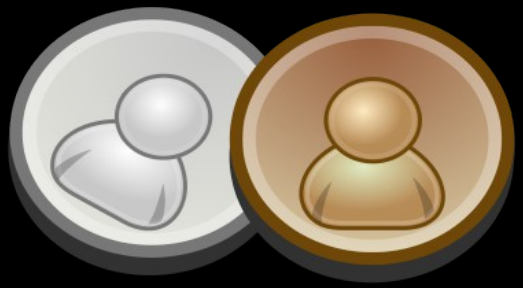
opencoin

open source digital cash



finance is changing

old world

- banks, paypal - storage and transfer
- national monopoly on money creation
  (commercial cartel - Banking Act 1848)
- centralised stock and commodity markets

finance is changing

new world

- p2p protocols
- Internet-based currencies
- crowd-funding

this talk

opencoin project

disruptive financial technology

opencoin, bitcoin, ripple

- functional properties
- technical background

what is opencoin?

digital cash

p2p transfer

anonymity/private

what is opencoin?

Open Source project (2007)

- digital cash protocol
- reference implementation
- security audit - Royal Holloway
- legal report - Queen Mary

what is opencoin?

international start-up team

- crypto
- developers
- business/economics
- legal

using banks

money created by banks

transferred by banks

transfers are records in a ledger

system resilience - crisis

banks for the user

expensive

slow

bank accounts not universally available

bad internet integration - c.f. email

cash

lives in your pocket

transferred peer to peer (p2p)

cash for the user

good privacy

cheap p2p transfer

risky to transfer long distance

no internet integration

digital cash

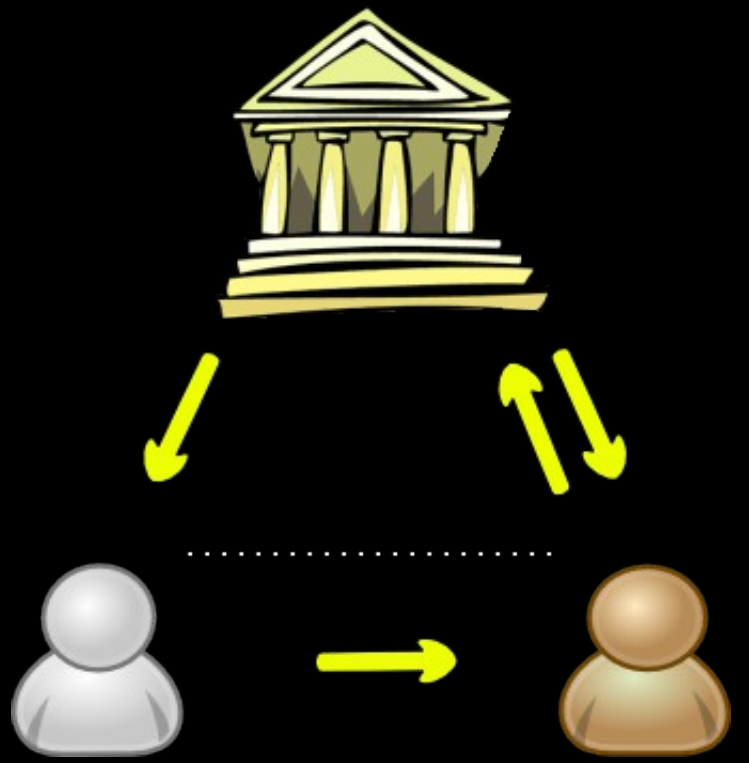
minted electronic tokens

transferred p2p (untracable)

(patent of David Chaum, expired 2005)

using digital cash

1. Alice gets coins from mint
2. Alice transfers to Bob
3. Bob exchanges or redeems



double spending

Alice gives copy of coin to Bob.

Is coin still valid? Was it spent twice?

Contact issuer to veryify validity of coin

Issuer has double spending database

opencoin protocol

...and now for some technical detail...

RSA Background

asymmetric crypto (public-private key)

RSA

- 2 large prime-numbers 'p' and 'q'
- n = p*q
- given n its hard to find p and q

standard rsa signature

key pair: public key, private key

signature = message ^ private key

blind rsa signature

blind = message * secret

blindsignature = blind ^ private key

signature = blindsignature / secret

*math simplified

opencoin issuer preparation

master key

currency description document (CDD)

- public master key, denominations, etc.

one mint key per denomination

payload creation

Alice creates payload

- serial
- info fields: denomination, mint key id, etc

blind creation

Alice chooses secret (random number)

blind = payload * secret

* math simplified

minting request

Alice:

- authenticates with issuer
- sends blind to issuer
- requests minting for denomination d

minting

issuer charges Alice's account

issuer selects private mint key for d

blind_signature = blind ^ mintkey_d

issuer sends back blind_signature

* math simplified

unblinding / creating coin

Alice unblinds

- signature = blind_signature / secret
- coin = payload, signature

payload visibility

Alice didn't send payload to issuer

=> issuer created signature on blind

=> issuer never saw payload

coin transfer

Alice sends coin to bob

any mode of transportation

- email, jabber, skype, pidgeon

coin renewal

Bob

- validates signature of coin
- creates new payload (same value as coin)
- creates blind from new payload

coin renewal II

Bob sends coin & new blind to issuer

issuer checks double spending database

issuer signs Bob's blind

issuer returns blind_signature

coin renewal III

Bob unblinds, has his own new coin

opencoin for the user

good privacy (untracable)

cheap p2p transfer (free)

fast transfer

media agnostic

open source

alternative payment systems

- bitcoin
- ripple

what are bitcoins?

there are no coins :-(

history of transactions between accounts

history kept in distributed ledger

account: pair of keys

account number: hash of public key

bitcoin ledger

history of transactions

transaction: Alice -50-> Bob

transaction signed by Alice

what is a crypto hash?

Function with output of fixed length:

1. easy to compute hash value for message
2. hard to generate message for given hash
3. can't modify message w/o changing hash

bitcoin process

transaction gets flooded to everyone

miners collect transactions into blocks

miners check if transactions are valid

- enough funds, valid signature, etc.

bitcoin blocks

miners collect transactions into blocks:

1. hash of previous block
2. freely chosen number !!
3. transaction: thin air -25-> miner
4. collected transactions

mining

find: hash(block) < x

change nonce, check hash(block), repeat...

first miner to find suitable hash wins

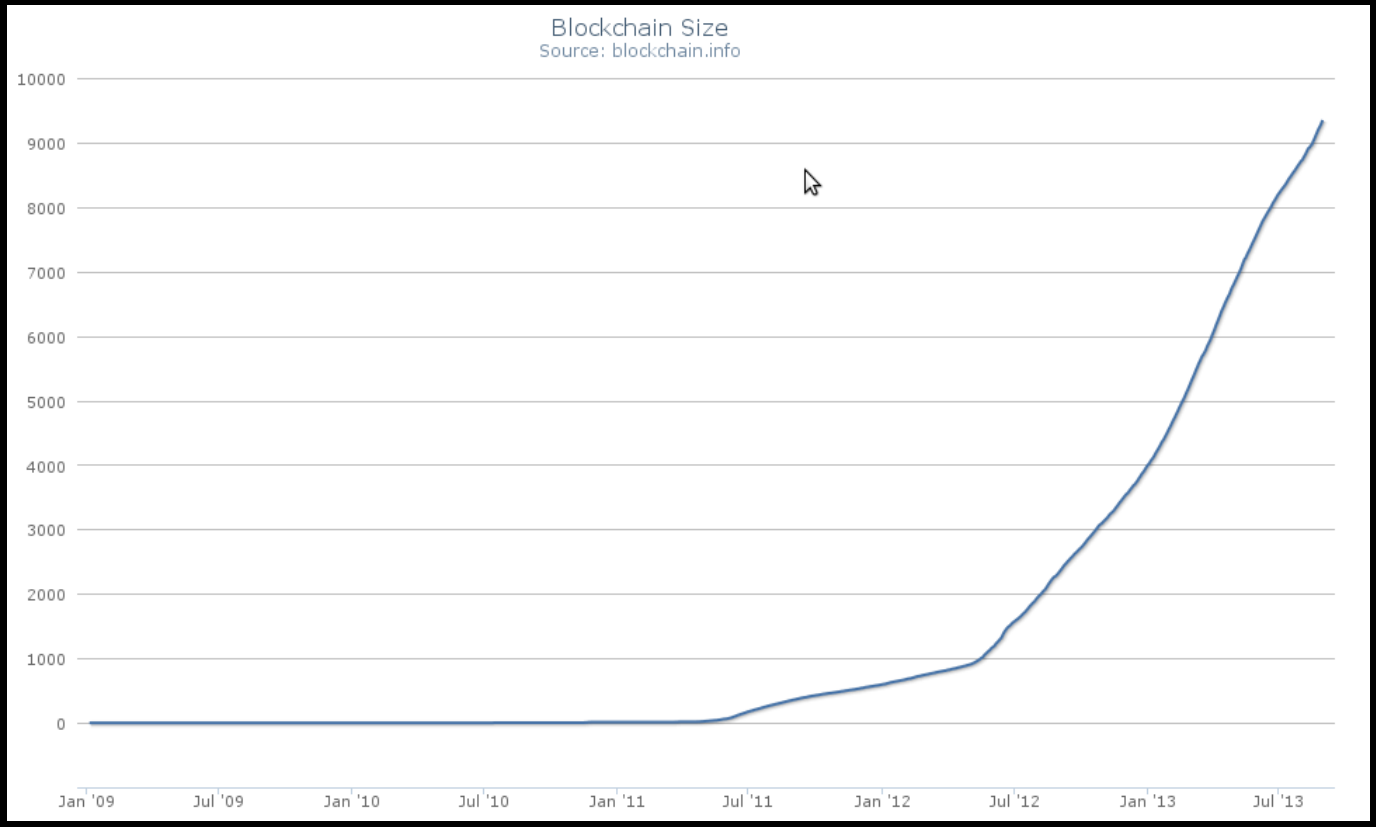
=> txn block authenticated

x is adjusted to mining speed

bitcoin vs. opencoin

bitcoin	opencoin
decentralised ledger	centralised minting
public ledger	p2p coin transfers
integrated currency	coins are tokens - any currency

bitcoin blockchain growth



currently 9 gigabytes

blockchain.info

bitcoin criticism

mining consumes a lot of power

bloomberg (April)*:

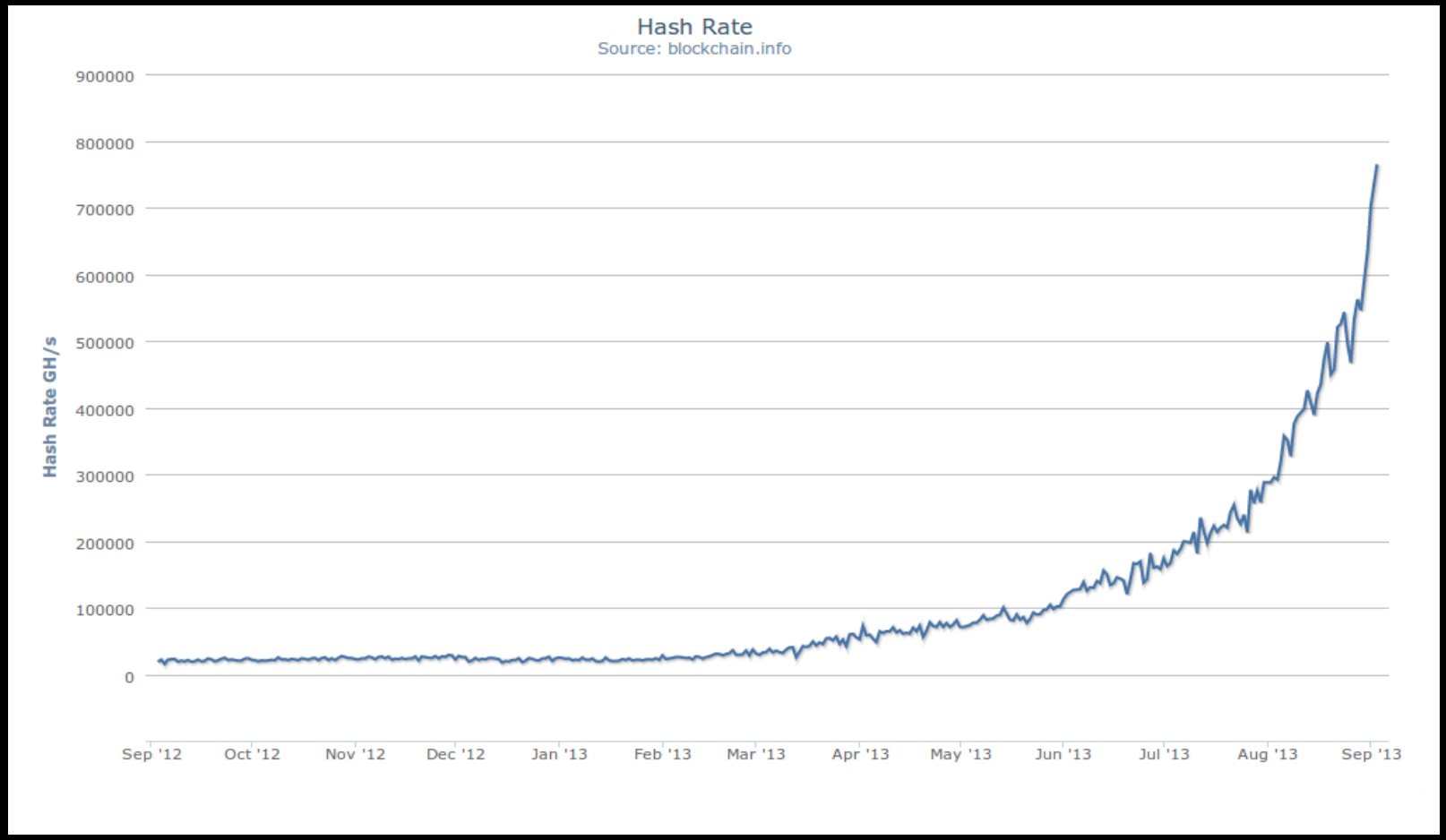
~ 1 gigawatt/hour (31,000 US homes)

transactions need ~30mins to be trusted

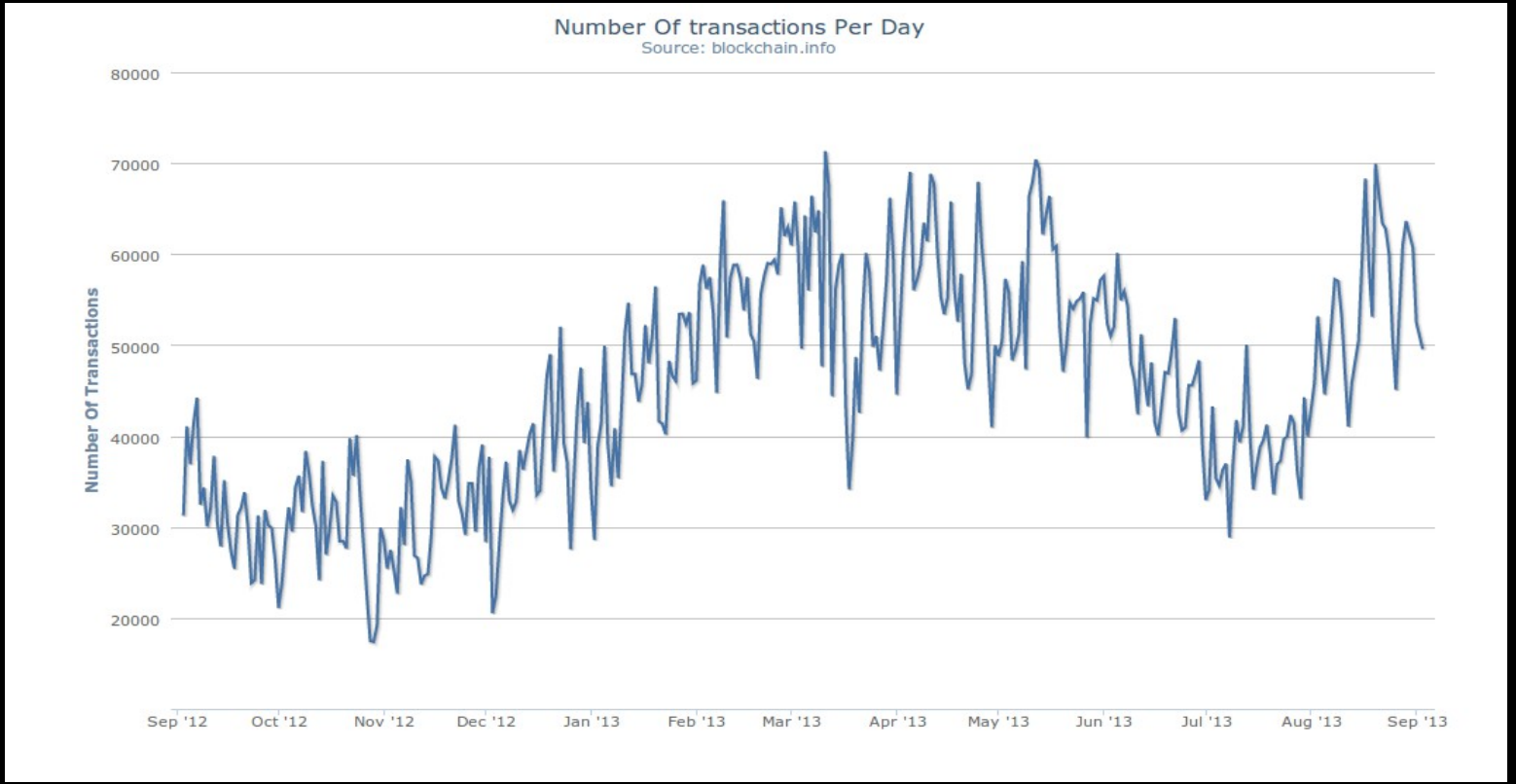
public ledger = limited privacy

* http://www.bloomberg.com/news/2013-04-12/virtual-bitcoin-mining-is-a-real-world-environmental-disaster.html

hash rate


Hash Rate
Source: blockchain.info
Hash Rate GH/s
900000
800000
700000
600000
500000
400000
300000
200000
100000
0
Sep '12
Oct '12
Nov '12
Dec '12
Jan '13
Feb '13
Mar '13
Apr '13
May '13
Jun '13
Jul '13
Aug '13
Sep '13

number of transactions/day



mining operating margin

bitcoin criticism - currency

total quantity of bitcoins limited

if txn volume continues to increase:

=> value of bitcoins will increase

=> incentive to hoard

commodities are not good currencies

ripple ledger

decentralized ledger w/o mining

consensus based system

each server trusts a set of servers

majority of trusted servers agree

=> server accepts txn

ripple payment paths

everyone can issue IOUs

Alice trusts Bob's, Bob trusts Carol's IOUs

Alice doesn't trust Carol's IOUs

Carol's can't pay Alice directly

Carol's pays Bob, Bob pays Alice

ripple

Internal currency called XRP

txn fees paid in XRP

IOUs in any currency

transfers in seconds

ripple

no coherent description of inner workings

no source code for server (yet?)

all XRP owned by producers (initially)

ripple confusion

Opencoin = opencoin.org

opencoin.org established 2007

producers of ripple.com: opencoin.com

established 2012

opencoin for the user

good privacy (untracable)

cheap p2p transfer (free)

fast transfer

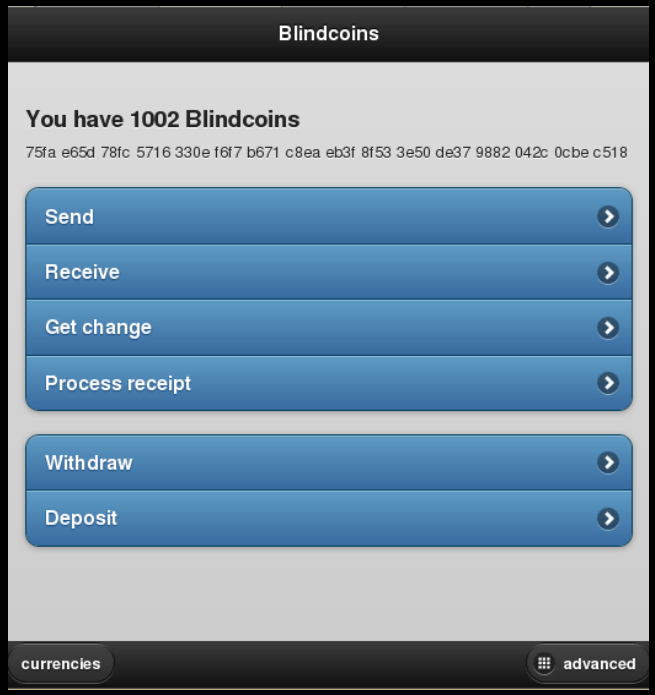
media agnostic

open source

opencoin prototypes

#1 python

#3 javascript



opencoin use cases

micropayment (content, email, etc.)

bank account alternative

international transfers

many more....

example: remittance market

more than $250 billion p.a

underdeveloped financial infrastructure

high cost critisized by World Bank, G8, governments,...

risk and operational cost

paypal	opencoin
centralised ledger	wallet security
centralised ledger	decentralised risk
defenses => cost	must only defend mint
	=> cheaper

finance is changing

banking crisis

txn system tied to investment system

systemic risk, private profit, public distrust

national and commercial monopolies

finance is changing

ecosystem of new innovations

hope for the future

high-growth potential

competition and democratic uptake

thank you!

tom@opencoin.org

http://opencoin.org

slides: http://opencoin.org/campusparty13