Ostali primeri javnih blokčejn tehnologija

SOLANA

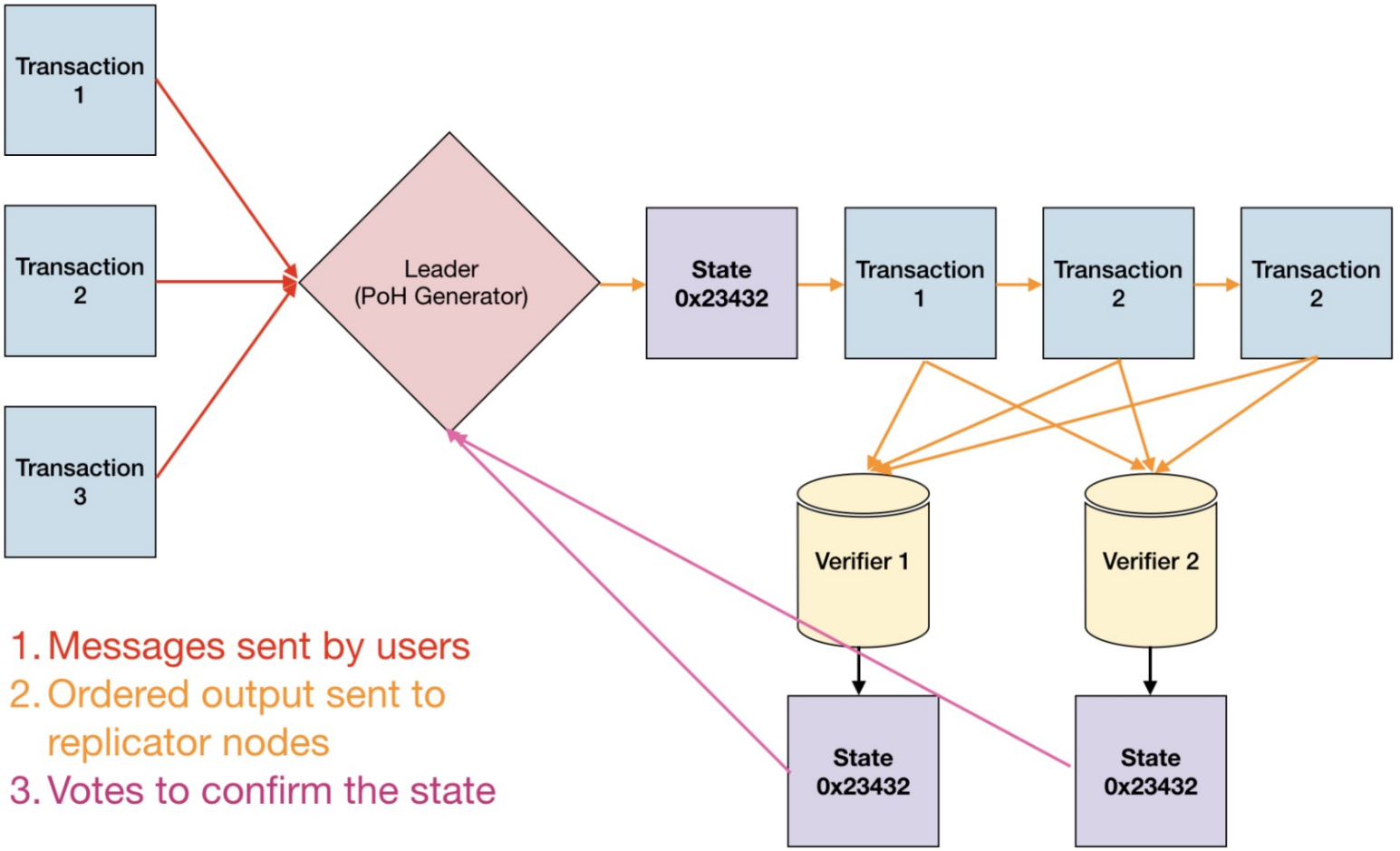
- Sajt: https://solana.com/
- Open source projekat, Solana Foundation registrovana u Švajcarskoj
- **Anatoly Yakovenko**, novembar 2017, Solana Whitepaper (https://solana.com/solana-whitepaper.pdf)
- ”Solana is a decentralized blockchain built to enable scalable, user-friendly apps for the world.”
- Incijalno napisana u **C**-u, pa reimplementirana u **Rust**-u
- **Solana** je **javni blokčejn** sa fokusom na **visokim performansama** (blok na 400 ms), skalabilnosti i niskoj ceni transakcija (<0.01 USD)
- Github: https://github.com/solana-labs/
- Dokumentacija: https://docs.solana.com/introduction

SOLANA

- Nativna kriptovaluta – token SOL, 1 lamport je 10^{-9} SOL
- **Proof of History** konsenzus algoritam – tehnika za beleženje protoka vremena među računarima koji ne veruju jedni drugima
  - **Proof of History** (**PoH**) i ubrzani **Proof of Replication** (**PoR**) – originalno predložen za Filecoin
- Koncept **Solana klastera** (skup validatora sa liderom), spolja vidljiv kao jedinstven sistem
  - lider klastera je izabrani generator Proof of History
  - verifikatori repliciraju stanje blokčejna i omogućavaju njegovu visoku dostupnost
- Teorijski limit za 1 Gbps mrežu: 1 Gbps / 176 B = 710k tps
- Ekosistem sa više stotina aplikacija (NFT, DeFi, Web3, …); https://solana.com/ecosystem

Izvor: https://medium.com/solana-labs/solanas-network-architecture-8e913e1d5a40

SOLANA

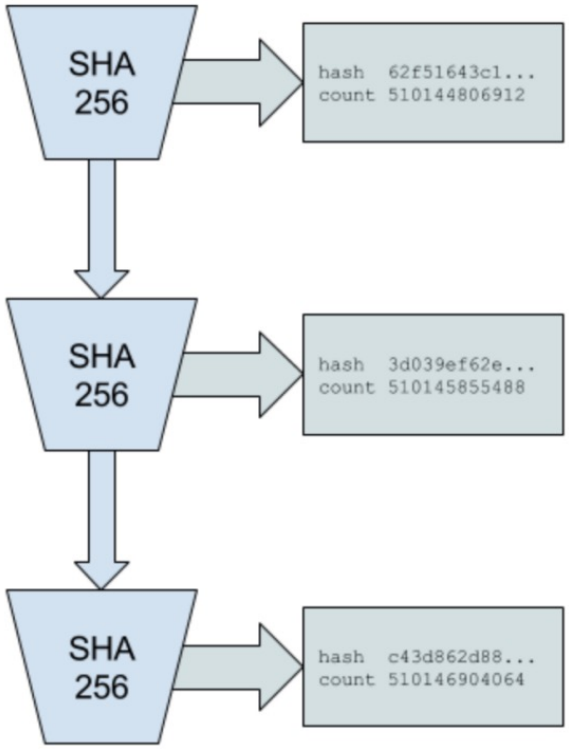


Izvor: https://solana.com/solana-whitepaper.pdf

SOLANA

PoH Sequence

Index	Operation	Output Hash
1	sha256("any random starting value")	`hash1`
200	sha256(`hash199`)	`hash200`
300	sha256(`hash299`)	`hash300`

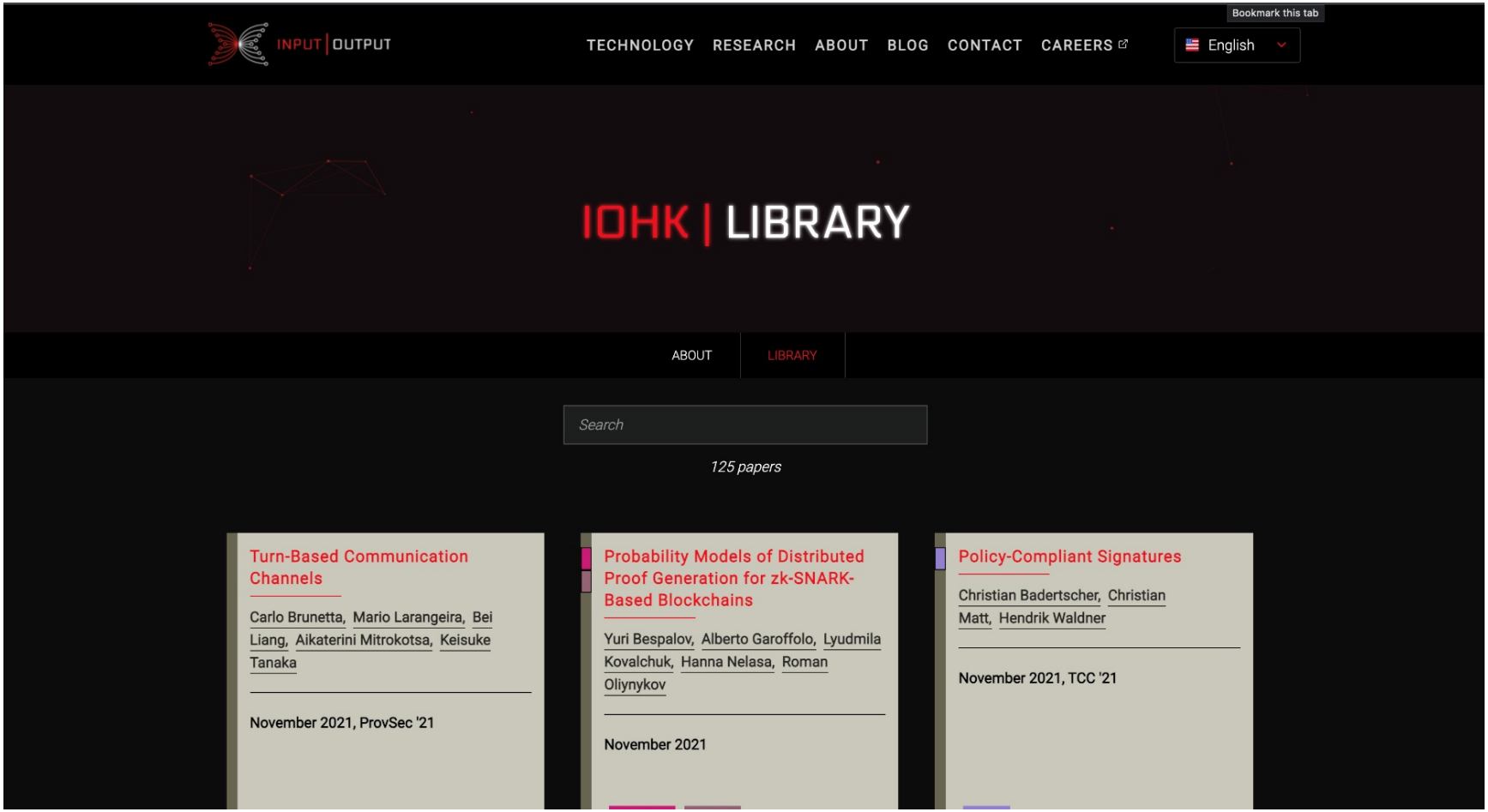


Izvor: https://solana.com/solana-whitepaper.pdf

- Sajt: https://www.cardano.org
- Cardano je open-source decentralizovani javni blokčejn i kriptovaluta, razvija se pod okriljem Cardano Foundation registrovane u Švajcarskoj
- Pokrenut od strane Čarlsa Hoskinsona (jedan od suosnivača Ethereum-a) 2015, finansiran kroz ICO
- Prva blokčejn platforma nastala na osnovu "scientific philosophy and a research-first driven approach", napisan u Haskellu, jezici Plutus i Marlowe
- Kriptovaluta – token Ada (ADA), 1 ADA = 10^6 lovelace
- Vizija Cardana: "Its new style of regulated computing will bring greater financial inclusion by providing open access for all to fair financial services."
- Cardano koristi poseban Proof of Stake konsenzus algoritam – "Ouroboros: A Provably Secure Proof-of-Stake Blockchain Protocol" (https://eprint.iacr.org/2016/889.pdf)

CARDANO

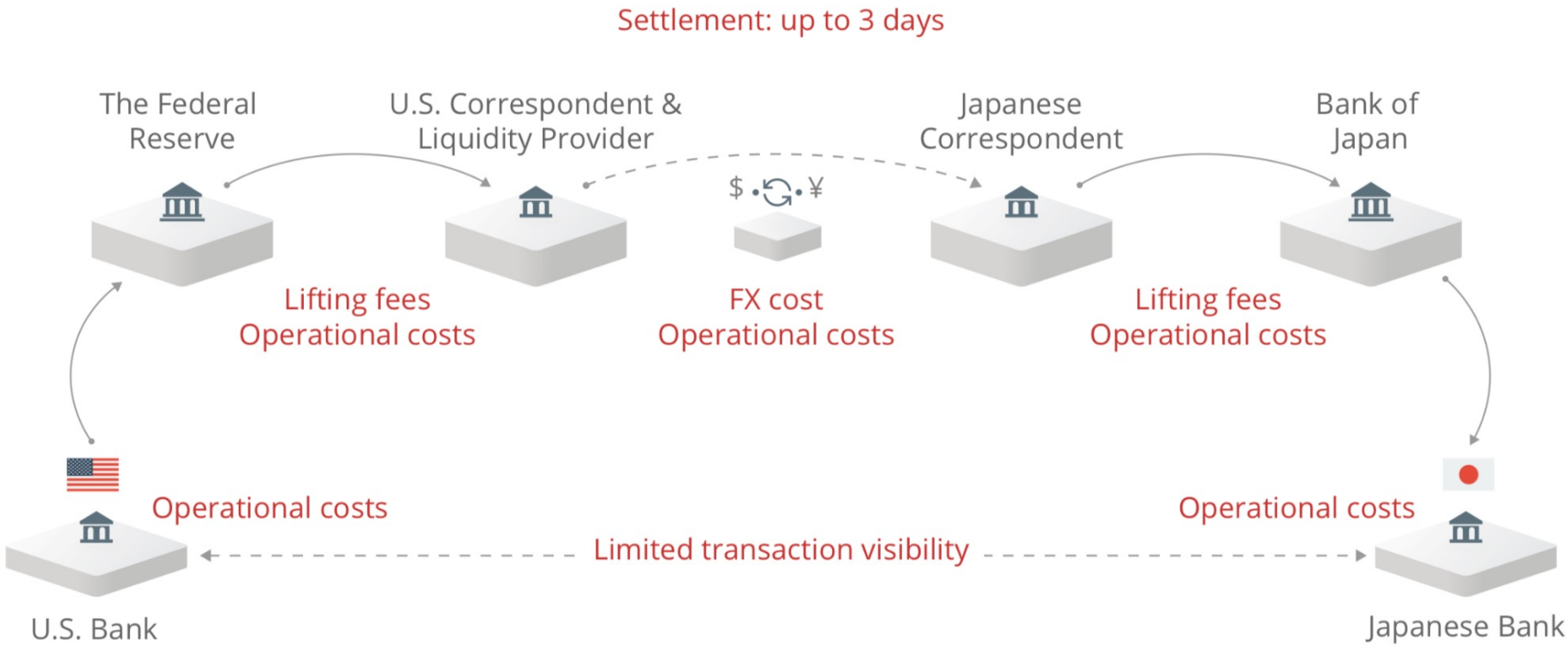
- Biblioteka radova: https://iohk.io/research/library/



- Sajt: https://ripple.com, predstavljen 2012. (od 2004. Ripplepay, pa potom kao OpenCoin) – Arthur Britto, David Schwartz, Ryan Fugger, Jed McCaleb
- **Ripple** je **sistem za poravnavanje** (engl. *settlement*) **transakcija u realnom vremenu** i **razmenu valuta** koji pruža **mrežu za novčane pošiljke** (engl. *remmitance*)
- Kriptovaluta – ripple (XRP)
- Transakcije se kompletiraju za 2 do 3 sekunde
- Cena transakcije je 0.00001 XRP (10 drops)
- **Dva proizvoda u produkciji** koriste XRP:
  - **xRapid** je komercijalni proizvod koji omogućava bankama da koriste XRP kako bi globalno prenosile novac
  - **xCurrent** omogućava bankama da globalno prenose novac tako da mogu da prate kako i gde se prenosi

ripple

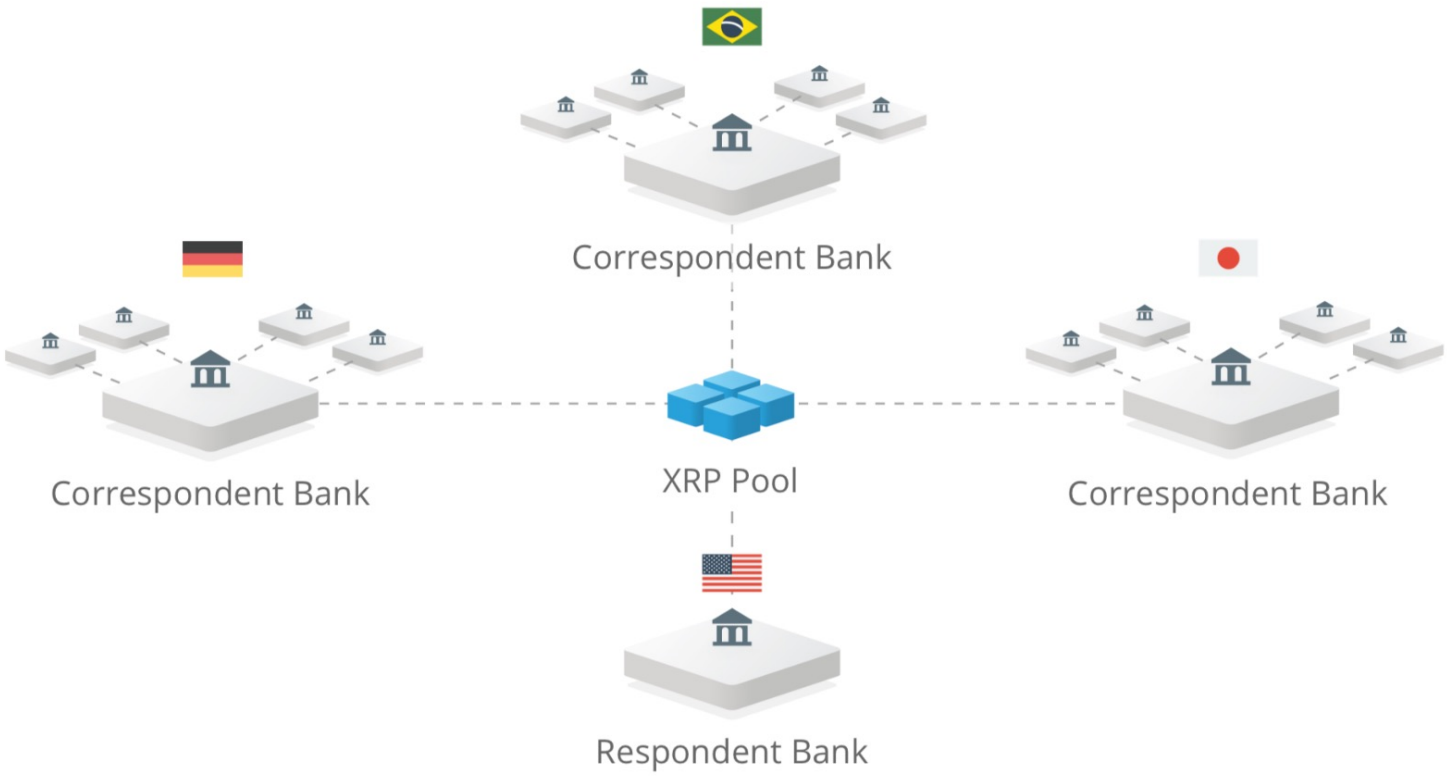
- Tradicionalne međunarodne bankarske transakcije:



Izvor: https://ripple.com/files/xrp_cost_model_paper.pdf

ripple

- Ripple sistem za međunarodne bankarske transakcije:

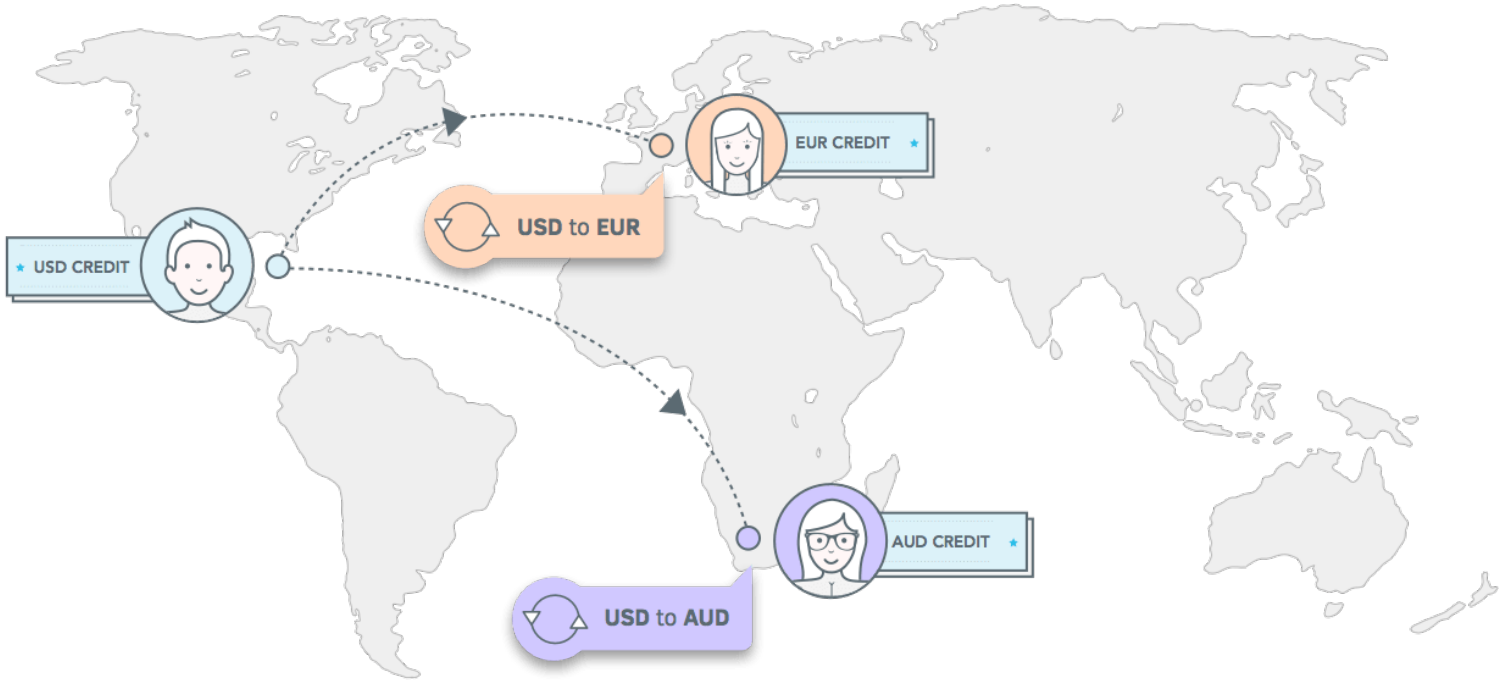


Izvor: https://ripple.com/files/xrp_cost_model_paper.pdf

- Sajt: https://www.stellar.org
- Stellar je **open-source, decentralizovani protokol za transfer digitalnih u fiat valute** koji omogućava međunarodna plaćanja između bilo koje dve valute
- Pokrenut 2014. – Jed McCaleb, suosnivač i CTO, prethodno eDonkey, Mt.Gox BTC berza, Ripple (2011), David Mazieres (Stanford) – Chief Scientist
- Kriptovaluta – lumen (XLM)
- FBA konsenzus algoritam (https://www.stellar.org/papers/stellar-consensus-protocol.pdf)
- Slučajevi korišćenja vrlo slični kao kod Ripple:
  - **novčane pošiljke** (engl. *remittances*) – brzo i jeftino međunarodno slanje novca u različitim valutama
  - **mikroplaćanja** (engl. *micropayments*) – povećanje efikasnosti i smanjivanje cene malih transfera
  - **servisi za osobe ranije bez bankovnih računa** (engl. *services for the unbanked*) – snižavanje cene usluga kako bi se došlo do novih klijenata – računi sa niskom cenom održavanja, pozajmice i mikroštednja

STELLAR

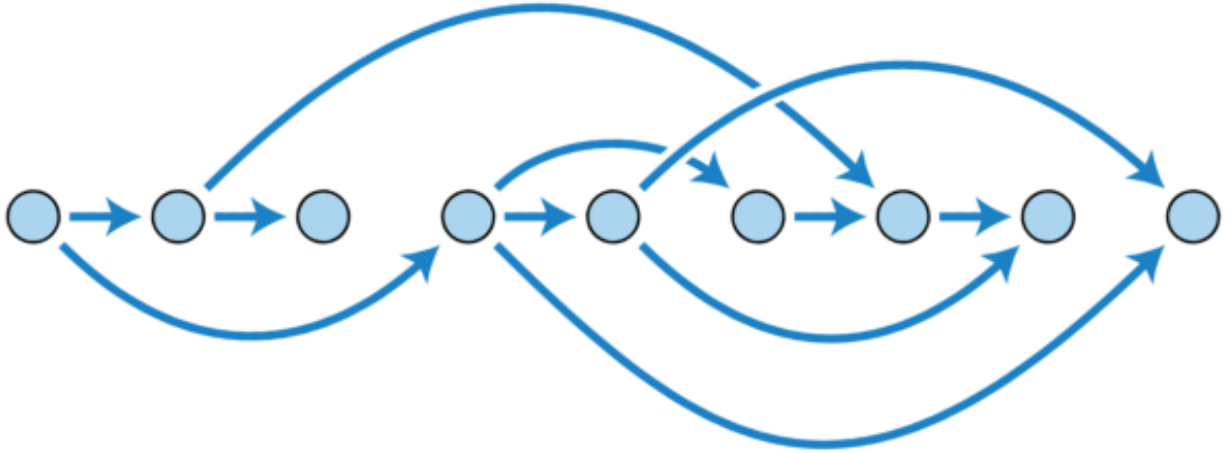
- Brze međunarodne transakcije sa različitim valutama sa vrlo malim provizijama:



Izvor: https://www.stellar.org

Constellation

- Sajt: https://constellationnetwork.io/
- Constellation je sistem baziran na Hypergraph HGTP sa acikličnim usmerenim grafom (engl. *directed acyclic graph – DAG*), napisan u Skali
- Arhitektura DAG, svaki poteg je transakcija:



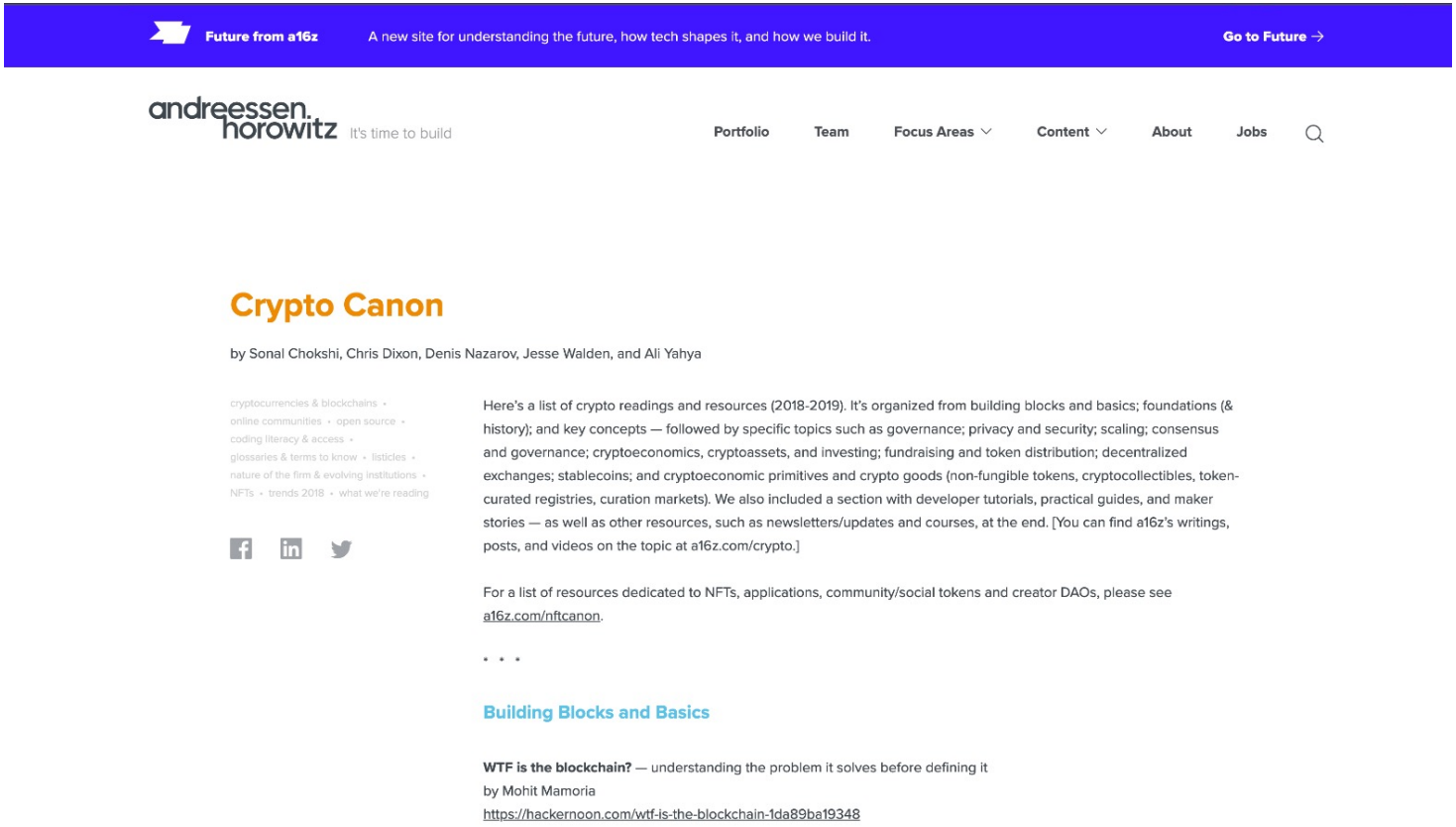
Izvor: https://www.reddit.com/r/CryptoCurrency/comments/pbw024/blockchain_vs_dag_an_overview/

Constellation

- Ekosistem mikroservisa (koncept kanala stanja – engl. *state chanell*) za rad sa velikim skupovima podataka
- Nativna kriptovaluta – token DAG
- Konsenzus algoritam PRO (engl. *Proof of Reputable Observation*)
- ”A Technology Ecosystem that
  Bridges Real-World Businesses with Crypto Economies”
- DeFi platforma Lattice Exchange sa tokenom LTX:
  https://constellationnetwork.io/solutions/lattice/
- White Paper: https://constellationnetwork.io/discover/whitepapers/

Online resursi

- Andreessen Horowitz (a16z) – Crypto Cannon: https://a16z.com/2018/02/10/crypto-readings-resources/



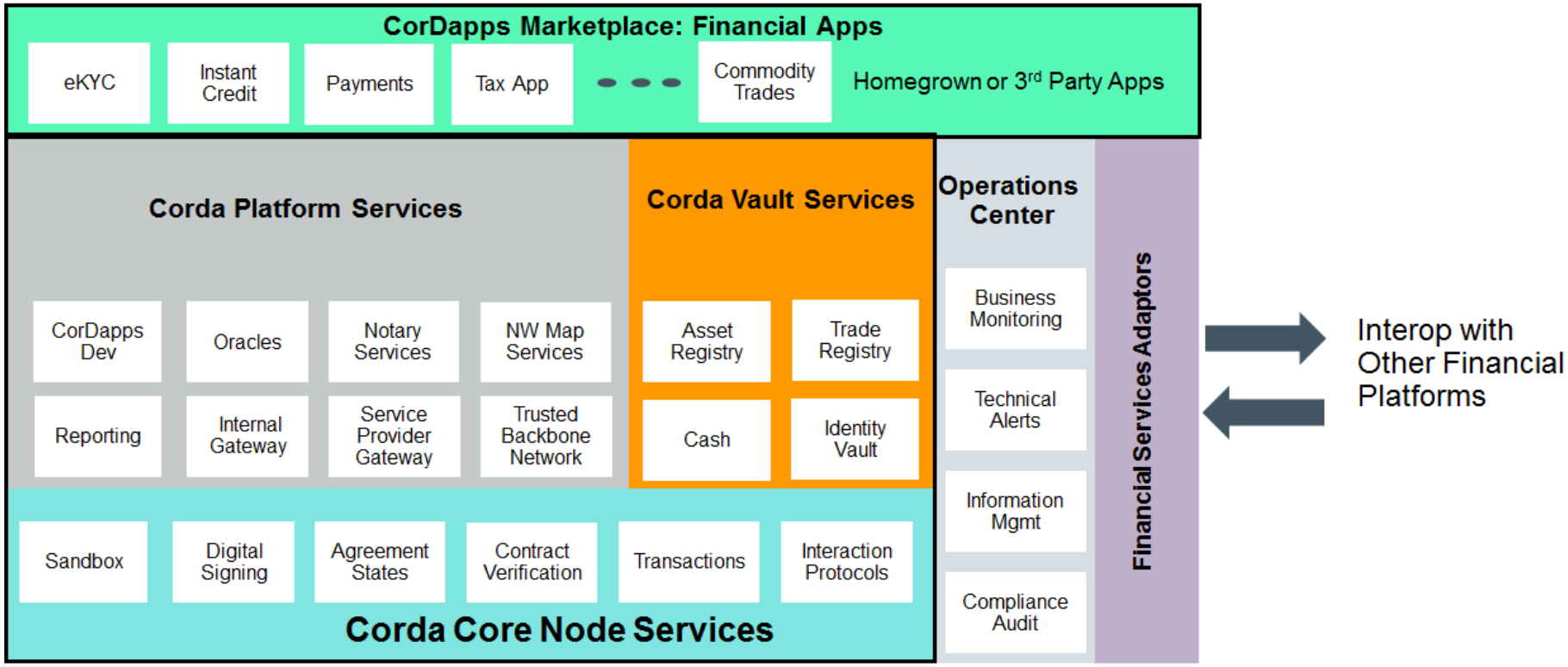
Primeri privatnih DLT

r3·c·rda

- **R3** nastao kao konzorcijum devet banaka (Bank of America, HSBC, UBS, Credit Suisse, ING, …)
- Primene u **poslovnom domenu** (bankarstvo, osiguranje, tržišta kapitala, međunarodna trgovina),
- **Privatna mreža sa kontrolom pristupa**
- Koristi **JVM**, pametni ugovori u **Javi** ili **Kotlinu**
- **DLT** koji **nije blokčejn**, transakcije se ne organizuju u blokove, već se obrađuju na pojedinačnom nivou u realnom vremenu
- Onlajn resursi: https://github.com/chainstack/awesome-corda
- Osobine:
  - **privatnost**
  - **performanse**
  - **skalabilnost**
  - **open source**

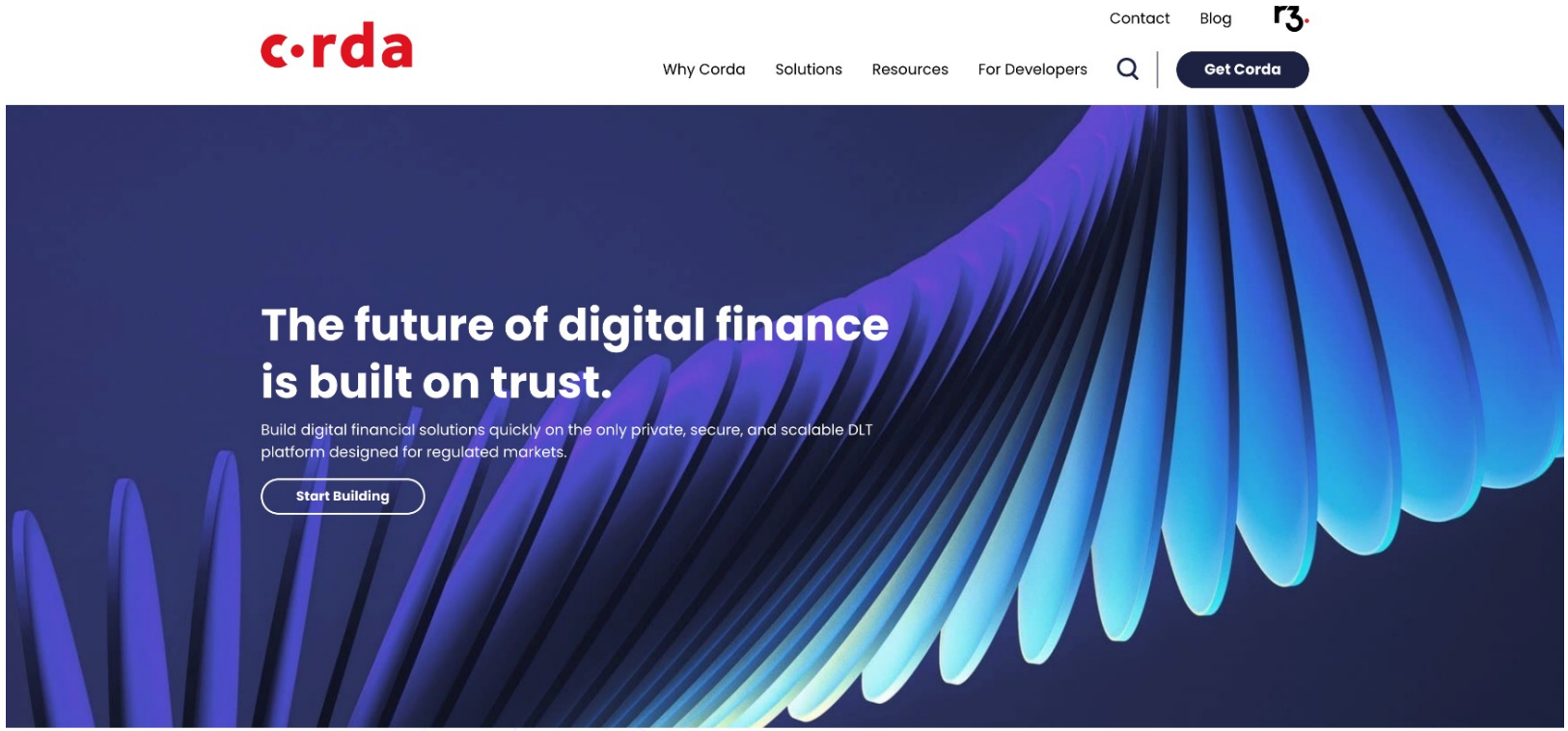
r3·c·rda

Corda Application Architecture



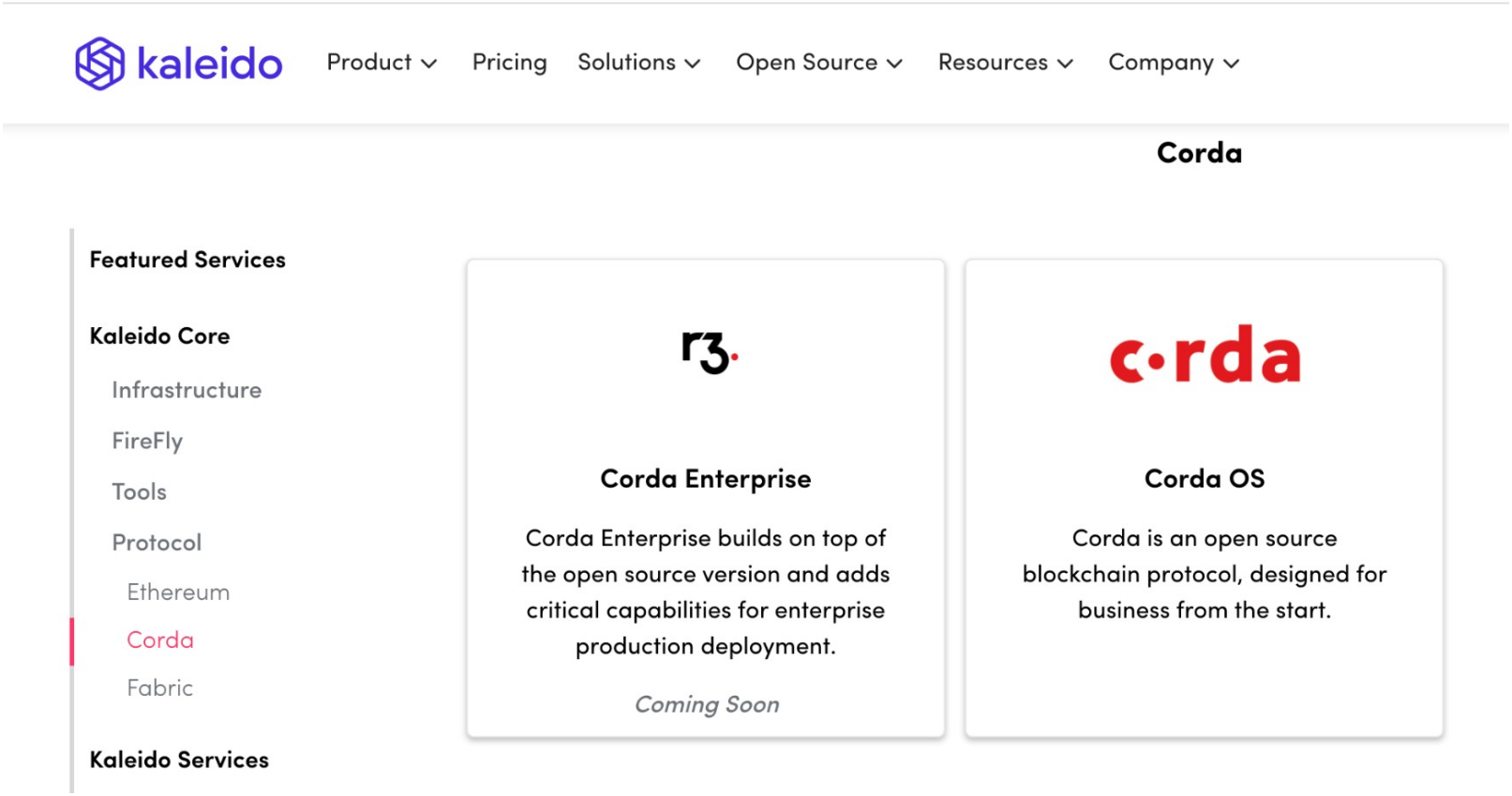
Izvor: http://arunkottolli.blogspot.com/2017/10/r3-corda-application-architecture.html

- **Corda** i **Corda Enterprise**
- R3 Corda platforma (https://www.r3.com/corda-platform/)
- R3 Conclave (https://www.conclave.net/) – confidential computing



Izvor: https://www.r3.com/corda-platform/

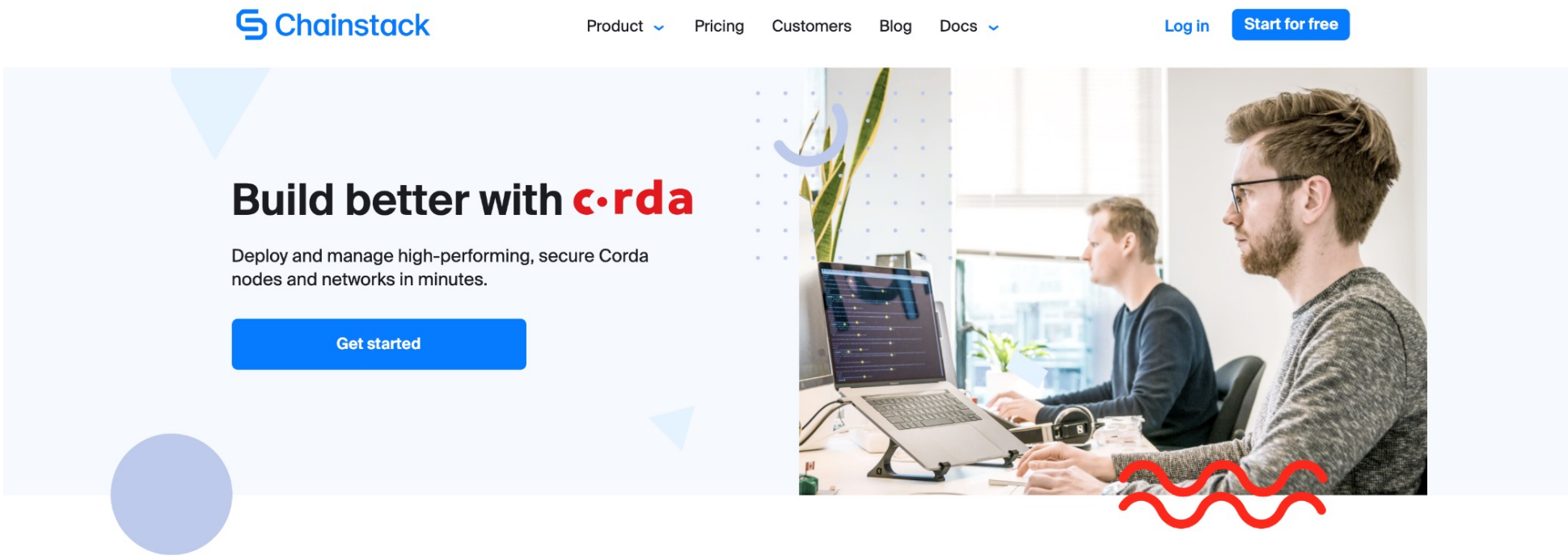
- **Kaleido Corda** (https://www.kaleido.io/product/features#protocol-corda)



Izvor: https://www.kaleido.io/product/features#protocol-corda

r3·c·rda

- **Chainstack Corda** (https://chainstack.com/protocols/corda/)



Izvor: https://chainstack.com/protocols/corda/

HYPERLEDGER

- **Hyperledger** je **open-source kolaborativna inicijativa** stvorena kako bi se **unapredile blokčejn tehnologije** i njihova **primena u različitim sektorima poslovanja** (engl. ***enterprise***)
- Nosilac je inicijalno bila Linux fondacija, a potom Hyperledger fondacija

  https://www.hyperledger.org/

THE LINUX FOUNDATION

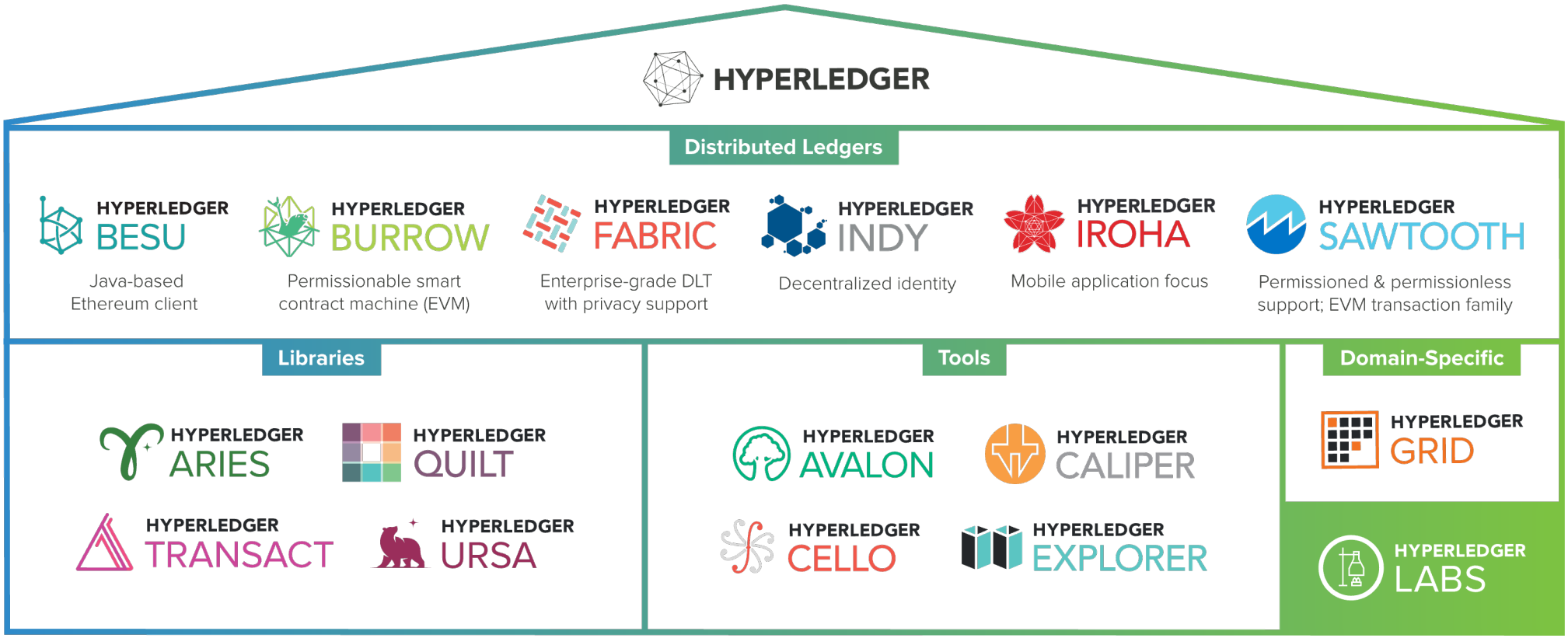
- Pokrenuta krajem 2015. na inicijativu većeg broja kompanija (IBM, Intel, SAP, …)
- Februara 2016. početak aktivnog razvoja
- Obuhvata veći broj radnih okruženja i alata (ukupno 16 projekata na kraju 2020.)

Hyperledger članovi

Hyperledger projekti

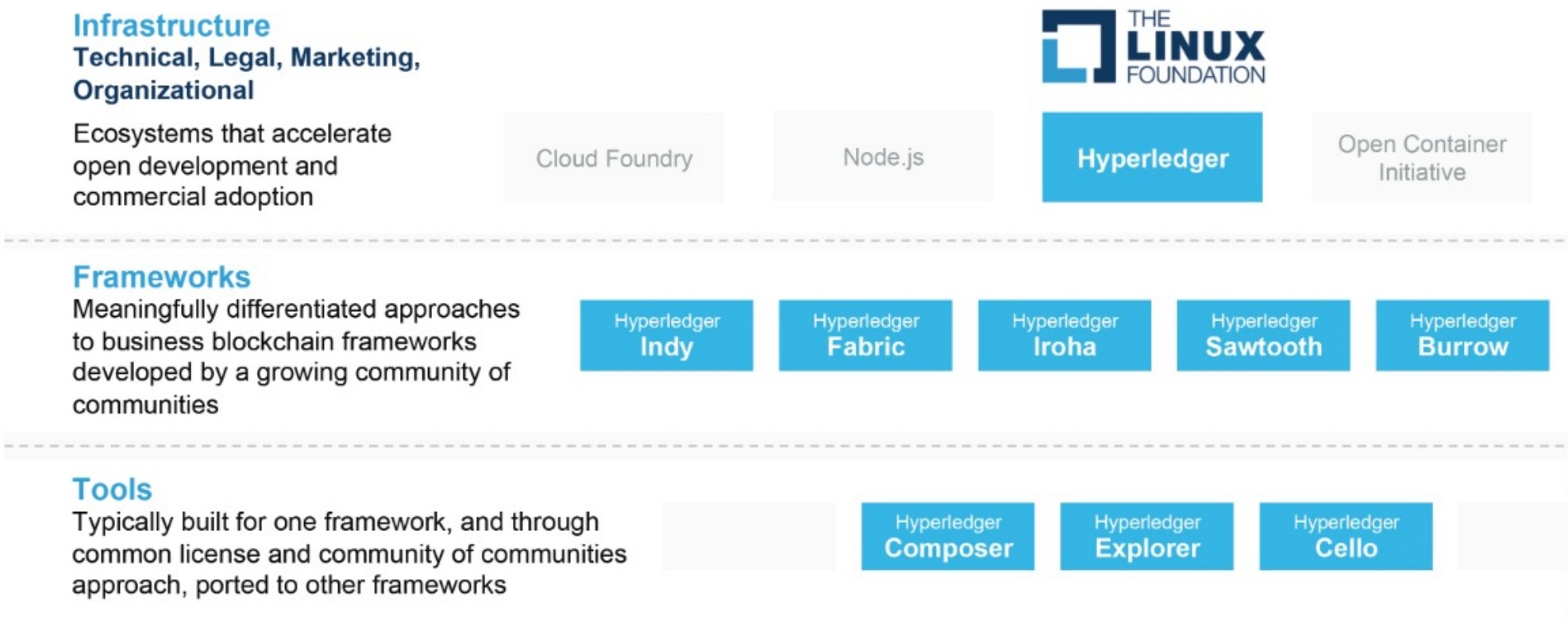
- **Distribuirane knjige** (engl. *distributed ledgers*):
  - Fabric
  - Sawtooth
  - Iroha
  - Indy
  - Burrow
  - Besu
- **Alati** (engl. *tools*):
  - Avalon
  - Cello
  - Explorer
  - Caliper
- **Namenski** (engl. *domain-specific*):
  - Grid
- **Biblioteke** (engl. *libraries*):
  - Quilt
  - Ursa
  - Aries
  - Transact

Hyperledger projekti



Izvor: https://www.hyperledger.org

Hyperledger projekti



Izvor: https://www.hyperledger.org/wp-content/uploads/2017/08/HyperLedger_Arch_WG_Paper_1_Consensus.pdf

Hyperledger slučajevi korišćenja

Cross-Border Payments

Transferring money across international borders is still complicated, time consuming and expensive. Payments routed abroad can take several days to get settled. Existing money transfer systems suffer furthermore from long lines, exchange rate losses, counter-party risks, bureaucracy and extensive paperwork. Cross-border payments have become a critical part of millions of lives as we moved towards a more globalized world and multicultural societies.

After months of work, a global team of developers have completed a cross-border POC built with Hyperledger Fabric. Designed to test whether moving member bank accounts to a distributed ledger could help the inter-bank payments platform Swift reconcile in real time, the blockchain trial is now ready for its next phase of testing with General members ANZ, BNP Paribas, BNY Mellon and Wells Fargo.

Hyperledger Fabric enables real-time visibility on the liquidity of Nostro accounts, easing reconciliation and allowing liquidity savings while meeting key industry requirements such as governance, data privacy, standardisation, and identity.

HYPERLEDGER
BLOCKCHAIN TECHNOLOGIES FOR BUSINESS

SWIFT ANZ WELLS FARGO

BNY MELLON BNP PARIBAS

Read about the POC in Coindesk.

Hear about the collaboration in the ANZ Community Spotlight video.

Izvor: https://www.hyperledger.org/wp-content/uploads/2018/03/The-Hyperledger-Vision-11-1.pdf

Hyperledger slučajevi korišćenja

Seafood Supply Chain Traceability

Blockchain technologies are being used in the fishing industry to drive fish catch towards more ethical practices, obstructing pirate fisherman and fish that are caught outside of legal fishing areas from being sold.

Hyperledger Premier member Intel is collaborating with the Hyperledger community to implement a modern approach to seafood traceability. Leveraging the Hyperledger Sawtooth framework, the seafood journey can now be recorded from ocean to table.

IoT sensors can be attached to any object (like fish) that is entrusted to someone else for transport, with trackable ownership, possession, and telemetry parameters such as location, temperature, humidity, motion, shock and title. The final buyer can access a complete record of information and trust that the information is accurate and complete. Revolutionizing the seafood supply chain is just one example of the many ways Hyperledger Sawtooth can have real world benefits.

HYPERLEDGER
BLOCKCHAIN TECHNOLOGIES FOR BUSINESS

intel

Intel has revealed a public demo that finds it showcasing how a seafood supply chain can be built using Hyperledger Sawtooth.

Watch the explainer video and read the full case study on the Hyperledger Sawtooth project page.

Read about the demo.

Izvor: https://www.hyperledger.org/wp-content/uploads/2018/03/The-Hyperledger-Vision-11-1.pdf

- **Hyperledger Fabric** je **platforma za rešenja sa distribuiranom glavnom knjigom i mrežom sa kontrolisanim pristupom** (engl. *permissioned network*), koja se zasniva na **modularnoj arhitekturi** i omogućava **visok stepen poverljivosti**, **otpornosti**, **fleksibilnosti** i **skalabilnosti**
- IBM donirao značajan deo koda
- Github: https://github.com/hyperledger/fabric
- Osobine:
  - **Modularnost**
  - **Poverljivost**
  - **Otpornost** (resiliency)
  - **Fleksibilnost**
  - **Skalabilnost** i **visoke performanse**

Izvor: https://developer.ibm.com/tv/the-creation-of-hyperledger-fabric-v1-for-stable-blockchain-networks/

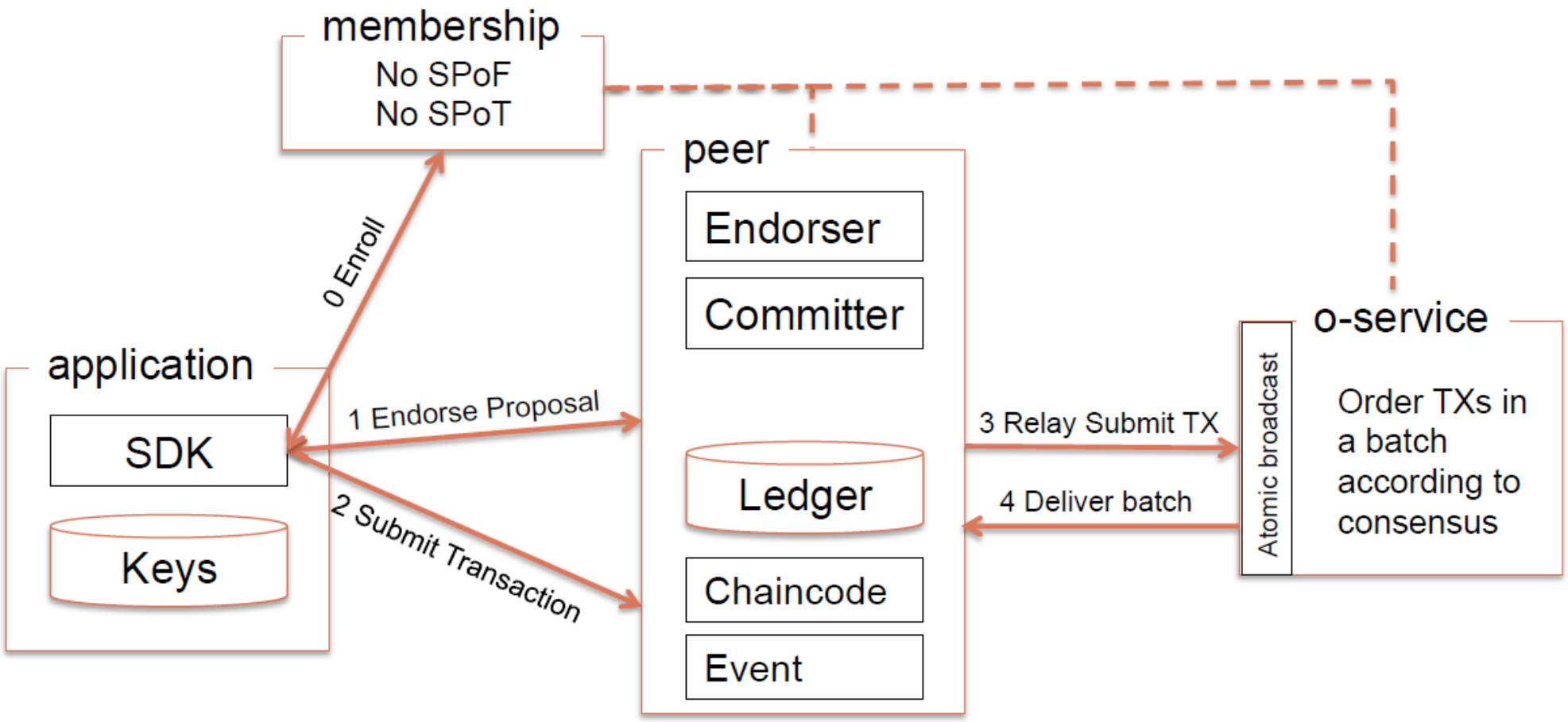
Bitcoin vs Etherum vs Hyperledger Fabric

	Bitcoin	**Ethereum**	**Hyperledger Fabric**
Kriptovaluta	bitcoin	etar	/
Mreža	javna	javna ili privatna sa kontrolom pristupa	privatna sa kontrolom pristupa
Transakcije	anonimne	anonimne ili privatne	javne ili poverljive
Konsenzus	Proof of Work	Proof of Stake	RAFT, PBFT u najavi
Pametni ugovori	/	da (Solidity, LLL, …)	da (chaincode – Go, JavaScript, Java)
Jezici	C++	C++, Python, Go	Go, JavaScript, Java

Fabric – osnovni koncepti

- Dve mreže: **uređivačka** (engl. *ordering*) i **peer**
- Tipovi čvorova (engl. *nodes*): **klijent, peer** i **uređivač** (engl. *orderer*)
- Peer: može igrati dve uloge – **endorser, commiter**
- Transakcije: **deploy**, **invoke** i **query**
- **Pružalac servisa članstva** (engl. *Membership Services Provider* – MSP) – Fabric CA
- **Servis za uređivanje** (engl. *Ordering Service*) – orderer: ranije SOLO i Apache Kafka, RAFT, PBFT u najavi
- Koncept **kanala** (engl. *chanells*) – **podmreže** sa posebnom glavnom knjigom, omogućavaju **poverljive transakcije**

Fabric arhitektura



Izvor: https://jira.hyperledger.org/secure/attachment/10056/FabricNext-Community.pdf

Fabric pružalac usluga članstva

- **Pružalac usluga članstva** (engl. *Membership Services Provider* – MSP) realizuje komponenta **Fabric CA** (Certificate Authority)
- Može se koristiti i OpenSSL za sertfikate – važno je da se generišu ECDSA sertifikati
- Kod Fabrica v0.6 je MSP bio jedinstvena tačka otkaza (engl. *Single Point of Failure* – SPoF)!
- Od Fabrica v1.0 i nadalje dosupni višestruki MSP
- **Root sertifikat** za svakog člana (member) i **enrollment sertifikat** za svakog autorizovanog korisnika
- Ključevi zasnovi na kriptografiji sa eliptičnim krivama (**ECC**) i Rivest-Shamir-Adelman (**RSA**) kriptosistemu, ECC ključevi jači

Chaincode

- **Programski kod** koji u Hyperledger Fabricu implementira **pametne ugovore**
- **Čitanje iz i upis u glavnu knjigu** moguć je **samo preko chaincode-a**
- Mogu se izvršavati paralelno nad disjunktnim skupovima endorser-a
- Programski jezici opšte namene za pisanje chaincode: **Go**, **Node.js** (**JavaScript**), **Java** (od v1.3)
- Funkcije:
  - Init (incijalizacija chaincode-a, kreiranje dobara, upis stanja)
  - Invoke (get, set, delete), Query
  - main(): `err := shim.Start(new(SimpleChaincode))`

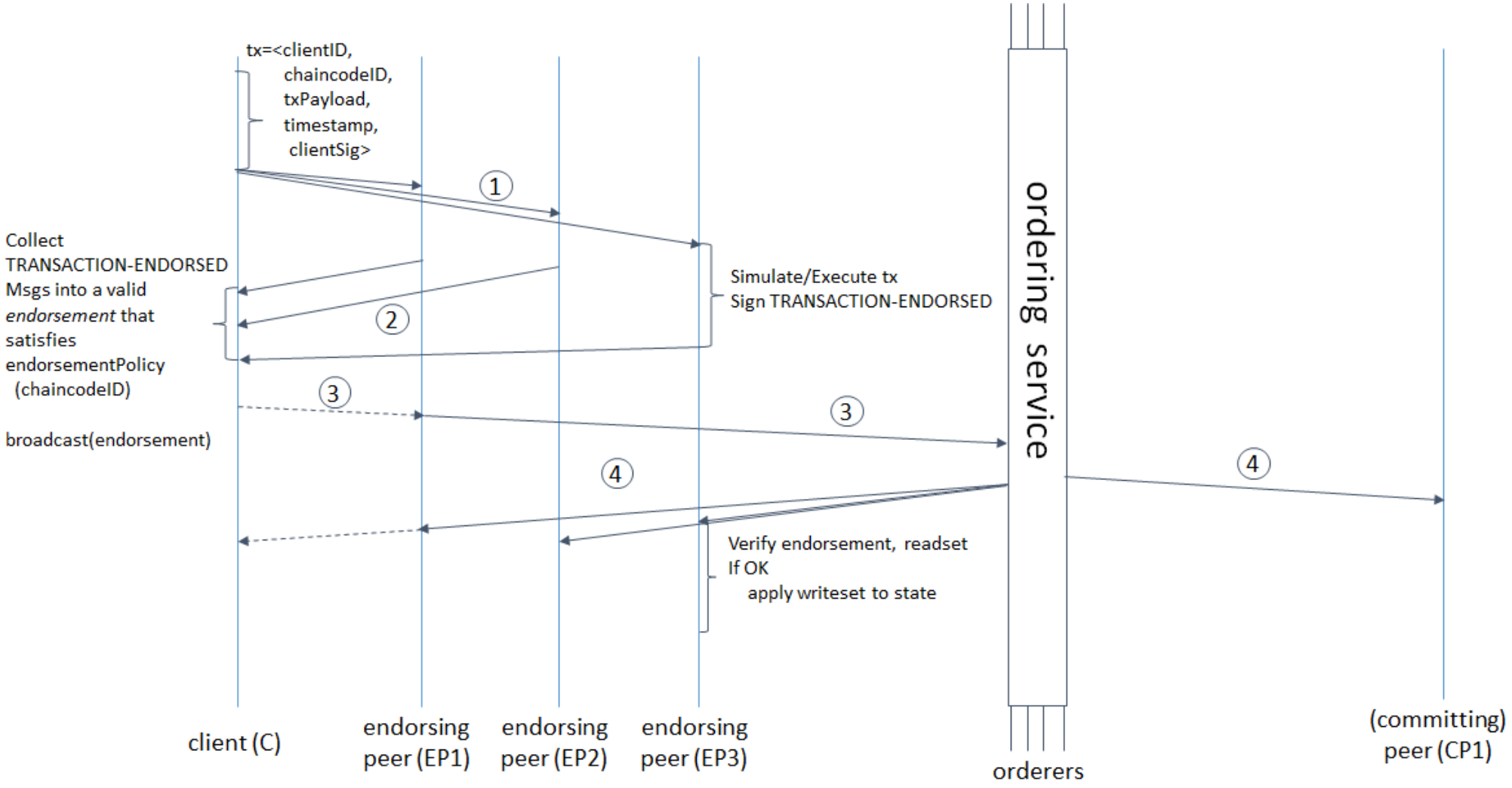
Fabric servis za uređivanje

- Poseban **skup čvorova uređivača** (engl. **orderers – consenters**) koji uređuju transakcije u blokove čini **servis za uređivanje** (engl. **ordering service**)
- Radi **nezavisno od peer mreže** i uređuje transakcije po FCFS (engl. *First-Come-First-Served*) principu za sve kanale na mreži
- Izvršavanje chaincode-a, koje je potencijalno skupo, je uklonjeno sa kritične putanje servisa za uređivanje – **veći propusni opseg** i **bolja skalabilnost** (https://arxiv.org/abs/1801.10228)
- Lako zamenjiva implementacija: **RAFT**, u planu PBFT implementacija
- **Zajednička tačka za celu mrežu** – čuva i **sistemski lanac** koji sadrži blokove sa podacima o konfiguraciji (MSP, pravila, podaci o identitetu članova...)

Fabric konsenzus algoritam

- **Konsenzus algoritam** kod **Hyperledger Fabrica** izvršava se u tri faze:
  1. **saglasnost** (engl. ***endorsement***) – vodi se odgovarajućim pravilima (npr. najmanje *m* od *n* potpisa) po kojima učesnici podržavaju određenu transakciju
  2. **uređivanje** (engl. ***ordering***) – prihvataju se podržane transakcije i postiže se konsenzus o njihovom redosledu u bloku koji će biti upisan u ledger
  3. **validacija** (engl. ***validation***) – uzima se blok uređenih transakcija i potvrđuje se tačnost rezultata, uključujući proveru politike saglasnosti (engl. endorsement policy) i dvostruke potrošnje (engl. double-spending)

Fabric tok transakcije



Izvor: https://www.hyperledger.org/wp-content/uploads/2017/08/HyperLedger_Arch_WG_Paper_1_Consensus.pdf

Fabric glavna knjiga

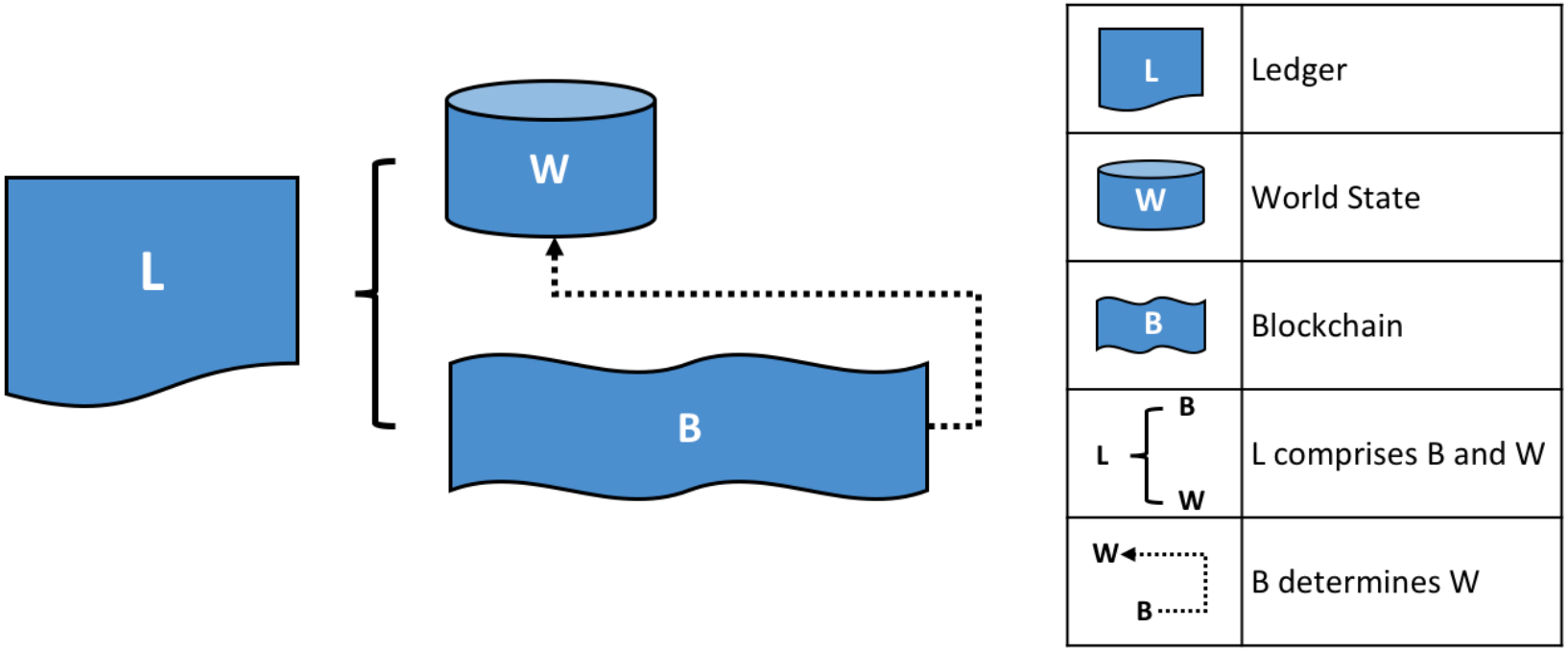
- U glavnoj knjizi se **beleže sve promene stanja** (transakcije) **nastale kao rezultat poziva chaincode-a. Svaka transakcija rezultuje skupom ključ-vrednost parova** (engl. *key-value pairs*) koji se upisuju u glavnu knjigu

glavna knjiga = log transakcija + stanje sveta

- **Log transakcija** (engl. *transaction log*) je lanac, tj. blokčejn
- **Stanje sveta** (engl. *world state*) čuva se u izabranom sistemu za rad sa parovima ključ-vrednost (engl. *key-value store* – KVS) (LevelDB – default, CouchDB, ...)
- Za svaki kanal postoji po jedna glavna knjiga
- Svaki peer čuva kopiju glavne knjige za svaki od kanala čiji je član
- Veličina i frekvencija izdavanja blokova su programabilni

Fabric glavna knjiga

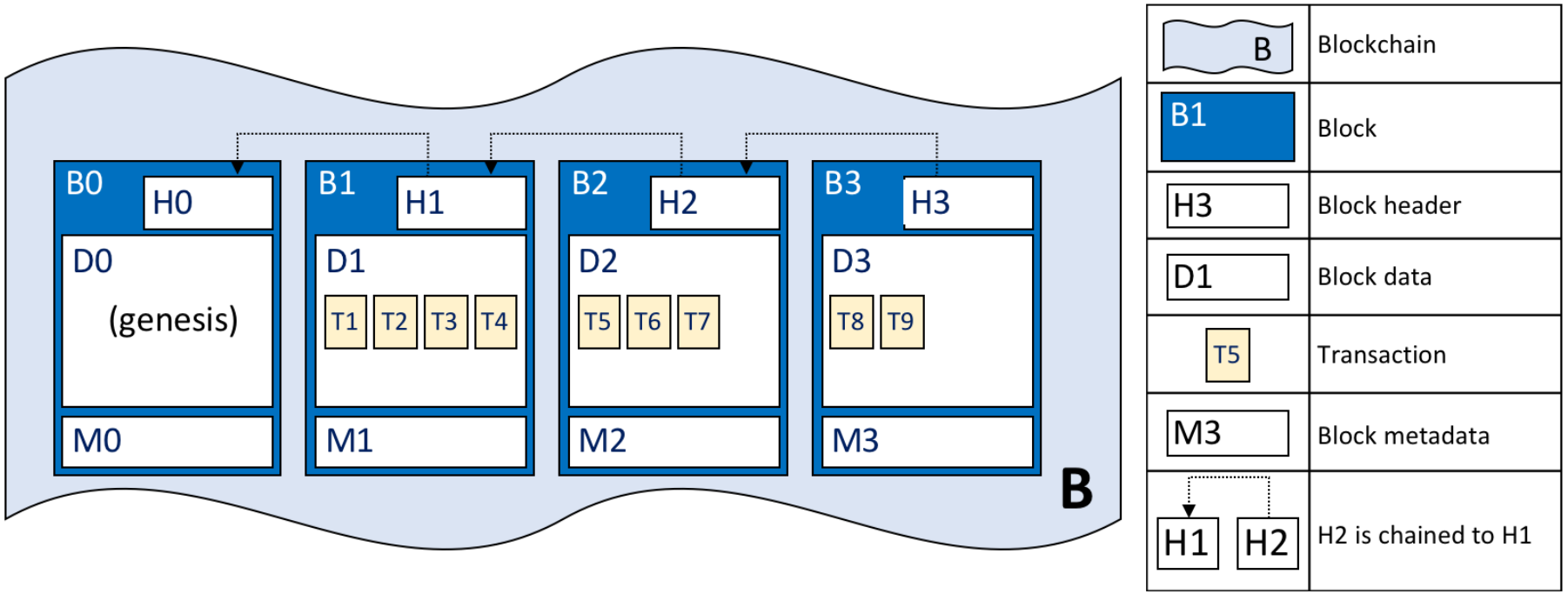
- **Glavna knjiga** (Ledger – L) sastoji se od **blokčejna** (Blockchain – B) i **stanja sveta** (World state – W), pri čemu blokčejn B određuje stanje sveta W, tj. stanje sveta W je izvedeno iz B



Izvor: https://hyperledger-fabric.readthedocs.io/en/latest/ledger/ledger.html

Fabric blokčejn

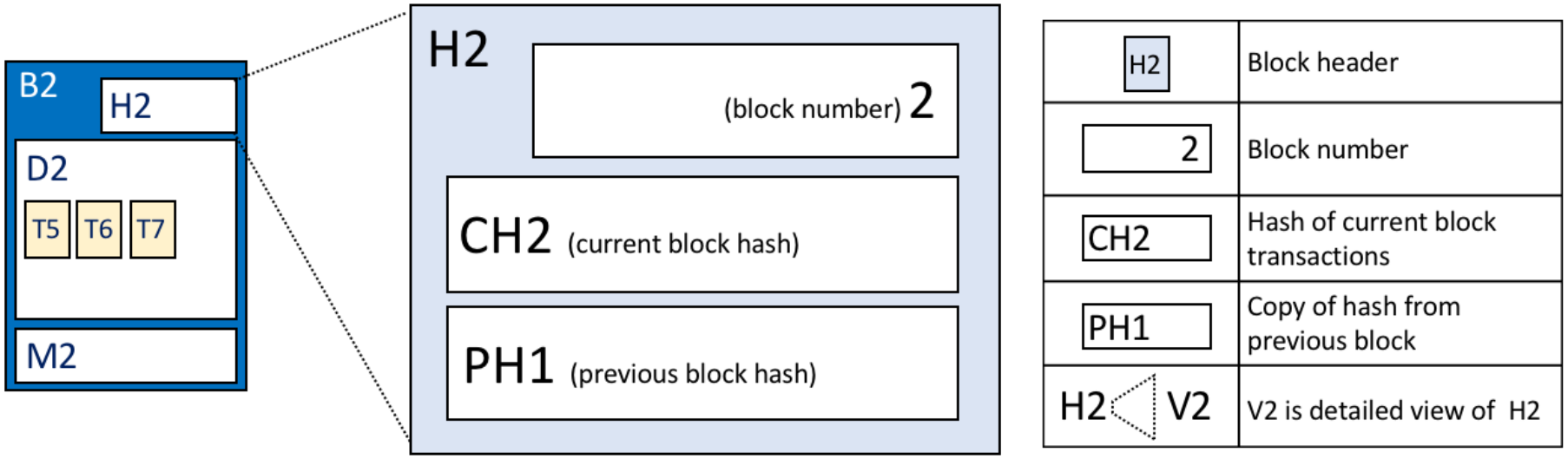
- Primer Fabric blokčejna sastavljenog od 4 bloka (B0, B1, B2, B3)
- B0 je **blok postanka** (engl. *genesis block*) – sadrži konfiguracionu transakciju koja sadrži inicijalno stanje kanala mreže



Izvor: https://hyperledger-fabric.readthedocs.io/en/latest/ledger/ledger.html

Fabric blok

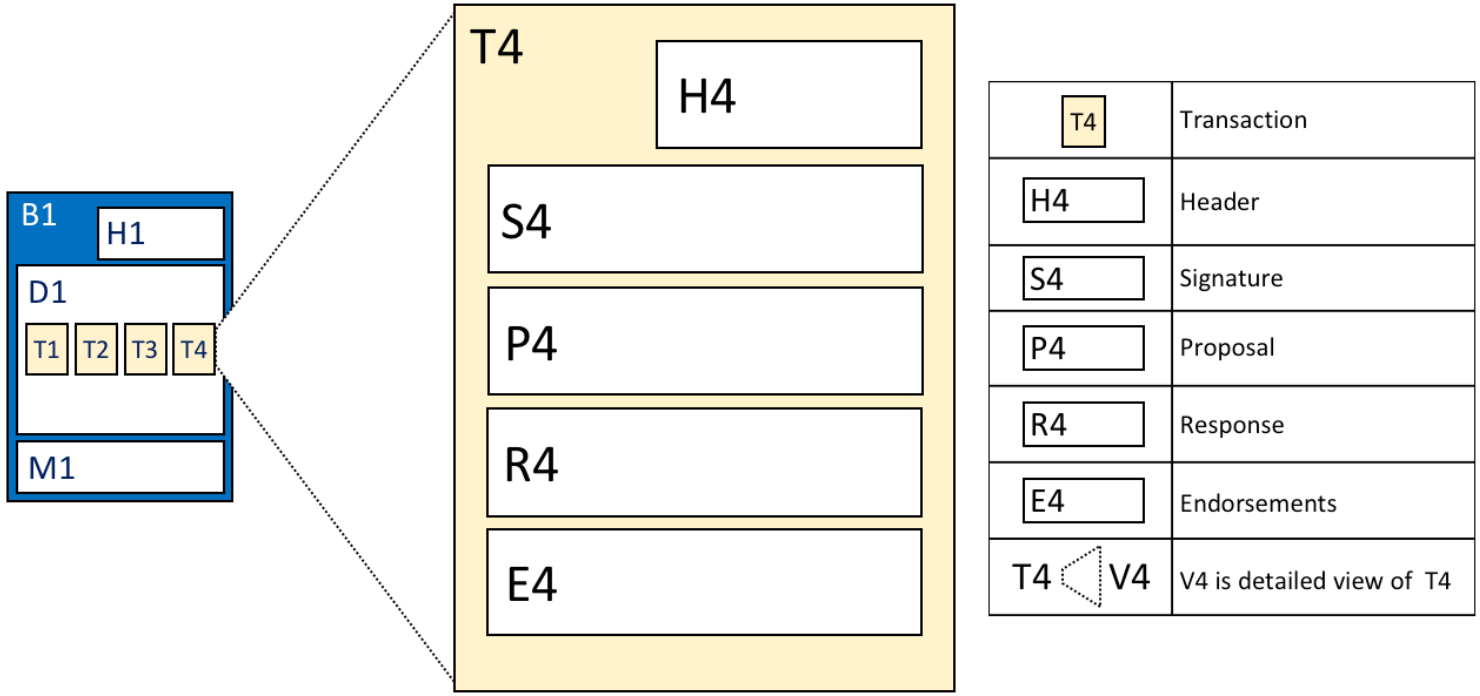
- Zaglavlje Fabric bloka ima tri polja: **broj bloka, heš trenutnog bloka** i **heš iz zaglavlja prethodnog bloka**
- **Blok** sadrži i **podatke bloka** (engl. *blockdata*) i metapodatke



Izvor: https://hyperledger-fabric.readthedocs.io/en/latest/ledger/ledger.html

Fabric transakcija

- **Transakcija** u **podacima bloka** (engl. *blockdata*) sastoji se od **zaglavlja** (engl. *transaction header*), **potpisa** (engl. *transaction signature*) klijentske aplikacije, **predloga** (engl. *transaction proposal*) – ulaznih parametara za chaincode, **odgovora na transakciju** (engl. *transaction response*) – izlaz chaincode-a, i **liste podrške** (engl. *list of endorsements*)



Izvor: https://hyperledger-fabric.readthedocs.io/en/latest/ledger/ledger.html

Online resursi – Hyperledger

- Hyperledger White Papers:
  https://www.hyperledger.org/learn/white-papers
- Hyperledger Architecture, Volume 1:

  https://www.hyperledger.org/wp-content/uploads/2017/08/HyperLedger_Arch_WG_Paper_1_Consensus.pdf
- Official documentation:

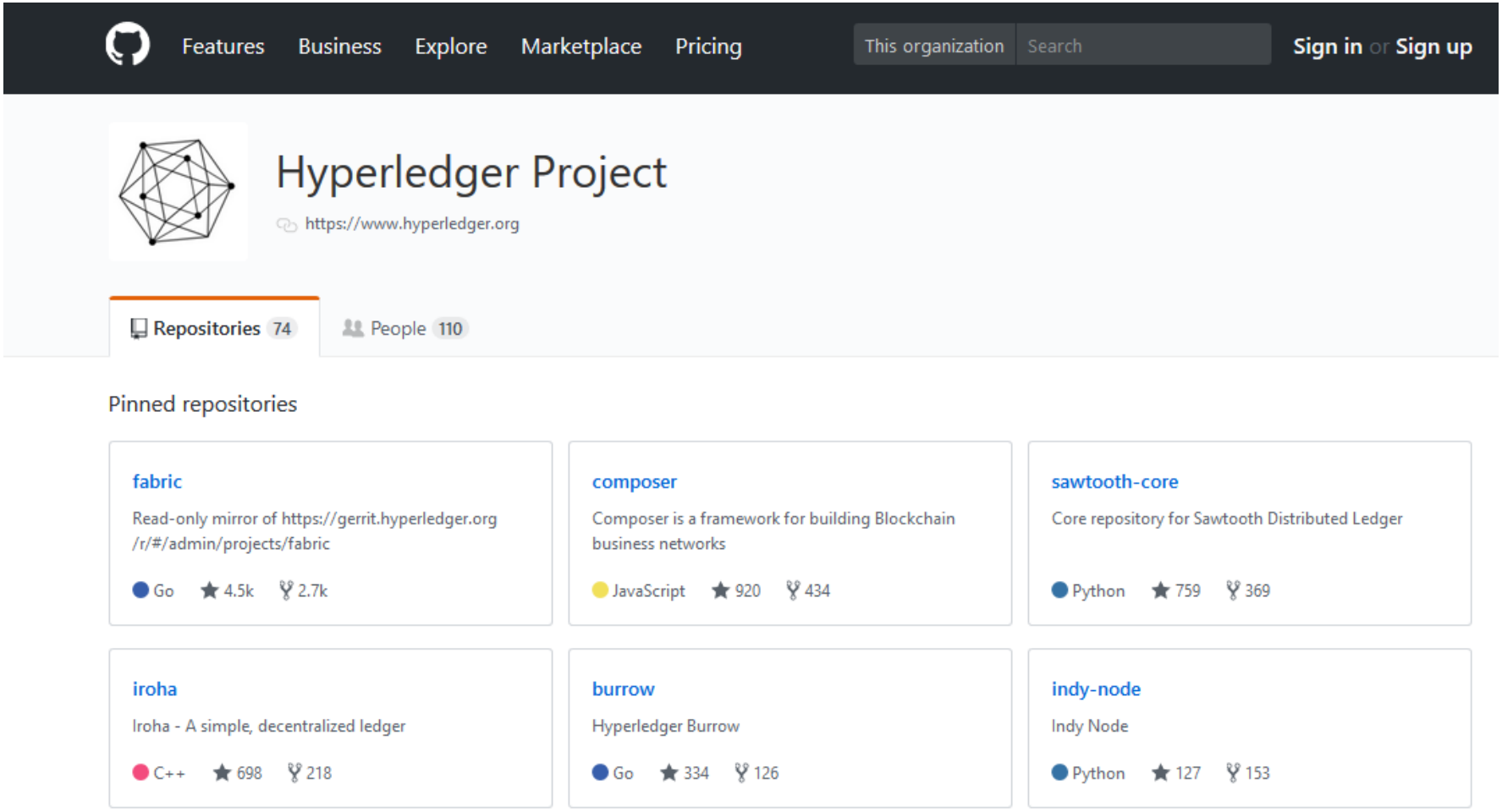
  https://hyperledger-fabric.readthedocs.io/en/latest/
- Rocket Chat:

  https://chat.hyperledger.org/
- StackOverflow:

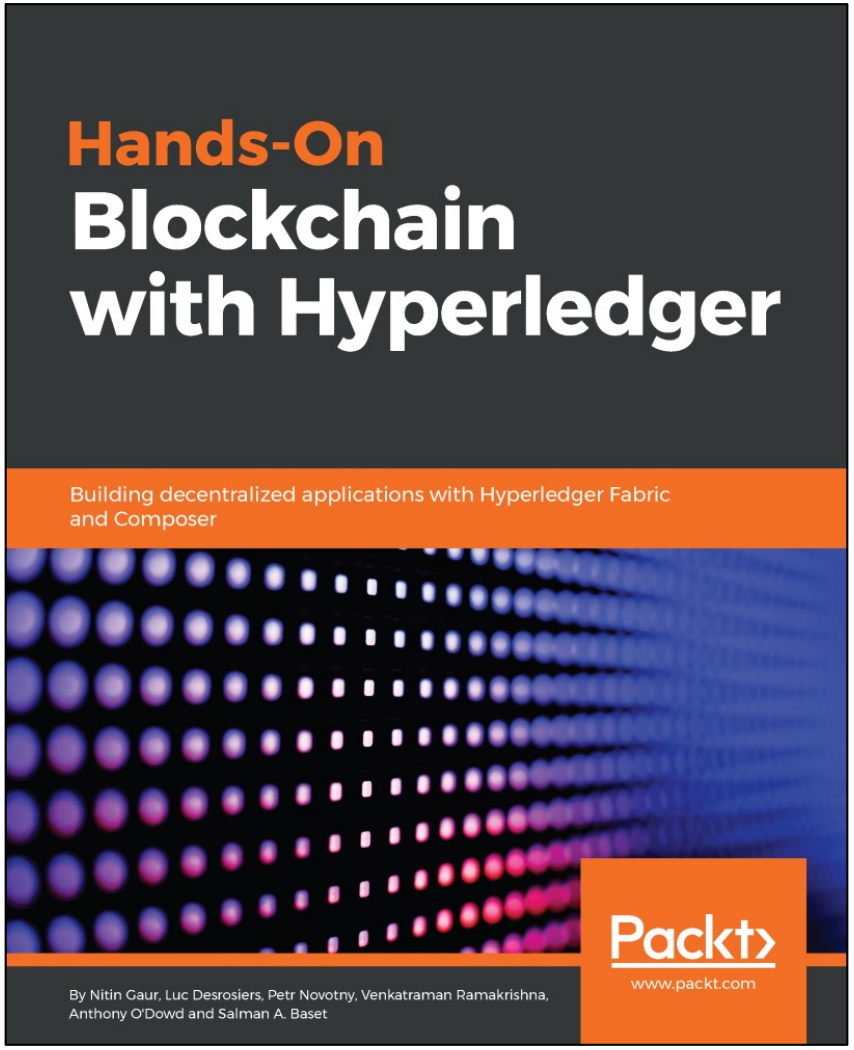
  https://stackoverflow.com/questions/tagged/hyperledger-fabric

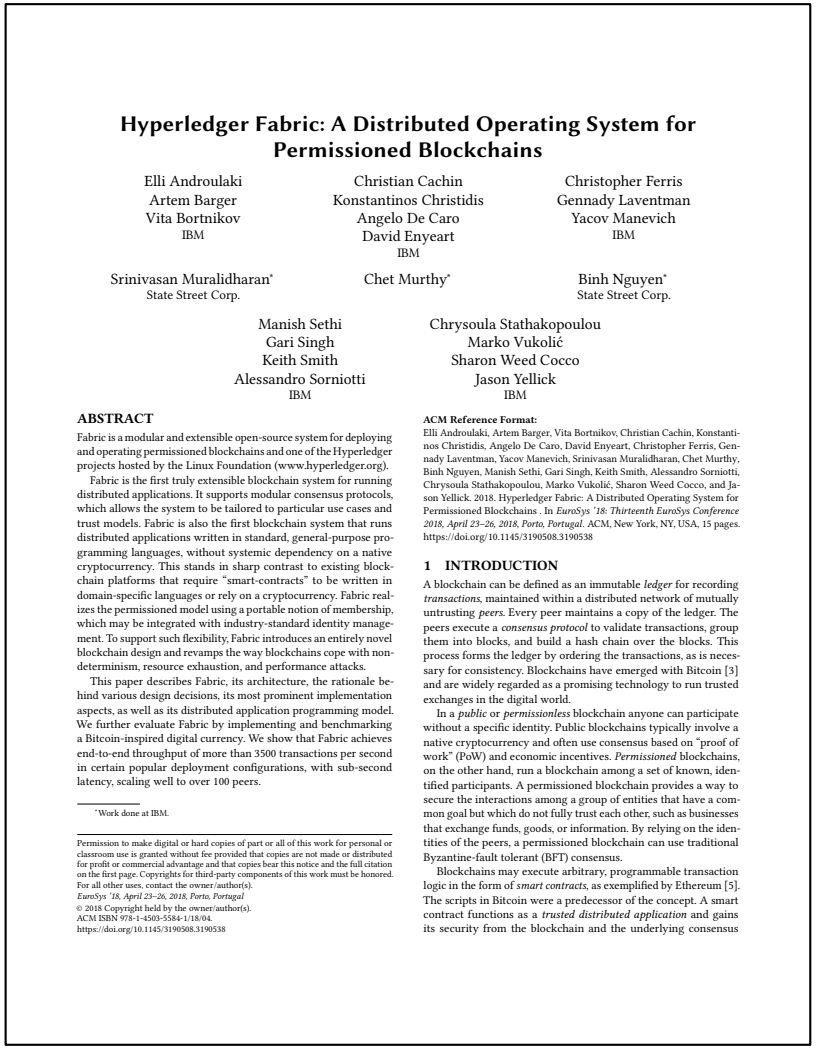
Hyperledger online resursi i reference

- Hyperledger Github (https://github.com/hyperledger):



Literatura – Hyperledger Fabric





Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains

Elli Androulaki, Artem Barger, Vita Bortnikov — IBM
Christian Cachin, Konstantinos Christidis, Angelo De Caro, David Enyeart — IBM
Christopher Ferris, Gennady Laventman, Yacov Manevich — IBM
Srinivasan Muralidharan*, Chet Murthy*, Binh Nguyen* — State Street Corp.
Manish Sethi, Gari Singh, Keith Smith, Alessandro Sorniotti — IBM
Chrysoula Stathakopoulou, Marko Vukolić, Sharon Weed Cocco, Jason Yellick — IBM

ABSTRACT

Fabric is a modular and extensible open-source system for deploying and operating permissioned blockchains and one of the Hyperledger projects hosted by the Linux Foundation (www.hyperledger.org).

Fabric is the first truly extensible blockchain system for running distributed applications. It supports modular consensus protocols, which allows the system to be tailored to particular use cases and trust models. Fabric is also the first blockchain system that runs distributed applications written in standard, general-purpose programming languages, without systemic dependency on a native cryptocurrency. This stands in sharp contrast to existing blockchain platforms that require "smart-contracts" to be written in domain-specific languages or rely on a cryptocurrency. Fabric realizes the permissioned model using a portable notion of membership, which may be integrated with industry-standard identity management. To support such flexibility, Fabric introduces an entirely novel blockchain design and revamps the way blockchains cope with non-determinism, resource exhaustion, and performance attacks.

This paper describes Fabric, its architecture, the rationale behind various design decisions, its most prominent implementation aspects, as well as its distributed application programming model. We further evaluate Fabric by implementing and benchmarking a Bitcoin-inspired digital currency. We show that Fabric achieves end-to-end throughput of more than 3500 transactions per second in certain popular deployment configurations, with sub-second latency, scaling well to over 100 peers.

*Work done at IBM.

EuroSys '18, April 23–26, 2018, Porto, Portugal

ACM ISBN 978-1-4503-5584-1/18/04.
https://doi.org/10.1145/3190508.3190538

ACM Reference Format:
Elli Androulaki, Artem Barger, Vita Bortnikov, Christian Cachin, Konstantinos Christidis, Angelo De Caro, David Enyeart, Christopher Ferris, Gennady Laventman, Yacov Manevich, Srinivasan Muralidharan, Chet Murthy, Binh Nguyen, Manish Sethi, Gari Singh, Keith Smith, Alessandro Sorniotti, Chrysoula Stathakopoulou, Marko Vukolić, Sharon Weed Cocco, and Jason Yellick. 2018. Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains . In *EuroSys '18: Thirteenth EuroSys Conference 2018, April 23–26, 2018, Porto, Portugal.* ACM, New York, NY, USA, 15 pages. https://doi.org/10.1145/3190508.3190538

1 INTRODUCTION

A blockchain can be defined as an immutable *ledger* for recording *transactions*, maintained within a distributed network of mutually untrusting *peers*. Every peer maintains a copy of the ledger. The peers execute a *consensus protocol* to validate transactions, group them into blocks, and build a hash chain over the blocks. This process forms the ledger by ordering the transactions, as is necessary for consistency. Blockchains have emerged with Bitcoin [3] and are widely regarded as a promising technology to run trusted exchanges in the digital world.

In a *public* or *permissionless* blockchain anyone can participate without a specific identity. Public blockchains typically involve a native cryptocurrency and often use consensus based on "proof of work" (PoW) and economic incentives. *Permissioned* blockchains, on the other hand, run a blockchain among a set of known, identified participants. A permissioned blockchain provides a way to secure the interactions among a group of entities that have a common goal but which do not fully trust each other, such as businesses that exchange funds, goods, or information. By relying on the identities of the peers, a permissioned blockchain can use traditional Byzantine-fault tolerant (BFT) consensus.

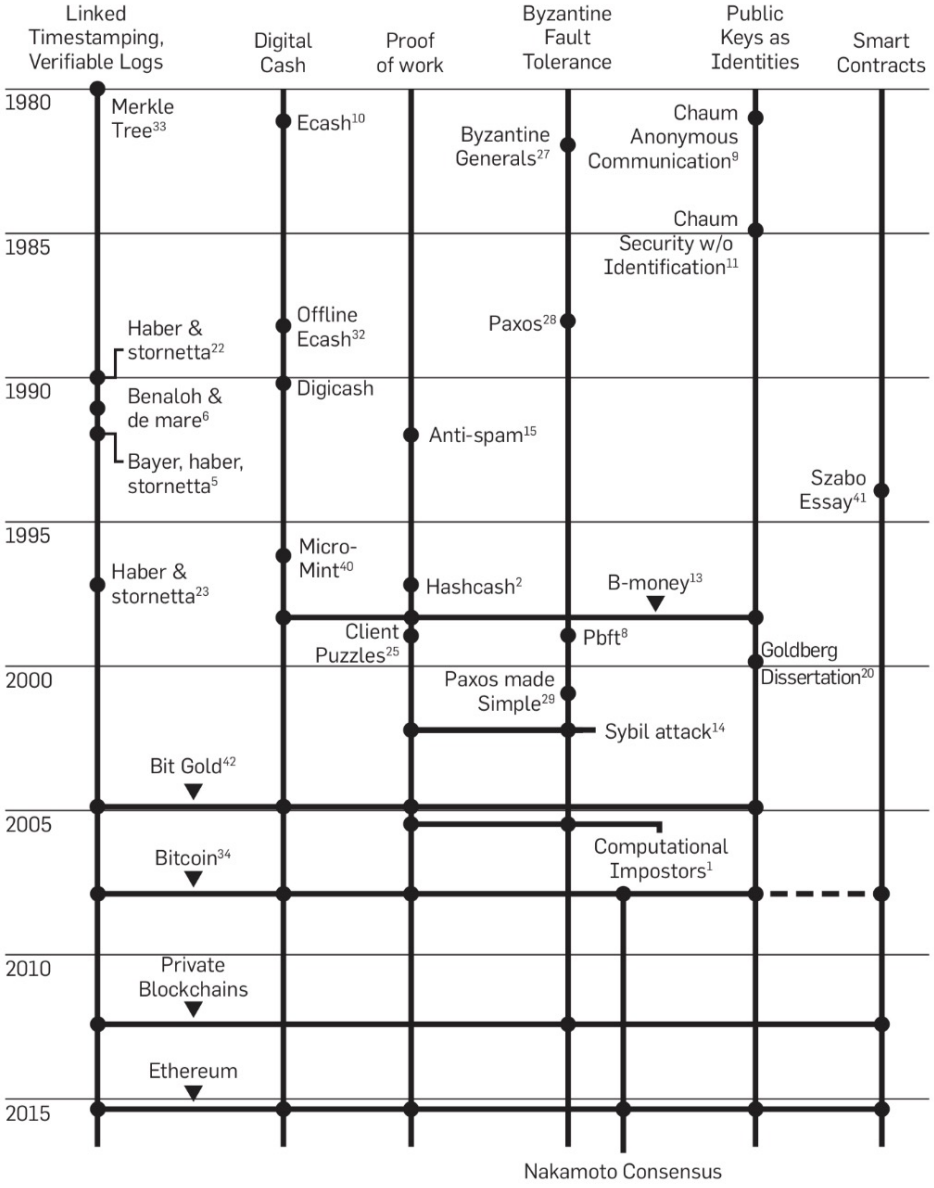
Blockchains may execute arbitrary, programmable transaction logic in the form of *smart contracts*, as exemplified by Ethereum [5]. The scripts in Bitcoin were a predecessor of the concept. A smart contract functions as a *trusted distributed application* and gains its security from the blockchain and the underlying consensus

https://arxiv.org/abs/1801.10228

Budućnost blokčejna

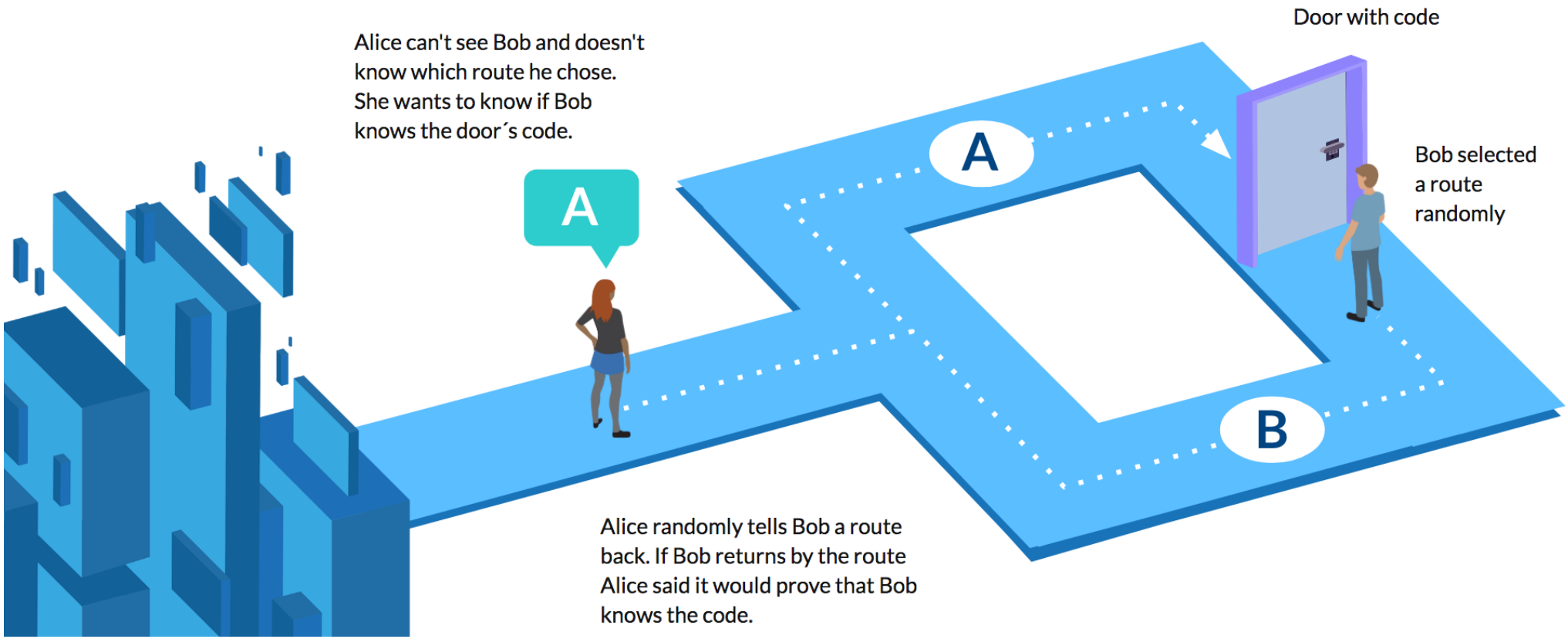
Put do blokčejna

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

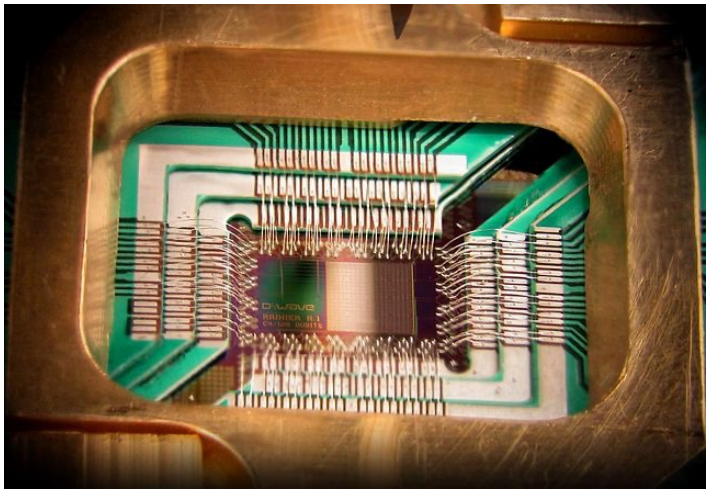
- **Dokaz sa nultim znanjem** (engl. **zero-knowledge proof** – ZKP) je metod kojim jedna strana (**dokazivač** – engl. *prover*) može dokazati drugoj strani (**verifikator** – engl. *verifier*) da zna vrednost *x*, bez pružanja bilo koje dodatne informacije osim činjenice da poznaje vrednost *x*
- Suština 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

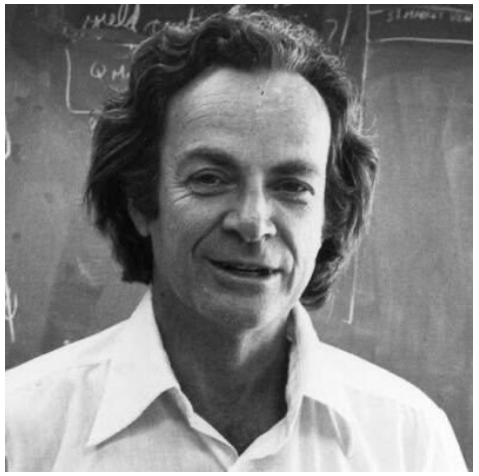
Zero Knowledge Proofs

- 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

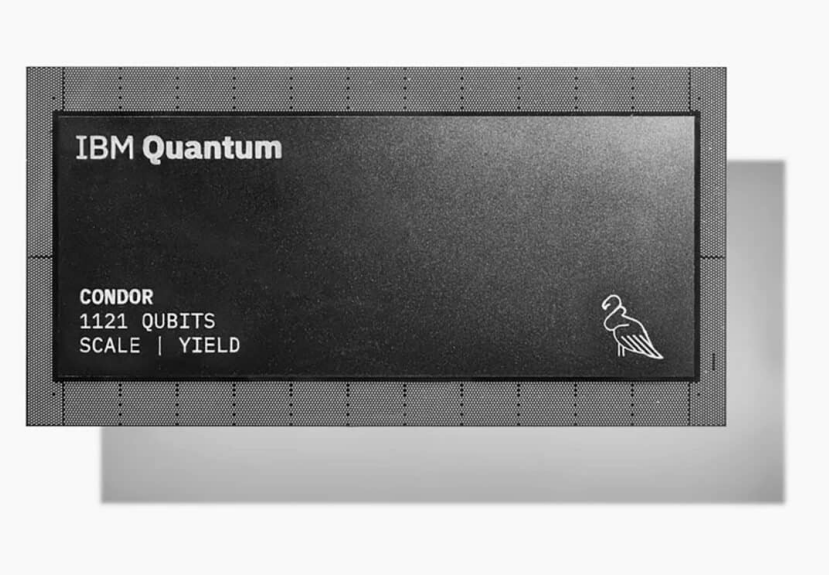
- 1959. Richard Feynman predavanje "*There's Plenty of Room at the Bottom*" – mogućnost kvantnog računarstva, 1981. "*Simulating Physics with Computers*"
- Danas u aktivan razvoj uključeni IBM, Google, Intel, D-Wave
- 2017. D-Wave prodaje kvantne računare sa 2000 kjubita (engl. *qubit*), ali zasnovane na principu kvantnog čeličenja (engl. quantum annealing) specijalizovanom za probleme optimizacije
- 2023. IBM Condor sa 1121 kjubitom, univerzalni kvantni računar, zasnovan na neutralnim atomima i superprovodnicima

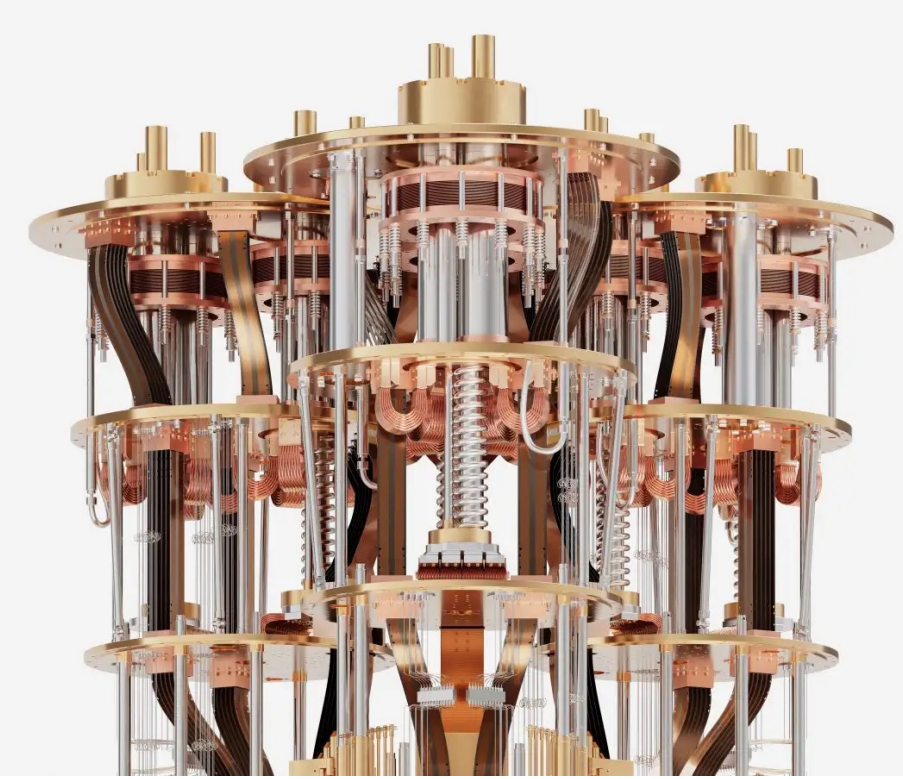




Richard Feynman
(1918-1988)

IBM Condor

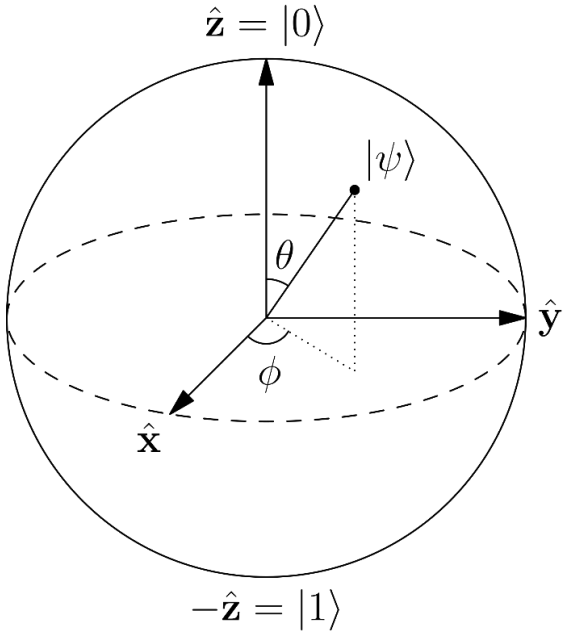




Izvori: https://postquantum.com/industry-news/ibm-condor/,
https://www.newscientist.com/article/2405789-ibms-condor-quantum-computer-has-more-than-1000-qubits/

Kvantni računari

- **Kjubiti** (engl. *qubit*) se mogu nalaziti u **kvantnim stanjima** 0 i 1, kao i u superpoziciji ovih stanja. Rezultat merenja stanja kjubita je uvek 0 ili 1, ali verovatnoća rezultata zavisi od kvantnog stanja u kome se kjubit nalazio
- **Kvantna logička kola** (Toffoli, Fredkin, Hadamard, Pauli, …)
- **Šorov algoritam** za **faktorizaciju**
- **Groverov algoritam traženja**
- **Kvantna Furijeova transformacija**
- Januara 2019. IBM predstavio **komercijalni kvantni računar** – IBM Q System One
- Jezici: QASM, Qiskit (IBM), Cirq (Google), Q#…
- Quantum Computers Explained: https://www.youtube.com/watch?v=B3U1NDUiwSA

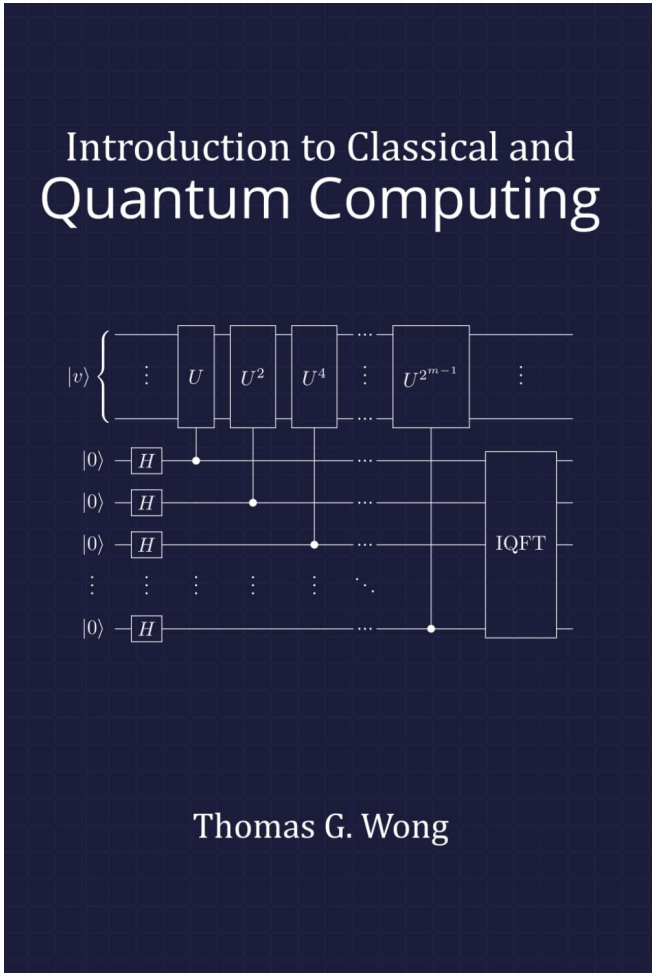


Blohova sfera

Preporučena literatura

- Thomas Wong

Introduction to Classical and Quantum Computing



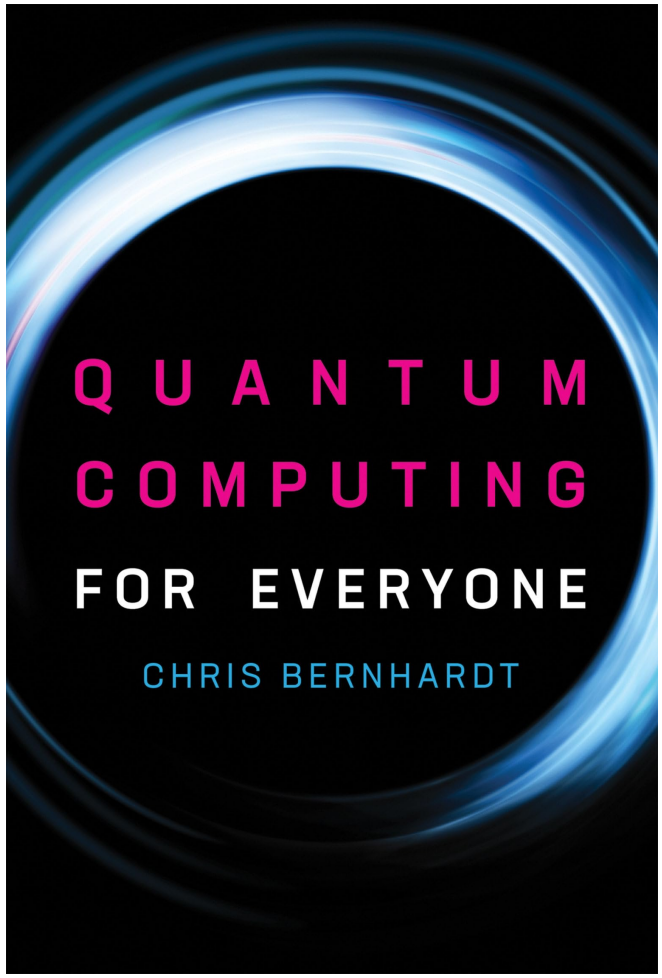
- 2022
- Rooted Grove

Preporučena literatura

- Chris Bernhardt

Quantum Computing for Everyone

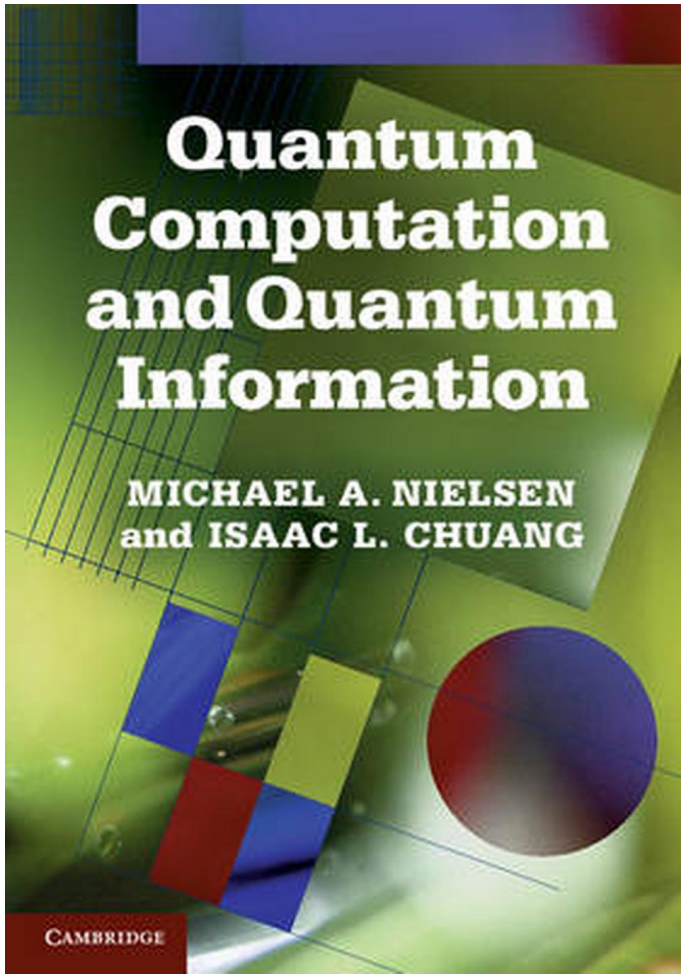
- 2020
- The MIT Press



Preporučena literatura – napredni nivo

- Michael Nielsen,
  Isaac Chuang

Quantum Computation and Quantum Information,
10th Anniversary Edition



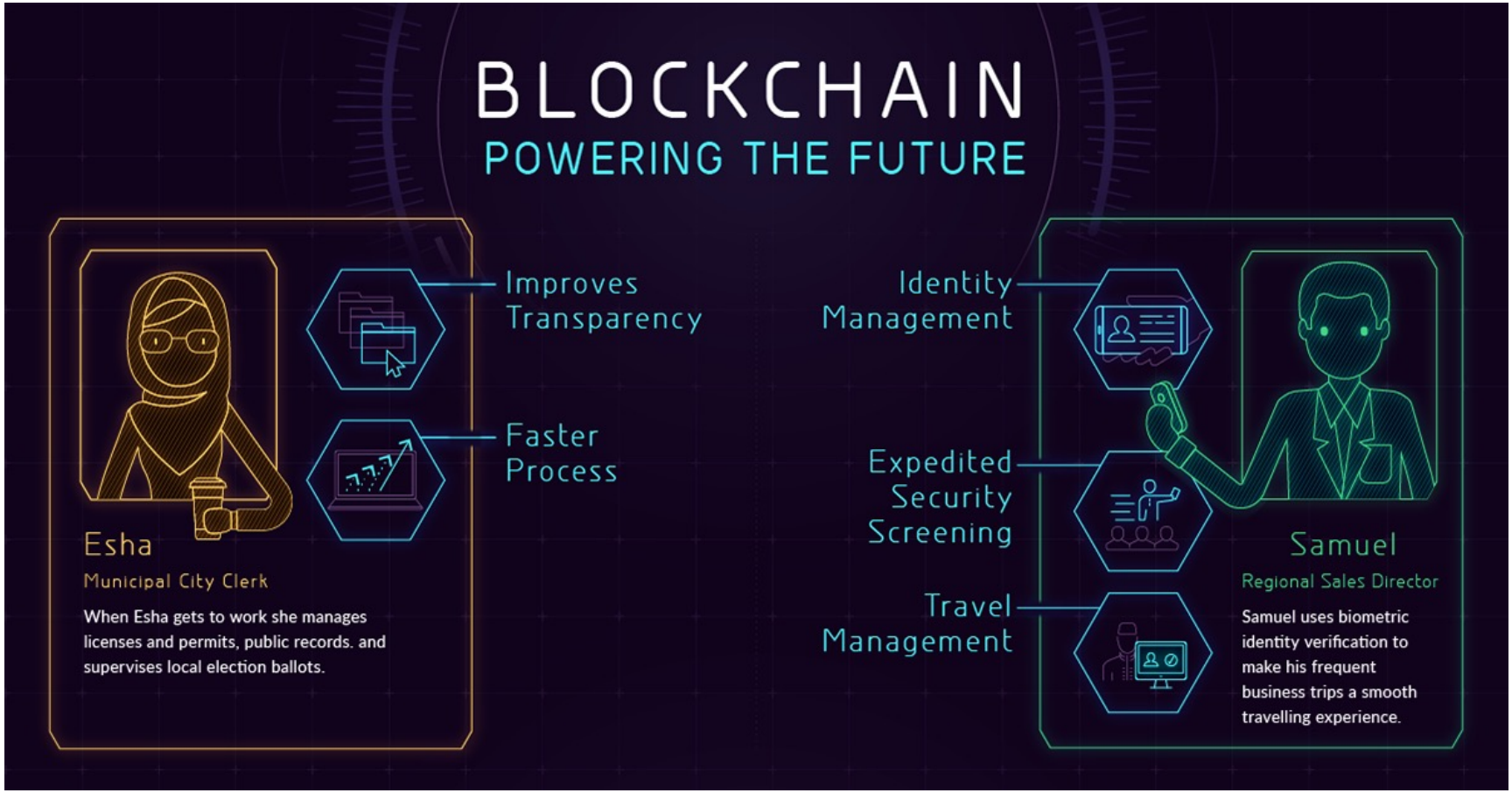
- 2011
- Cambridge University Press

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

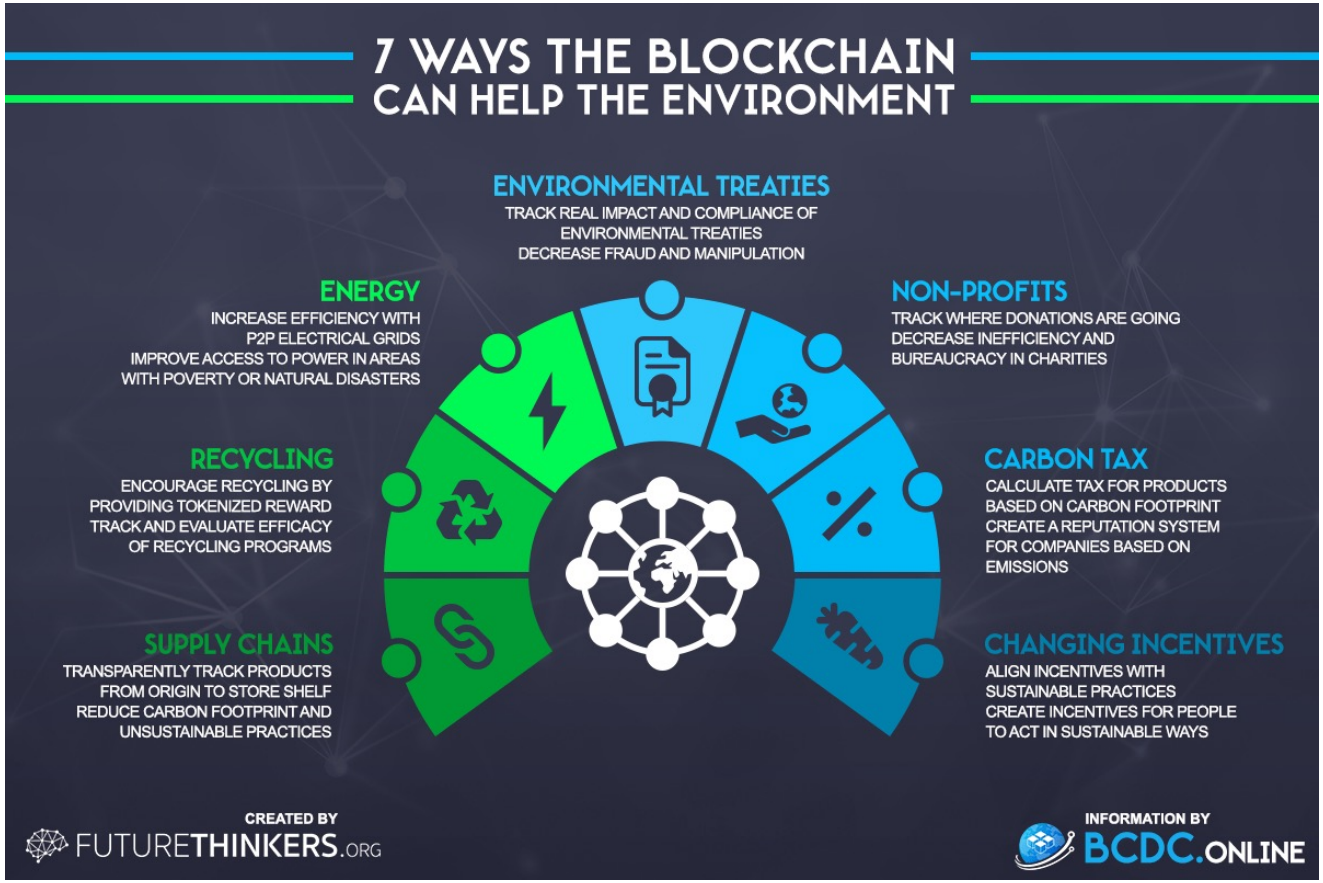
Budućnost blokčejna

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



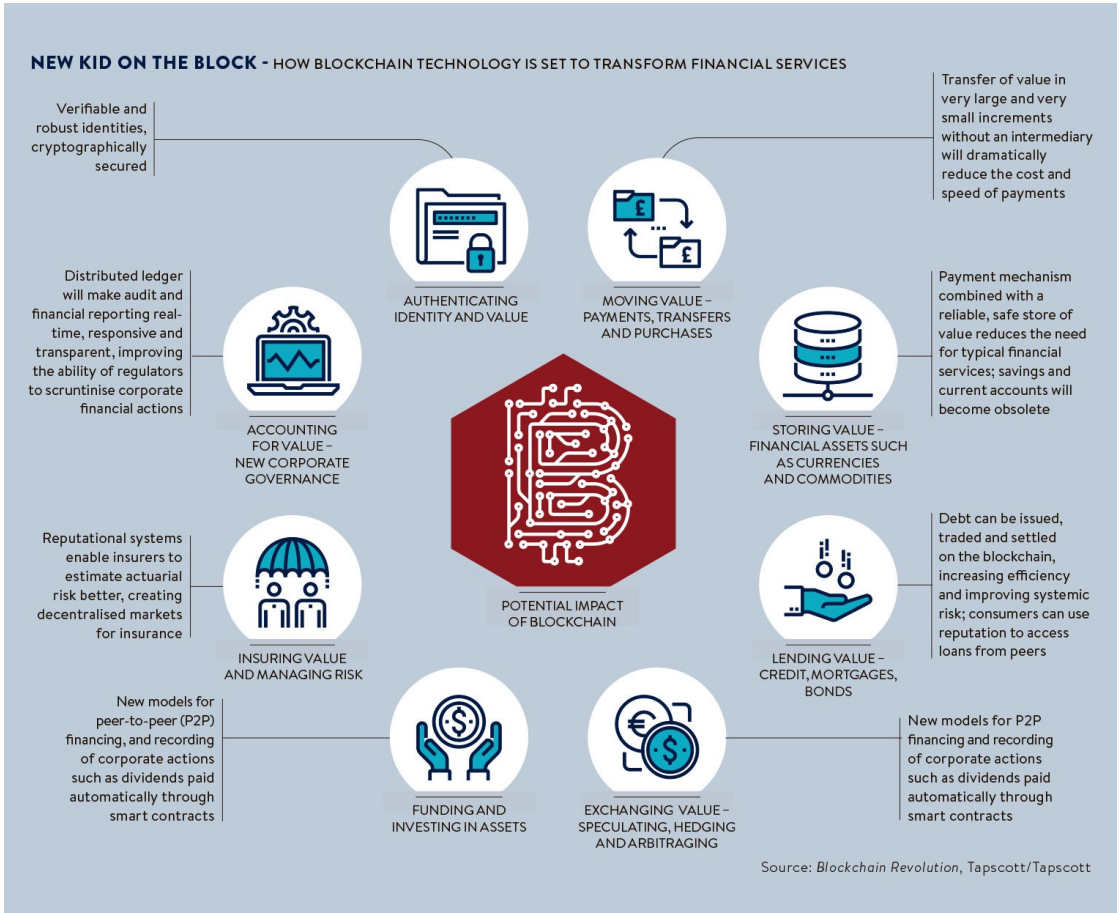
Budućnost blokčejna

- 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