Westpac GROUP

Bitcoin, Banking and the Blockchain

SFMW

Sean Carmody

March 2015

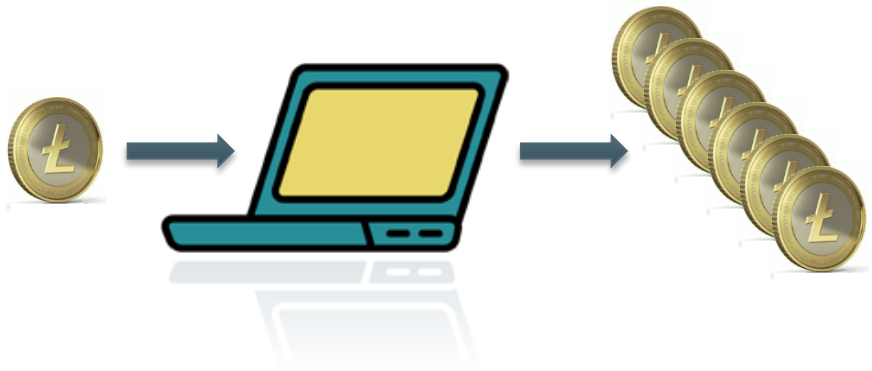
Virtual currencies are needed for a virtual world

The internet has provided a great stimulus to the globalising of communication and trade. Virtual currency is a natural complement to the virtual marketplace.

Appeal of virtual currencies:

- Facilitate international payments
- Reduce transaction costs
- Anonymity and privacy
- Lack of trust in banks or governments

But there is a “double spend” problem to solve



If virtual currency is digital, how do we prevent people making multiple copies?

Trust a central authority

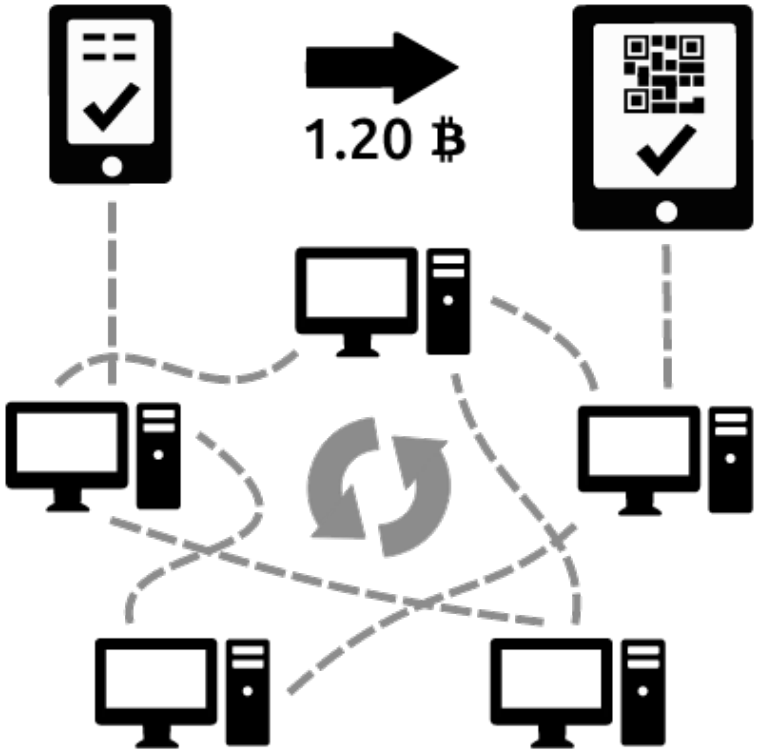
- Controls the currency
- Transactions cleared centrally
- Examples: Second Life “Linden Dollars”

“Trust the math”

- Bitcoin protocol innovation
- Cryptography replaces authority
- The “blockchain” prevents double spending of bitcoins

The blockchain offers a de-centralised solution

- The blockchain is a **shared public record** of bitcoin transactions
- A **transaction** is an instruction to transfer value from one **wallet** to another **wallet**
- Bitcoin wallets use a **secret key** to prove the transaction is authentic
- Wallets are connected in peer-to-peer network which validates the validity of transactions and maintains the blockchain



All tips payable to
1Q31t2vdeC8XFdbTc2J26EsrPrsL1DKfzr

There are a number of ways to obtain bitcoin

Bitcoin mining

- The reward for validating the blockchain
- Computationally intensive: requires serious computer hardware

Sell stuff!

Sell goods, services (or pizza) for bitcoin

https://en.bitcoin.it/wiki/Trade

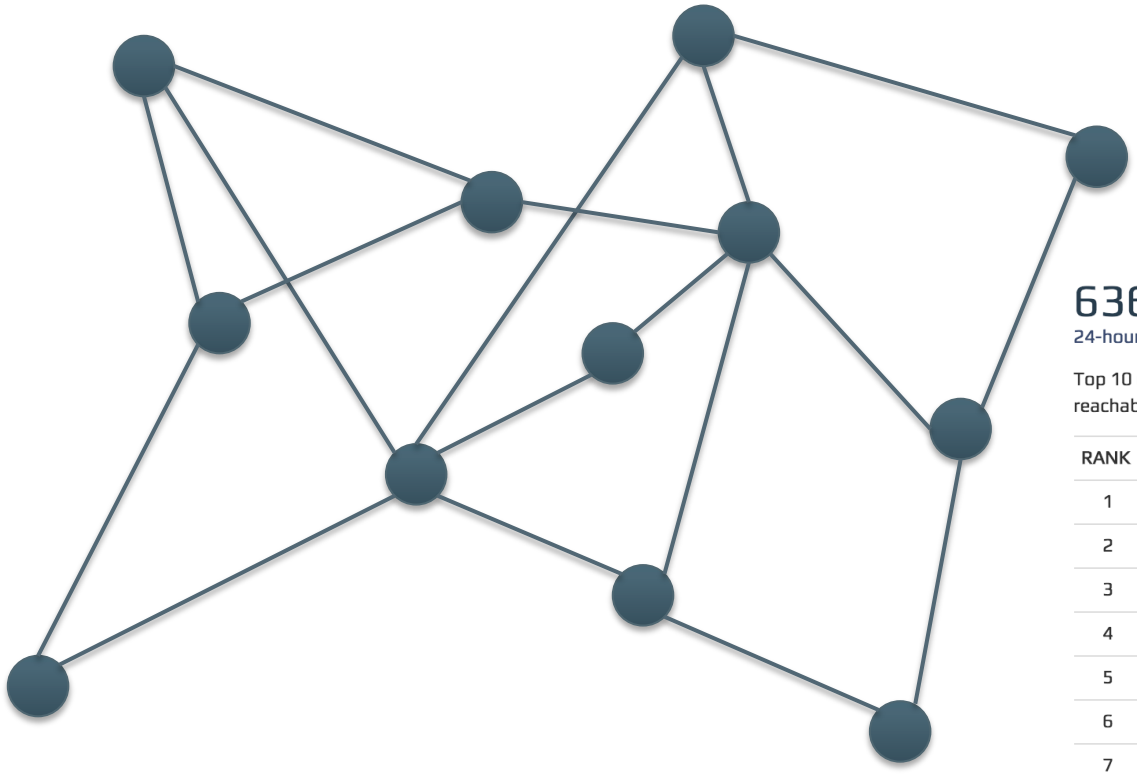
Digital currency exchanges

Buy and sell bitcoin for “real” currency

Dogecoin, Litecoin and other digital currencies operate in a similar way

- Total bitcoin outstanding: circa 13.5 million BTC or $4b in value
- The supply of bitcoin will be capped at 21 million
- Can transact in fractions of a bitcoin – 0.00000001BTC = 1 satoshi

Bitcoin peer-to-peer network provides the foundation



6368 nodes

24-hour charts »

Top 10 countries with their respective number of reachable nodes are as follow.

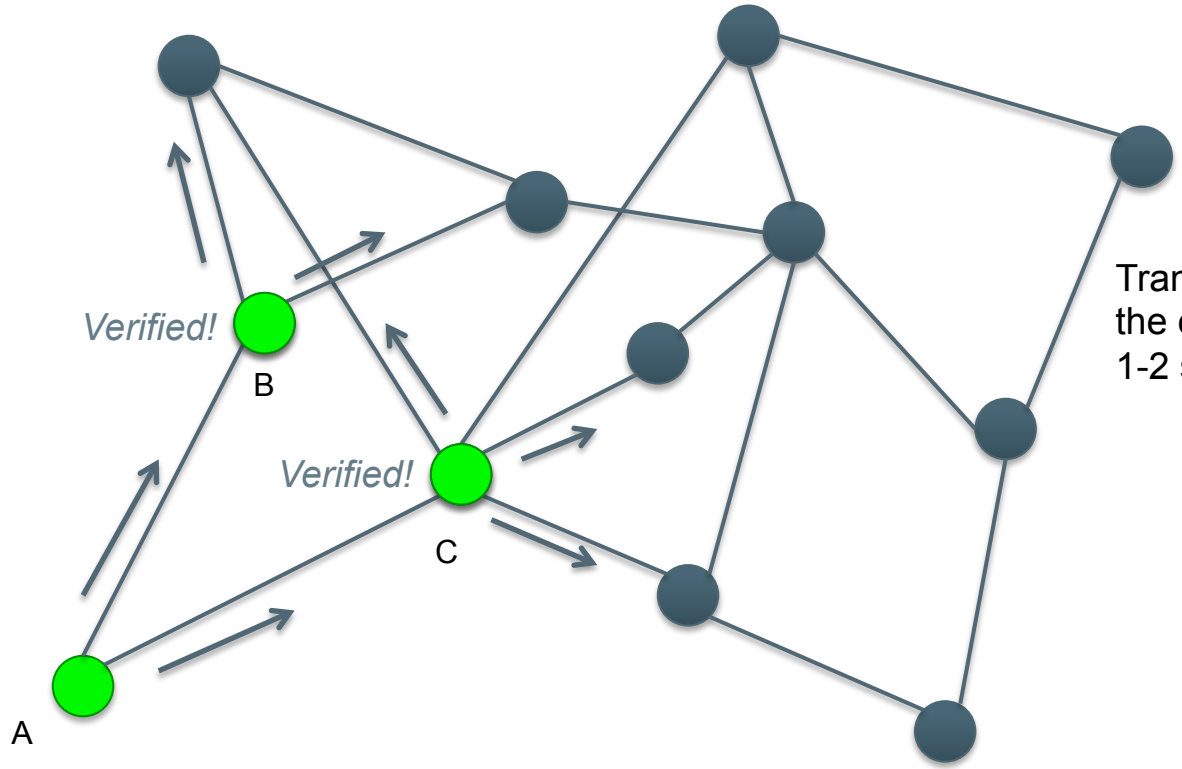
RANK	COUNTRY	NODES
1	United States	2478 (38.91%)
2	Germany	568 (8.92%)
3	France	413 (6.49%)
4	United Kingdom	389 (6.11%)
5	Canada	347 (5.45%)
6	Netherlands	301 (4.73%)
7	Russian Federation	220 (3.45%)
8	Australia	137 (2.15%)
9	China	127 (1.99%)
10	Sweden	122 (1.92%)

https://getaddr.bitnodes.io/

Each node in the network is a machine running Bitcoin client software

number of clients not accepting incoming connections circa 10x larger

Peers announce transactions to the network



Transmission across the entire network takes 1-2 seconds.

XYZ pays 1.2 BTC to ZYX

Node A announces a transaction to its peers B and C. If the transaction is verified, B and C forward the transaction to their peers. The transactions propagate rapidly across the network

Verification of transactions

Transactions are cryptographically **signed** by the owner of the source wallet

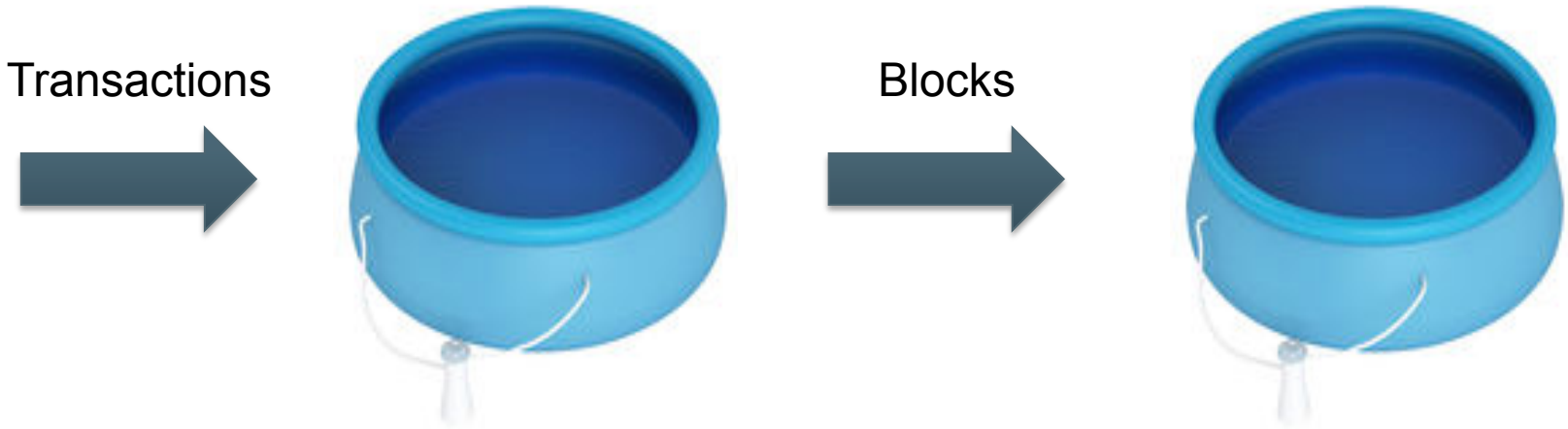
Nodes in the network verify transactions by:

1. Checking the authenticity of the signature
2. Checking the blockchain ledger to confirm the source wallet owns sufficient bitcoin to make the payment – the way this is done is the real the **innovation** in the Bitcoin protocol

Verified transactions are added to a "transaction pool" maintained across the network but do not form part of the ledger until added to a block by a "miner"

*The "**double spend**" problem is solved because bitcoins are not digital file which can be copied. Bitcoins only exist in the publicly maintained blockchain – the ledger has all the information about how many bitcoins each wallet owns.*

The bitcoin network shares its knowledge of two pools



"We have proposed a system for electronic transactions without relying on trust. We started with the usual framework of coins made from digital signatures, which provides strong control of ownership, but is incomplete without a way to prevent double-spending. To solve this, we proposed a peer-to-peer network using proof-of-work to record a public history of transactions that quickly becomes computationally impractical for an attacker to change if honest nodes control a majority of CPU power."

Bitcoin: A Peer-to-Peer Electronic Cash System
Satoshi Nakamoto (2009)

Trapdoor functions

"Trapdoor" functions are a broad class of functions that form the foundations of cryptography, including:

- Public-key cryptography
- Hash functions
- Keyed hash functions
- *Cryptographic* hash functions

A **cryptographic hash function** *h* takes a message *M* and returns a fixed length "hash" or "digest" value with the following properties:

- **Computability**
  h(*M*) is easy to compute (not necessarily by hand)
- **Pre-image resistance**
  given *d*, it is it computationally difficult to determine *M* such that *d* = *h*(*M*)
- **Collision resistance***
  it is computationally difficult to find *M* and *M'* such that *h*(*M*) = *h*(*M'*)

The SHA-2 family of functions are the current state of the art – the Bitcoin protocol uses SHA-256

* Collision resistance implies *second pre-image resistance*, namely given *M* it is computationally difficult to find *M'* such that *f*(*M*) = *f*(*M'*). Second pre-image resistance is sometimes included in the definition of cryptographic hash functions.

Public key cryptography

A **public key** encryption scheme involves a family of trapdoors function $E(k,\_)$ and a mechanism for generating pairs of **keys** (P, p) with the property that:

$$E(P, E(p, M)) = M$$

$$E(p, E(P, M)) = M$$

- *P* and *p* are **mutual decrypters**
- Share the **public key** *P* with the world, keep the **private key** *p* secret
- **Encryption**: the world encrypts using *P*, you decrypt using *p*
- **Authentication**: send out *M* and $E(p, M)$, others decrypt using *P*

- **Plain text attacks** make this approach to authentication dangerous – better practice is to send out *M* and $E(p, h(M))$ where *h* is an agreed upon hash function
- There are many other public key signature schemes – the Bitcoin protocol uses the Elliptic Curve Digital Signature Algorithm (ECDSA) known as **secp256k1**

Adding nonces makes block creation hard work

A “nonce” is a number or string only used once

For example: add a 5 digit nonce to the string “Bitcoin”:

SHA-256(‘Bitcoin [00000]’) =

A1e2246362756d82bbd442d55f9183572a8341f5bc593c1abbe982886e904acf

Challenge: find a nonce that yields a hash with a specified “difficulty”, i.e. the required number of leading zeros

Solution: use a brute-force search – but the more leading zeros, the longer the search is likely to take

Finding the nonce for a block would now take years on most laptops!

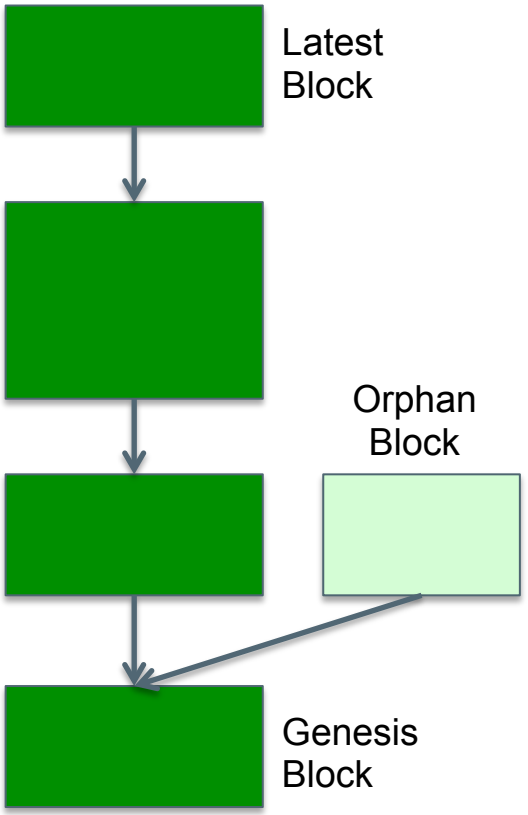
Message	SHA-256
Bitcoin [00000]	a1e2246362756d82bbd...
Bitcoin [00027]	0e69a2695aed2f112e8...
Bitcoin [01778]	009b37ae462a71c76cc…
Bitcoin [13855]	000921b4762782c5d5c…
Bitcoin [24354]	00007974c50fd431022…
Bitcoin [26605]	00000341a0effddcc593…

6167 nonces lead a leading zero, 423 nonces yield at least 2 leading zeros, 27 at least 3, 2 at least 4 and only one yields 5 yielding zeros.

Bitcoin miners work hard to create blocks

Bitcoin miners take transactions from the pool and try to bundle them into a block, which involves hashing the **block header**, which consists of:

- Protocol version
- Hash of the previous block (acts as a pointer)
- Timestamp
- Nonce
- Current hashing difficulty ("bits")
- Hash derived from the transactions ("Merkel tree")
- A transaction is considered **confirmed** once it is included in a block
- Blocks are considered part of the blockchain if they are in the longest chain from the **genesis block** – otherwise they are considered "orphans" and are ignored
- Most Bitcoin clients will not verify a transaction until it is confirmed **six blocks deep**



Finding the nonce for a block would now take years on most laptops!

An attacker would require significant power

- The Bitcoin protocol solves the **Byzantine Generals Problem**
- Imagine the network is split between an attacker and honest nodes

  p = probability an honest node finds the next block
  q = probability the attacker finds the next block

- The probabilities are determined by the share of **hashing power**

  q_z = probability the attacker will ever catch up from z blocks behind

- Assuming p > q

  $q_z = (q/p)^z$

- But if $q > p$ then $q_z = 1$ – the 51% attack, which is a real threat with **mining pools**

Why choose a depth of six?

q = 0.1 and p = 0.9

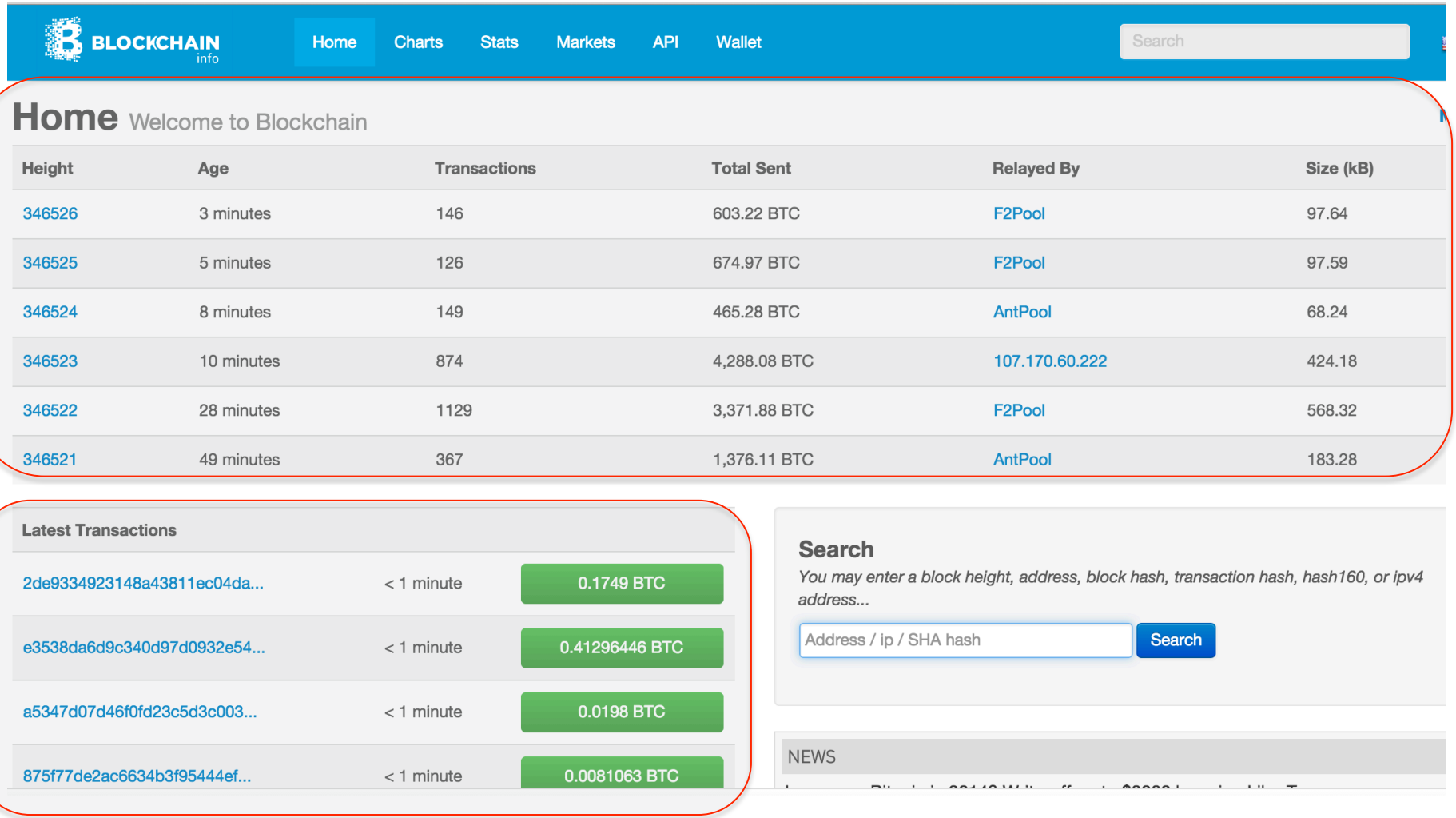
Depth	P
1	0.2045873
2	0.0509779
3	0.0131722
4	0.0034552
5	0.0009137
6	**0.0002428**
7	0.0000647
8	0.0000173
9	0.0000046
10	0.0000012

- The longer the depth in the block chain, the less chance the blocks are invalid – the probabilities shrink exponentially
- If attackers cannot control a significant proportion of the network, **a depth of six is plenty**
- When an attacker's control grows, the risks become far more signicant
- **Beware the mining pools** – ghash.io has already achieved over 50% control

q = 0.3 and p = 0.7

Depth	P
5	1.0000000
10	0.1773523
15	0.0416605
20	0.0024804

Blockchain.info provides a window onto the blockchain



The blockchain has potential beyond bitcoin

- Transaction verification can be more than just checking a signature
- A **scripting language** is built into the protocol – so more complex operations (e.g. multiple signing) are possible
- Signature verification:

```
OP_DUP OP_HASH160 4d15af3c442fc70884dbe5f975abb1083522eb20
OP_EQUALVERIFY OP_CHECKSIG
```

- Potential applications of the blockchain:
  - Equities
  - Voting rights associated with financial instruments
  - Land titles
  - Passports
  - Birth/death certificates
  - Escrow
  - Electronic keys
  - Sim cards

The mega-master blockchain list:

- A crowd-sourced brainstorm

http://ledracapital.com/blog/2014/3/11/bitcoin-series-24-the-mega-master-blockchain-list

As well as the fans, there are many bitcoin skeptics

- "if the technology is to survive and prosper, and well it should, then the other three – the pretend currency, the pretend commodity and the anarchist mob [the conspiracy-loving Bitcoin aficionados] – will have to be rudely shoved out of its way"

  Jeffrey Robinson

- "Blockchains and consensus ledgers may find traction outside of **niches** only if they satiate mass consumer appeal, not just **hobbyist interest**"

  Tim Swanson

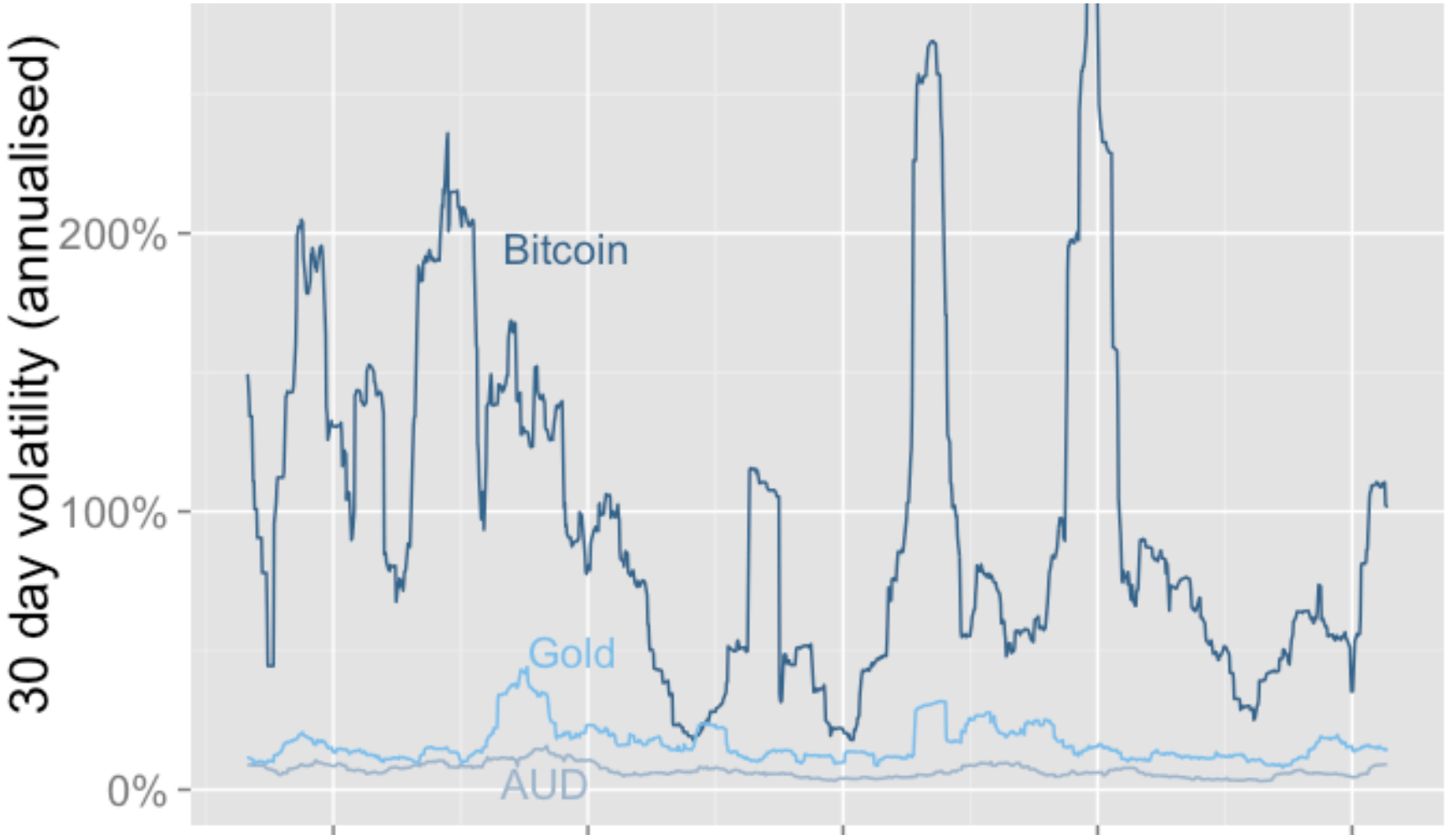
- "the hope that a whole new protocol — bitcoin — will essentially do for digital transactions what the internet did for communications, just by dint of being cheap and open-source. I wish it luck, but it's going to need it."

  Felix Salmon

The value of bitcoin has had a rocky road

Around US$5m in bitcoin is traded daily across the major exchanges, including Bitfinex, Bitstamp and btc-e

Bitcoin is an order of magnitude more volatile than A$



Bitcoin presents a range of challenges for banks

	Area	Impact
1		**Anonymity and obfuscation** Virtual currencies can facilitate rapid and anonymous movement of funds across jurisdictional borders without identification and verification of the customer and reporting of suspicious transactions.
2		**Criminal attraction** Virtual Currency is "cash for the internet" and like cash, while there are legitimate uses criminals also use to buy illicit online services (e.g. Silk Road) and setting up **scams/ frauds** for investors.
3		**Vulnerable to cybercrime** DCEs, traders and users of virtual currencies are all vulnerable to cyber attacks including malware, ransomware, denial of service attacks and cyber-pick pocketing of the virtual wallet.
4		**Lack of regulation and/or scrutiny** Virtual currencies, DCEs and traders are not currently regulated in Australia, hence no governance structure, business oversight or complaints process. Transactions are not reversible. The newly formed Australian Digital Currency Commerce Association (ADCCA) is lobbying Government and Regulators to be regulated and recognised.
5		**Lack of AML/CTF legislation** Currently no requirements under Australian AML/CTF legislation for DCEs to have an AML/CTF Program or obligations to know, monitor or report their customers. The ADCCA is promoting self-regulation by its members of AML/CTF requirements such as KYC and transaction monitoring.

Bitcoin mining isn't very green

"Currently, the miners on the Bitcoin network are doing about 25 million gigahashes per second. That is, every second about 25,000,000,000,000,000 blocks gets hashed. I estimate (very roughly) that the total hardware used for Bitcoin mining cost tens of millions of dollars and uses as much power as the country of Cambodia."

Ken Shiriff

http://www.righto.com/2014/02/bitcoin-mining-hard-way-algorithms.html

Dedicated bitcoin mining hardware

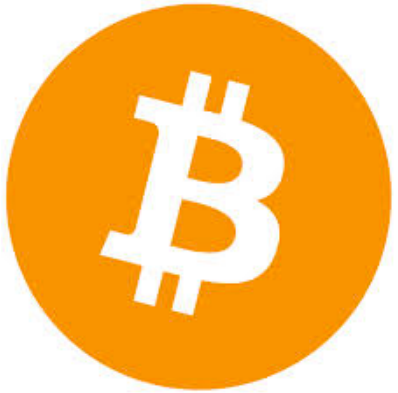
In practice the need for trust has not been removed

"The root problem with conventional currency is all the trust that's required to make it work. The central bank must be trusted not to debase the currency, but the history of fiat currencies is full of breaches of that trust."

Satoshi Nakamoto, 2009

- Many bitcoin transactions are now mediated through online wallets, which are far more **convenient** but are based on **trust** in the wallet provider
- Bitcoin loss or theft from **inputs.io**, **MtGox** and, most recently, **Bitstamp** show that this trust can be misplaced
- With large mining pools like ghash.io gaining close to 50% of the hashing power, it becomes necessary to trust their bona fides too

So what is the future of bitcoin?



"In many ways it is akin to Napster, the pioneering file-sharing service that upended the music industry in 1999 by allowing internet users to call up almost any song at will. Though Napster, unlike Bitcoin, was illegal, it demonstrated that there was enormous demand for what it provided, prompting many other services to spring up in its wake. Just as Napster paved the way for BitTorrent, iTunes and Spotify, Bitcoin has triggered a surge of innovation in digital money."

The Economist (November 2013)