SVEUČILIŠTE U ZAGREBU
Fakultet elektrotehnike i računarstva

Diplomski studij

Informacijska i komunikacijska tehnologija:

Telekomunikacije i informatika

Računarstvo:

Programsko inženjerstvo i informacijski sustavi

Računarska znanost

Raspodijeljeni sustavi

13. Tehnologija raspodijeljene glavne knjige (engl. *Distributed Ledger Technology*, DLT)

Ak. god. 2020./2021.

Creative Commons

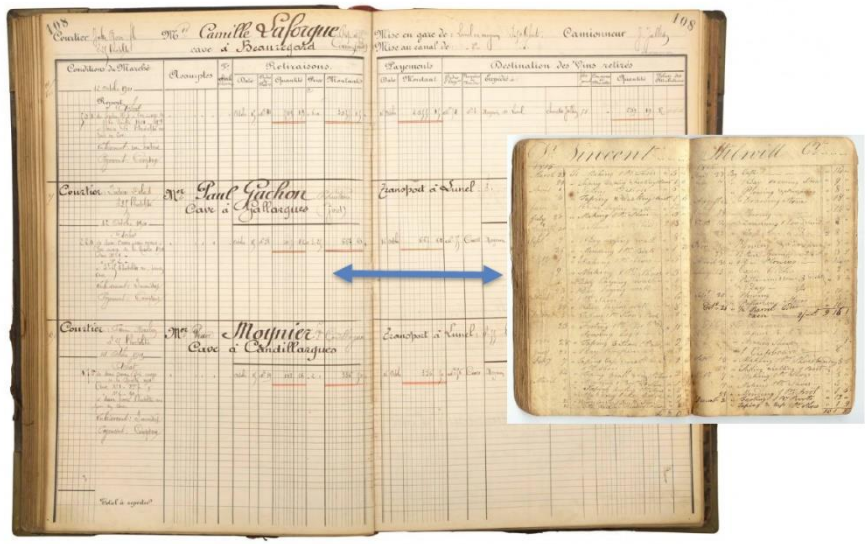
- slobodno smijete:
  - **dijeliti** — umnožavati, distribuirati i javnosti priopćavati djelo
  - **prerađivati** djelo
- pod sljedećim uvjetima:
  - **imenovanje:** morate priznati i označiti autorstvo djela na način kako je specificirao autor ili davatelj licence (ali ne način koji bi sugerirao da Vi ili Vaše korištenje njegova djela imate njegovu izravnu podršku).
  - **nekomercijalno:** ovo djelo ne smijete koristiti u komercijalne svrhe.
  - **dijeli pod istim uvjetima:** ako ovo djelo izmijenite, preoblikujete ili stvarate koristeći ga, preradu možete distribuirati samo pod licencom koja je ista ili slična ovoj.

U slučaju daljnjeg korištenja ili distribuiranja morate drugima jasno dati do znanja licencne uvjete ovog djela.
Od svakog od gornjih uvjeta moguće je odstupiti, ako dobijete dopuštenje nositelja autorskog prava.
Ništa u ovoj licenci ne narušava ili ograničava autorova moralna prava. *Tekst licence preuzet je s http://creativecommons.org/*

Sadržaj

- Raspodijeljena glavna knjiga: motivacija i pojmovi
- Blockchain: struktura podataka
- Blockchain: centralizirana i decentralizirana izvedba
- Konsenzus
- Bitcoin i druge primjene
- Ethereum i pametni ugovor

Motivacija za nastanak raspodijeljene glavne (javne) knjige



Ledger: računovodstvena knjiga

Distributed Ledger?

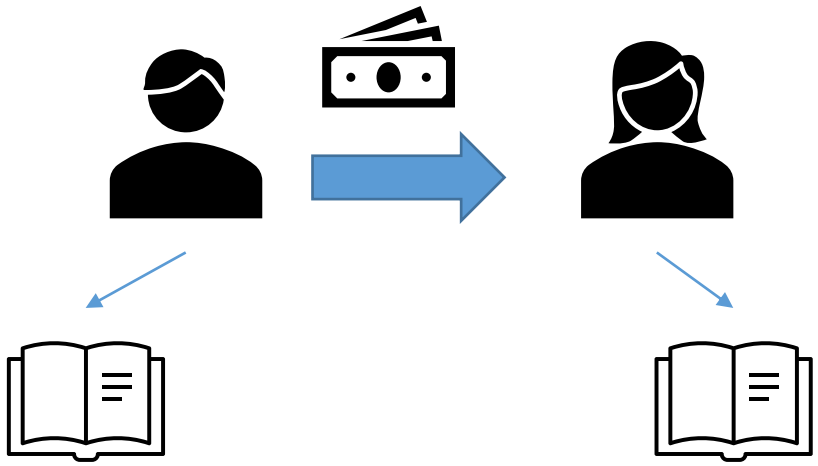
Bitcoin Whitepaper 2008 [4]

Bitcoin, digitalna valuta kriptovaluta

2009

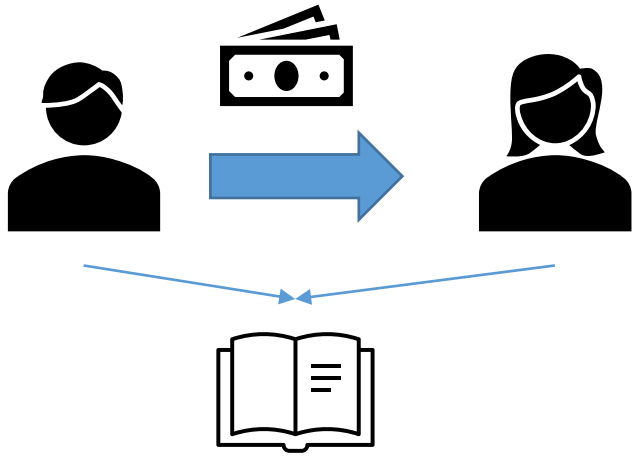
Razmjena digitalnih dobara

Klasično: svaka strana čuva listu transakcija



Dogovor o provedenoj transakciji
Moguće pogreške

DLT



Zajednička dijeljena glavna knjiga
Zapisi su nepromjenjivi i trajni

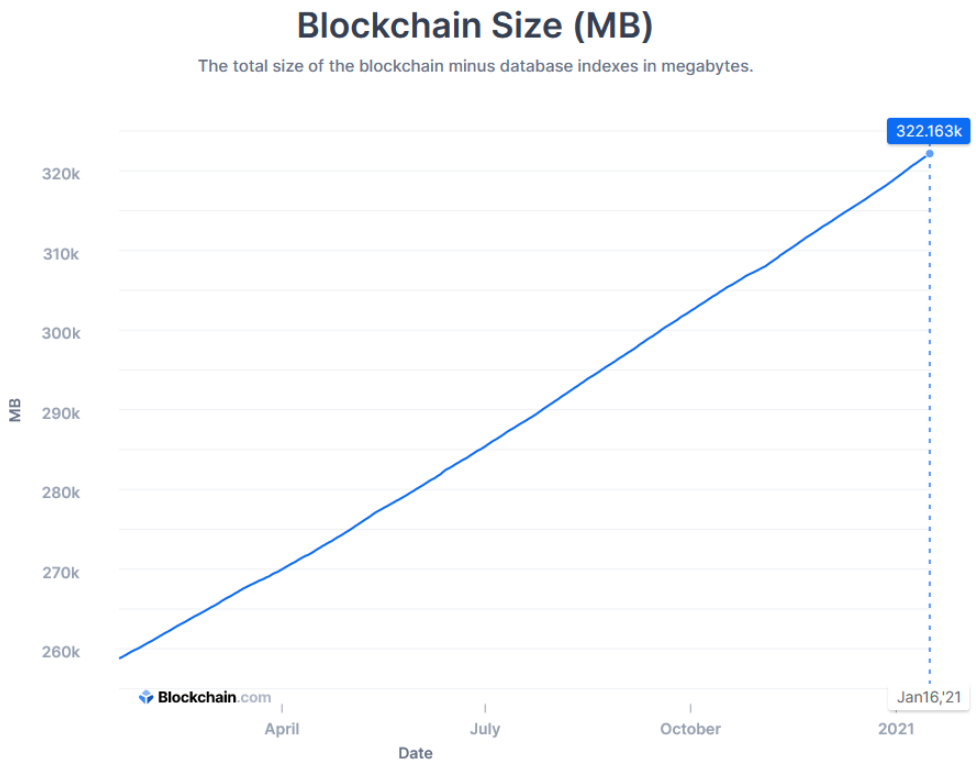
Ne postoji povjerenje među sudionicima

Raspodijeljena glavna knjiga

- Nova vrsta „pouzdanog posrednika” koja se temelji na raspodijeljenim algoritmima i kriptografiji
- Omogućuje izvođenje transakcija u raspodijeljenom okuženju s velikim brojem dionika koji si međusobno ne vjeruju (*intermediary in a trustless environment*)
- Na primjeru kriptovaluta: zamjena za banku
- Što ova tehnologija može, a ne mogu raspodijeljene baze podataka?

Tehnologija raspodijeljene glavne knjige

- *Distributed Ledger Technology* (DLT)
- Sustav koji održava popis provedenih transakcija na decentralizirani način u mreži peerova
- Svaki peer održava kopiju svih transakcija
- Omogućuje jedino zapisivanje (konstantno dodavanje) novih transakcija, glavna knjiga kontinuirano raste
- Zapisane transakcije se ne mogu obrisati, nepromjenjive su i svi ih mogu čitati i provjeriti (javni ledger)



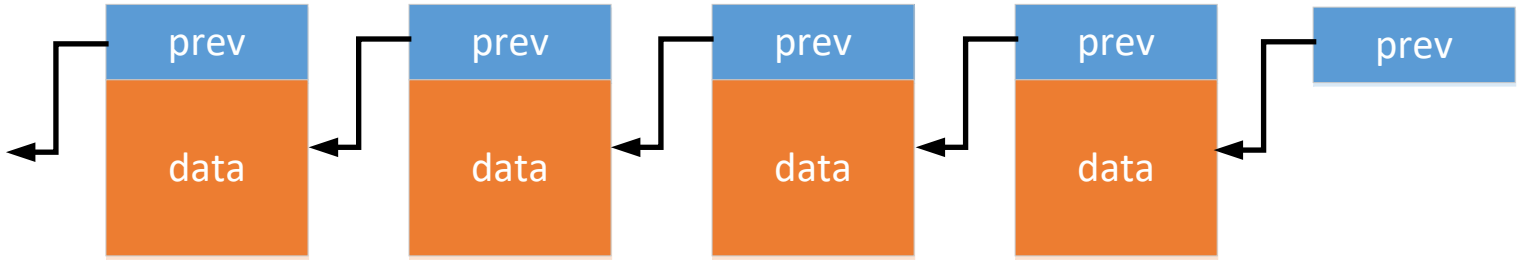
Size of the Bitcoin blockchain
https://www.blockchain.com/charts/blocks-size

Što je *blockchain*?

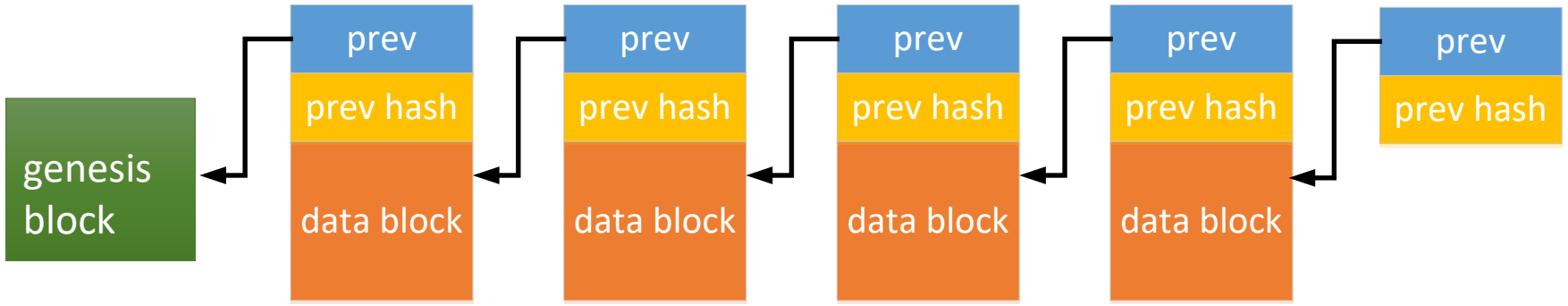
- Struktura podataka koja se sastoji od blokova (blok-lanac)
- Zapisnik (*append-only log*) u koji se **novi blokovi mogu dodavati**, ali se **stari ne mogu brisati ili naknadno mijenjati** (falsificirati)
- Blokovi su uređeni (u vremenu) i pohranjuju transakcije
  - postoji relativna uređenost blokova zapisa u vremenu
  - transakcije unutar bloka su također relativno uređene u vremenu
  - blokovi su otvoreni za čitanje (za public blockchain)
- Zapisuje se i prati **globalno stanje sustava**, no kako se peerovi mogu dogovoriti o uređenosti transakcija i blokova?

Blok-lanac: struktura podataka

- slična jednostrukoj povezanoj listi

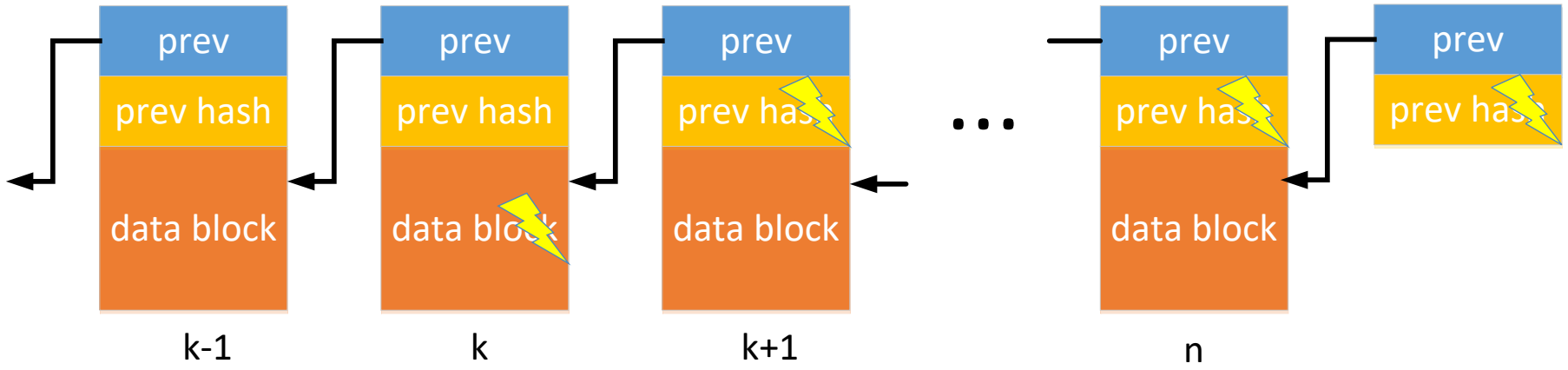


- U *blockchainu* **svaki blok ima zaglavlje** koje među ostalim metapodacima sadrži pokazivač na prethodni blok i sažetak prethodnog bloka (*hash*) **+ blok** (sadrži transakcije)



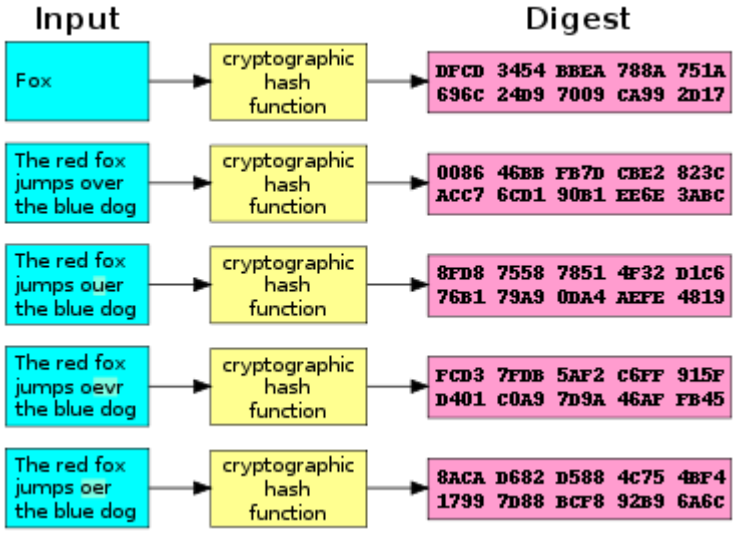
Zašto se zapisi blok-lanca ne daju falsificirati?

- Tko god ima pohranjen ispravan sažetak (*hash*) prethodnog bloka može utvrditi da je došlo do promjene nekog bloka
  - Nakon izmjena zapisa u bloku *k*, njegov novi sažetak neće odgovarati starom sažetku koji je pohranjen u sljedećem bloku *k+1*
  - Nakon toga niti novi sažetak bloka k+1 neće odgovarati njegovom starom sažetku



Može li falsificirani blok proći neopaženo?

- Ovo bi se moglo dogoditi kad bi **novi sažetak (*hash*) nekog bloka bio (namješten da bude) identičan njegovom starom sažetku**
- Za izračun sažetka se koriste posebne kriptografske jednosmjerne funkcije (npr. SHA-256) sa sljedećim svojstvima
  - ulaz: niz znakova proizvoljne duljine
  - izlaz: niz znakova fiksne duljine
  - jednostavno je izračunati sažetak za zadani ulaz
  - nije moguće na osnovu sažetka regenerirati ulaz
  - **nije moguće odrediti ulaz koji bi imao zadani sažetak**
  - neizvedivo da se pronađu dva različita ulaza s istim sažetkom
  - promjena jednog bita na ulazu rezultira potpuno drugačijim izlazom



Izvor:https://en.wikipedia.org/wiki/Cryptographic_hash_function#/media/File:Cryptographic_Hash_Function.svg

Može li održavanje blok-lanca biti centralizirano?

- Procedura centraliziranog pohranjivanja blok-lanca na poslužitelju (tj. centralnom autoritetu) je moguća
  - Transakcije koji se žele dodati u blok-lanca se moraju poslati centralnom autoritetu
  - Centralni autoritet provjerava valjanost primljene transakcije i zapisuje ih u nove blokove koje dodaje u blok-lanac (što je s redoslijedom transakcija?)
  - Centralni autoritet objavljuje nove blokove koje dodaje u blok-lanac
  - Svatko može provjeriti integritet blok-lanca: tko ima *prev_hash* na neki objavljeni blok može provjeriti da nema naknadnih falsifikata u blokovima koji prethode tom bloku

Koji su problemi centraliziranog održavanja blok-lanca?

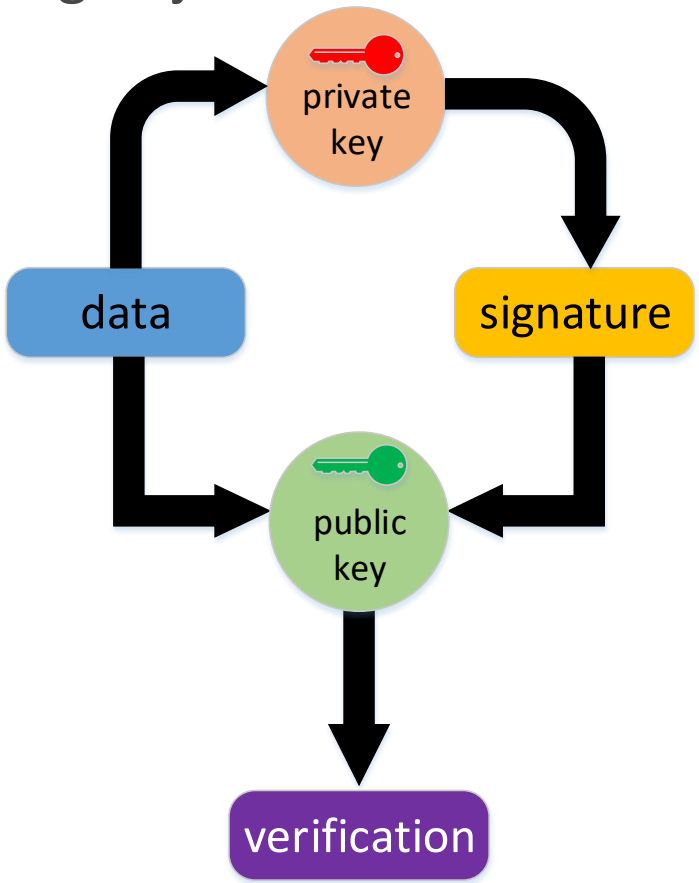
- Centralni autoritet može **narušiti cjelovitost transakcije** (promijeniti primljenu transakciju prije pohrane)
  - U slučaju kriptovaluta centralni autoritet može proizvoljno mijenjati iznose
  - U slučaju papirnog novca to bi bilo identično krađi od strane banke prilikom transakcije
  - **Problem cjelovitosti zapisa se rješava digitalnim potpisom!**

Kako digitalni potpis čuva cjelovitosti zapisa?

- Digitalni potpis se temelji na primjeni asimetrične kriptografije
- Koristi tri algoritma
  - Algoritam za generiranje para ključeva (privatni i javni ključ)
  - Algoritam za digitalno potpisivanje:

  (podatak, privatni ključ) → potpis
  - Algoritam za provjeru potpisa:

  (podatak, potpis, javni ključ) → {⊤, ⊥}
- Ako se uz zapis u blok-lanac pohrani i njegov potpis
  - algoritmom za provjeru potpisa se lako utvrđuje je li podatak promijenjen ili nije
  - Bitcoin koristi javni ključ za identificiranje korisnika



Koji su problemi centraliziranog blockchaina?

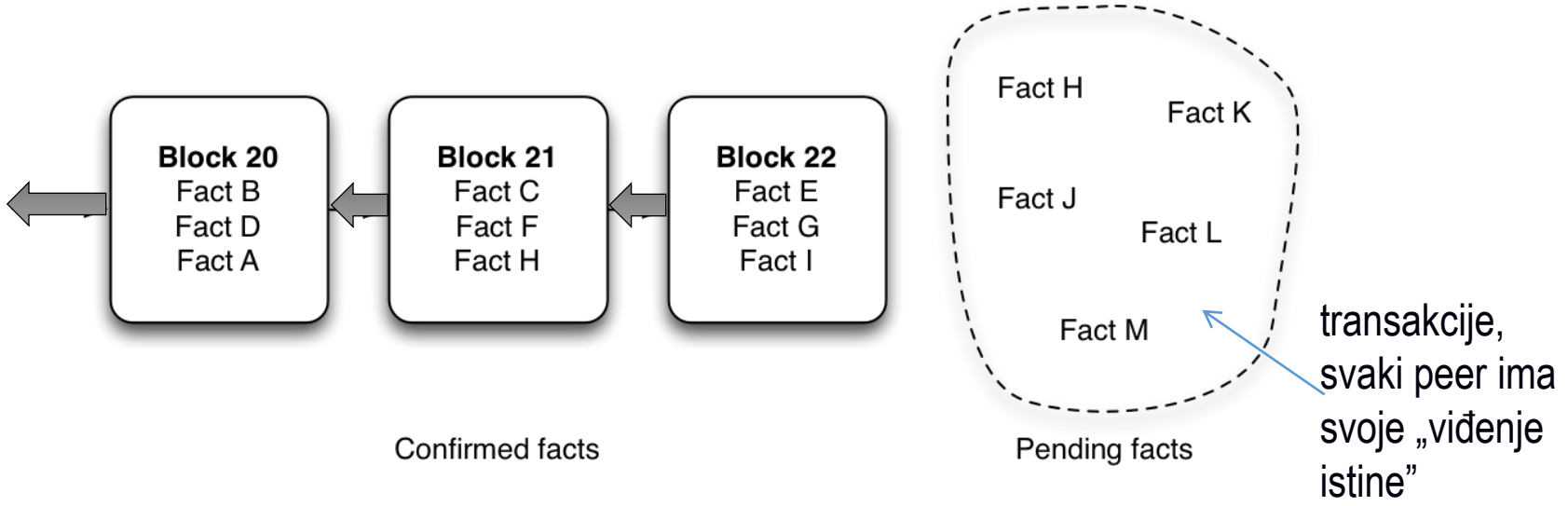
- Centralni autoritet može **uskratiti uslugu** (odbiti transakciju)
  - U slučaju kriptovaluta, centralni autoritet može odbiti provesti transakcije
  - **Problem selekcije zapisa koji se upisuju u blok-lanac se rješava raspodijeljenom implementacijom *blockchaina***
- **Blockchain održava mreža čvorova (peerova)**
- **Svi čvorovi pohranjuju blok-lanac u potpunosti** (naravno uz sve probleme koje uvodi ovakva replikacija)

Kako raspodijeljenost sprječava uskraćivanje usluge?

- U raspodijeljenom sustavu za provjeru i pohranu novog bloka može svaki put biti zadužen drugi čvor
- Dok god je većina čvorova dobronamjerna (pa ne vrši selekciju zapisa) postoji garancija da će pohrana transakcije biti provedena u budućnosti
  - Bit će provedena kad na red za provjeru i pohranu novog bloka dođe jedan od većine dobronamjernih čvorova
- Ako postoji puno zlonamjernih čvorova, pohrana zapisa može potrajati, što ruši povjerenje u čitav sustav raspodijeljenog održavanja blok-lanca

Raspodijeljeno održavanje blok-lanca

- Blockchain održava mreža čvorova (peerova) koji istovremeno i generiraju transakcije (tj. primaju korisničke transakcije)
  - Kako će se peerovi dogovoriti o redoslijedu izvođenja transakcija (koja je transakcija generirana prije, a koja kasnije u P2P mreži)?



https://marmelab.com/blog/2016/04/28/blockchain-for-web-developers-the-theory.html

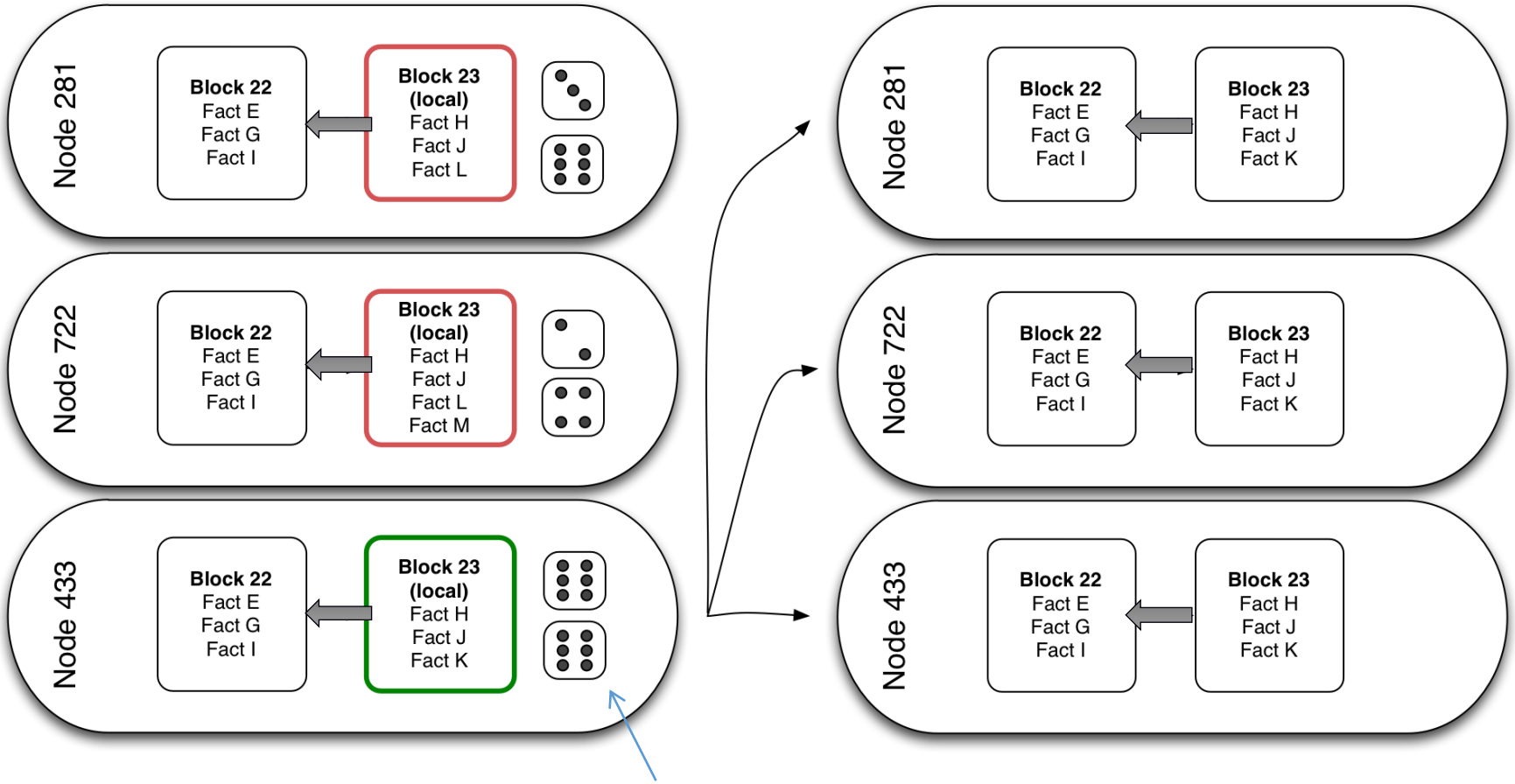
Raspodijeljeni konsenzus

- Prilikom raspodijeljenog održavanja blok-lanca je potrebno postići dogovor (*konsenzus*) oko sljedećeg:
  1. koje transakcije se trebaju nalaziti u sljedećem bloku u lancu i
  2. koji je njihov ispravan redoslijed u tom bloku
- Postizanje raspodijeljenog *konsenzus*a je općenito složen problem (8. predavanje)
  - raspodijeljeni sustav čini mnogo čvorova od kojih neki mogu biti neispravni, a drugi u Bizantskom ispadu (zlonamjerni)
  - propagacija poruka u asinkronoj mreži: svaki čvor ima drugačiji pogled na slijed primljenih transakcija

Raspodijeljeni konsenzus

- Pojednostavljeni algoritam koji se koristi za postizanje dogovora oko sljedećeg bloka u lancu
  1. Mreža se preplavljuje transakcijama
  2. Čvorovi prikupljaju ispravne transakcije i slažu ih u blokove
  3. Odabire se jedan čvor za dodavanje novog bloka u blok-lanac (onaj čvor koji riješi kriptografsku zagonetku)
  4. Odabrani čvor preplavljuje mrežu svojim blokom (mala je vjerojatnost da se istovremeno odabere više ovakvih čvorova, ali postoji)
  5. Ostali čvorovi prihvaćaju blok ako je ispravan i dodaju ga u svoj blok-lanac

Čvorovi, blockchain i dodavanje novih blokova



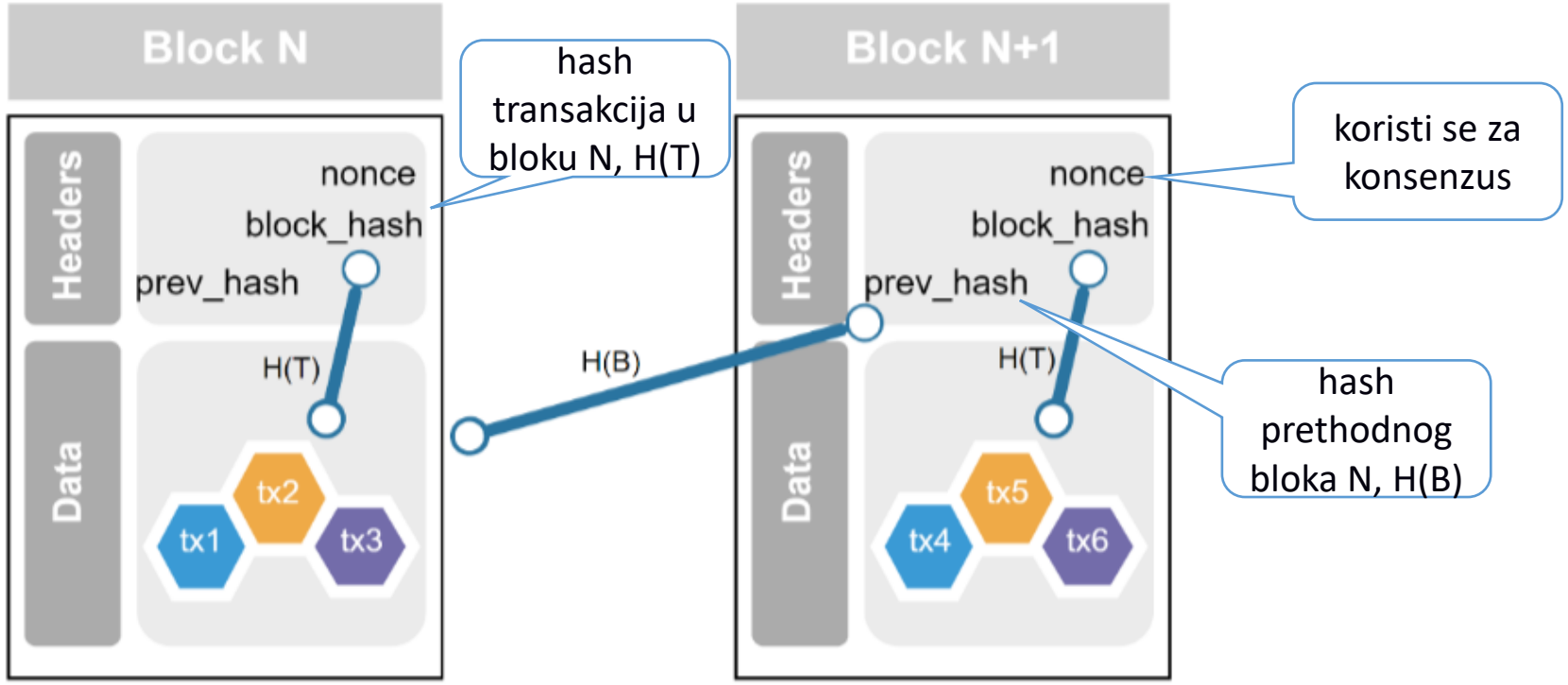
Odabir čvora? U ovom primjeru pobjeđuje onaj čvor koji baci dvije šestice

https://marmelab.com/blog/2016/04/28/blockchain-for-web-developers-the-theory.html

Raspodijeljeni konsenzus: *Proof of Work*

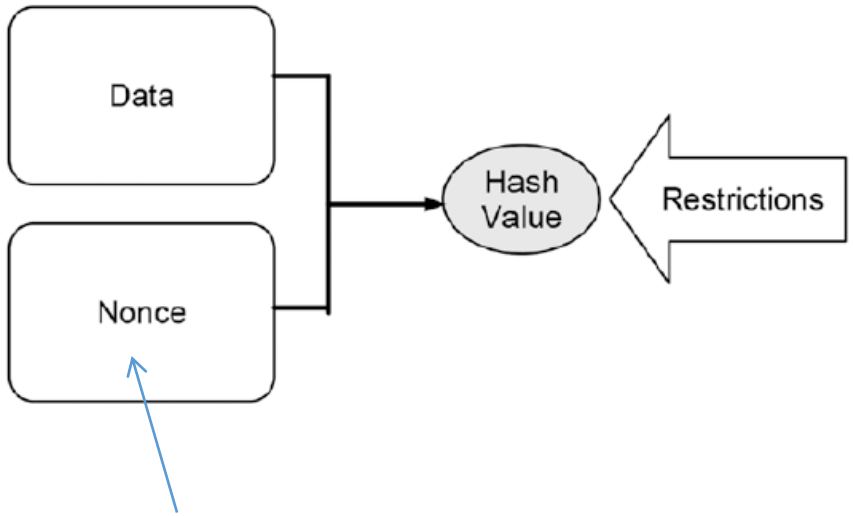
- U praksi pobjeđuje onaj čvor koji riješi kriptografsku zagonetku (tzv. „rudarenje”)
  - Računalno zahtjevan problem
    - kod kriptovalute Bitcoin je potrebno imati znatne procesorske resurse za njeno rješavanje (u prosjeku iz cijele mreže čvorova u 10 min jedan riješi zagonetku, rudarenje troši jako puno el. energije)
  - Težina zagonetke se periodički usklađuje
    - Kod kriptovalute Bitcoin se pokušava prosječno vrijeme do rješenja zagonetke (tj. objave sljedećeg bloka) držati na 10 minuta
  - Trivijalno je provjeriti je li zagonetka riješena
- Zašto bi čvor trošio resurse na rješavanje zagonetke?
  - rudarenje se nagrađuje u kriptovaluti

Struktura podataka blok-lanca



Nepromjenjiva (engl. *immutable*) struktura podataka zbog korištenja kriptografskih funkcija

Primjer rješavanja zagonetke (*Proof of Work*)



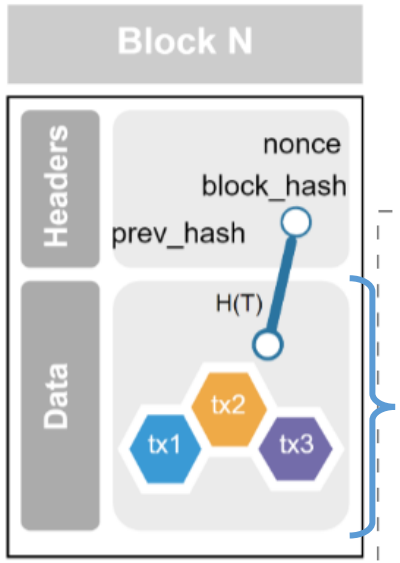
Nonce	Text to Be Hashed	Output
0	Hello World! 0	4EE4B774
1	Hello World! 1	3345B9A3
2	Hello World! 2	72040842
3	Hello World! 3	02307D5F
	...	
613	Hello World! 613	E861901E
614	Hello World! 614	**00068A3C**
615	Hello World! 615	5EB7483F

Traži se nonce koji uz zadanu poruku generira hash vrijednost koja počinje s npr. 3 nule

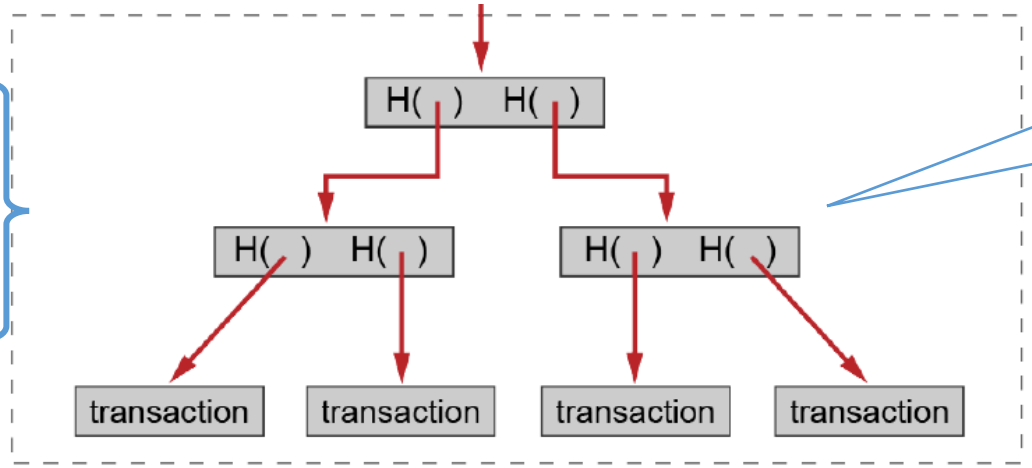
http://www.blockchain-basics.com/HashPuzzle.html

https://demoblockchain.org/block

Kako se zapisuju transakcije u blok?



Za više informacija:
https://www.youtube.com/watch?v=s0fruNfgW30



Transakcije u bloku se zapisuju u posebno stablo (Merkle tree)

This allows for efficiently verifiable proofs that a transaction was included in a block.

The second is internal to each block and is a Merkle Tree of transactions within the blocks.

A blockchain actually contains two different hash structures. The first is a hash chain of blocks that links the different blocks to one another.

Kako u se u načelu izvode transakcije?

Izvor [3]

- *Users interact with the blockchain via a pair of private/public keys. They use their private key to sign their own transactions, and they are addressable on the network via their public key.*
- *Every signed transaction is broadcasted by a user's node to its one-hop peers. The neighboring peers check this incoming transaction is valid before relaying it any further; invalid transactions are discarded.*
- *The transactions that have been collected and validated by the network using the process above during an agreed-upon time interval, are ordered and packaged into a timestamped candidate block. Nodes perform mining. The winning node broadcasts its block in the network.*
- *The nodes verify that the suggested block (a) contains valid transactions, and (b) references via hash the correct previous block on their chain. If yes, the block is added to the chain. If not, the proposed block is discarded. This marks the end of a round.*

Primjer drugih algoritama za konsenzus

- *Proof of Stake*
  - Vjerojatnost da čvor bude izabran za rudarenje sljedećeg bloka ovisi o njegovom ulogu koji u vidu kriptovalute ulaže za taj posao
  - Planira se uvesti u Ethereum
- PBFT (*Practical Byzantine Fault Tolerance*)
  - Koristi se u privatnim DL rješenjima (npr. *Hyperledger*)
  - Čvor koji želi dodati blok postaje leader
  - Koristi three-phase commit protokol za glasanje uz pretpostavku da je manje od trećine čvorova neispravno (potrebno je 3f + 1 ispravnih čvorova da bi se postigao sporazum)
- *Proof of Capacity, Proof of Authority, Proof of Burn*, *Proof of Elapsed Time*

Raspodijeljenost?

Što je raspodijeljeno, podaci ili proces izvođenje transakcija?

- Blockchain je primjer ledgera koji se održava na raspodijeljeni način u mreži čvorova, ali **svaki čvor sadrži repliku podatkovne strukture sa svim transakcijama**!
  - Dakle, blockchain kao struktura podataka NIJE RASPODIJELJEN kao Distributed Hastable u P2P mrežama
- Danas nastaju nove verzije raspodijeljenog ledgera
  - Primjer je IOTA koja se temelji na DAG-u (Directed Acyclic Graph) gdje svaki čvor predstavlja 1 transakciju

Skalabilnost: značajan problem!

- Na dan 05.01.2018.
  - *186.951 pending transactions in the Bitcoin network and*
  - *around 22.473 pending in the Ethereum network*
- Mjeri se *transaction throughput*
  - ne povećava se s povećanjem broja čvorova
- Bitcoin: novi blok se rudari u prosjeku svakih 10 min uz veličinu bloka od 1 MB
  - 3 do 7 transakcija u sekundi
- Ethereum: novi blok se rudari u prosjeku svakih 15 s uz varijabilnu veličinu bloka
  - 7 do 15 transakcija u sekundi

Kako kriptovalute koriste raspodijeljeni *ledger*?

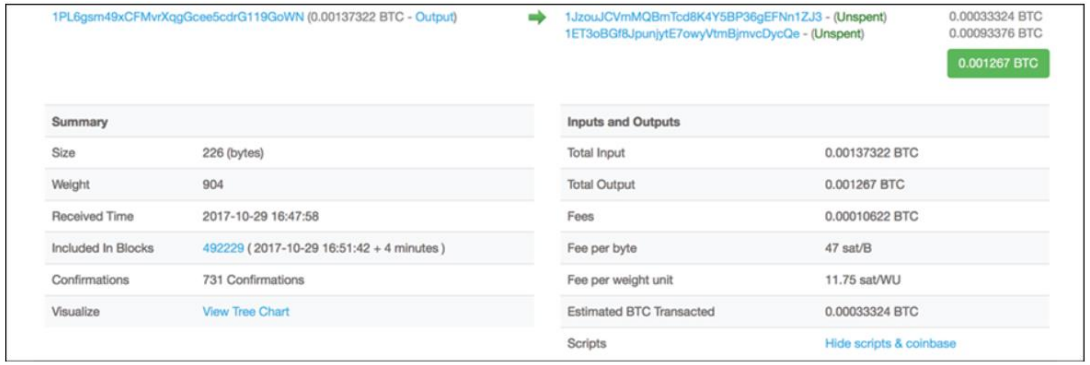
https://coinmarketcap.com/

- Zapisi predstavljaju transakcije između računa (adresa)
- Svaka transakcija mora definirati ulaze novca i njegove izlaze
- Transakcija je ispravna ako ulazi novca (koji su izlazi neke prethodne transakcije) imaju više novca od onog koje treba završiti na izlazima
- Tri problema
  - Krađa novca od drugog korisnika
    - Nemoguća zbog digitalnog potpisa
  - Uskraćivanje usluge
    - Nemoguće zbog raspodijeljenosti
  - Trošenje novca kojeg nema (double-spending problem)
    - Ovaj problem se rješava odbacivanjem neispravnih transakcija i čekanjem na pojavljivanje transakcije u *blockchainu*

Izvor:https://s-media-cache-ak0.pinimg.com/originals/25/d2/46/25d246a383ac7fafbe641d6735a51113.png

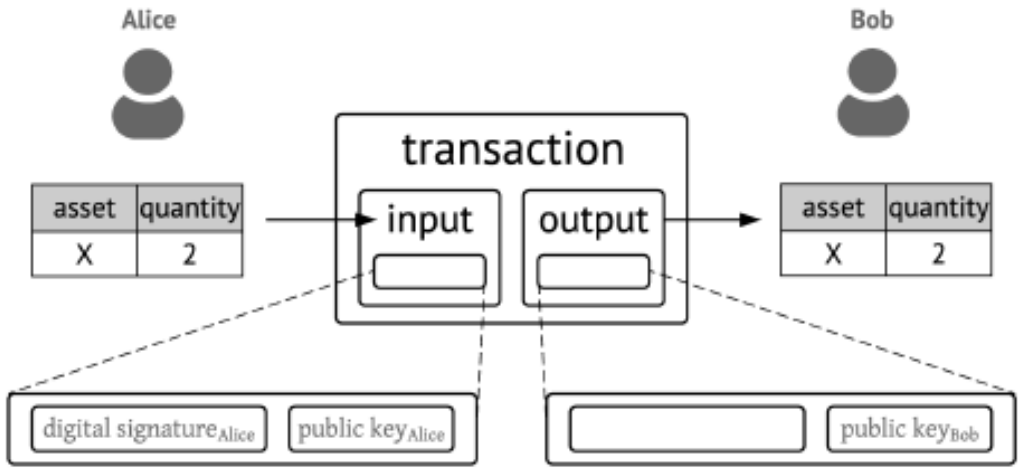
Bitcoin: pojmovi

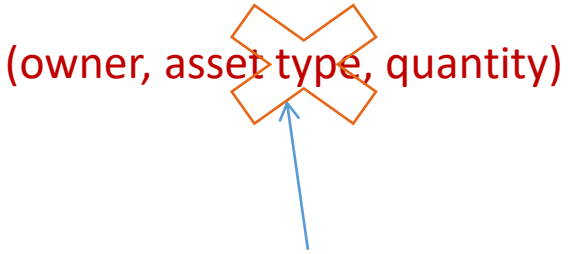
- Bitcoin wallet: sadrži privatni i javni ključ vlasnika te ključeve na transakcije koje na izlazu referenciraju vlasnika walleta
- Kada nekome prebacujete bitcoin – referencirate se na njegov javni ključ
- Bitcoin address: hash nad javnim ključem
- Različite verzije čvorova: full node, miner, simple payment verification (SPV) node (wallet + routing)



Primjer transakcije
Transakcija se smatra potvrđenom kada je iz njenog dodano još 6 blokova

Primjer transakcije u Bitcoinu





- Kako bi prebacila 2 bitcoina Bobu, Alice mora dokazati da je u prethodnim transakcijama ona primila 2 ili više bitcoina (Alice se mora referencirati na prethodne transakcije gdje je ona referencirana u izlazu)
- Svaki čvor sadrži kopiju svih transakcija i provjerava sve transakcije od izvorne!
  Za više informacija: https://www.youtube.com/watch?time_continue=379&v=Lx9zgZCMqXE ili http://www.imponderablethings.com/2013/07/how-bitcoin-works-under-hood.html

Kako izgleda transakcija kod *Bitcoina*?

- Metapodaci kao što su veličina transakcije, broj ulaza i izlaza novca te sažetak transakcije (predstavlja i njen jedinstveni ID)
- Ulazi
  - Jedinstveni ID prethodne transakcije čiji će se izlaz koristiti kao ulaz ove
  - Redni broj izlaza u prethodnoj transakciji koji će se koristiti kao ulaz ove
  - Skripta `scriptSig` u posebnom jeziku Script (*Bitcoin scripting language*)
- Izlazi
  - Vrijednost
  - Skripta `scriptPubKey` u jeziku Script

```
Input:
Previous tx:
f5d8ee39a430901c91a5917b9f2dc19d6d1a0e9cea205b00
9ca73dd04470b9a6
Index: 0
scriptSig:
304502206e21798a42fae0e854281abd38bacd1aeed3ee37
38d9e1446618c4571d10
90db022100e2ac980643b0b82c0e88ffdfec6b64e3e6ba35
e7ba5fdd7d5d6cc8d25c6b241501

Output:
Value: 5000000000
scriptPubKey: OP_DUP OP_HASH160
404371705fa9bd789a2fcd52d2c580b65d35549d
OP_EQUALVERIFY OP_CHECKSIG
```

Javni i privatni ledgeri

Javni (public and permissionless)

ethereum

IOTA

Privatni (private and permissioned)

HYPERLEDGER

svi korisnici su autenticirani, svi čvorovi imaju potrebu rudariti, nema opasnosti za Sybil attack (jedan predstavnik uzima više različitih identiteta), manje mreže do npr. 80 čvorova

Može li DLT podržavati bilo koju aplikaciju?

- *Bitcoinov* jezik *Script* je vrlo jednostavan
  - Namijenjen je obavljanju jednostavnih poslova (npr. provjera ispravnosti transakcije)
  - Temelji se na stogu te ne koristi dodatnu memoriju niti varijable
  - Može se procijeniti koliko će neko izvođenje trajati i koliko će memorije zahtijevati
  - Nije *Turing-complete* jezik (njime se ne mogu izvesti baš sve proizvoljne funkcije)
- Platforma *Ethereum* podržava nekoliko *Turing-complete* jezika (primarni jezik je *Solidity*)
  - Nad njim se može napraviti bilo kakva (smislena) raspodijeljena aplikacija
  - Ethereum je za *blockchain* ono što je univerzalno računalo za namjenska računala

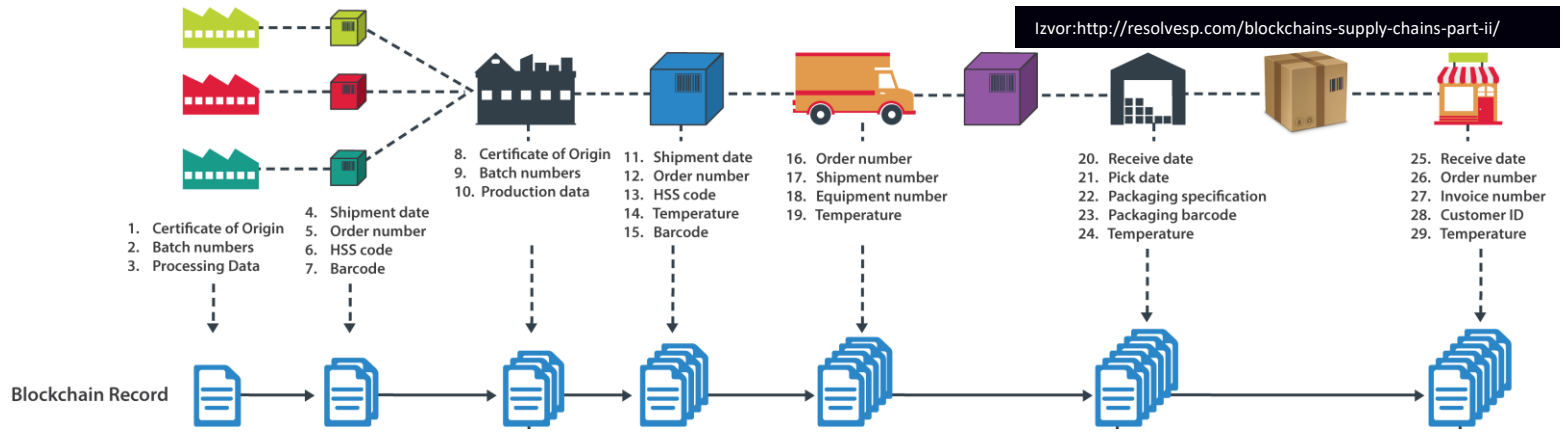
Koje su primjene tehnologije *blockchain?*

- Bankarstvo
- Plaćanja i prijenosi novca
- Kibernetička sigurnost
- Edukacija
- Glasovanje
- Internet stvari (IoT)
- Trgovanje stvarima i dionicama
- Osiguranje
- Zdravstvo
- Upravljanje opskrbnim lancima (sljedivost)
- Donacije
- Masovno financiranje (*crowdfunding*)

Izvor:https://www.cbinsights.com/research/industries-disrupted-blockchain/

Praćenje sljedivosti

- Uobičajeni problemi u prehrambenim opskrbnim lancima
  - Prijevare vezane uz zamjenu, mijenjanje i krivo označavanje hrane
  - Ilegalna proizvodnja hrane
  - Pokvarena hrana
- Korištenjem tehnologije blockchain se čitav lanac opskrbe može digitalno potpisati pa su podaci o lancu opskrbe
  - Djeljivi (*shareable*)
  - Dokazivi (*traceable*)
  - Transparentni (*transparent*)



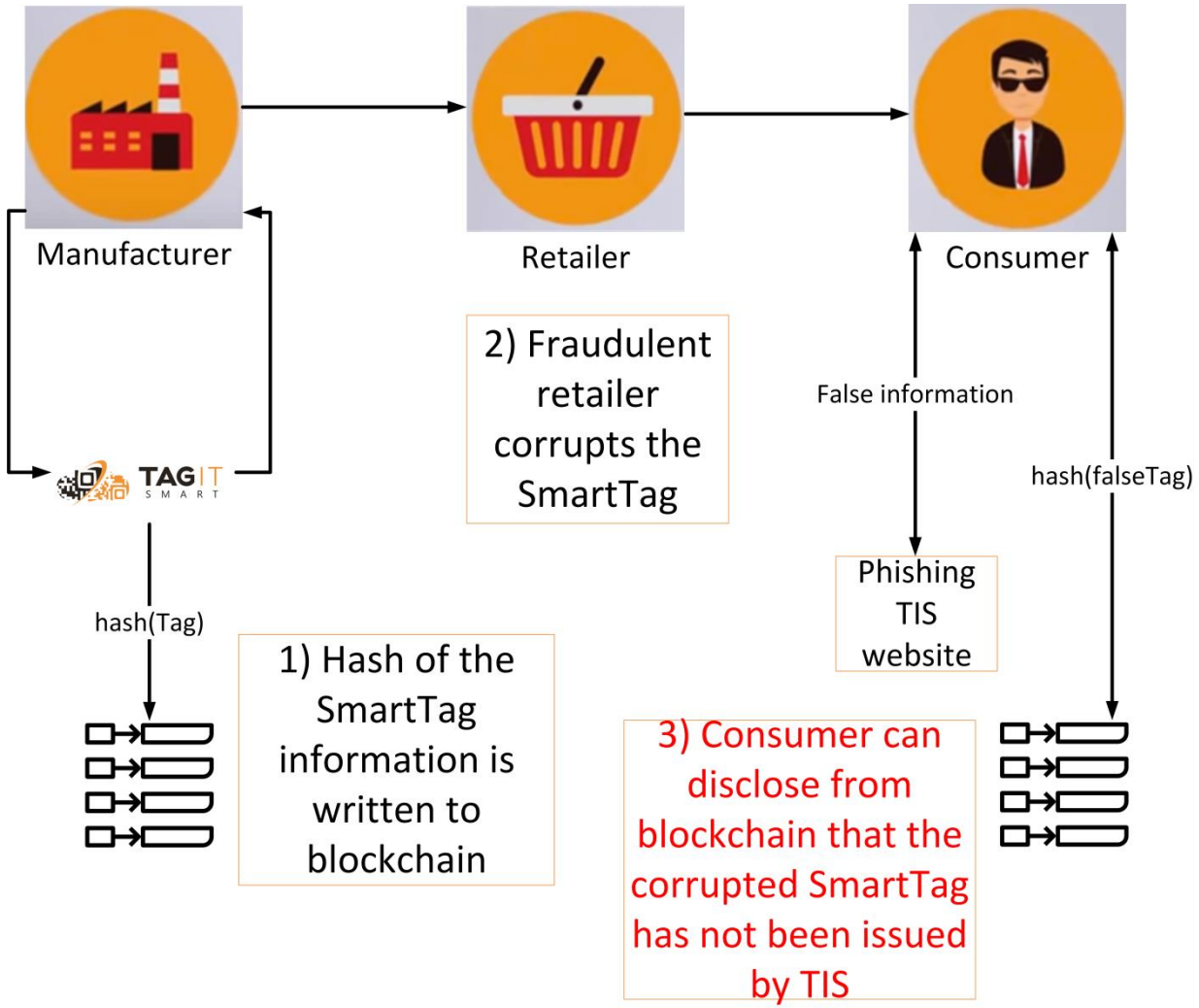
Rješenje razvijeno na Zavodu za telekomunikacije

DL-Tags: *Decentralized, privacy-preserving and verifiable management of Smart Tags*

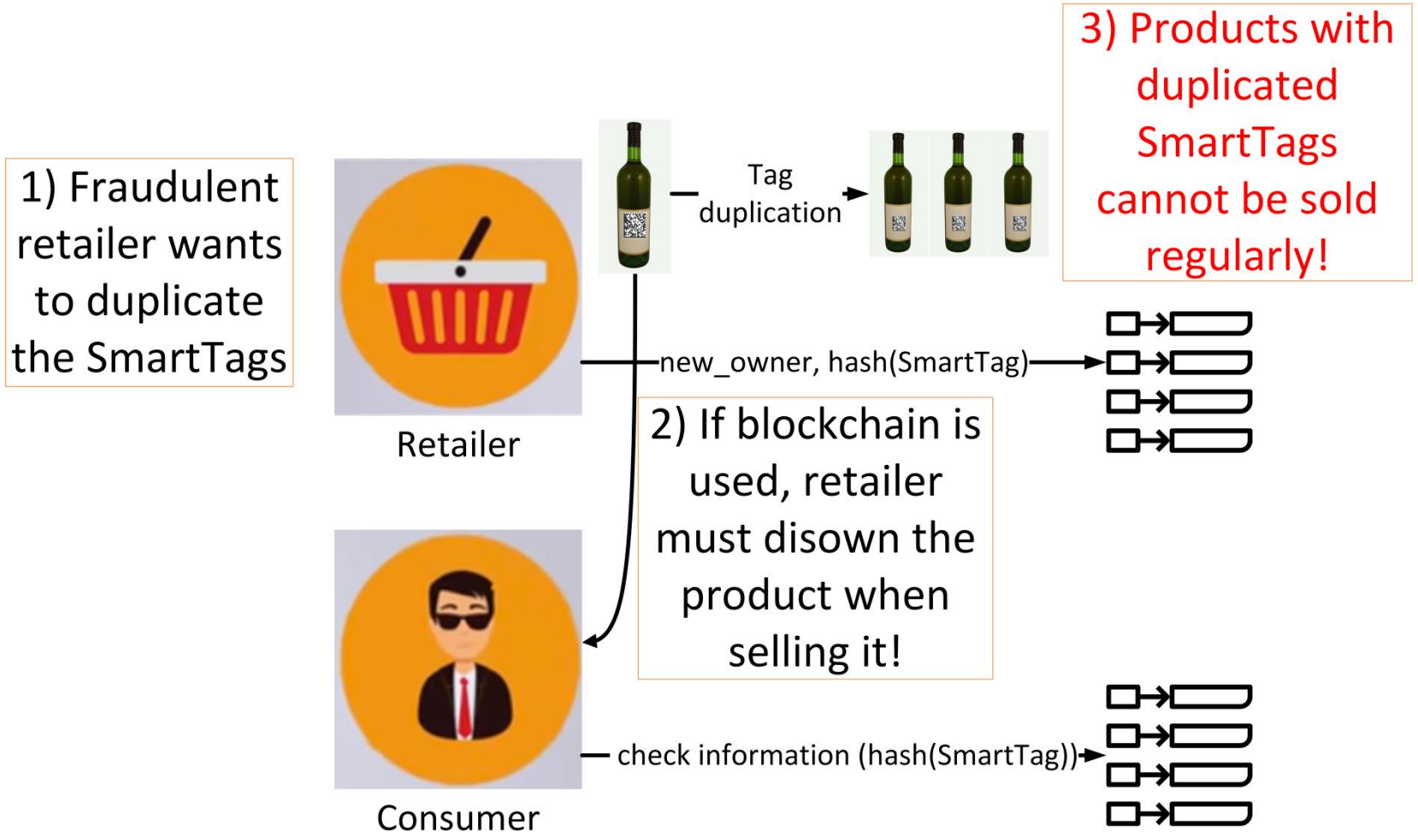
- Distributed Ledger (DL) Technology to track state changes of products labelled by Smart Tags
- DL is a trustless intermediary between the stakeholders
- Involved stakeholders: product owners, TIS platform, eCommerce platform (Magento), customers

- Innovation
  - Decentralized, privacy-preserving and verifiable approach for storing and sharing product-related data, thus ensuring data integrity
  - No need for data storage outside the stakeholders' space

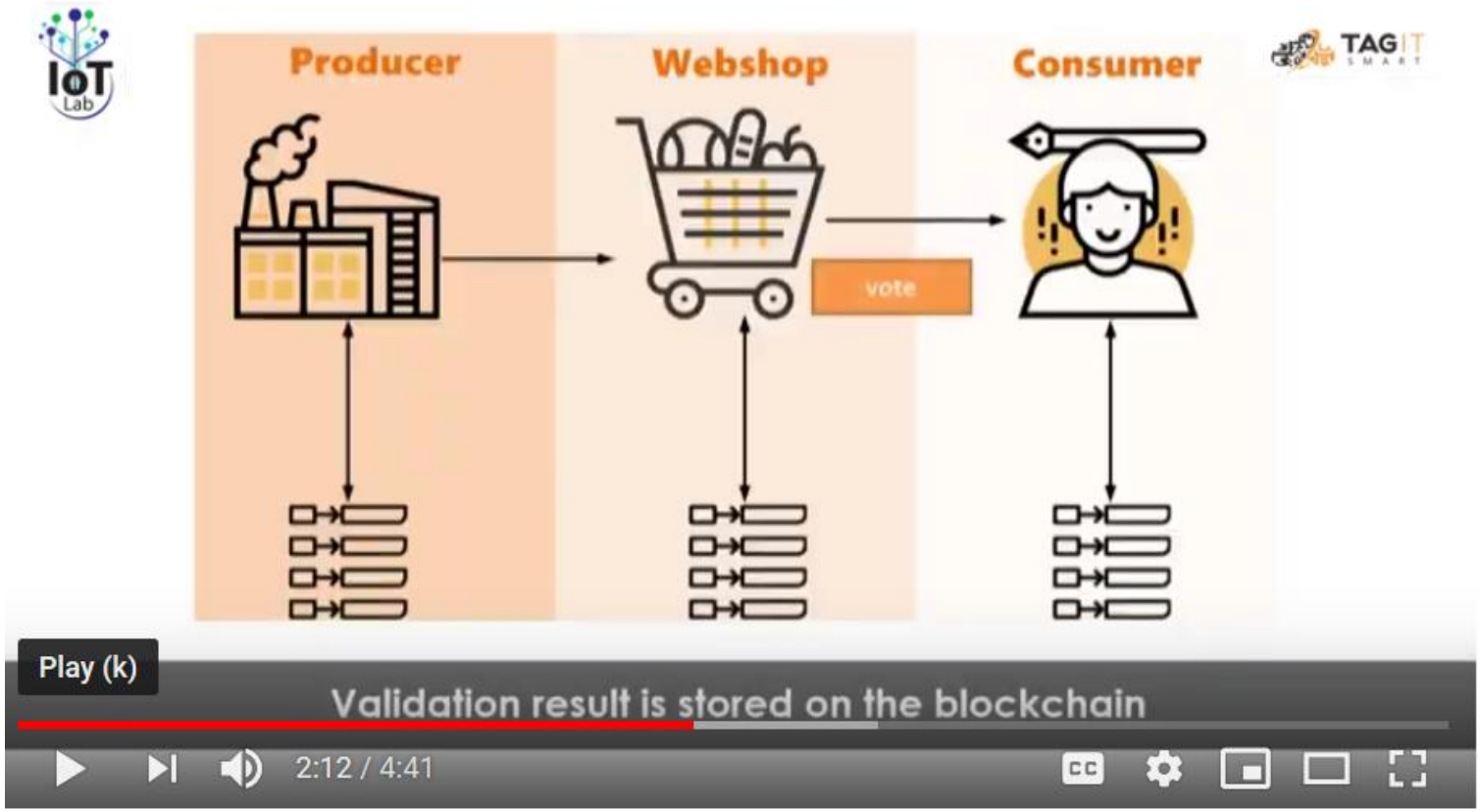
Prevention of Smart Tag corruption



Prevention of Smart Tag duplication



DL-Tags video



https://www.youtube.com/watch?v=JCC98iMCPOs

Ethereum i pametni ugovori

Sadržaj

- Upoznavanje s terminologijom
- Upoznavanje s razvojnim okruženjem
- Pokretanje lokalnog Ethereum čvora
- Upoznavanje s jezikom Solidity
- Izrada vlastitog tokena po ERC20 standard (demo)

Što je *Ethereum*?

- Javna platforma otvorenog koda temeljena na tehnologiji blok-lanca, koristi povezanu kriptovalutu *Ether*
- Podržava pametne ugovore (*smart contracts*)
  - Aplikacije sa stanjem pohranjenim u *blockchainu*
  - Mogu biti u interakciji s ostalim pametnim ugovorima
  - Mogu donositi odluke
  - Mogu prosljeđivati *Ethere* drugima
- Problem s resursima pri izvođenju programa
  - Izvođenje svake instrukcije se plaća
  - Svaka pohrana podatka se plaća

ethereum

Izvor:https://www.ethereum.org/images/logos/ETHEREUM-LOGO_PORTRAIT_Black_small.png

Pametni ugovor

Smart contracts are software programs that live on a blockchain and form the basis of many of the new blockchain applications and schemes. They are essentially automated systems that can provide services in exchange for cryptocurrency. However, because blockchains are not good for storing large amounts of data nor for querying the state of the outside world, they need services that exist off the blockchain to do those things for them.

Izvor: https://spectrum.ieee.org/computing/networks/how-smart-contracts-work

Upoznavanje s terminologijom

- Ether (ETH) – valuta povrh platforme Ethereum
- Ethereum – platforma, raspodijeljena mreža
  - Najmanja jedinica – 1 Wei

Jedinica	Vrijednost u Weima
Kwei (babbage)	1,000 Wei
Mwei (lovelace)	1,000,000 Wei
Gwei (shannon)	1,000,000,000 Wei
microether (szabo)	1,000,000,000,000 Wei
milliether (finney)	1,000,000,000,000,000 Wei
ether	1,000,000,000,000,000,000 Wei : 10^{18}

Upoznavanje s terminologijom

- Pametni ugovor
  - aplikacija koja se izvodi u distribuiranom okruženju
- Solidity
  - jezik kojim pišemo Pametne ugovore
  - postoje i Vyper i LLL
  - prevodi se u EVM bytecode
- EVM
  - Ethereum Virtual Machine
  - svaki čvor u mreži ima mogućnost izvršavanja EVM bytecodea
- Ethereum možemo promatrati kao automat stanja
  - Stanje se mijenja provedbom transakcija

Upoznavanje s terminologijom

- Transakcije se provode onda kada se pronađe novi blok
  - ~ 15 sekundi za blok
- Svaku transakciju koja izaziva operaciju pisanja potrebno je platiti
  - Gas - jedinica kojom plaćamo izvedbu koda na Ethereum platformi
  - Odvojena jedinica od ETH
  - Cijena izvođenja nije volatilna kao cijena ETH
- Gas Limit – maksimalna količina Gasa za transakciju
- Gas Price – količina ETH po jedinici gasa
  - najčešće Gwei

Upoznavanje s razvojnim okruženjem

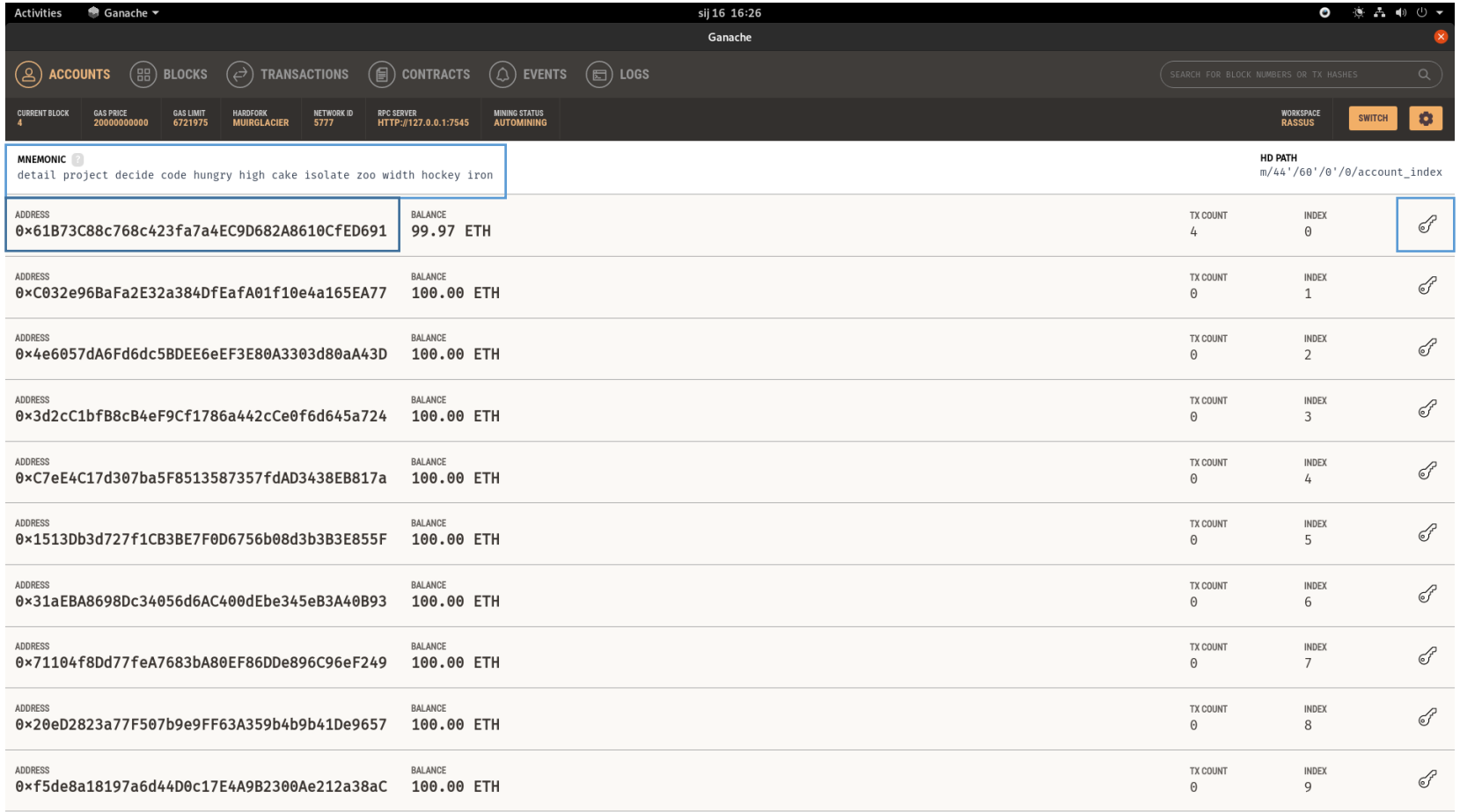
- Editor – Visual Studio Code, solidity ekstenzija
  - https://code.visualstudio.com/
  - https://marketplace.visualstudio.com/items?itemName=JuanBlanco.solidity
- Lokalni Ethereum čvor
  - https://www.trufflesuite.com/ganache
- Razvojni okvir Truffle
  - https://www.trufflesuite.com/

Arhitektura sustava

Lokalni Ethereum čvor

- Ne moramo preuzimati cijelu raspodijeljenu knjigu
- Ne trošimo Ether (barem ne pravi)
- Ne čekamo novi blok
  - transakcija se izvodi u realnom vremenu
  - PoA
- Lako je obrisati lanac i početi isponova
- Opcije:
  - Ganache
  - ganache-cli

Ganache


Activities
Ganache
sij 16 16:26
Ganache
ACCOUNTS
BLOCKS
TRANSACTIONS
CONTRACTS
EVENTS
LOGS
SEARCH FOR BLOCK NUMBERS OR TX HASHES
CURRENT BLOCK 4
GAS PRICE 20000000000
GAS LIMIT 6721975
HARDFORK MUIRGLACIER
NETWORK ID 5777
RPC SERVER HTTP://127.0.0.1:7545
MINING STATUS AUTOMINING
WORKSPACE RASSUS
SWITCH
MNEMONIC
detail project decide code hungry high cake isolate zoo width hockey iron
HD PATH
m/44'/60'/0'/0/account_index
ADDRESS 0x61B73C88c768c423fa7a4EC9D682A8610CfED691 BALANCE 99.97 ETH TX COUNT 4 INDEX 0
ADDRESS 0xC032e96BaFa2E32a384DfEafA01f10e4a165EA77 BALANCE 100.00 ETH TX COUNT 0 INDEX 1
ADDRESS 0x4e6057dA6Fd6dc5BDEE6eEF3E80A3303d80aA43D BALANCE 100.00 ETH TX COUNT 0 INDEX 2
ADDRESS 0x3d2cC1bfB8cB4eF9Cf1786a442cCe0f6d645a724 BALANCE 100.00 ETH TX COUNT 0 INDEX 3
ADDRESS 0xC7eE4C17d307ba5F8513587357fdAD3438EB817a BALANCE 100.00 ETH TX COUNT 0 INDEX 4
ADDRESS 0x1513Db3d727f1CB3BE7F0D6756b08d3b3B3E855F BALANCE 100.00 ETH TX COUNT 0 INDEX 5
ADDRESS 0x31aEBA8698Dc34056d6AC400dEbe345eB3A40B93 BALANCE 100.00 ETH TX COUNT 0 INDEX 6
ADDRESS 0x71104f8Dd77feA7683bA80EF86DDe896C96eF249 BALANCE 100.00 ETH TX COUNT 0 INDEX 7
ADDRESS 0x20eD2823a77F507b9e9FF63A359b4b9b41De9657 BALANCE 100.00 ETH TX COUNT 0 INDEX 8
ADDRESS 0xf5de8a18197a6d44D0c17E4A9B2300Ae212a38aC BALANCE 100.00 ETH TX COUNT 0 INDEX 9

Komunikacija s čvorom - Json RPC

- Json
  - format za razmjenu podataka, opisuje brojeve, stringove, liste, i mape.
- Json RPC
  - stateless, protokol za poziv udaljene metode (RPC). Neovisan o transportnoj metodi, možemo ga koristiti putem socketa, preko HTTP-a i slično.
  - Primjer poziva:

```
#!/usr/bin/env bash
curl -H "Content-Type: application/json" -X POST --data
'{"id":1337,"jsonrpc":"2.0","method":"evm_mine","params":[1231006505000]}'
 http://localhost:7545
```

Metamask

- Ethereum wallet
  - wallet u sebi sprema privatne ključeve
  - često nudi neke dodatne funkcionalnosti – digitalno potpisivanje
- Metamask
  - Ethereum wallet u pregledniku
  - Interakcija s blockchainom u pregledniku
  - https://metamask.io/

ERC20 token

- Ethereum Improvement Proposals
  - https://eips.ethereum.org/EIPS/eip-20
- Valuta povrh Ethereuma (nije ETH)
  - ICO boom 2017
- Neke od funkcija:
  - function name() public view returns (string)
  - function symbol() public view returns (string)
  - function totalSupply() public view returns (uint256)
  - function balanceOf(address _owner) public view returns (uint256 balance)
  - function transfer(address _to, uint256 _value) public returns (bool success)

Literatura

1. K. Pripužić: Blockchain – sigurnost, sljedivost, predavanje na konferenciji RFID 2017.
2. M. E. Peck: Blockchains: How They Work and Why They'll Change the World, IEEE Spectrum, Sept 2017. https://spectrum.ieee.org/static/special-report-blockchain-world
3. K. Christidis and M. Devetsikiotis, "Blockchains and Smart Contracts for the Internet of Things," in *IEEE Access*, vol. 4, pp. 2292-2303, 2016.
4. S. Nakamoto: "Bitcoin: A peer-to-peer electronic cash system", 2008.
5. V. Buterin: "Ethereum white paper: A Next-Generation Smart Contract and Decentralized Application Platform", 2017.
6. Dinh, Tien Tuan Anh, et al. "Untangling Blockchain: A Data Processing View of Blockchain Systems." arXiv preprint arXiv:1708.05665 (2017).