Paweł Marczewski

Bitcoin

kryptograficzne złoto

Przesyłanie pieniędzy teraz

- opłaty za przelew (nawet kilka %)
- potrzebne konto bankowe na nazwisko, adres itp.
- często długi czas oczekiwania
- na łasce pośredników (problemy z Wikileaks, liczne problemy u Paypal, itd.)

Co, gdyby pieniądze dało się przesyłać przez Internet **tak łatwo jak pliki?**

Pomysł

Chcemy mieć **zdecentralizowaną** cyfrową walutę:

- Bez centralnego banku, który mógłby dodrukować
- Bez głównego serwera, który przechowuje stan kont
- Łatwą do przesyłania samemu
- Bezpieczną

Bitcoin

- *Kryptowaluta* - waluta kryptograficzna
- Projekt open source rozpoczęty w 2009 roku
- Najważniejsze elementy: komunikacja P2P, moc obliczeniowa, kryptografia

http://en.wikipedia.org/wiki/File:Bitcoin.png

Kryptografia klucza publicznego

Generujemy parę liczb:

To, co zaszyfrowano jednym, można odszyfrować drugim.

Przydaje się do

- poufnego przesyłania informacji
- podpisywania wiadomości

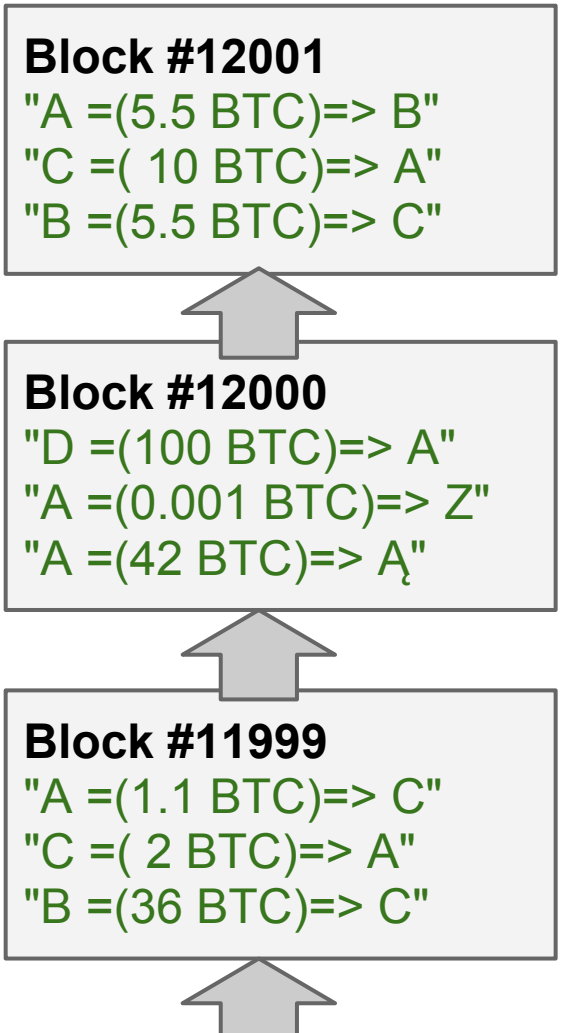
Transakcja

Klucz publiczny może być adresem
("numerem konta")

Transakcja: "A =(5.5 BTC)=> B"
(A wysyła B 5.5 bitcoina)

- Transakcja podpisana kluczem prywatnym A
- Klucz prywatny służy do wysyłania pieniędzy, publiczny do odbierania
- Adresy są zazwyczaj jednorazowe

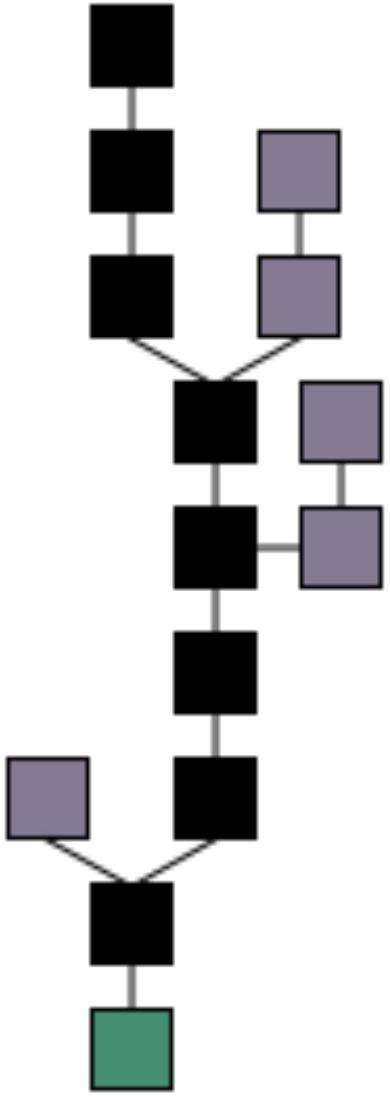
Blockchain



- Ciąg transakcji - wspólna wersja prawdy
- Przechowywany przez wszystkich użytkowników
- Obecnie ok. 2 GB

Rozgałęzienia

- Nie ma centralnego serwera, więc mogą być rozgałęzienia
- Więcej niż jedna wersja prawdy - można dwa razy wydać te same pieniądze!
- Rozwiązanie: niech dodawanie nowych bloków będzie trudne

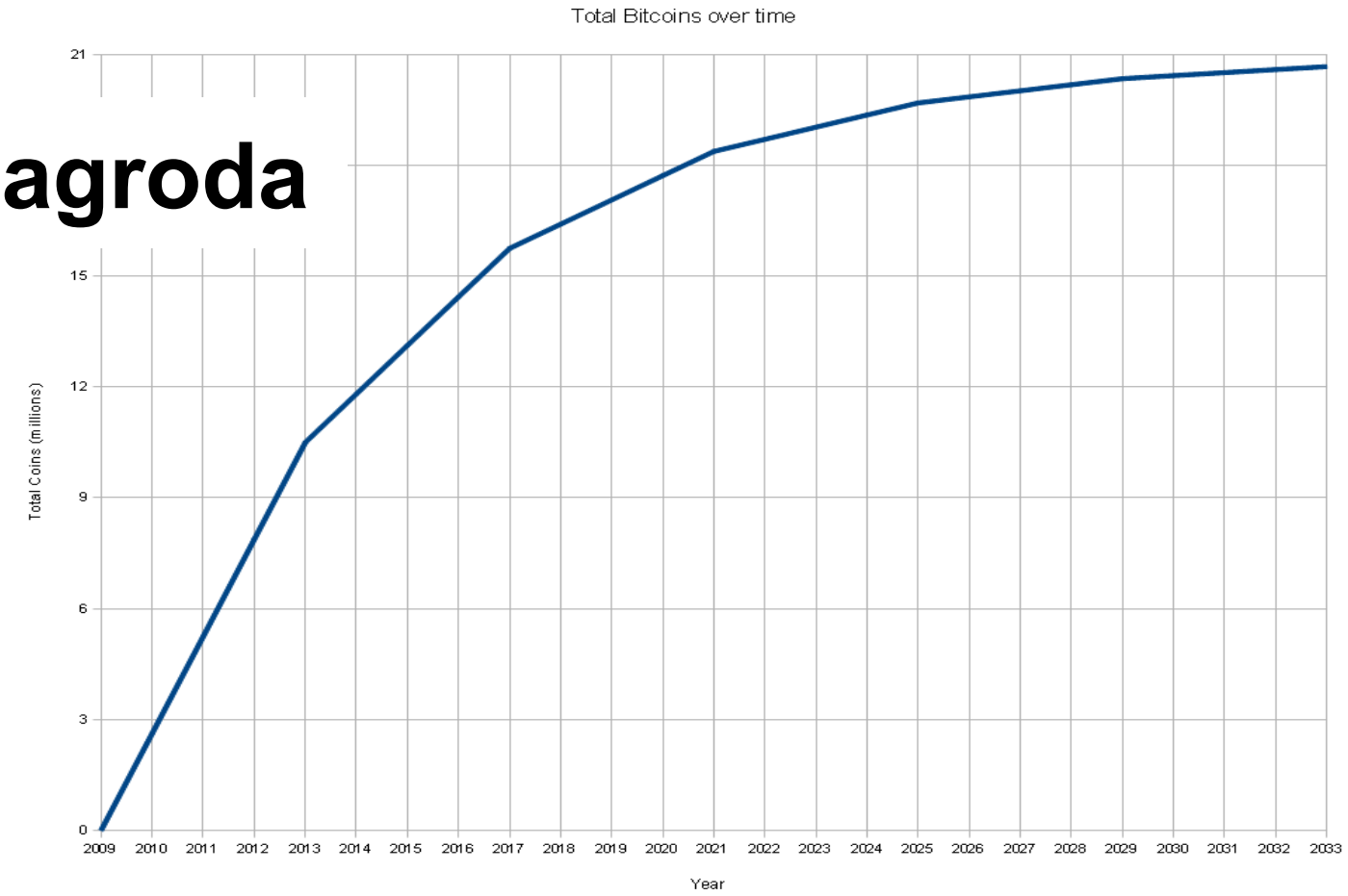


http://en.wikipedia.org/wiki/File:Blockchain.svg

Kopanie (mining)

- *Proof of work*: dodanie nowego bloku jest kosztowne obliczeniowo
- Średnio nowy blok co 10 minut
- Obowiązuje najdłuższy istniejący łańcuch bloków
- Transakcję "przybitą" kilkoma blokami trudno unieważnić - moc obliczeniowa chroni sieć
- Do ataku trzeba kontrolować > 50% mocy sieci

Nagroda



- Zachęta dla kopaczy - nagroda 50 BTC za blok
- Wszystkie bitcoiny w obiegu pochodzą z kopania
- Co 2 lata nagroda jest zmniejszana o połowę
- Docelowo: 21 mln (z czego połowa już jest!)

https://en.bitcoin.it/w/images/en/e/e3/Total_bitcoins_over_time_graph.

Konsekwencje

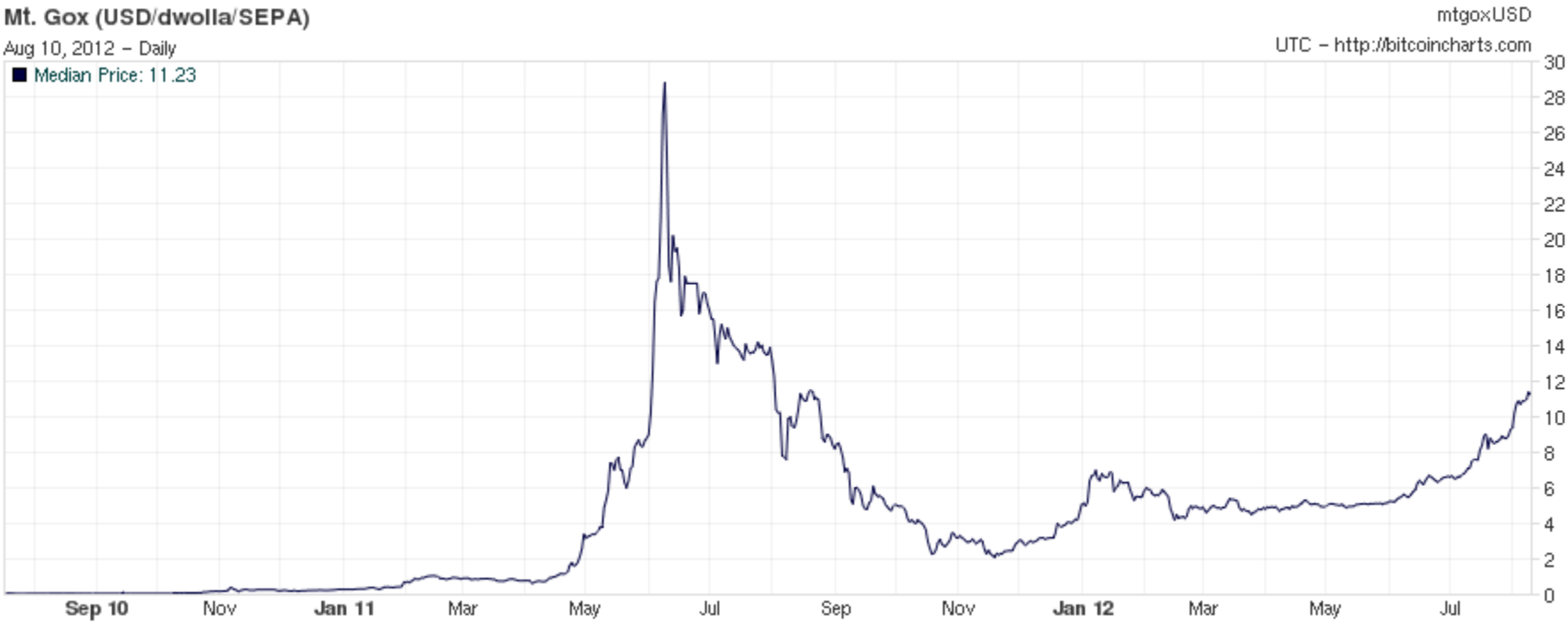
- transakcje są publiczne, ale trudno je powiązać z ludźmi
- pieniądze są w blockchainie, nie na naszym komputerze
- transakcje są szybkie i darmowe, niezależnie od ilości pieniędzy
- transakcje są nieodwracalne i nie do zablokowania
- napływ nowych BTC jest z góry ustalony - nikt nie "dodrukuje" więcej

Bitcoin obecnie

- Sporo możliwości kupna, giełd walutowych
- Nielegalny handel (Silk Road)
- Dużo spekulacji
- Early adopters: małe sklepy i firmy, indywidualny handel
- Problemy z bezpieczeństwem stron
- Duże wahania kursu

(Ilość bitcoinów) * (obecny kurs) = 100 mln USD

Historia kursu BTC



obecnie 1 BTC = 12 USD

http://bitcoincharts.com/ (mtgoxUSD)

Uwagi końcowe

- bardziej przypomina gotówkę niż pieniądze w bankach
- a jeszcze bardziej złoto
- ciekawe, jak będzie z legalnością / podatkami
- analogia do file-sharing?

Dziękuję za uwagę

Dyskusja, pytania?