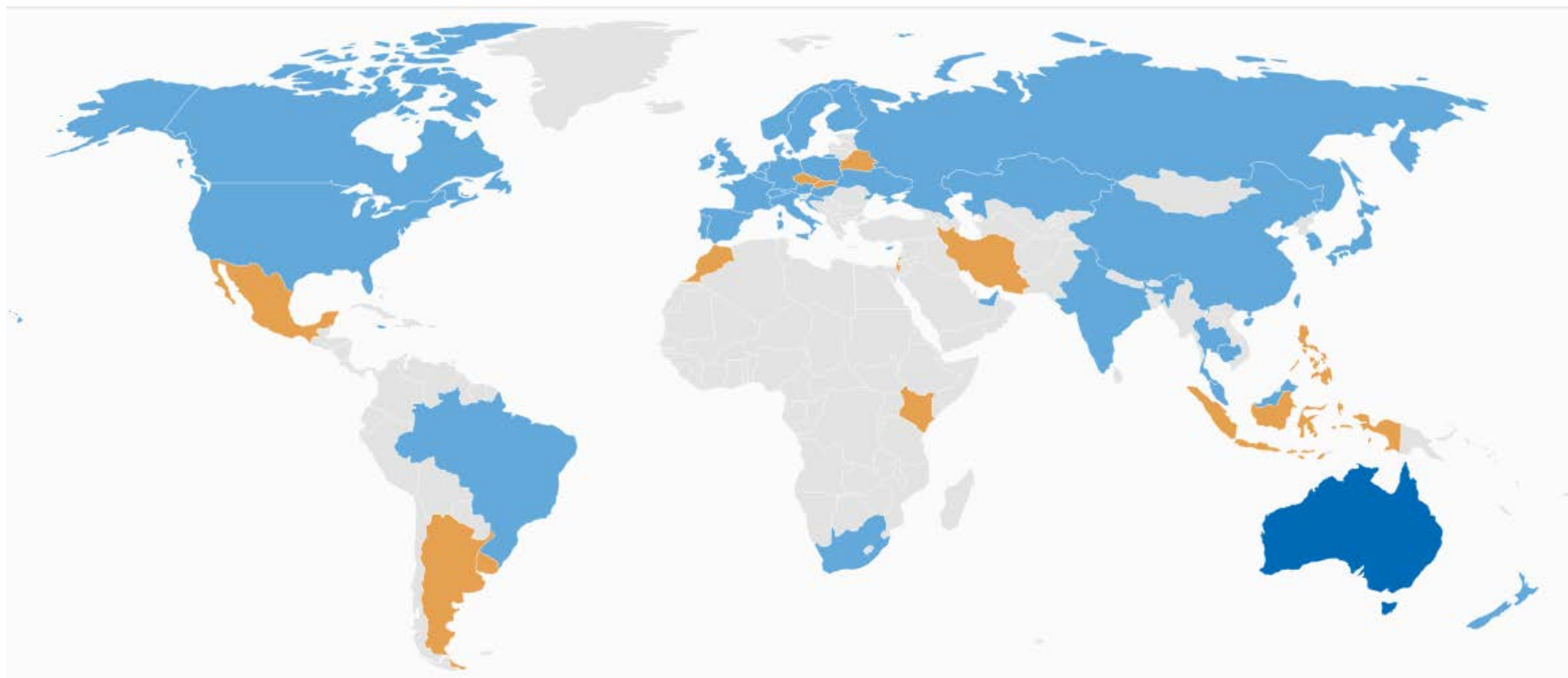
Liaison Committees to ISO/TC 307

Reference	Title	ISO/IEC
ISO/IEC JTC 1	Information technology	ISO/IEC
ISO/IEC JTC 1/SC 7	Software and systems engineering	ISO/IEC
ISO/IEC JTC 1/SC 17	Cards and security devices for personal identification	ISO/IEC
ISO/IEC JTC 1/SC 27	IT Security techniques	ISO/IEC
ISO/IEC JTC 1/SC 31	Automatic identification and data capture techniques	ISO/IEC
ISO/IEC JTC 1/SC 32	Data management and interchange	ISO/IEC
ISO/IEC JTC 1/SC 36	Information technology for learning, education and training	ISO/IEC
ISO/IEC JTC 1/SC 37	Biometrics	ISO/IEC
ISO/IEC JTC 1/SC 38	Cloud Computing and Distributed Platforms	ISO/IEC
ISO/IEC JTC 1/SC 40	IT Service Management and IT Governance	ISO/IEC
ISO/IEC JTC 1/SC 42	Artificial intelligence	ISO/IEC
ISO/PC 308	Chain of custody	ISO
ISO/TC 46/SC 11	Archives/records management	ISO
ISO/TC 68	Financial services	ISO
ISO/TC 68/SC 2	Financial Services, security	ISO
ISO/TC 154	Processes, data elements and documents in commerce, industry and administration	ISO
ISO/TC 184/SC 4	Industrial data	ISO
ISO/TC 211	Geographic information/Geomatics	ISO
ISO/TC 262	Risk management	ISO
ISO/TC 292	Security and resilience	ISO
ISO/TC 309	Governance of organizations	ISO

Liaison Committees from ISO/TC 307

Reference	Title	ISO/IEC
ISO/IEC JTC 1	Information technology	ISO/IEC
ISO/IEC JTC 1/SC 7	Software and systems engineering	ISO/IEC
ISO/IEC JTC 1/SC 17	Cards and security devices for personal identification	ISO/IEC
ISO/IEC JTC 1/SC 27	IT Security techniques	ISO/IEC
ISO/IEC JTC 1/SC 29	Coding of audio, picture, multimedia and hypermedia information	ISO/IEC
ISO/IEC JTC 1/SC 32	Data management and interchange	ISO/IEC
ISO/IEC JTC 1/SC 37	Biometrics	ISO/IEC
ISO/IEC JTC 1/SC 38	Cloud Computing and Distributed Platforms	ISO/IEC
ISO/IEC JTC 1/SC 40	IT Service Management and IT Governance	ISO/IEC
ISO/IEC JTC 1/SC 42	Artificial intelligence	ISO/IEC
ISO/PC 295	Audit data collection	ISO
ISO/PC 308	Chain of custody	ISO
ISO/TC 46	Information and documentation	ISO
ISO/TC 68	Financial services	ISO
ISO/TC 68/SC 2	Financial Services, security	ISO
ISO/TC 154	Processes, data elements and documents in commerce, industry and administration	ISO
ISO/TC 211	Geographic information/Geomatics	ISO
ISO/TC 215	Health informatics	ISO
ISO/TC 262	Risk management	ISO
ISO/TC 292	Security and resilience	ISO
ISO/TC 309	Governance of organizations	ISO

Participating and observing members



Consensus mechanisms

- Proof-of-work
- Concentration of miners
- Small number of miners
- Bitcoin alone consumes more energy than 150 countries
- Pollution: Paris Agreements, IPCC Report
- Proof of stake, capacity, storage: concentration of miners
- Proof-of-elapsed-time

Tamper-proof

- Encryption
- Tampering: watermarking
- Hash
- Multimedia content description interface (MPEG-7)
- Version control

General data protection regulation (GDPR)

- No personal identifiable information (PII)
- Governance especially for public blockchain
- Accountability
- Right to be forgotten
- Illegal content
- Content cannot be erased!!!



Public or private?

- Governance
- Elite or trusted third-party
- Consensus mechanism
- Registered users or wallets
- Fraud, crime

Cryptocurrency or not cryptocurrency, that is the question

- Cryptocurrency
- Token
- “**Dam Coin**”: convertible cryptocurrency: 1 D = 100 CAD
- **Speculation**
- **Nothing is free!!!**
- **Remember the 2007-2008 financial crisis**
- Initial coin offering (ICO)



Legal aspects

- The blockchain may be transnational but the law is not
- Legal implications
- Blockchain not recognized as a legal proof in many countries
- Legal intent
- Estonia



But nothing is perfect...

- **March 2014: Mt. Gox Hack**
- Perhaps the single biggest black eye on cryptocurrency security was a 2014 hack of the Mt. Gox exchange that resulted in the theft of **\$473 million in Bitcoin**. The hack eventually led to the bankruptcy of Mt. Gox later that year.
- **June 2016: Decentralized Autonomous Organization Hack**
- A vulnerability in the DAO code resulted in the theft of \$50 million in Ether and is responsible for the hard fork in Ethereum that occurred in 2016. The new branch of the Ethereum blockchain is what is now known as Ethereum, whereas the legacy chain is still around as Ethereum Classic.
Immutable???
- **January 2018: Coincheck Hack**
- Coincheck, a Japanese crypto exchange, came under government scrutiny after it said hackers stole **\$530 million** from its users. This would rank as the biggest hack ever.

Conclusions

- Content protection
- More efficient ecosystem
- Micropayments
- Consumer to consumer
- Automatization
- Thank you!!!