Dlaczego Bitcoin nie zastąpił fiatów i co próbujemy z tym zrobić.

POLSKIE STOWARZYSZENIE BITCOIN

BEAM

Silesia Blockchain Meetup

RAFAŁ „PROSTUJE BITCOINA” KIEŁBUS

KATOWICE, 3. KWIETNIA 2019

O mnie

Rafał prostuje Bitcoina

Na początku był manifest...

- Do czego miał służyć Bitcoin?
- Pierwotne założenia działania systemu
- Pierwsze implementacje
- Pierwsze transakcje
- Nadanie wartości

el Manifiesto

Bitcoin: A Peer-to-Peer Electronic Cash System

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

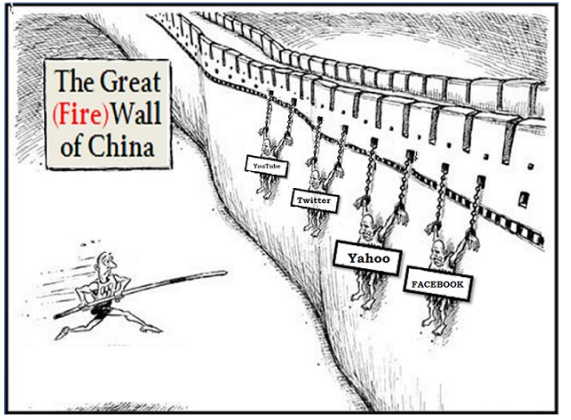
Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required 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.

Reality check

Ja kupowałem herbatę po 0.07

Ograniczenia techno-logiczne

- Jaki był internet w 2008/2009 roku?
- Ceny pamięci RAM i HDD
- Wymagania sprzętowe
- Wymagania stawiane górnikom



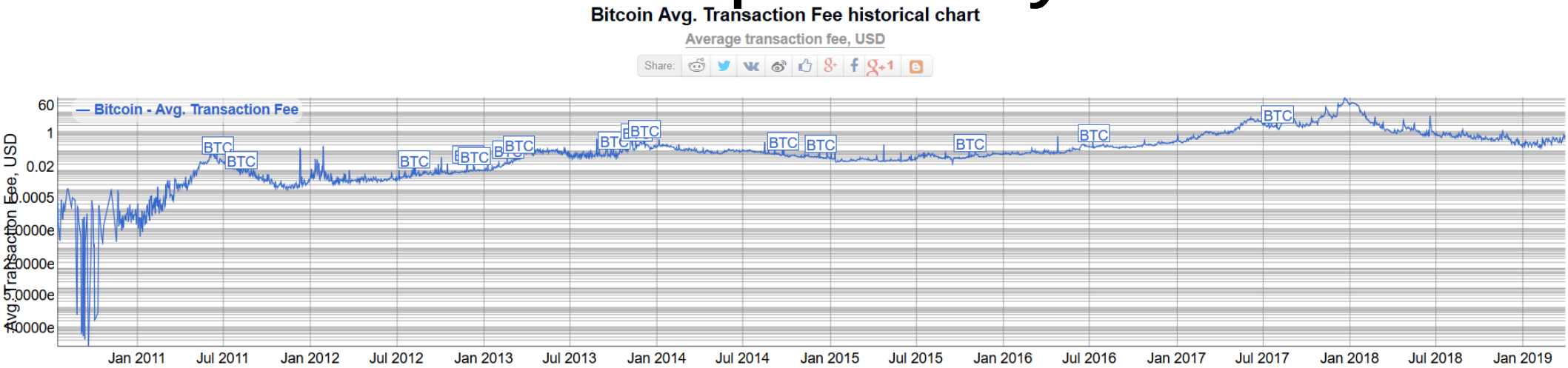
Drogo?

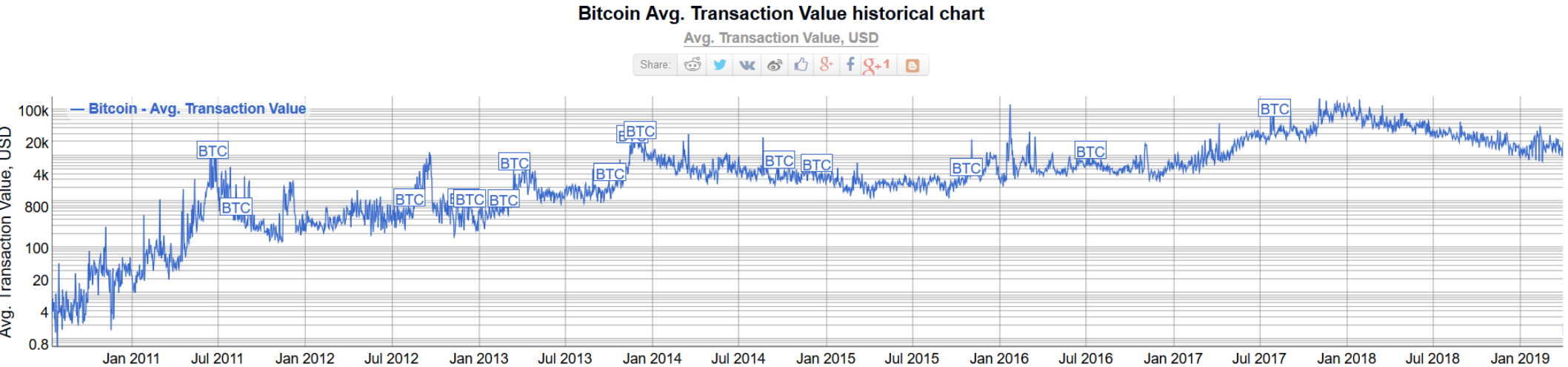
	4GB RAM	500GB HDD
2008	$85 (DDR2)	$100
2013	$25 (DDR3)	$25
2015	$20 (DDR3)	$15
2018	$20 (DDR3)	$12

Zabezpieczenie przed atakiem

- Opłata transakcyjna
- Limit wielkości bloku
- Limit ilości podpisów w bloku
- Ograniczenia języka skryptowego

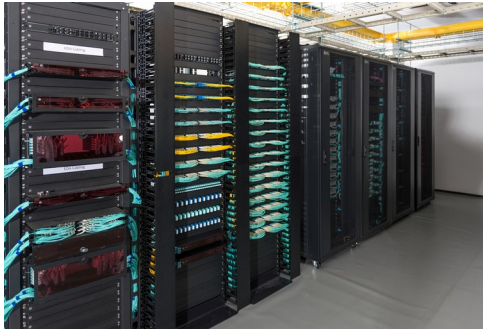
Tanie przelewy





Koszty utrzymania i używania

- Dane zajmują około 300GB
- Przyrost danych: do ok 200MB/dzień (78GB/rok)
- Czas pierwszej synchronizacji
- Utrzymanie pełnego węzła
- Ile naprawdę kosztuje transakcja?



Globalny koszt jednej transakcji

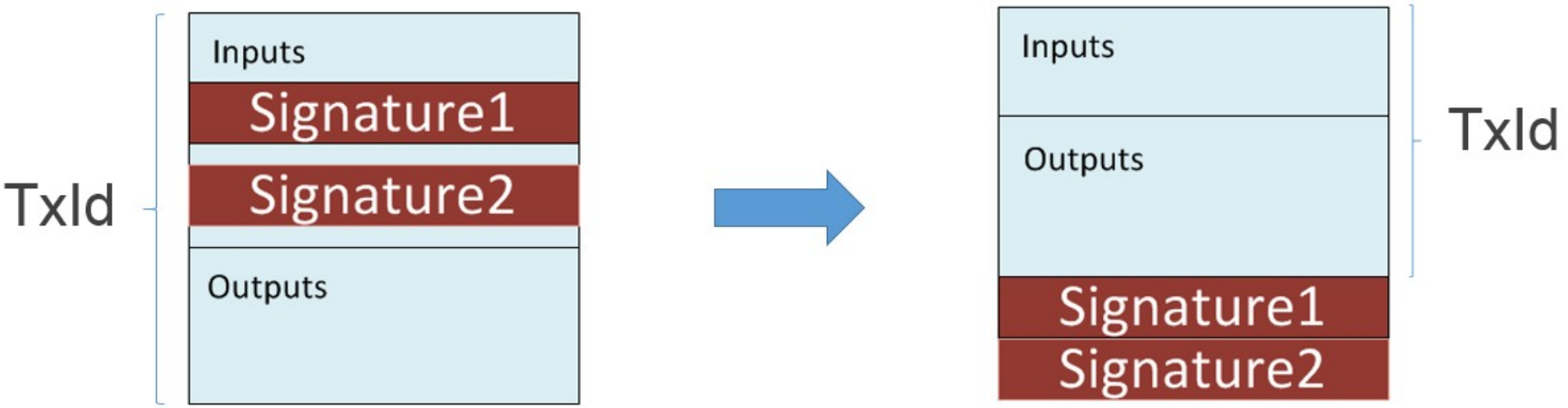
Description	Value
Bitcoin's current estimated annual electricity consumption* (TWh)	53.16
Bitcoin's current minimum annual electricity consumption** (TWh)	41.78
Annualized global mining revenues	$2,998,970,943
Annualized estimated global mining costs	$2,657,760,722
Current cost percentage	88.62%
Country closest to Bitcoin in terms of electricity consumption	Bangladesh
Estimated electricity used over the previous day (KWh)	145,630,724
Implied Watts per GH/s	0.119
Total Network Hashrate in PH/s (1,000,000 GH/s)	51,033
Electricity consumed per transaction (KWh)	459
Number of U.S. households that could be powered by Bitcoin	4,921,779
Number of U.S. households powered for 1 day by the electricity consumed for a single transaction	15.52
Bitcoin's electricity consumption as a percentage of the world's electricity consumption	0.24%
Annual carbon footprint (kt of CO2)	25,249
Carbon footprint per transaction (kg of CO2)	218.15

https://digiconomist.net/bitcoin-energy-consumption

Usprawnienia już działające

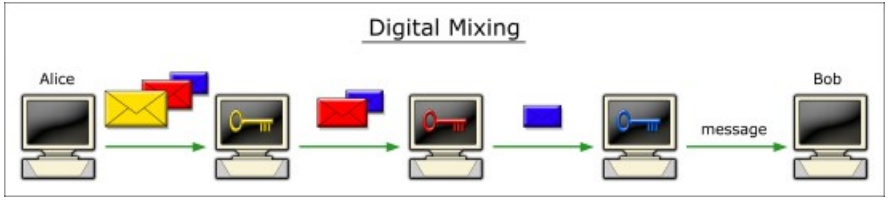
- Segregated Witness
  - Dlaczego softfork i konsekwencje tegoż
  - OPkod AnyoneCanSpend
  - Inny sposób liczenia wielkości transakcji
    - Inny sposób liczenia opłaty transakcyjnej
- Lightning network

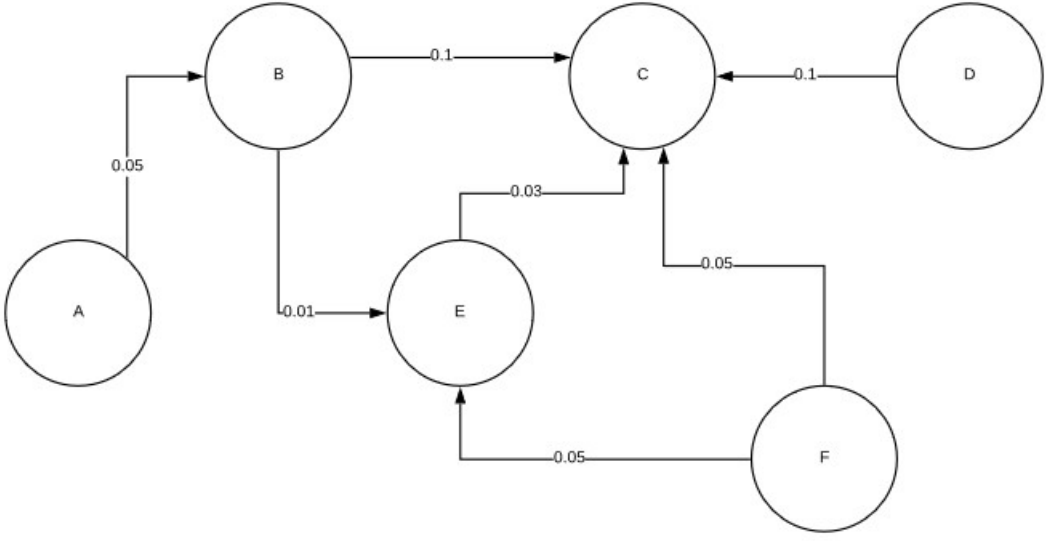
SegWait -> SegWit



https://programmingblockchain.gitbook.io/programmingblockchain/other_types_of_ownership/p2wpkh_pay_to_witness_public_key_hash

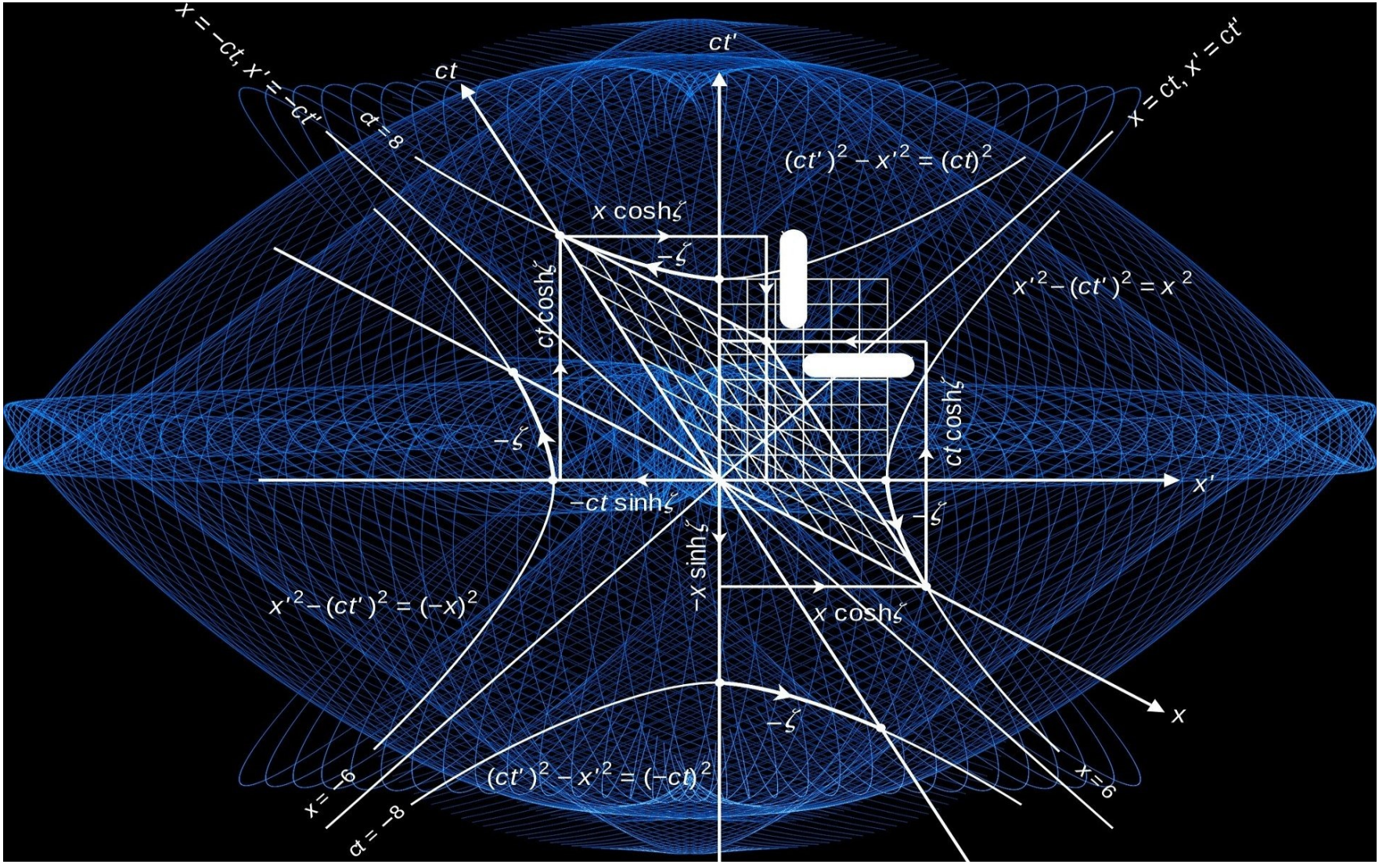
Lightning Network w trzech obrazkach





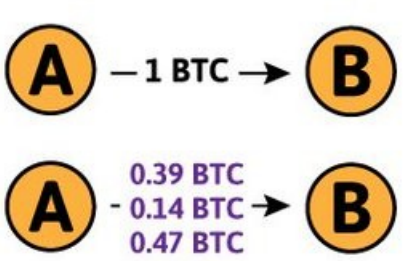
Najbliższa (?) przyszłość

- Podpisy Schnorra
- Łańcuchy poboczne
  - Rootstock
- MimbleWimble

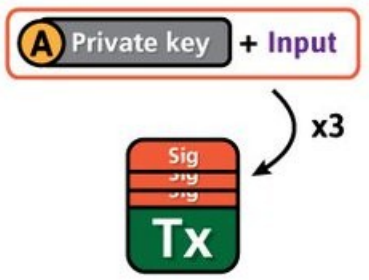

x = −ct, x′ = −ct′
ct
ct′
x = ct, x′ = ct′
ct = 8
(ct′)² − x′² = (ct)²
x cosh ζ
−ζ
x′² − (ct′)² = x²
ct cosh ζ
−ζ
ct cosh ζ
x′
−ct sinh ζ
−ζ
−x sinh ζ
x′² − (ct′)² = (−x)²
x cosh ζ
x
−ζ
(ct′)² − x′² = (−ct)²
x = −6
x = 6
ct = −8

Wersja dla ludzi xD

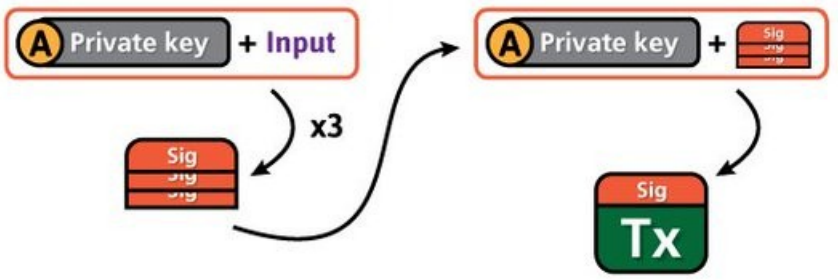
Schnorr (multi)signatures



Many Bitcoin **transactions** include multiple **inputs**, referring to the addresses bitcoins are sent from. In this case, a 1 BTC transaction consists of 3 'parts'.



Each of these **inputs** require the **signature** of the sender, and all these **signatures** are included in the **transaction**.

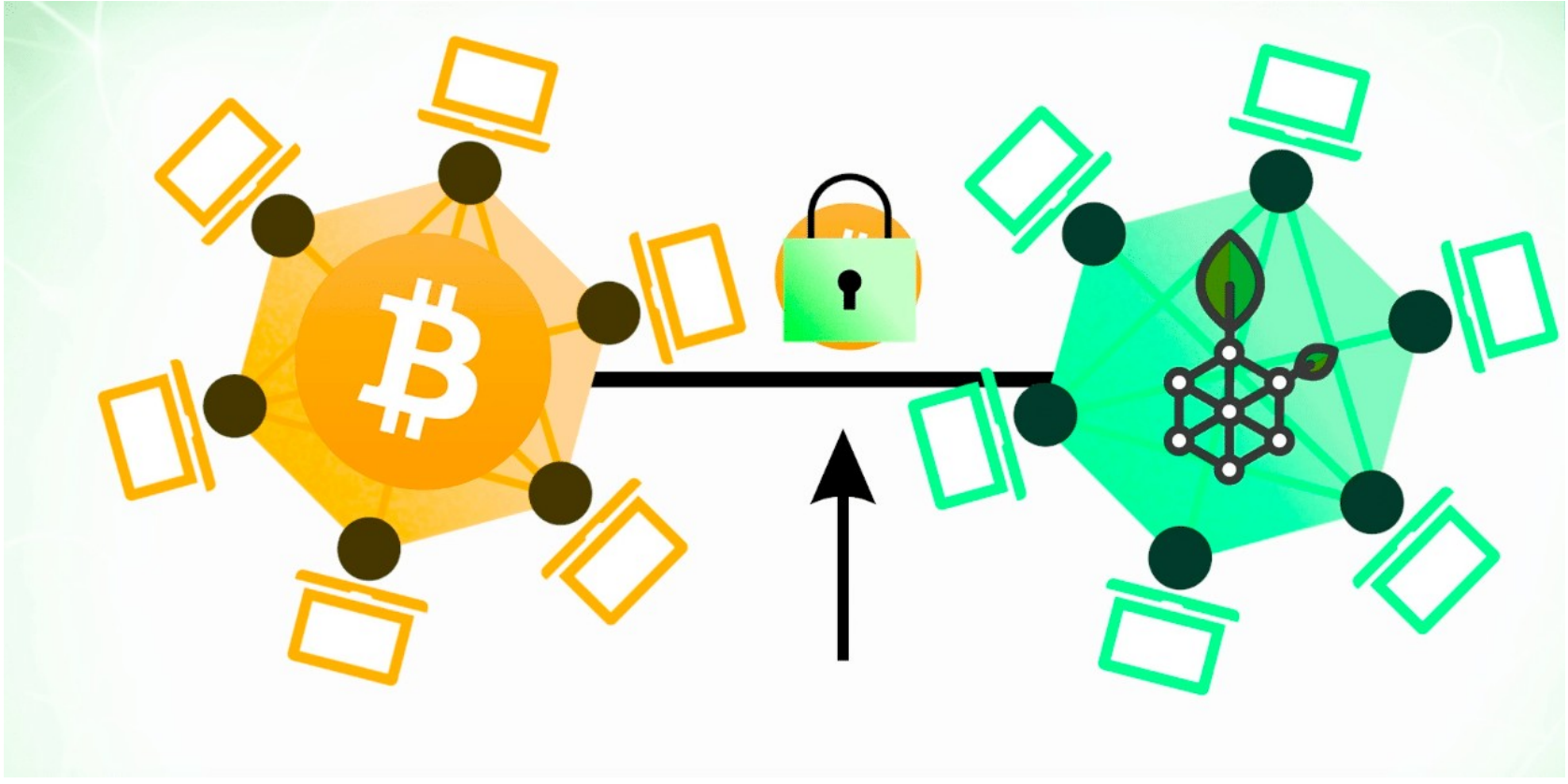


With Schnorr signatures, all **inputs** combined require only one **signature** to represent all the different **signatures**.

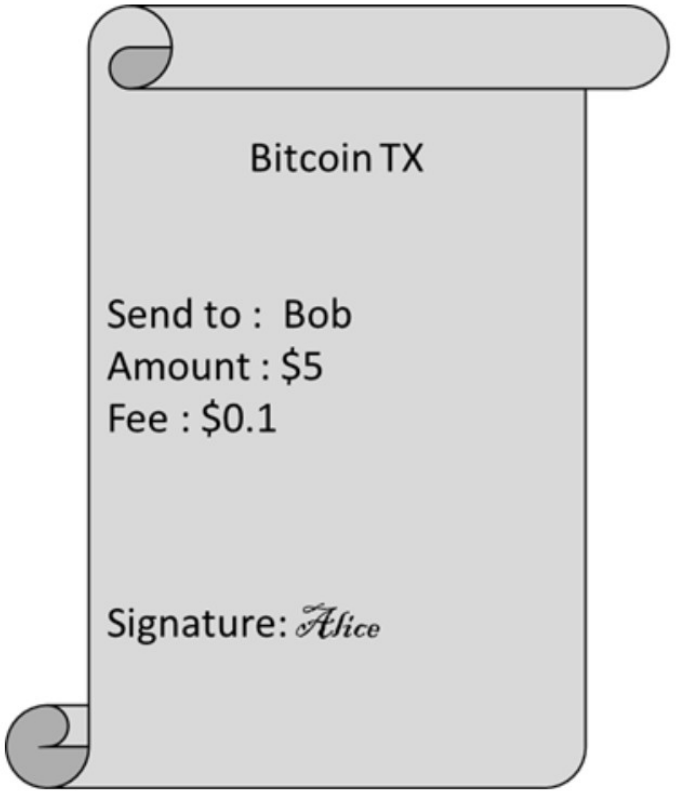
This means **transactions** are **smaller**, freeing up up to 40% more room in the block.

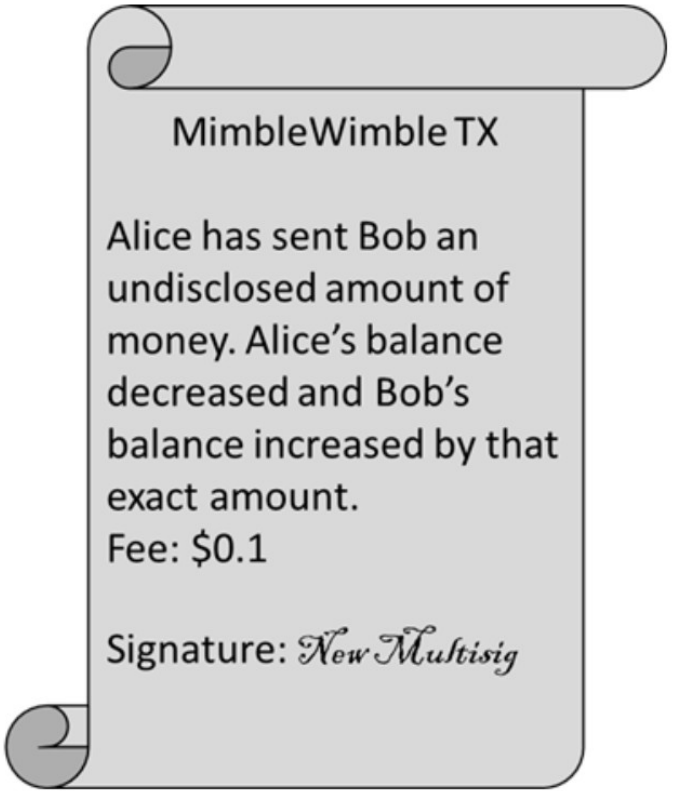
CryptoGraphics.info

~~Wood~~Rootstock



Alohamora!


Bitcoin TX
Send to : Bob
Amount : $5
Fee : $0.1
Signature: Alice


MimbleWimble TX
Alice has sent Bob an undisclosed amount of money. Alice's balance decreased and Bob's balance increased by that exact amount.
Fee: $0.1
Signature: New Multisig

Życie?


RAFAŁ, JAK TO JEST BYĆ BLOCKCHAINEM
Rozmiar obrazu:
144 × 144
Znajdź inne rozmiary tego obrazu:
Wszystkie rozmiary - Mały
Najtrafniejsze hasło dla obrazu: Blockchain
DOBRZE?