Kriptovalute, pametne pogodbe in drugi primeri uporabe

Kriptovalute, pametne pogodbe in drugi primeri uporabe

- Recap
  - Decentralized P2P networ
  - Trust layer with no SPOF
- Ethereum vs Bitcoin
  - Bitcoin nodes verify transactions (global payment system)
  - Ethereum nodes verify computation (global computing system)
- Pametne pogodbe
  - Properties
  - How do they work
  - Security risks
- Crypto žetoni
  - ERC20
  - Erc 721
  - ERC 1238
- Drugi primeri uporabe
  - Fundrasing (IPO)
  - Filecoin
  - Digital identity
  - Supply chain management
  - IoT
  - Insurance
  - Gaming and collectables
  - Tokenizing real assets
  - 0x Project
  - Reward Systems
  - Smart B/L
  - Loki
- Building the internet of value
  - Programmable money
  - M2M payment network
- Scalability concerns

Osvežitev

- Sensorship resistance
  - Pseudonimnost (javni ključ)
- Transparentnost
  - Vidne transakcije (Bitcoin, Ethereum, etc..)
  - Skrite transakcije (Monero)
- Brez potrebe po zaupanju (trustless)
  - Poslovanje med dvema strankama ne zahteva zaupanja med njima
  - Zaupanje vliva sistem skozi matemtično preverljiva dejstva
- Decentralizirano
  - Vozlišča v sistemu so "vsa" enakopravna
  - Sistem nima ene točke odpovedi

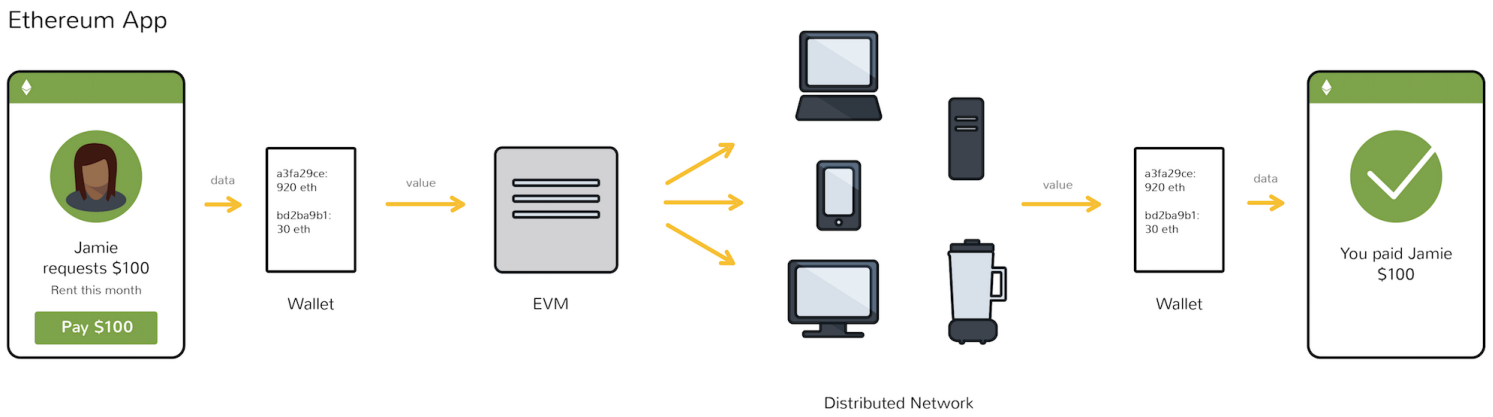
Ethereum vs Bitcoin

- Bitcoin kot digitalno zlato sistem za neposreden prenos vrednosti v digitalni obliki
  - Relativno počasen
  - Digitalno zlato
  - Ohranja vrednost zaradi omejene zaloge
  - Decentralizirana ura
  - Programabilen denar
  - UTXO model

- Ethereum kot svetovni računalnik na katerem živijo decentralizirane aplikacije
  - Omogoča preverljivo izvajanje programov
    - Pogodba je denarnica (javen ključ) z dodatkom programa, ki diktira njeno obnašanje
    - Vsa vozlišča izvedejo pogodbo in se strinjajo z rezultatom
    - Pogodbo izvedemo z transakcijo
  - Služi kot podatkovna baza aplikacijam
    - Hrmba informacij v verigi je relativno draga
  - Programabilen denar
    - Pogodbe lahko kot rezultat spreminjajo stanja denarnice
  - State model

Pametne pogodbe, kako delujejo?

- Neodvisnost od vhoda
  - Izračun ne more biti odvisen od vhoda, ki se spreminja
- Determinizem
  - Zagotavlja preverljivost rezultatov
- Okoren programski jezik, vendar popoln po Turingu
  - Visokonivojski jezik (Solidity)
  - Prevedba v binarno obliko (Bytcode)
  - Virtualni stroj (EVM)



Pametne pogodbe, kaj so?

- Program med dvema ali več osebama, ki definira pravila s katerimi se vsi podpisniki strinjajo
- Ob izvedbi, pravila določajo prehod v novo stanje (samodejno)
- Decentraliziran avtomatizem, ki preverja in uverljavlja pogoje pogodbe
- Omogoča prenos česarkoli vključno z denarjem, delnicami in lastnino popolnoma neposredno
- Pogodbe nadomeščajo vlogo sodišča

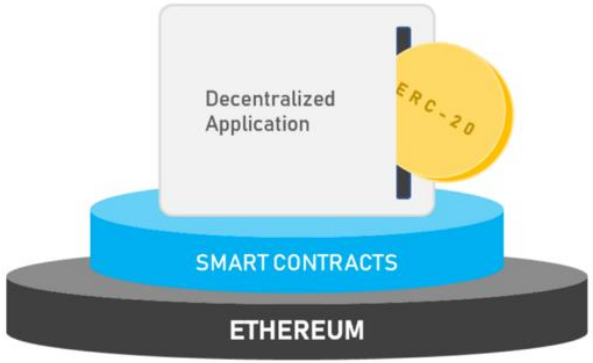
Pametne pogodbe, lastnosti

- Samo-preveljivost
- Samodejna izvedba (ne klic, temveč razsodba)
- Brez možnosti prirejanja (temper-proof)
- Cenovno ugodne (v primerjavi z tradicionalnimi pogodbami)
- Varne (vrnost zagotavlja veriženje blokov)
- Natančne (logična in deterministična pravila)
- Hitre

Varne?

- Varne, vendar ne odporne na napake uporabnika
  - Nekaterih pogodb ni mogoče spreminjati
  - Napak ni možno odpraviti, če je pogodba že podpisana
- Primeri kritičnih uporabniških napak
  - Re-entrancy
    - Pogodbe lahko prožijo klice zunanjih pogodb
    - Klic zunanje pogodbe je mogoče preusmeriti in prisiliti ponoven klic osnovne pogodbe z drugimi parametri
  - Armitmetična prelivanja
    - Če pogodba ne preverja uporabniškega vhoda lahko spreminjamo vrednosti spremenljivk
  - Prevzeta vidljivost funkcij
    - Nekatere funkcije pogodbe lahko izvede samo avtor, vendar mora to jasno definirati
  - Slaba naključnost
    - Pogodbe so deterministične, najključnosti ni
    - Zunanji generator naključnih števil (igre na srečo) je potencialna varnostna luknja

Žetoni



- Najbolj razširjena uporaba pogodb
- Virtualni žetoni znotraj Ethereum verige so pametne pogodbe, ki omogoča funkcionalnost žetona
- Običajno so žetoni valuta znotraj decentralizirane aplikacije
- Nekaj primerov uporabe
  - Decentralizirano upravljanje (glasovanje)
  - Nagrajevanje uporabnikov
  - Spodbuda
  - Lastništvo
  - Plačilo za storitev
  - ESCROW
  - ICO
  - Itd.

Žetoni, standardi

- Začetki so bili kaotični
  - Vsak žeton je bil malenkost drugačen
- Standardi ERC (analogno RFC)
  - Ethereum request for comments
  - Opisujejo množico funkcionalnosti, ki jih mora pogodba implementirati po standardu
  - Standardizacija omogoča gradnjo protokolov, in ostalih pogodb
  - Pogodbe (protokoli) lahko upravljajo z poljubnim žetonom, ki sledi standardu
  - Vsak ERC standard je jasno definiran in uporaben za specifičen namen
  - Standardi se gradijo in dodajajo

Kako do novega standarda? Kdo upravlja?

- Odprtokoden projekt, kdorkoli lahko prispeva
  - Prispevki pri nadgradnji programske opreme vozlišč, algoritma za rudarjenje, itd.
  - Ethereum fundacija skrbi za konsistenco in integriteto osnovnega nivoja
- EIP (Ethereum improvement proposal) proces
  - Predlogi za izboljšave (https://eips.ethereum.org/)
  - Predlogi za izboljšave so kategorizirani:
    - Core
    - Networking
    - Interface
    - ERC
    - Meta
    - Informational
  - Predlogi so javni in predmet diskusije
  - Skozi diskusijo in podporo javnosti prehajajo v sprejet standard

Ostali standardi

- ERC-20
  - Predlagal Vitalik leta 2015
  - Enostaven vmesnik za ustvarjanje žetonov, ki so uporabni znotraj decentralizirane aplikacije (DApp)
  - Vsak lahko naredi svoj ERC20 žeton
  - Najbolj uporabljen standard za zbiranje sredstev (ICO)
- ERC-721
  - Standard za ne-zamenljive žetone
  - Žetone je moč razlikovati in enolično določiti
  - Uporaben za predstavljanje lastništva sredstev
  - Omogoča digitalizacijo realni sredstev (nepremičnin, delnic, itd.)
  - Predstavlja lastništvo virtualnih sredstev (zbirateljstvo,

Katere standarde poznamo?

- ERC-223
  - Izboljšava ERC-20
  - Rešuje težave pri izgubo žetonov v primeru, da jih pomotoma pošljemo napačni pogodbi
  - Standard je sprejet, vendar trenutno še ni konkretne implementacije
- ERC-777
  - Zmanjšuje trenje pri interakciji z ERC-20 pogodbami
  - Pošiljanje ERC-20 kovancev zahteva 2 transakciji, medtem ko ERC-777 samo 1
- ERC-884
  - Predlagan po sprejemu zakonodaje (ZDA), ki dopušča spremljanje delniških registrov na verigi blokov
  - Omogoča spremljanje delnic v skladu z zakonodajo
- ERC-1337
  - Podpisovanje pogodb, ki omogočajo naročnine plačljivih storitev
  - Stranke lahko od pogodbe odstopijo kadarkoli, pravila določi pogodba

ERC20


Total supply
Limit reached
STOP
Transfer from
ERC20
Balance of
23
0x73295d3....
Approve
Transfer
ACCEPTED
Allowance

Primeri uporabe - splošno

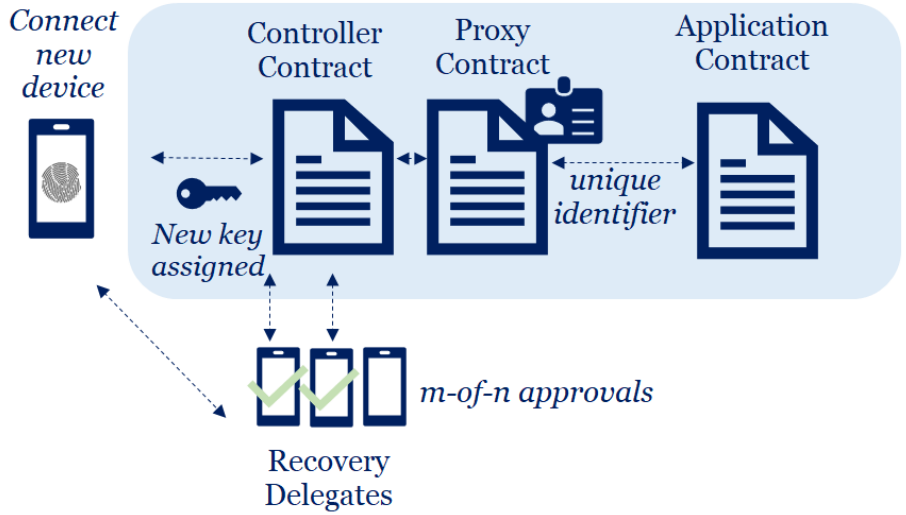
- Vsi poslovni procesi, ki temeljijo na posredniku, ki v verigi vrednosti ne doprinese ničesar razen zaupanja, varnosti, zavarovanja,…
- Delitev neizkoriščenih resursov v zameno za plačilo (žeton)
- Preprečevanje ponarejanja
- Vodenje lastništva
- Globalna trgovina brez potrebe po infrastrukturi
- Sledenje
- Lastništvo nad osebnimi podatki
- ICO

ICO

- ICO (Initial Coin Offering)
- Zbiranje začetnega kapitala za podjetja
- Nakazilo ETH kovancev na pogodbo nam vrne sorazmerno število žetonov, ki bodo običajno imeli funkcijo v platformi, ki jo podjetje razvija
- Špekulativna investicija
- Velik potencial za start-up
- Tvegana investicija zaradi pseudonimnosti in ne-reguliranega trga

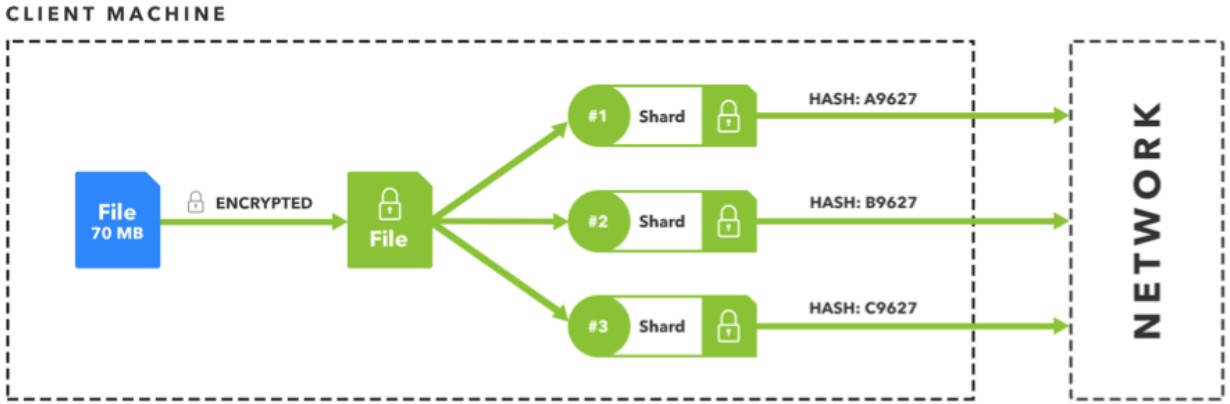
Digitalna identiteta

- Zunanja verifikacija (KYC, AML, etc..) v obliki preroka (Oracles)
- Podatki se razpršijo (preverljivost) in zapišejo v verigo
- Pogodbe omogočajo verifikacijo podatkov (identitete česarkoli)
- Pogodbe definirajo kako verifikacija deluje
  - Javna
  - Z dovoljenjem
  - Enkratna
  - Večkratna
  - Časovno omejena
- Uporaba za verifikacijo izdanih dokumentov
  - Univerza Cagliari (Italija) bo hranila identiteto diplom na Ethereum omrežju
- Microsoft digital identity (Bitcoin), TheKey, Civic, SelfKey, itd..



Hramba podatkov

- Decentralizirana hramba podatkov
- Ponudniki prejmejo nagrado glede na količino podatkov, ki jih hranijo
- Uporabniki plačajo glede na količino podatkov, ki jih hranijo
- Plačila diktira pametna pogodba
- Boljši izkoristek neizkoriščenega prostora na strežnikih
- Podatke varuje kriptografija, samo lastnik ima vpogled v vsebino
- Vozlišča v omrežju hranijo kose datotek (ne celotne datoteke)
- Projekti:
  - StorJ
  - FileCoin
  - SiaCoin
  - Swarm



Internet stvari (IoT)

- Omrežje naprav opremljenih s senzorji (meritve, stanja)
- Naprav glede na meritve prožijo aktuatorje
- Preverljivost
- Varnost
- Avtomatizacija
- Optimizacija

Upravljanje dobavne verige

- Beleženje količine in prenosa dobrin po verigi (palete, kontenjerji)
- Sledenje naročilom, spremembam naročil, obveščenje o spremembah pri trgovini oziroma dokumentaciji
  - Sledenje paketom v realnem času
  - Logistična optimizacija
- Dodeljevanje in preverjanje certifikatov oziroma lastnosti fizičnim produktom
  - Preverjanje avtentičnosti, kvalitete, sestavin produkta, itd..
- Povezovanje fizičnih dobrin z serijskimi številkami, bar kodami, digitalnimi identifikatorji kot naprimer RFID
  - Avtomatizirano vodenje od začetka do konca življenskega cikla produktov
  - Potimizacija proizvodnih procesov
- Deljenje informacij o proizvodnih processih, sestavi, dostavi in vzdrževanju produkta med dobavitelji, prodajalci in končnimi uporabniki
  - Preverljive knjige servisov
  - Optimizacija storitev

Privacy perservation (zasebnost)

- Ohranimo lastništvo nad svojimi podatki
- Dovolimo dostop do podatkov po lastni izbiri
- Ne dovolimo kopiranje podatkov
- ZK-SNARKS
- Privacy perserving computation
- Umetna inteligenca in Blockchain

M2M payments

- IoT
  - fizični nivo
  - naprave tvorijo omrežje
- Relacije
  - pravila med napravami opisujejo in diktirajo pametne pogodbe.
- Plačila
  - Mikrotransakcije in nano transakcije med napravami
  - Uporaba x časa stroja X lahko s pomočjo pogodbe zamenjamo za y časa na stroju Y
- Ideja
  - Tovarne kot storitev
  - Samodejna optimalna učinkovitost (finančna)
  - Industrja 4.0

Igre in zbirateljstvo

- Digtalne dobrine lahko predstavimo z žeton
- V igrah zbiramo virtualne valute in dobrine, katerih funkcija je omejena na igro
- Standard ERC-721 za unikatno določanje posameznega izdelka
- Sledenje standardu omogoča trgovanje žetonov na borzah
  - 0x Protocol, Kyber Network
- Globalna ekonomija med igrami
  - Enjin, Matic
- Trgovanje med zbiratelji
  - CryptoKitties

Predstavitev fizičnih dobrin z žetoni(tokenizing real assets)

- Globalna digitalna ekonomija za fizične dobrine
- Preko geografskih omejitev
- Prodaja nepremičnin
  - Ritzy Aspen Hotel
- Solastništvo premičnin, neprimičnin in podjetji
- Platforme za deljenje dobička skozi lastništvo
  - Atlant

Decentralizirane borze (0xProject)

- Množica pametnih pogodb, ki omogoča popolnoma neposredno menjavo žetonov
- Ustvarjalec (maker)
  - Pripravi seznam pogojev menjave po specifikaciji 0x protokla
  - Svojo denarnico (public key) vnese kot prodajalca
  - Podpiše celotn seznam z svojim privatnim ključem
  - Rezultat doda na konec seznama za preverljivost
- Odjemalec (taker)
  - Od koderkoli prejme seznam iz katerega razbere pogoje
  - Če se z pogoji strinja kot kupca vnese svojo denarnico (public key)
  - Podpiše z privatnim ključem in rezultat doda na seznam
  - Pošlje seznam pametni pogodbi
- Pogodba
  - Preveri podpise in stanje na denarnicah obeh
  - Izvede menjavo
  - Podpira ERC-20, ERC-721, ERC-1155
- Relayers

Upravljanje - Governance

- Žetone se uporavlja za glasovanje
- Glasuje se o smeri razvoja odprtokodnih protokolov
- Glasuje se o sproščanju sredstev organizaciji, ki skrbi za razvoj in raziskovanje
- Problemi kupovanja glasov
- Glasovanje predstavnikov, ki upravljajo konsens (dPoS, i.e. EoS)
- DAO (decentralized autonmous organizations)

Sistemi nadgrajevanja (Brave Browser)

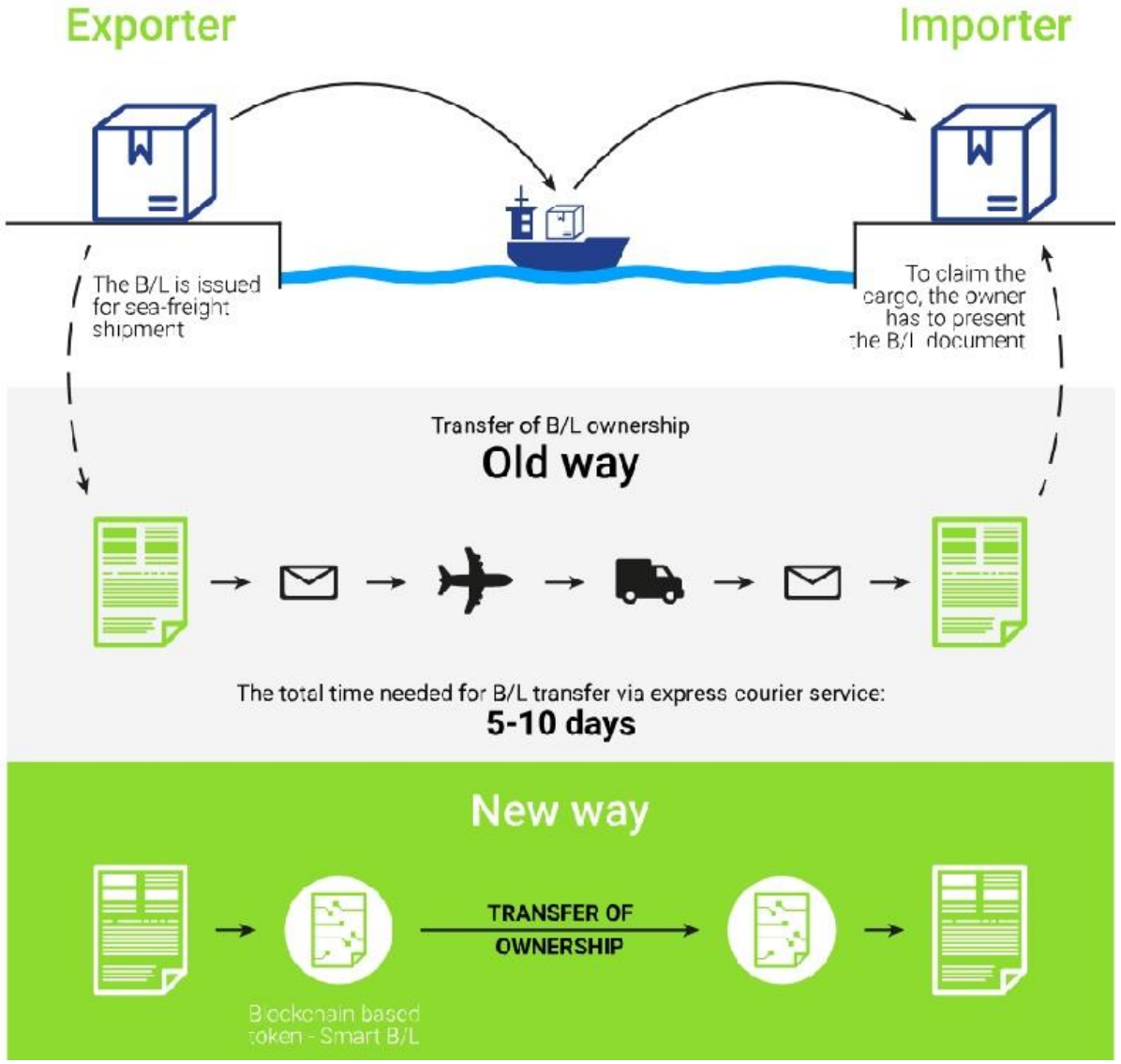
- Uporabnik odloča o deljenju podatkov
- Uporabnik je nagrajen za ogled oglasov
- Nagrajevanje tistih, ki si to zaslužijo (samodejno ali ročno)

- Marketing je bolj efektiven
- Nima negativnega vpliva
- Ceneje (ni posrednika)

- Velik "network effect".

Smart B/L (CargoX)

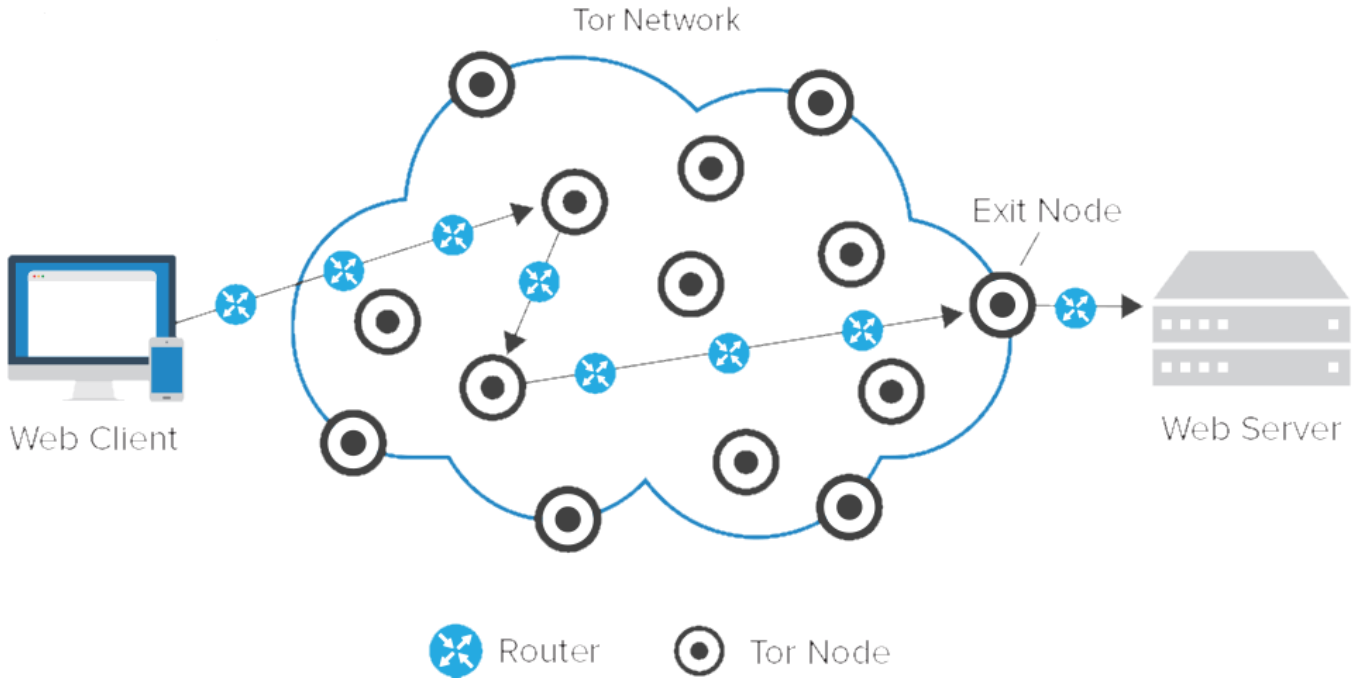
- Ni potrebe po zaupanju
- Ne potrebuje zavarovanja (ESCROW)
- Nižji stroški
- Digitalni dokumenti so preverljivo ne spremeni
- Pohitritev in optimizacija procesa



Zasebno brskanje (Loki)

- Omrežje ToR
- Anonimnost pri uporabi Interneta
- Nesledljivost
- Ni odporen na Sybil napade

- Rešitev: zastavljanje žetonov
- Plačevanje po prometu



Zavarovalništvo

- Zavarovalništvo kot pametna pogodba
- Za enostavne, objektivne in enostavno peverljive stvari
- Zelo efektivno in hitro
- Brez nepotrebne birokracije in postopkov
- Kako razsodimo?
  - Tako, da odločitve sprejemamo na preveljivih dejstvih
    - Zavarovanje pred sušo v Gani, Keniji in Ugandi
    - Po 7 dneh brez padavin, pametna pogodba prične z nakazili sredstev
  - Orakli (decentralizirana omrežja, ki odgovarjajo na vprašanja z resnico
    - Lahko so programski ali fizični
    - Odgovarjajo resnico z neko mero garancije
    - Intel Software Guarded Extensions (SGX)

DeFi

- Odprtokodnost in interoperabilnost
- Dostopnost finančnih inštrumentov
- Finančna transparentnost
- Stabilni kovanci (predstavljajo FIAT valute)
  - MakerDAO, decentraliziran stabilen kovanec
- kriptovalute kot zavarovanje
  - V primeru ne plačila
- Krediti, ki izplačujejo FIAT(DAI)
  - Posojanje izplačano v kritpovaluti, ki je stabilna
  - Zavarovanje v kriptovaluti
- Delujoči primeri:
  - ETHLend
  - Dharma
  - CoinLoan
  - Salt

Internet vrednosti

- Kripto valute kot nov sloj internet protokola
- Resnično globalna ekonomija
- Ogromen potencial za nerazvite države, kjer ljudje nimajo dostopa do finančnih ustanov
- Industrija 4.0
- Zelo učinkovita ekonomija
- Za enostavne posle ni potrebe po sodišču (pametna pogodba)

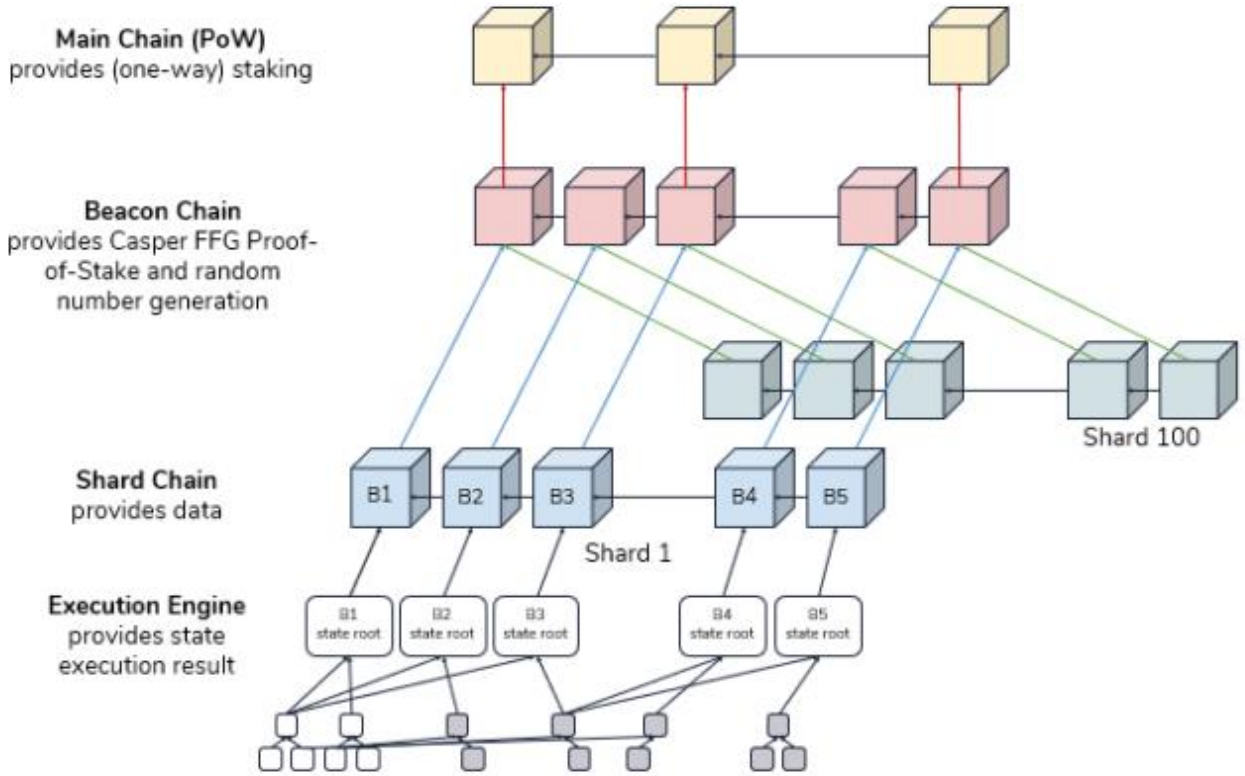
Skalabilnost

- Bitcoin: 3 transakcije na sekundo
- Ethereum 20 transakcij na sekundo
- Globalna ekonomija ?

- Kje je težava?
  - Velikost blokov
  - Konsenz
  - Ekonomska finalnost

Ethereum 2.0

- Casper FFG (PoS)
  - Validatorji
  - Hard-slash
  - VRF, VDF
- Sharded Chain
  - Periodični posnetki
  - Lokalne transakcije so hitre
  - Transakcij ne vpisujemo v glavno verigo
- Glavna veriga
  - Zmanjšana poraba prostora
  - Obdeluje samo spore
  - Vrhovno sodišče
  - Veriga zaupanja



Vprašanja