OMREŽJA IN PROTOKOLI KRIPTO VALUT

dr. Urban Sedlar
urban.sedlar@fe.uni-lj.si

Vsebina

- Tradicionalni plačilni sistemi
  - Kratka zgodovina
  - Slabosti
- Sodobne kriptografske valute
  - Nastanek
  - Poglavitne prednosti
- Tehnološke osnove
  - Kje in kako beležimo transakcije
  - Kakšno identiteto uporabljamo
  - Kako poteka nakazilo
  - Kako nastane nov denar
- Nekaj praktičnih vidikov
  - In primerov aplikacij

TRADICIONALNI PLAČILNI SISTEMI

Tradicionalni plačilni sistemi

- Blagovna menjava
  - Zamenjamo eno stvar za drugo
  - Številne težave
    - Kaj če druga oseba noče našega blaga? (obojestransko sovpadanje potreb)
    - Kaj če menjava ne more biti istočasna?
    - Kdo določa vrednost?
- Pojav menjalnih sredstev (primitiven denar)
  - Menjalna sredstva morajo imeti več lastnosti
    - redkost (količinska omejenost)
    - deljivost, prenosljivost, trajnost, prepoznavnost
  - Tipičen primer: zlato, srebro
- Standardiziran denar
  - Kovanci (najprej iz srebra, zlata)
  - Bankovci
    - Prvotno papir, ki je služil kot dokaz imetništva zlata v banki

Slabosti klasičnega denarja

- Pri vseh fizičnih oblikah denarja
  - Enostavna kraja
  - Ponarejanje
  - Niso možna takojšnja plačila na daljavo
- Z zakonitimi plačilnimi sredstvi upravljajo vlade
  - (ang. legal tender)
  - Takšna valuta se pogosto imenuje “fiat valuta”
  - Centraliziran nadzor
  - Tiskanje denarja po potrebi → inflacija in hiperinflacija!

Pojav bank in elektronskega denarja

- Banke prvotno namenjene hrambi denarja
- Danes
  - Zaračunavajo za vodenje računa in za transakcije
  - Omejujejo dostop do denarja (primer Grčije, ali vaše banke po 17h)
  - Banka lahko tudi propade
- Elektronski denar: transakcijski računi, kreditne kartice, in internetna podjetja (npr. PayPal)
  - Denar postane samo še številka na računu
  - Transakcije so lahko brezgotovinske
  - Centralna avtoriteta preverja, da ne pride do napačne uporabe

- Pri vseh oblikah klasičnega denarja moramo nekomu zaupati
  - Državi, banki, podjetju—pogosto celo vsem hkrati
  - Zgodovinsko gledano: kdor je imel (nenadzorovan) dostop do denarja, je običajno z njim pobegnil

KRIPTOGRAFSKE VALUTE

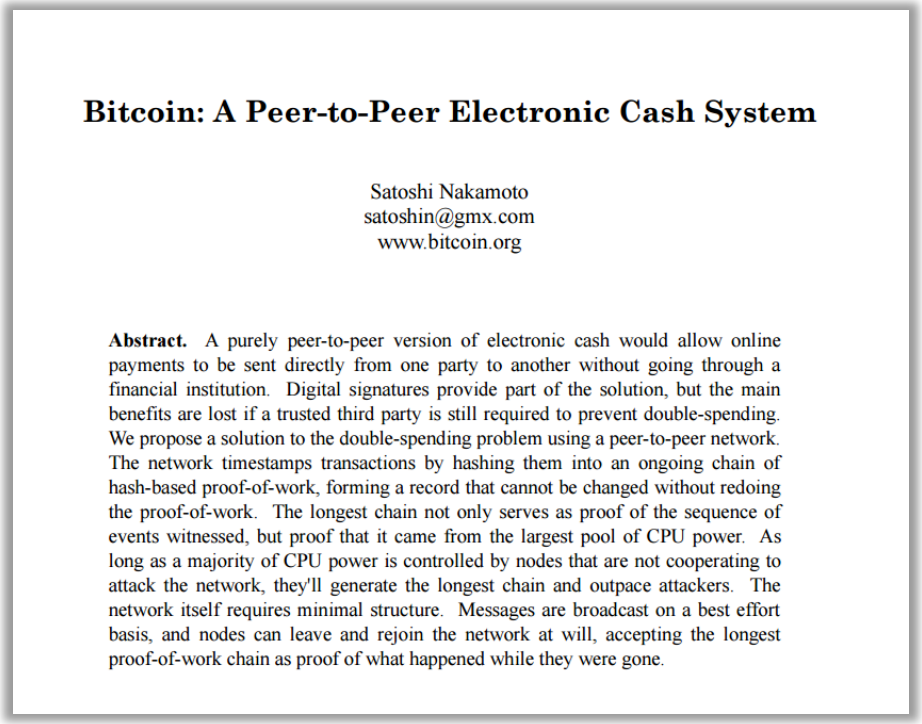
Enoten protokol za prenos vrednosti

Ključne prednosti kripto valut

- Decentraliziranost
  - Ni centralne avtoritete
  - Vsi uporabniki so enakopravni
    - Podobno kot pri BitTorrentu
- Potrebo po zaupanju določeni avtoriteti nadomestimo z matematiko (kriptografijo)
  - Digitalni podpis
  - Zgoščevalne funkcije
- Kriptografske valute na inovativen način rešujejo problem zaupanja in soglasja
  - Valuta je samo prva aplikacija teh mehanizmov!

Bitcoin

- Prvi primer decentralizirane elektronske kripto valute
  - Uporaba matematičnih kriptografskih primitivov
  - Še vedno v eksperimentalni fazi!
  - Navdihnila množico posnemovalcev (“altcoins”)
- Avtor: Satoshi Nakamoto
  - Psevdonim (identiteta neznana)
  - Članek, objavljen leta 2008
  - https://bitcoin.org/bitcoin.pdf



Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

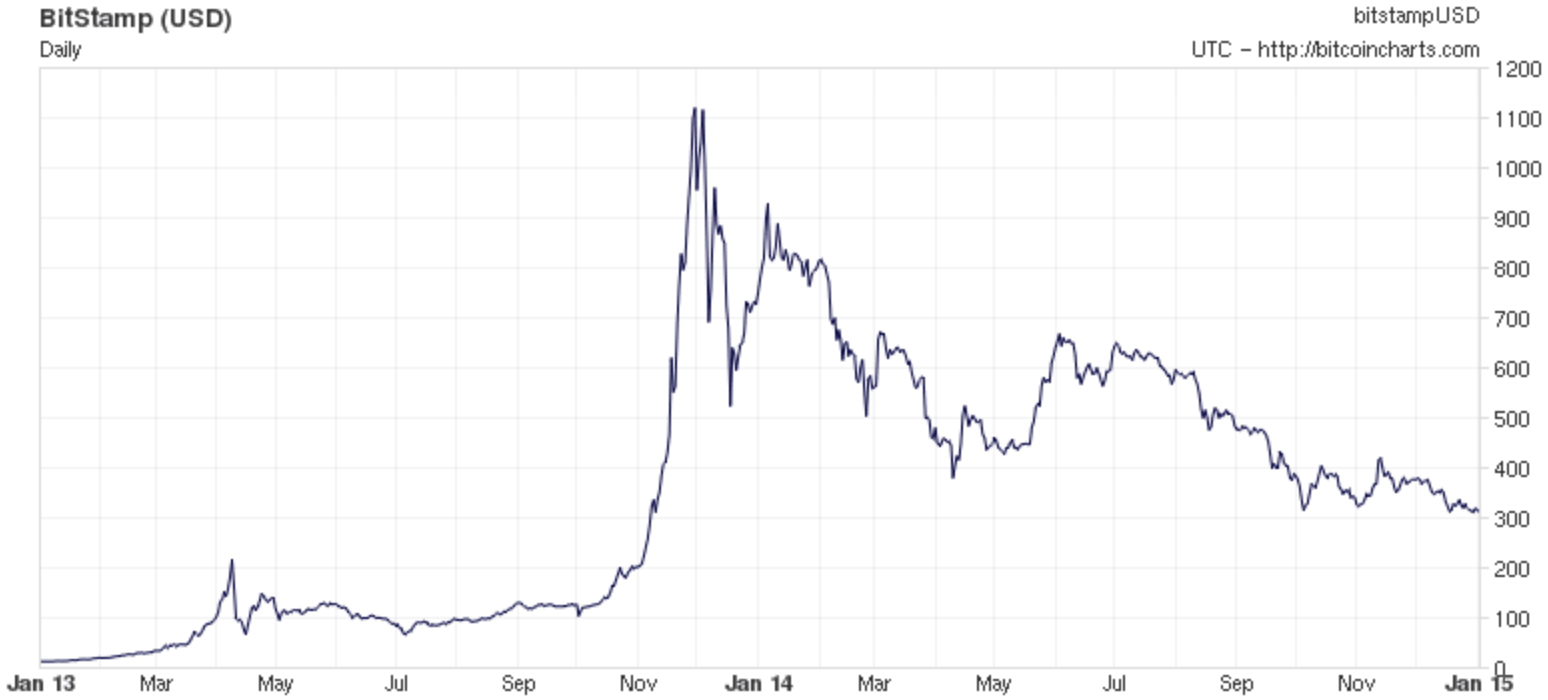
Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

Lastnosti Bitcoina

- Omejeno število kovancev
  - Ne moremo jih ustvariti več kot 21 milijonov
  - Lahko pa jih uničimo
    - Vgrajena deflacija
- Velika deljivost
  - Porabiti je mogoče 0.00000001 kovanca (“1 Satoši”)
  - Enaka provizija ne glede na vrednost, pošiljatelja in prejemnika
- Potrjevanje transakcij vsakih 10 minut
  - Za veliko gotovost potrditve je smiselno počakati ~6 potrditev (~1h)
- Globalen, decentraliziran in popolnoma nevtralen

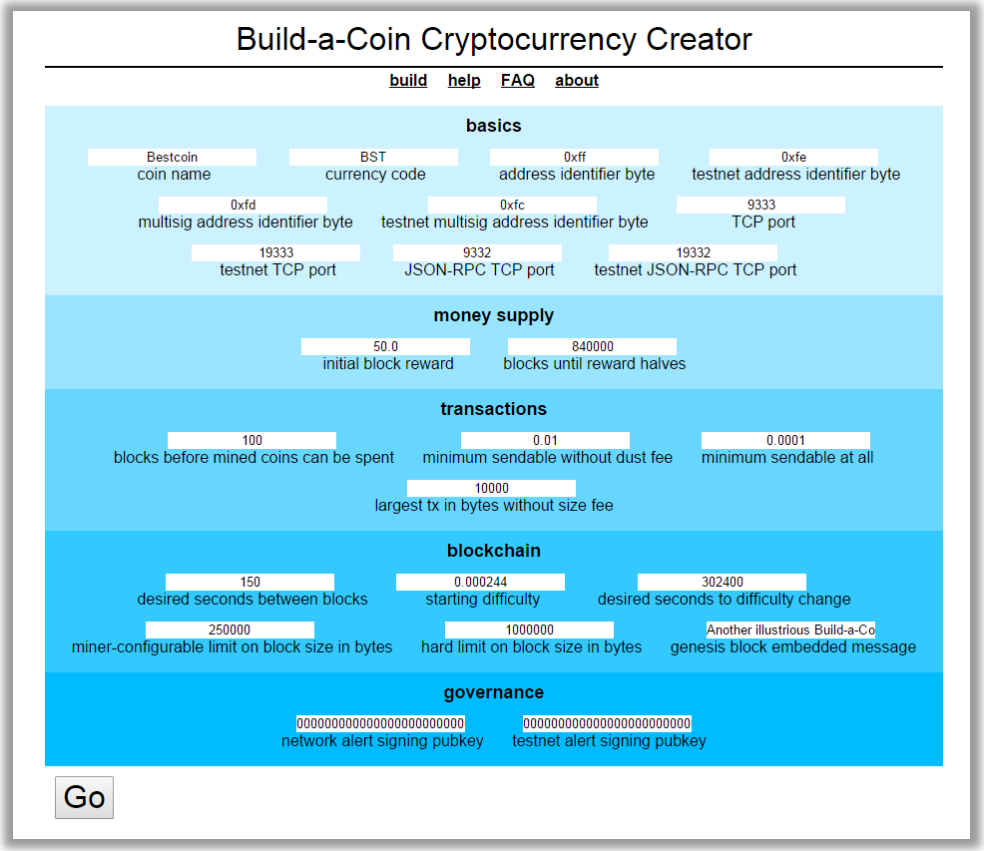
Gibanje vrednosti

- Trenutno velika volatilnost
  - Močan porast cene leta 2014
  - Vrednost je to, kar so ljudje pripravljeni plačati
  - Bitcoin sam po sebi nima vrednosti



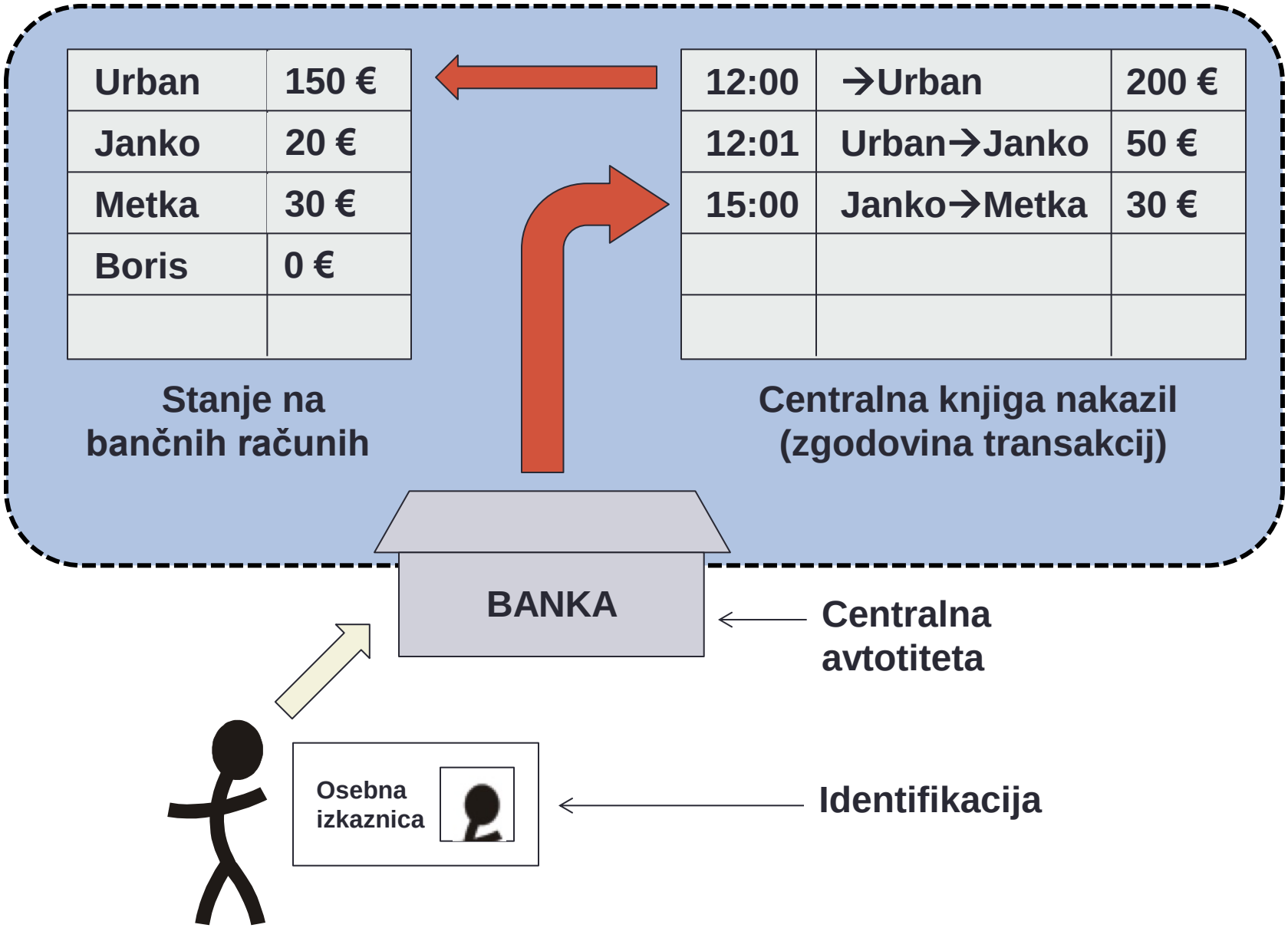
Druge kriptografske valute

- Bitcoin je navdahnil množico drugih valut
  - Litecoin, Namecoin, Primecoin; več kot 40 sprejetih kripto valut
- Vse bazirajo na isti ideji
  - z majhnimi spremembami
- Ideje so celo tako dobro sprejete, da obstajajo generatorji valut
  - Spremenimo samo parametre (max. št. kovancev, čas potrjevanja, ipd.)
  - http://build-a-co.in



TEHNOLOŠKO OZADJE

Plačevanje v klasičnih sistemih

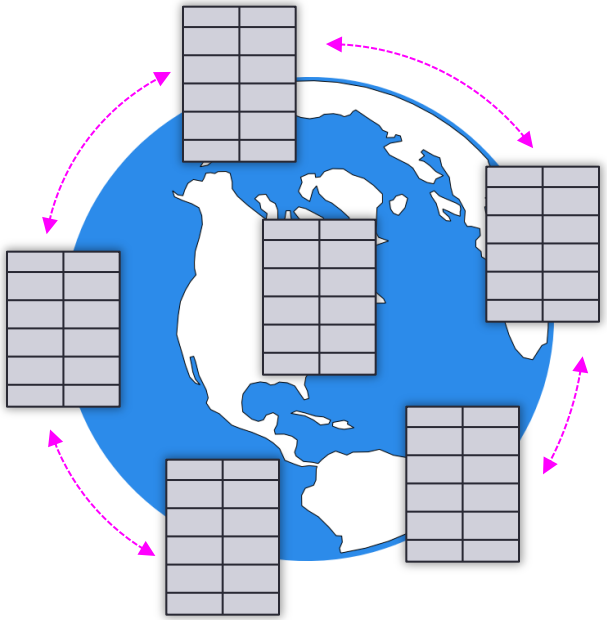


Centralna knjiga nakazil

- Možne težave centralne knjige nakazil
  - Ustanova ne dovoli transakcije
  - Včasih za transakcijo potrebuje 3 delovne dni
  - Transakcije lahko potrjuje samo v uradnih urah
  - Ustanova lahko bankrotira
- Imamo samo eno točko odpovedi
  - Ang. single point of failure
- Kriptografske valute uporabljajo javno knjigo nakazil
  - Ang. public ledger

Javna knjiga nakazil

- Vsak uporabnik si na svoj računalnik naloži celotno zgodovino vseh transakcij v sistemu



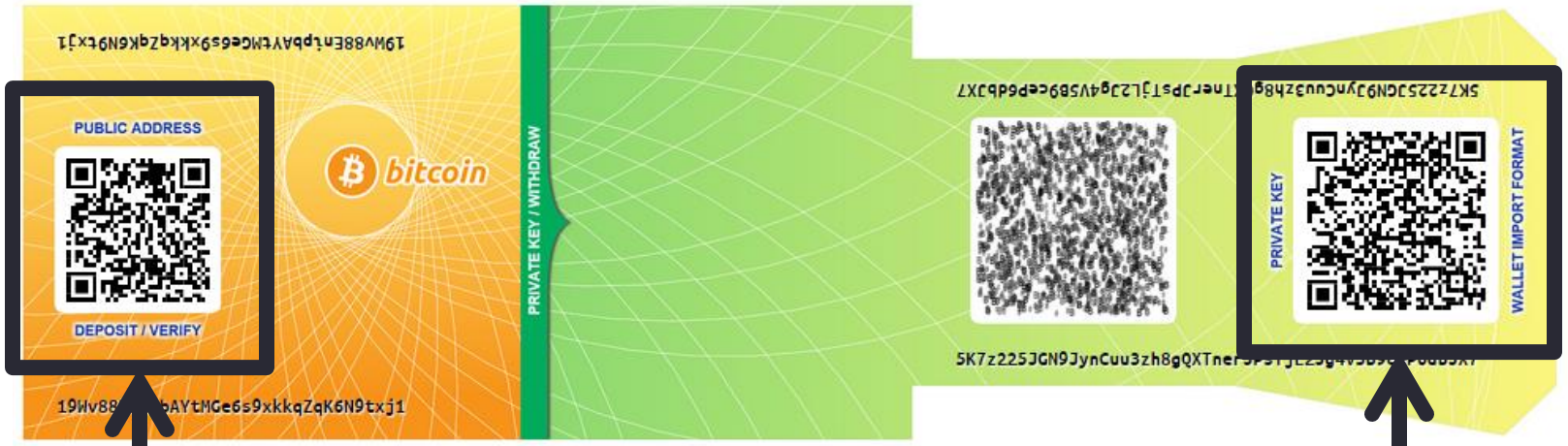
- Uporabniki si med seboj posredujejo tudi vse spremembe
  - Podobno kot omrežju BitTorrent (peer-to-peer)
- Celotna zgodovina transakcij sistema je lahko velika
  - Bitcoin (december 2015): ~50 GB

Identiteta uporabnika

- Če so vse transakcije javno na voljo, zagotovo ne bomo želeli uporabljati imena in priimka
- Ustvarili bomo par ključev asimetrične kriptografije
  - Javni ključ, ki bo služil kot naš naslov za sprejemanje denarja
  - Zasebni ključ, ki bo služil za plačevanje (podpisovanje nakazil)
- Javni ključ bo naša identiteta
  - Vsak uporabnik si lahko ustvari poljubno število naslovov
  - Podobno kot e-mail, le da ne potrebujemo centralne avtoritete
- Primerjava: poštni nabiralnik
  - Vsak ki ve naslov lahko pošlje denar
  - Samo lastnik zasebnega ključa pa lahko nabiralnik odpre in vzame denar

Identiteta

- Število možnih naslovov
  - 2^160, oz. 1461501637330902918203684832716283019655932542976
  - Zanemarljivo majhna možnost, da 2 uporabnika izbereta istega
- Vse kar potrebujemo sta zasebni in javni ključ
  - Lahko ju natisnemo na papir → papirnata denarnica



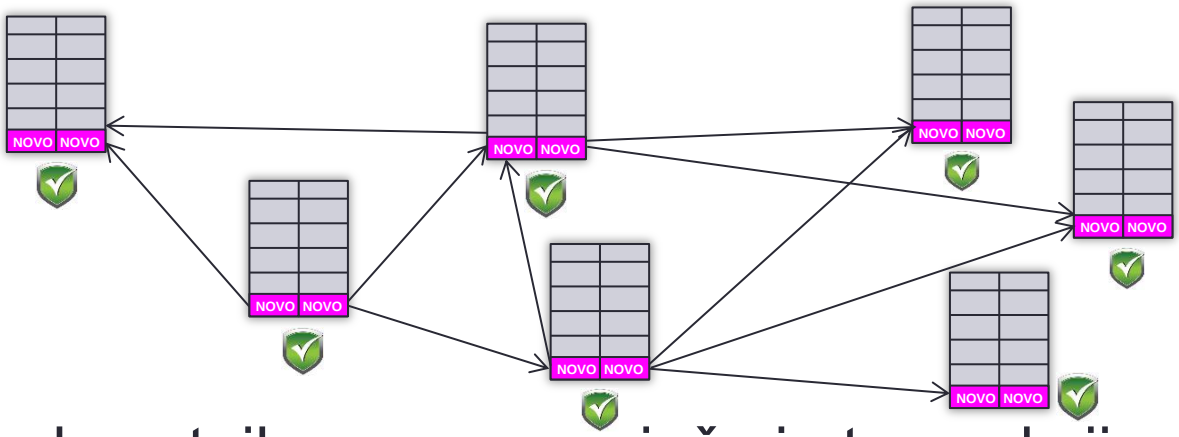
Javni ključ
Sem lahko kdorkoli nakaže denar

Matematična povezava

Zasebni ključ
Samo z njim lahko do tega denarja dostopamo

Izvedba plačila

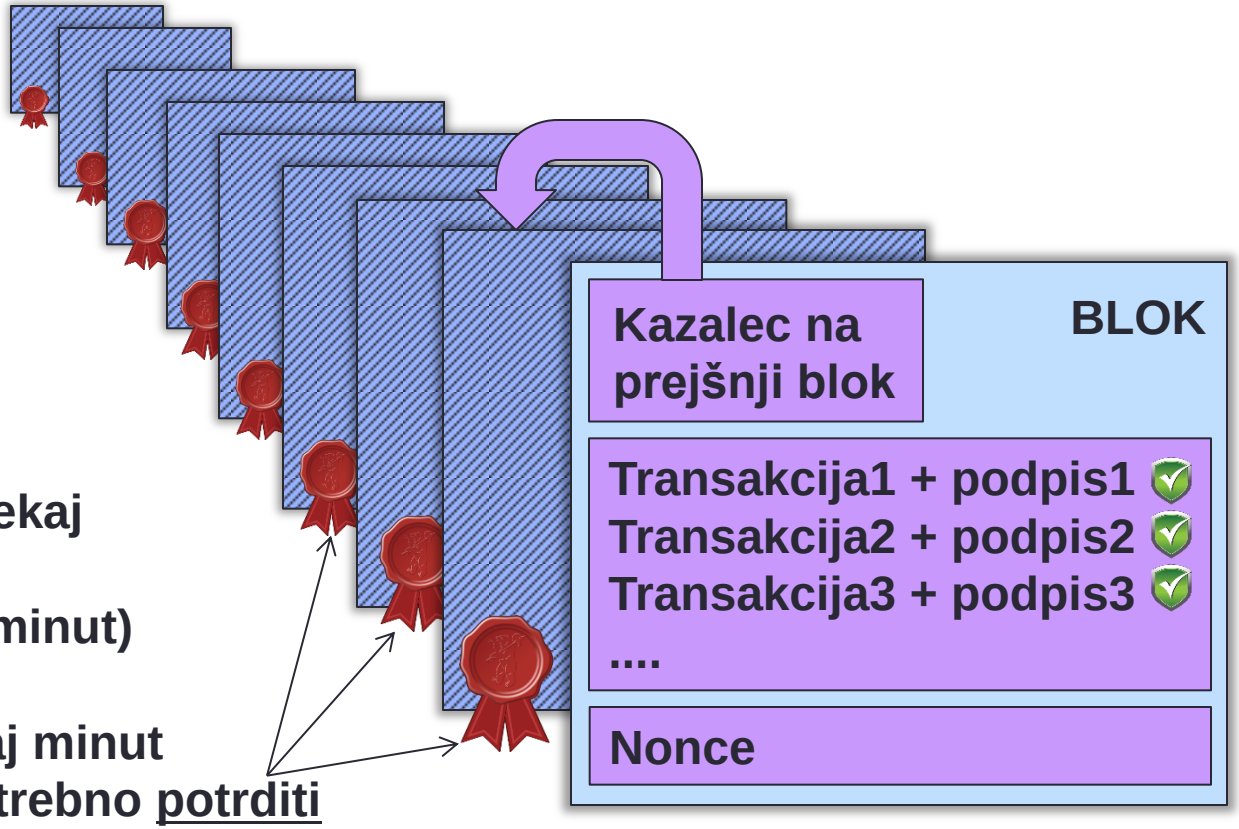
- Transakcijo podpišemo s svojim zasebnim ključem
- In jo sporočimo vsem našim vrstnikom v omrežju
  - Vsak od njih jo sporoči vsem svojim vrstnikom



- Nato vsak vrstnik zase preveri, če je transakcija veljavna
  - Podpis se mora ujemati z naslovom, ki denar pošilja
  - Kovanci, ki jih pošiljamo, še ne smejo biti zapravljeni
    - Nujen pregled zgodovine transakcij
- Vse nove transakcije, ki jih posamezen vrstnik dobi, tvorijo blok nepotrjenih transakcij
  - Potrebna potrditev bloka

Transakcije so urejene v bloke

- Celotna zgodovina transakcij tvori verigo blokov
  - angl. blockchain
  - Vsak blok mora biti potrjen, kar zahteva veliko dela
  - Vsaka naslednja potrditev tako potrdi tudi vse predhodne bloke
- Veriga blokov

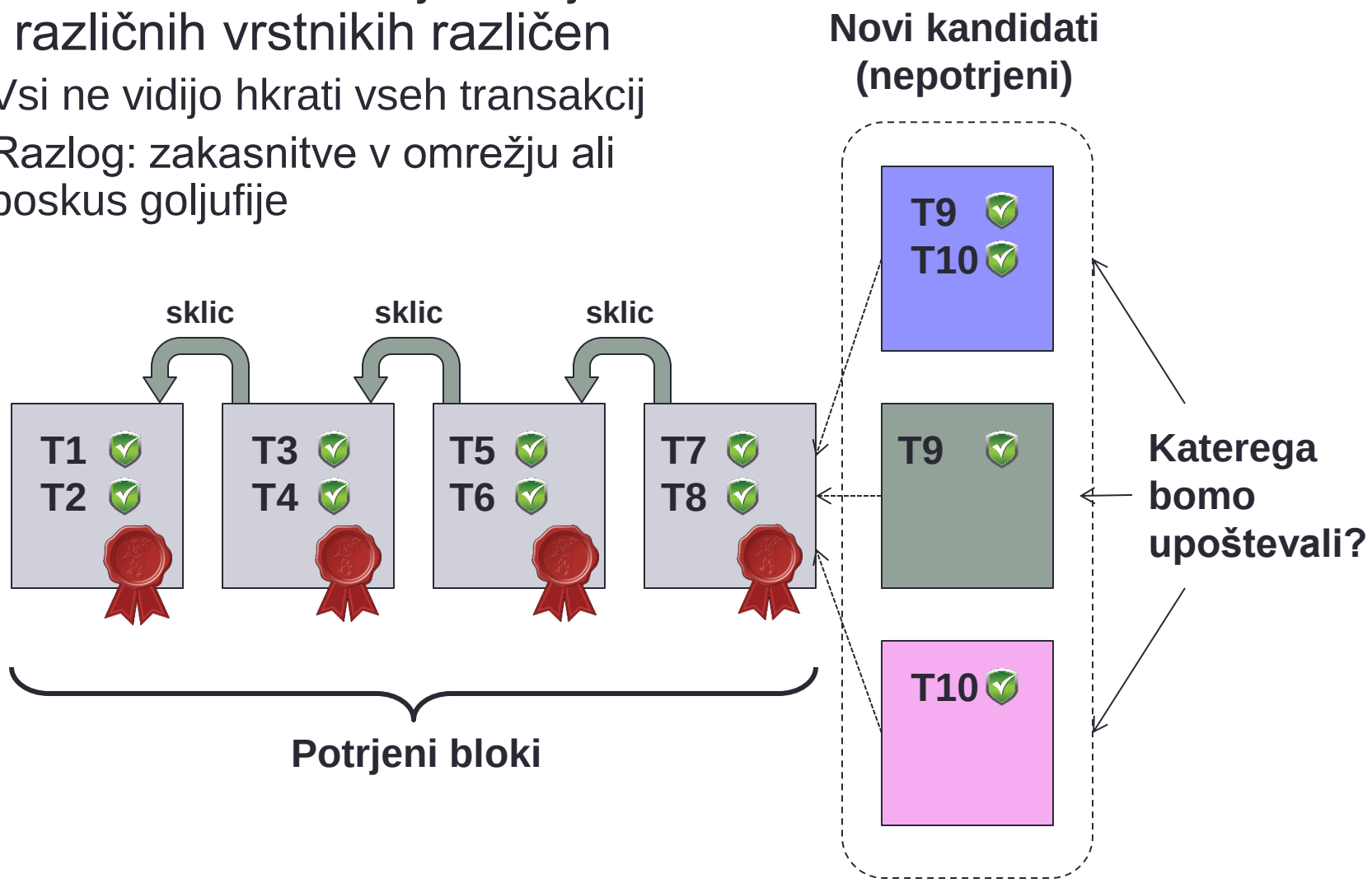


En blok vsebuje za nekaj minut transakcij (Primer: Bitcoin ~10 minut)

Ko se nabere za nekaj minut transakcij, je blok potrebno potrditi

Vrstniki se o bloku ne strinjajo vedno

- Kandidat za naslednji blok je lahko pri različnih vrstnikih različen
  - Vsi ne vidijo hkrati vseh transakcij
  - Razlog: zakasnitve v omrežju ali poskus goljufije



Kdo torej potrdi naslednji blok

- Vrstniki lahko vidijo različne transakcije
  - Če ni centralne avtoritete, kdo se odloči čigav blok bo obveljal
- Potrjevalca izberemo po količini dela, ki jo lahko opravi
  - Organiziramo tekmo v reševanju matematičnega problema med vrstniki
  - Tisti, ki prvi najde rešitev težavnega problema, dobi nagrado
  - In njegov potrjen blok bo prišel v verigo blokov
- Problem je zasnovan tako, da vedno traja približno 10 minut
  - Če računalniki postanejo hitrejši, se poveča težavnost
  - Če se v reševanje vključi več vrstnikov, se poveča težavnost

Dokaz dela (“rudarjenje”)

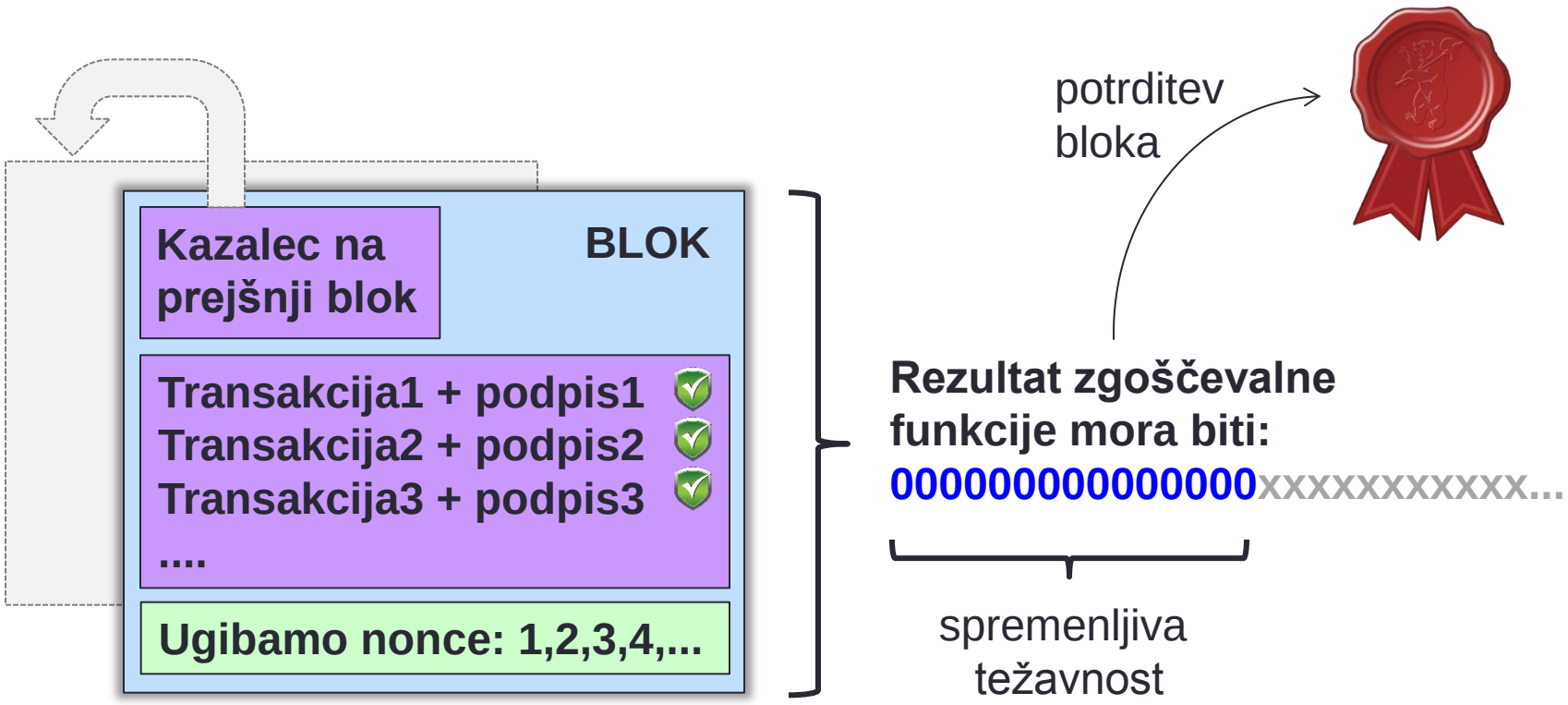
- Potrditev bloka je “dokaz dela” (angl. proof-of-work)
  - Če najdemo rešitev potrjevanja, smo dokazali, da smo opravili delo
  - Za eno samo tako potrditev bi en računalnik potreboval nekaj let
  - Pri veliki količini računalnikov se statistično “posreči” ena rešitev na ~10 minut
- Kakšen problem rešujemo
  - Ugibamo številke, ki nam dajo določen rezultat zgoščevalne funkcije
- Kako motiviramo rudarje
  - Iskanje rešitve je zelo potratno in drago
  - Velika poraba električne energije
- Kdor prvi potrdi blok, dobi nagrado
  - V Bitcoin omrežju je nagrada trenutno 25 BTC oz. ~8000 EUR
  - Nagrada se razpolovi vsaka 4 leta, po letu 2140 pa je ne bo več
  - Rudarjenje je edini način za ustvarjanje novih kovancev Posledično je maksimalno možno število kovancev 21 milijonov (Bitcoin)

Zgoščevalni postopki

- Angl. *one-way hash function*
- Postopek, ki preslika poljubno dolg niz vhodnih podatkov v povzetek fiksne dolžine
- Lastnosti zgoščevalnih postopkov
  - Enak niz podatkov se vedno preslika v enak povzetek
  - *Praktično* nemogoče je najti dve različni sporočili, ki bi ju postopek preslikal v enak povzetek
  - Vsaka najmanjša sprememba vhodnega niza povzroči veliko spremembo povzetka
- Nekaj znanih zgoščevalnih postopkov
  - MD5, SHA1, SHA2, bcrypt, scrypt
- Primer:
  - http://urbansedlar.com/files/bitcoin/hash

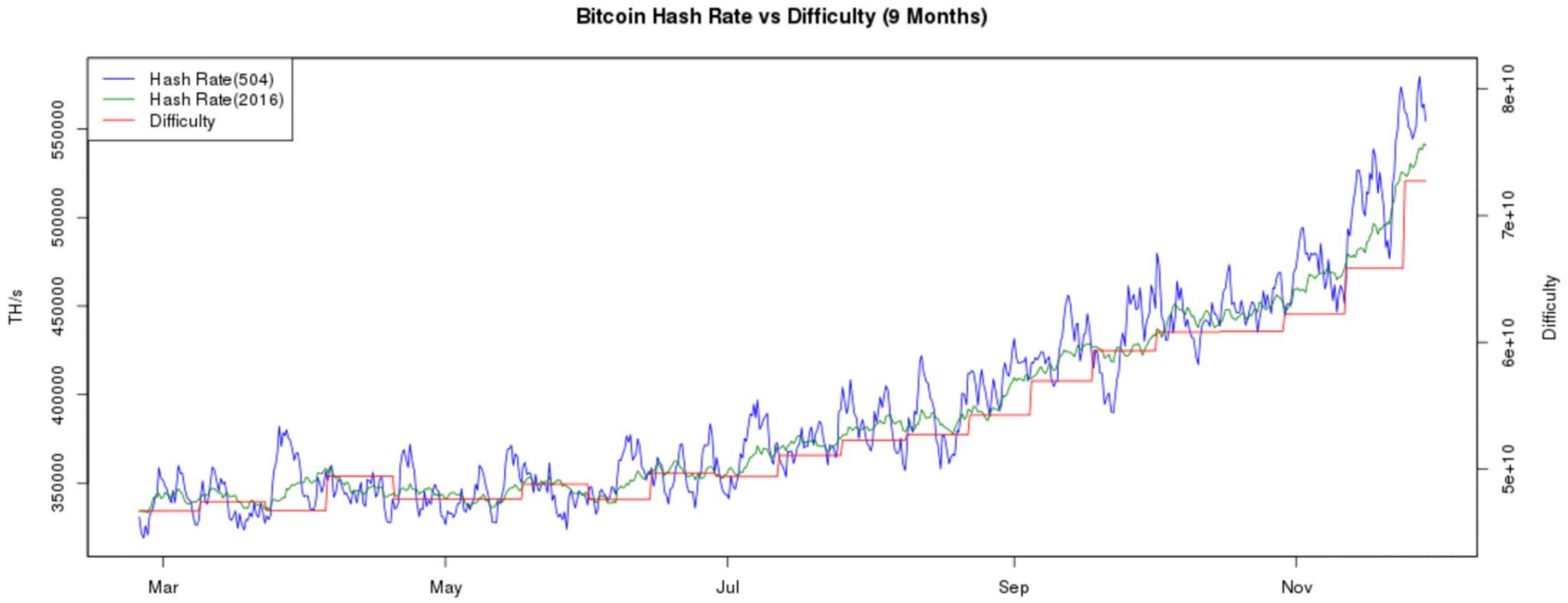
Potrditev

- Kakšen nonce moramo izbrati, da bo imel rezultat zgoščevalne funkcije na začetku npr. 15 ničel?
  - Potrebno je preizkusiti veliko število možnosti (zelo dolgotrajno)
  - Ko pa je blok potrjen, je nonce mogoče preveriti v trenutku



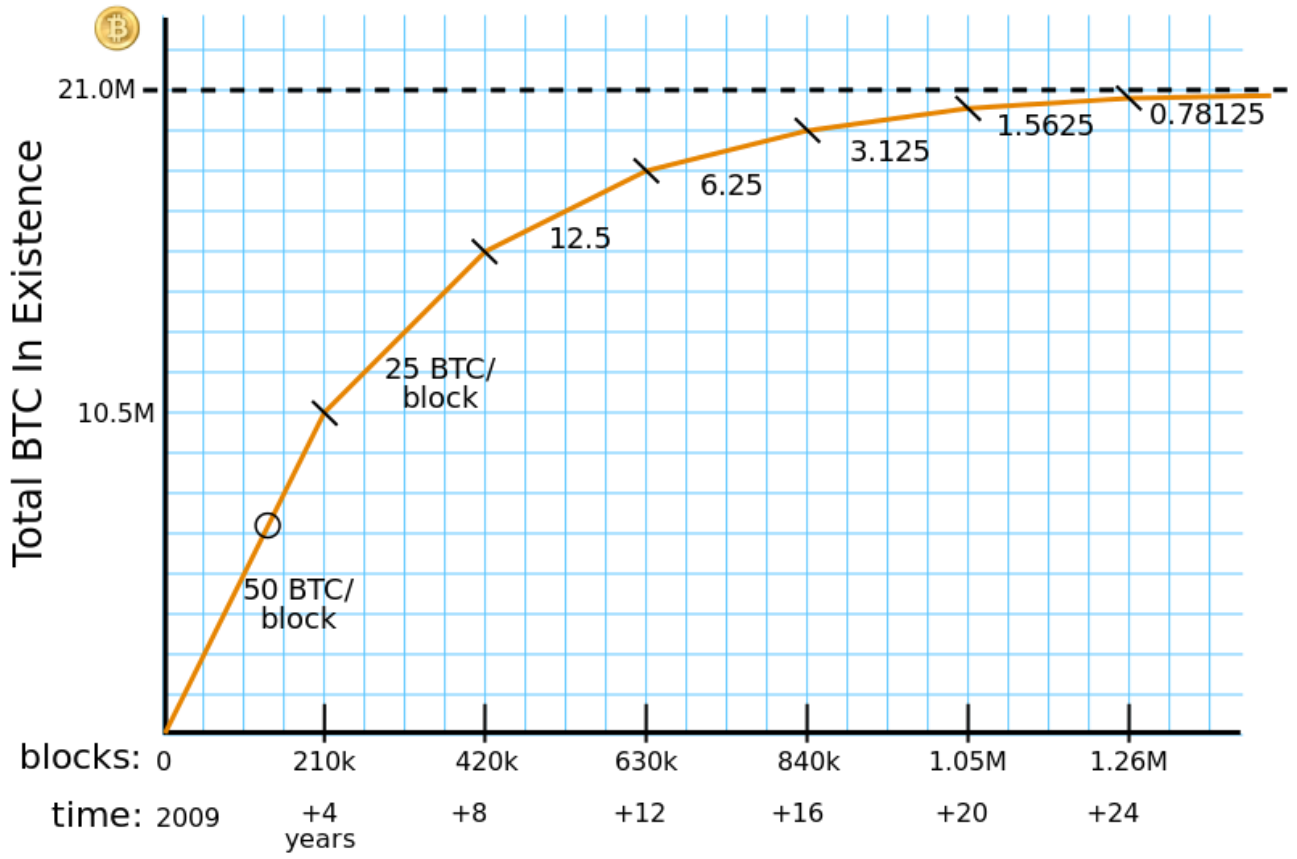
Primer: spremenljiva težavnost

- Bitcoin
  - Težavnost: rdeča črta
  - Trenutna težavnost: 72722780643
    - To pomeni 17 ničel: **00000000000000000**5b1c59f7d60ed8c026aa42....
  - Težavnost se prilagodi vsakih 2016 blokov (1-2 tedna)



Nagrada v omrežju Bitcoin

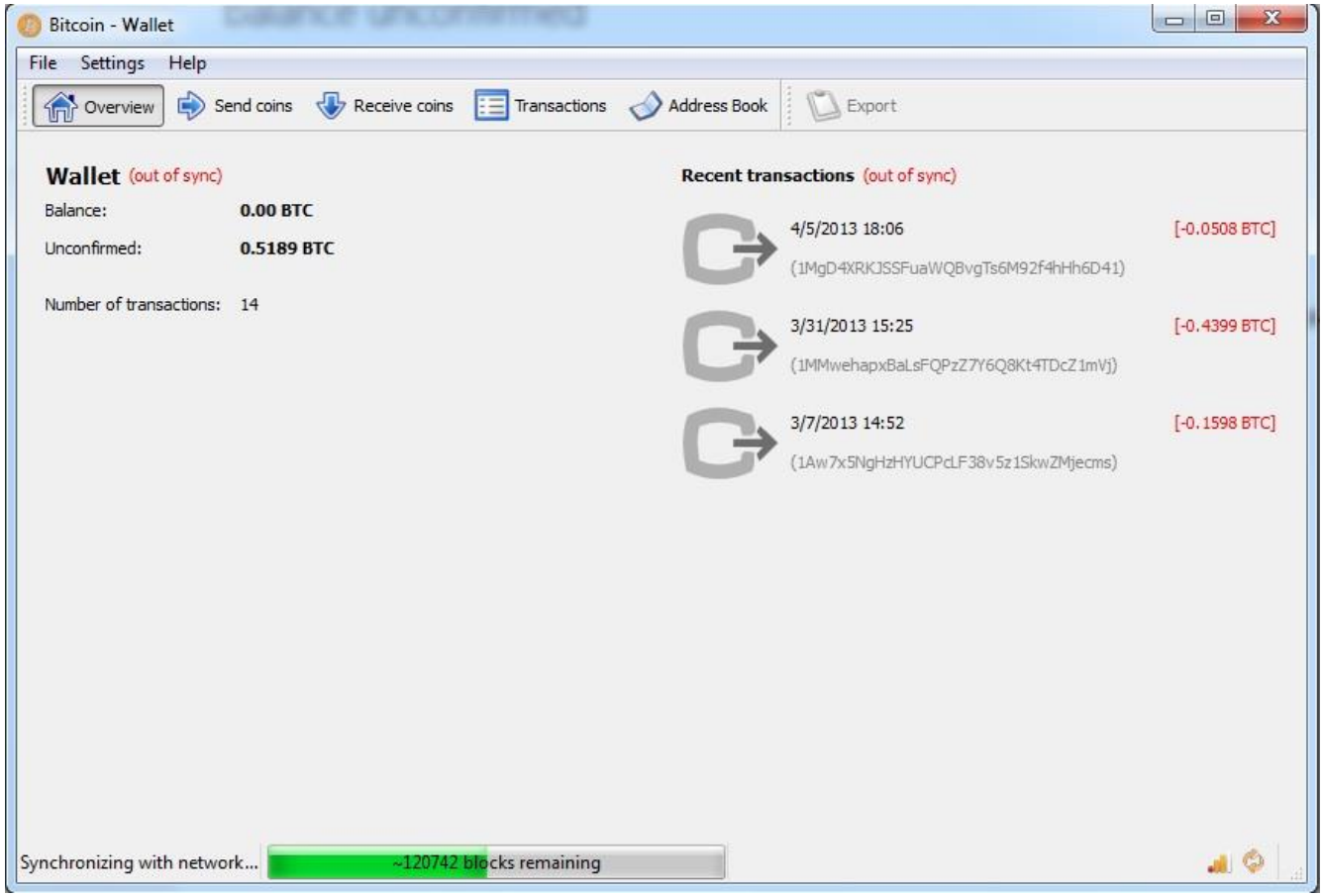
- Nagrada je edini način za ustvarjanje novih konvancev
  - Vsaka 4 leta se razpolovi (začenši s 50 BTC za blok)
- Skupna številka bo prišla do 21 milijonov



PRAKTIČNI VIDIKI IN PRIMERI

Denarnica

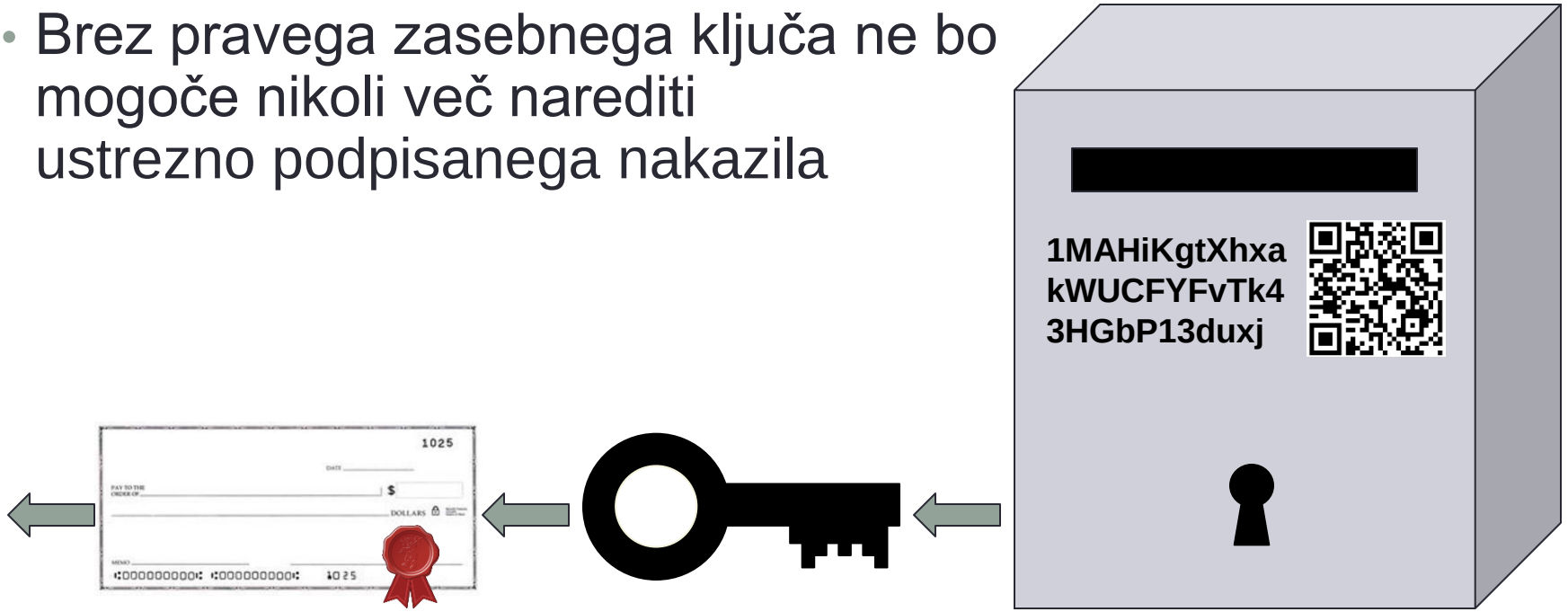
- Vsaka valuta ima svojo denarnico, ki posluša svoje omrežje
  - Denarnica ne potrebuje celotne verige blokov (50GB za Bitcoin), ker lahko transakcije namesto nje validirajo vrstniki v omrežju



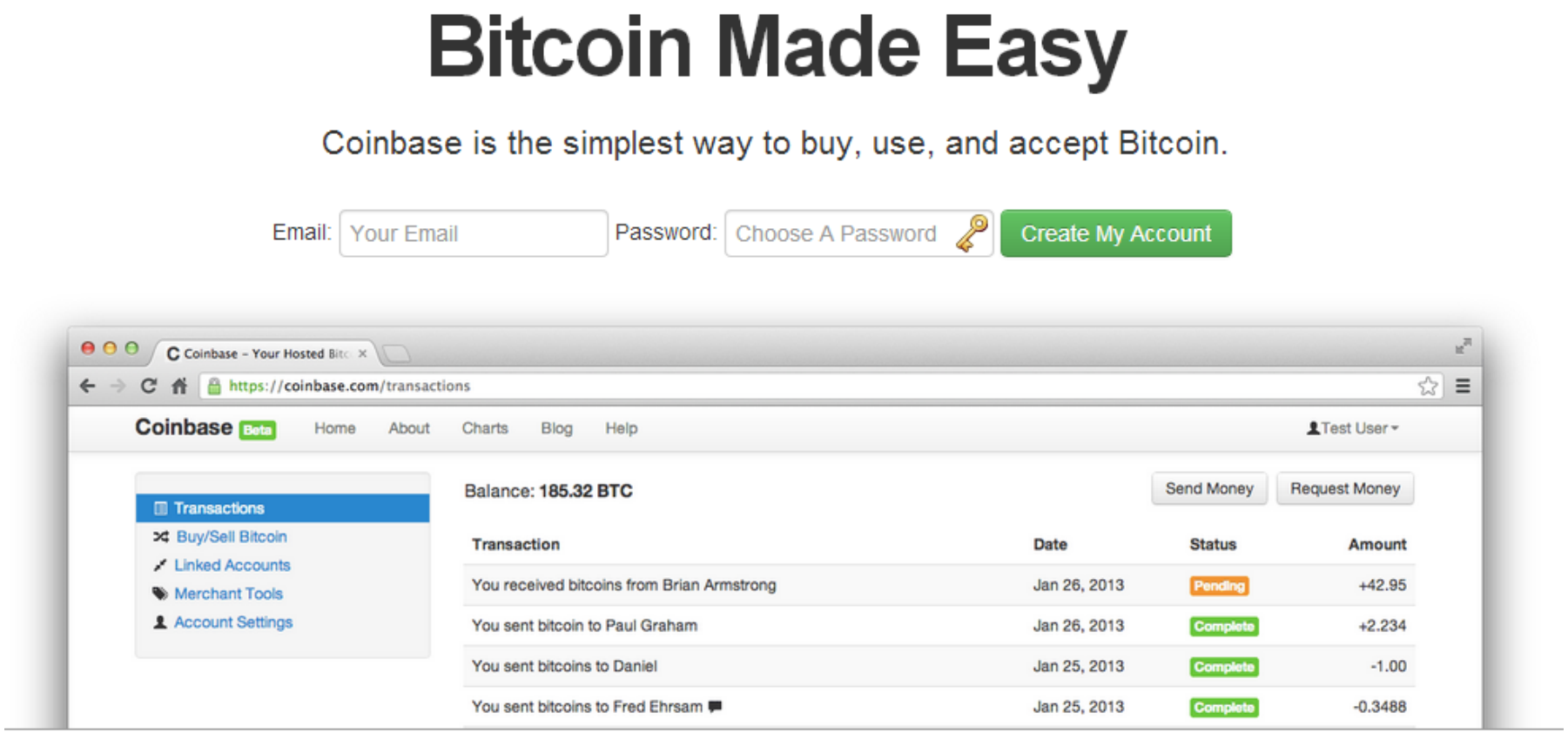
V vsaki denarnici lahko uporabljamo več naslovov (in ključev), ter ustvarjamo nove

Izguba zasebnega ključa

- Če izgubimo zasebni ključ 
  je naše dobroimetje izgubljeno za vedno
  - “Nabiralnika” ne moremo odpreti na silo,
    ker fizično ne obstaja
  - Obstaja samo transkcija,
    ki je prenesla vrednost na nek račun
- Brez pravega zasebnega ključa ne bo
  mogoče nikoli več narediti
  ustrezno podpisanega nakazila



Pojav spletnih menjalnic in bank



- Ironija: izum distribuirane valute, ki jo je pretežko uporabljati, zato uporabniki drvimo nazaj na centralizirane ponudnike
  - Vendar: še vedno zdrava konkurenca in odprtost sistema

Nekaj številk bitcoin rudarjenja

- Rudarjenje s CPU
  - 20 milijonov hashev / s (20 MH/s)
  - trenutno cca. 495.000 let da bi z enim računalnikom potrdili blok
- Rudarjenje z GPU
  - do 200 milijonov hashev / s (200 MH/s)
  - samo 49.500 let
- FPGA
  - 1 milijarda hashev / s (1GH/s)
  - 9900 let
- ASICs (pojavijo se 2014)
  - Ang. Application-Specific Integrated Circuits
  - danes modeli z do 7,7 TH/s
  - ena taka naprava bi potrebovala samo še 1.2 leti za blok

- Ocenjujejo, da rudarjenje trenutno troši med 250 in 500 MW

Razširjenost in uporaba

- Vse več ponudnikov sprejema Bitcoin
  - nekateri tudi druge kripto valute (predvsem LiteCoin)
- Posamezniki že eksperimentirajo, če se da preživeti samo z Bitcoini
  - V tujini je to že mogoče
- Bitcoin bankomati
  - SLO proizvajalec: Bitnik

Bitcoin ATM in Ljubljana - World Trade Center

Added on July 17, 2015

Address:
Dunajska Cesta 156
1000 Ljubljana
Slovenia

→ Read More

Prodajalci

- Vse več prodajalcev pri nas in v tujini

bitpay

BitCoffee
Coffee Store

Irish coffee (bean) – 100g

฿0.0233

ADD TO CART

200,000 Hotels Now Accept Bitcoin Through Online Travel Agency CheapAir

Pete Rizzo (@pete_rizzo_) | Published on February 4, 2014 at 00:21 GMT

2 NAČIN DOSTAVE

Trgovina

Osebni prevzem **0,00 €**

Pošiljanje

Pošta Slovenije / GLS **0,00 €**

3 DOSTAVA

Takoj, ko mogoče!

Izberite želen datum dostave.

4 NAČIN PLAČILA

Plačilo po predračunu

Plačilo z gotovino ob prevzemu

Plačilo z Bitcoini (BTC)

Za plačevanje z bitcoini potrebujete BTC denarnico (npr. Blockchain denarnico). Trgovina vam izračuna vrednost nakupa v BTC, znesek plačate iz vaše denarnice. Ko je vaše naročilo plačano, je nakup zaključen.

shopify Ways to sell Pricing Blog More Log in Get started

Start accepting ฿bitcoin payments today

Bitcoin payment gateway for your ecommerce website

Nekaj referenc

- Originalni članek
  - https://bitcoin.org/bitcoin.pdf
- Informacije o bitcoinu
  - https://bitcoin.org/sl/
- Pregled zgodovine v verigi blokov
  - https://blockexplorer.com/
- Rudarjenje
  - https://en.bitcoin.it/wiki/Mining_hardware_comparison
  - http://motherboard.vice.com/read/chinas-biggest-secret-bitcoin-mine
- Druge pomembnejše kripto valute
  - https://en.wikipedia.org/wiki/List_of_cryptocurrencies