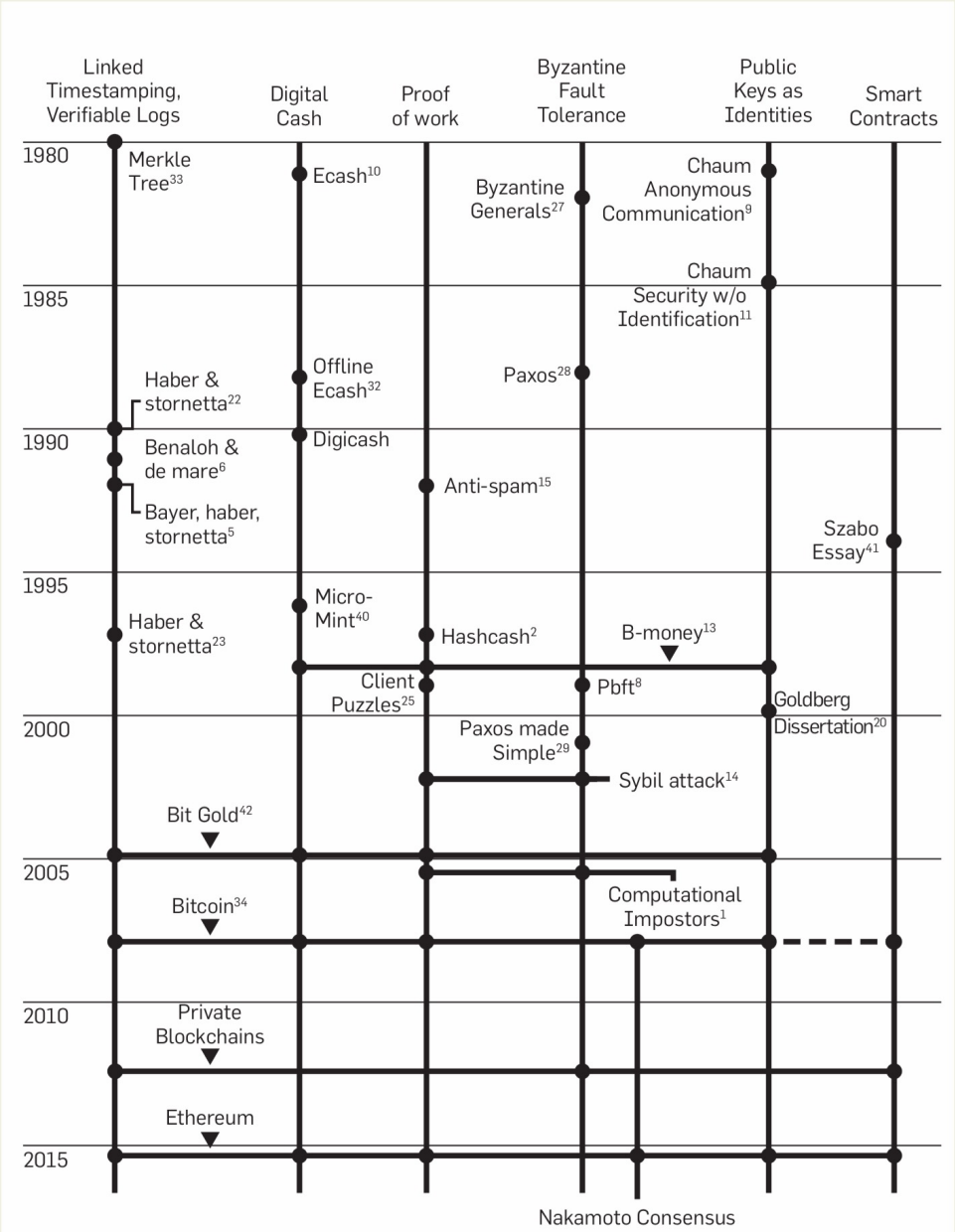
Budućnost blokčejna

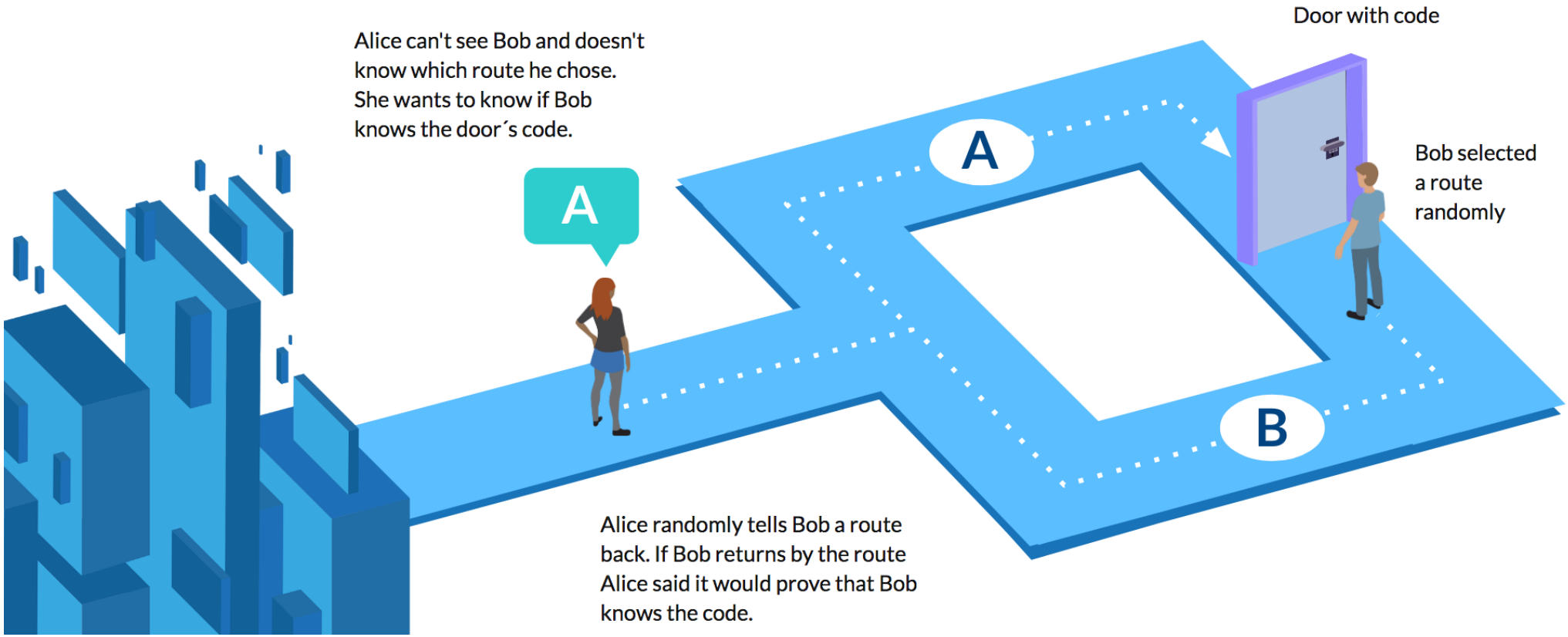
Put do blokčejna

Figure 1. Chronology of key ideas found in bitcoin.



Zero Knowledge Proofs

- **Dokaz sa nultim znanjem** (engl. *zero-knowledge proof* – ZKP) – **Ali Babina pećina**:



Izvor: https://www.bbva.com/en/zero-knowledge-proof-how-to-maintain-privacy-in-a-data-based-world/

Zero Knowledge Proofs

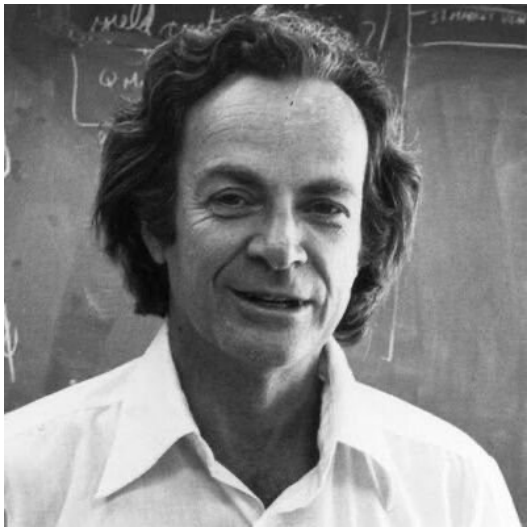
- **Dokaz sa nultim znanjem** (engl. **zero-knowledge proof** – ZKP) je metod kojim jedna strana (**dokazivač** – engl. *prover*) može dokazati drugoj strani (**verifikator** – engl. *verifier*) da zna vrednost *x*, bez pružanja bilo koje dodatne informacije osim činjenice da poznaje vrednost *x*
- Suština ZKP je u tome što je trivijalno dokazati da neko ima određenu informaciju tako što je otkrije. Izazov je dokazati poznavanje informacije bez njenog otkrivanja ili pružanja bilo kakvog dodatnog podatka
- Dokaz sa nultim znanjem mora zadovoljiti sledeća tri svojstva:
  - **kompletnost** (engl. *completeness*): ako je tvrđenje tačno, pošteni verifikator (tj. onaj koji ispravno prati protokol) će biti ubeđen u ovu činjenicu od strane poštenog dokazivača
  - **valjanost** (engl. *soundness*): ako je tvrđenje netačno, nijedan lažljivi dokazivač ne može ubediti poštenog verifikatora da je tačno, osim sa određenom malom verovatnoćom
  - **nulto znanje** (engl. *zero-knowledge*): ako je tvrđenje tačno, nijedan verifikator ne saznaje ništa više od činjenice da je tvrđenje tačno. Drugim rečima, samo poznavanje tvrđenja (ne i tajne) je dovoljno da se zamisli scenario u kome dokazivač zna tajnu

Zero Knowledge Proofs

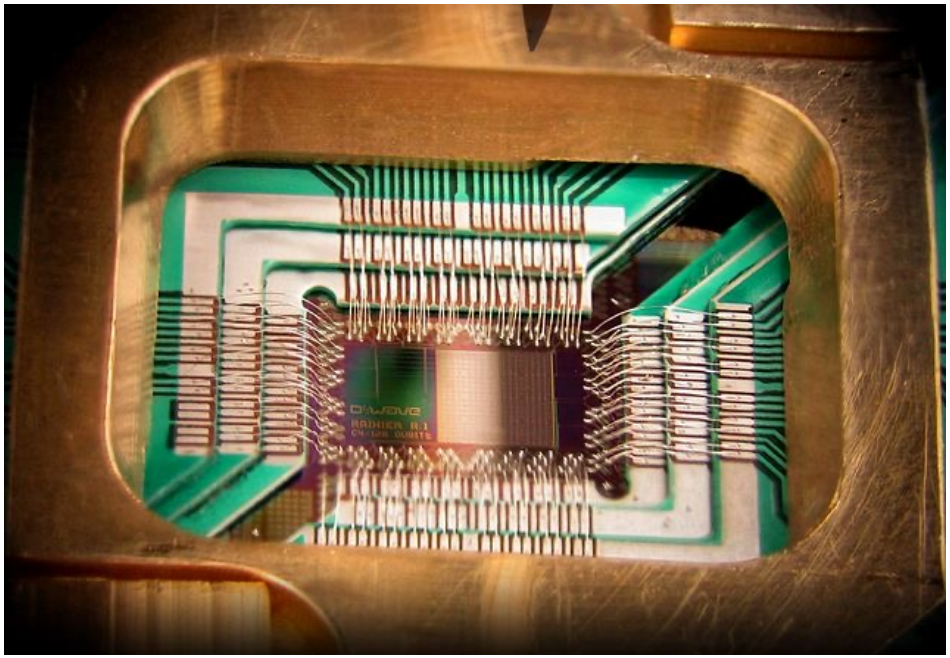
- Goldwasser, S.; Micali, S.; Rackoff, C. (1989), "The knowledge complexity of interactive proof systems", *SIAM Journal on Computing*, Philadelphia: Society for Industrial and Applied Matehmatics, 18 (1):186-208
  - http://people.csail.mit.edu/silvio/Selected%20Scientific%20Papers/Proof%20Systems/The_Knowledge_Complexity_Of_Interactive_Proof_Systems.pdf
- Zcash – MIT, Technion, Johns Hopkins, Tel Aviv University i Berkeley
  - https://z.cash
  - "Zero-knowledge proofs allow transactions to be verified without revealing the sender, receiver or transaction amount."
- Explain Like I'm 5: Zero Knowledge Proof (Halloween Edition)
  - https://hackernoon.com/eli5-zero-knowledge-proof-78a276db9eff
- What is ZKP? A Complete Guide to Zero Knowledge Proof
  - https://101blockchains.com/zero-knowledge-proof/
- On Zero-Knowledge Proofs in Blockchains
  - https://medium.com/@argongroup/on-zero-knowledge-proofs-in-blockchains-14c48cfd1dd1

Kvantni računari

- 1959. Richard Feynman predavanje "*There's Plenty of Room at the Bottom*" – mogućnost kvantnog računarstva
- Danas u aktivan razvoj uključeni Google, IBM, Microsoft, D-Wave…
- 2019. IBM predstavio komercijalni kvantni računar – IBM Q System One



Richard Feynman
(1918-1988)

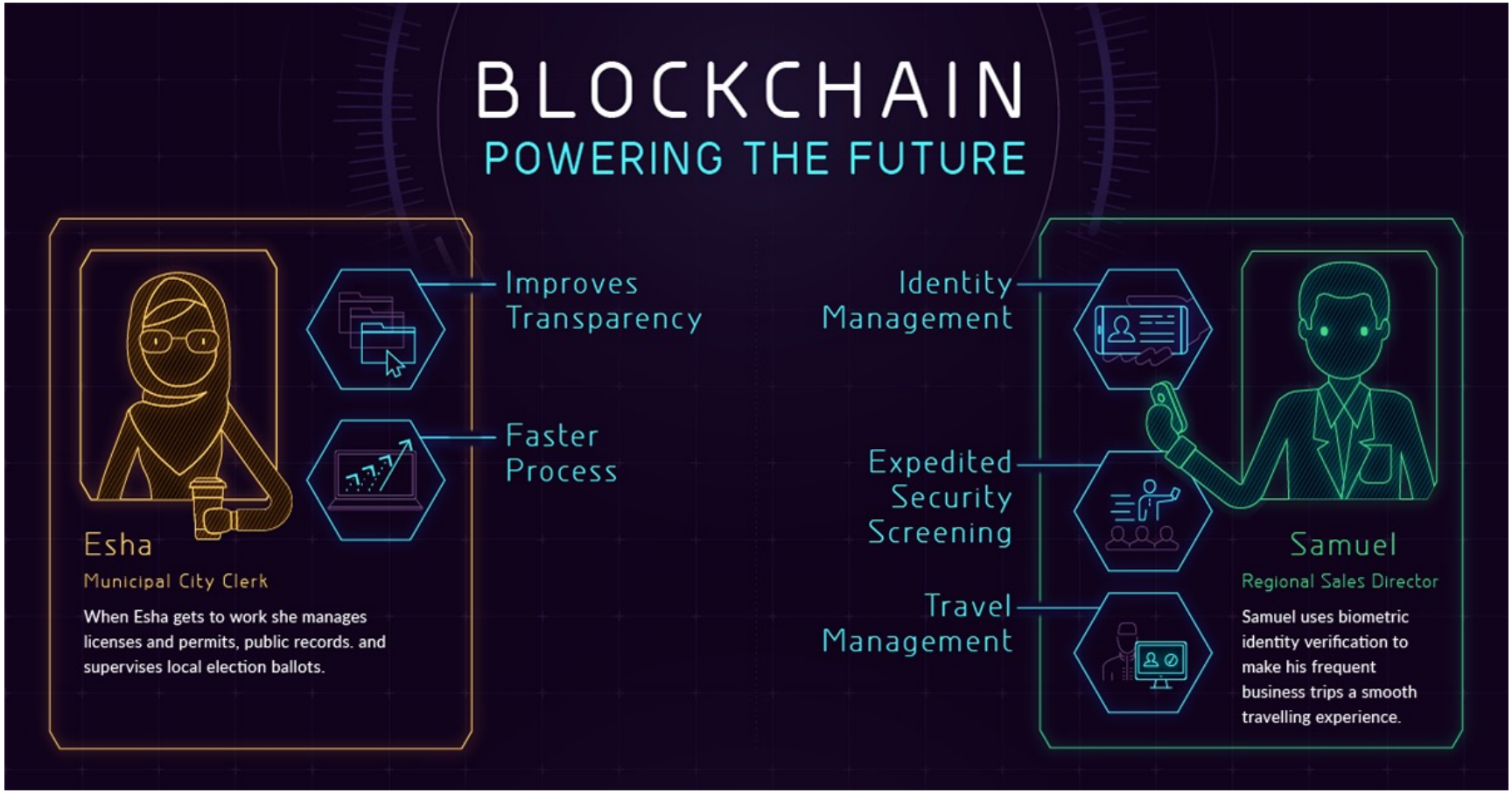


Blokčejn i kvantna apokalipsa

- PhD Comics – Quantum Computers Animated
  - https://www.youtube.com/watch?v=T2DXrs0OpHU
- Is Quantum Computing an Existential Threat to Blockchain Technology?
  - https://singularityhub.com/2017/11/05/is-quantum-computing-an-existential-threat-to-blockchain-technology/#sm.00000d336zn3wlez6vdpwya0ao6ll
- Quantum Resistant Ledger
  - https://github.com/theQRL/Whitepaper/blob/master/QRL_whitepaper.pdf
- Blockchained Post-Quantum Signatures
  - https://eprint.iacr.org/2018/658.pdf

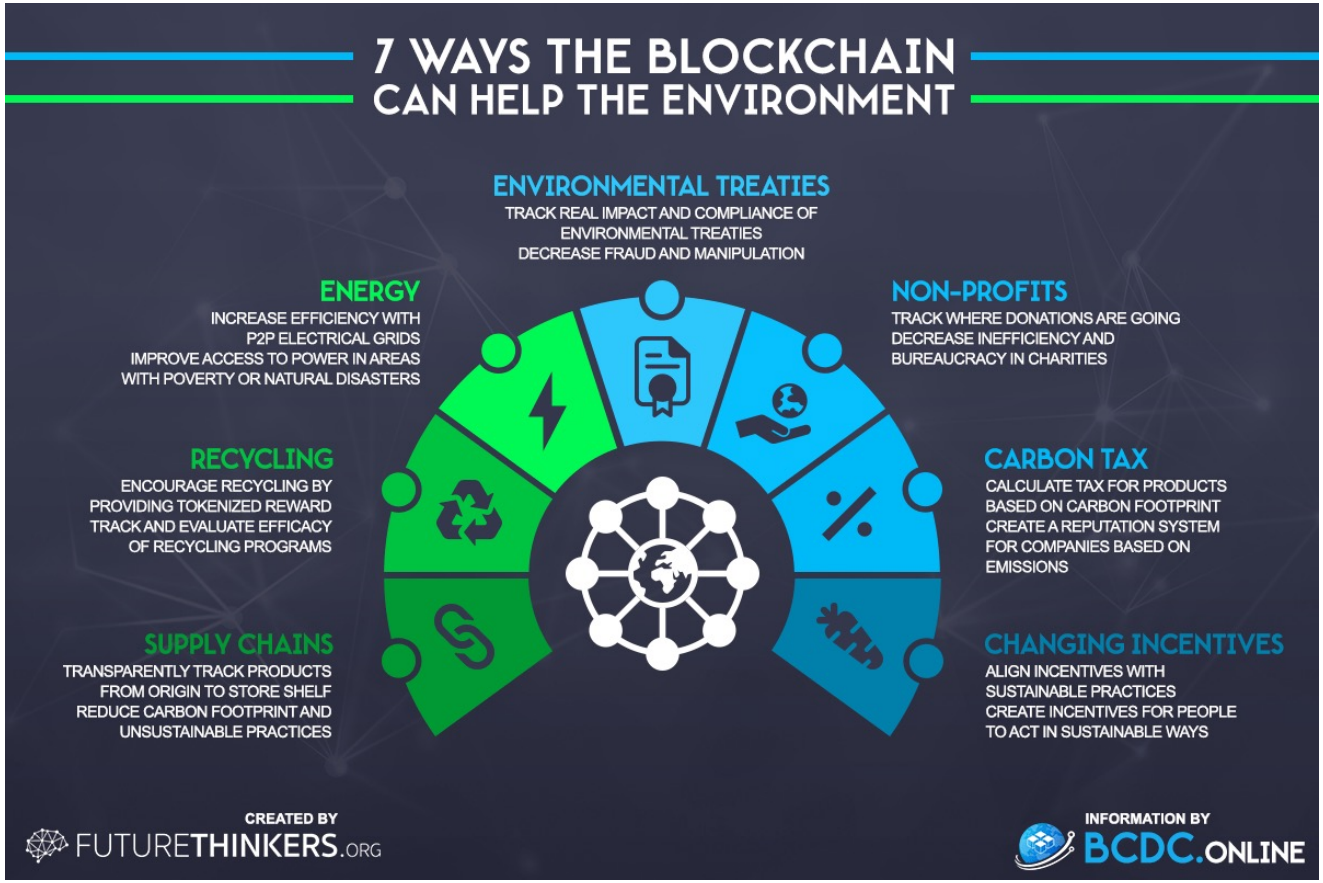
Budućnost blokčejna

- Infographic: How the Blockchain is Powering Our Future:
  - https://www.visualcapitalist.com/blockchain-powering-future/



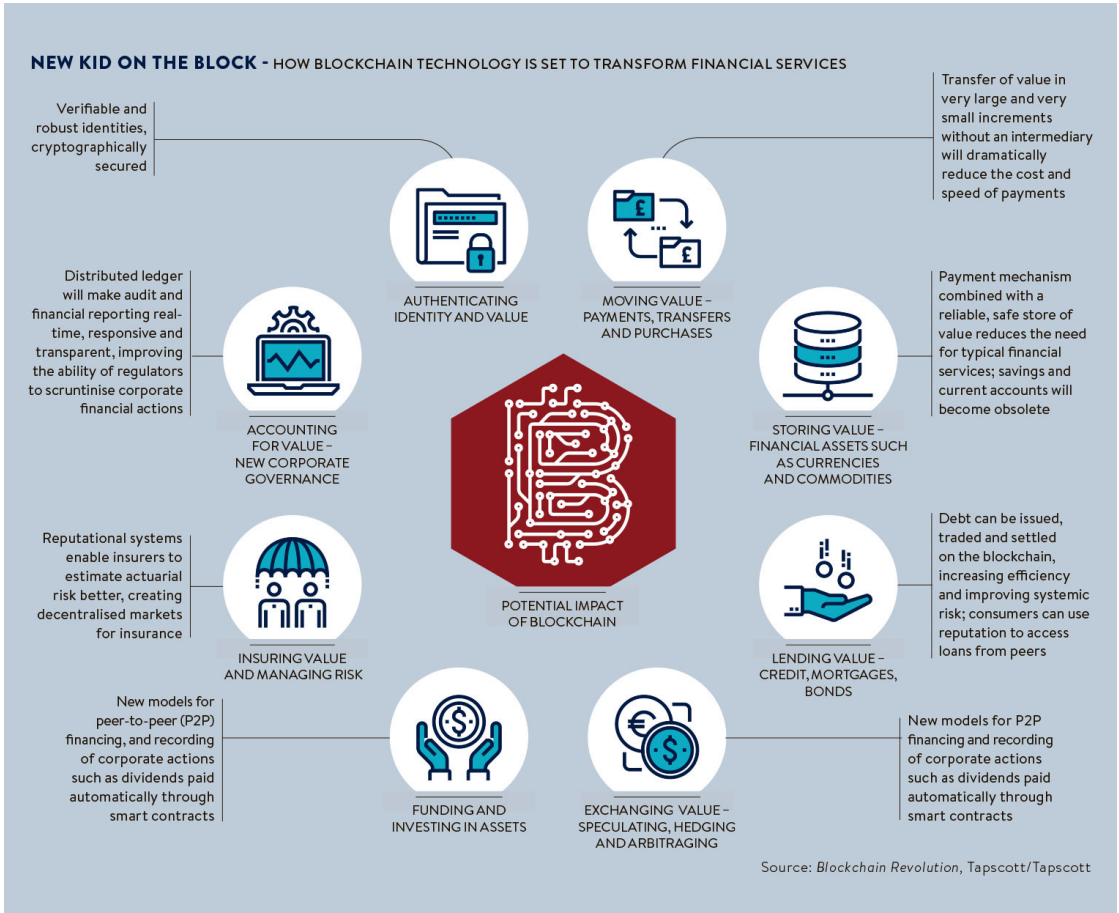
Budućnost blokčejna

- 7 Ways The Blockchain Can Save The Environment and Stop Climate Change
  - https://futurethinkers.org/blockchain-environment-climate-change/



Budućnost blokčejna

- The future of blockchain in 8 charts
  - https://www.raconteur.net/business-innovation/the-future-of-blockchain-in-8-charts



Budućnost blokčejna

- The future of blockchain in 8 charts
  - https://www.raconteur.net/business-innovation/the-future-of-blockchain-in-8-charts