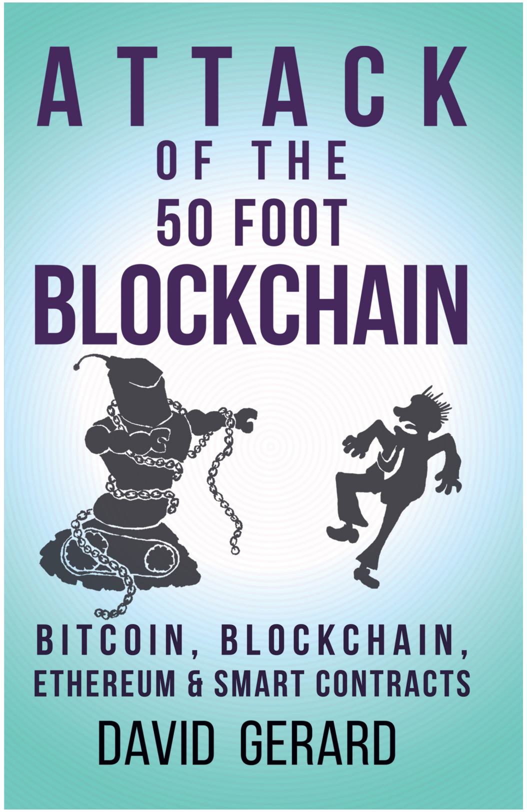
Welcome to the Blockchain

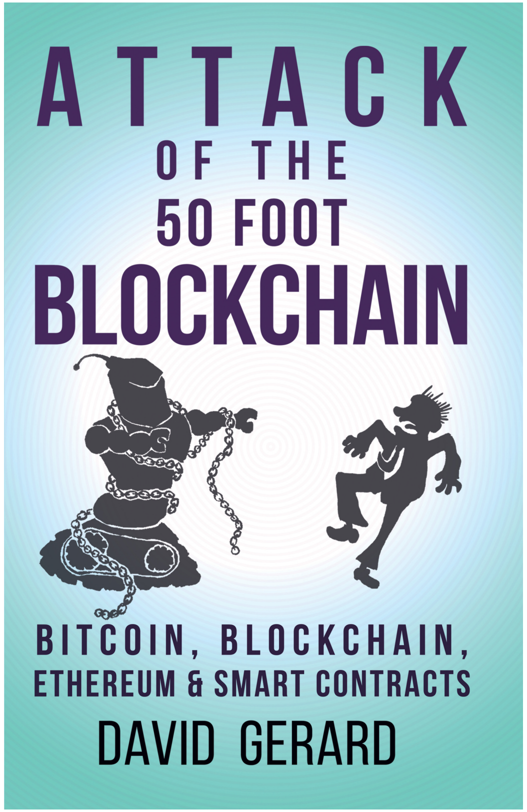
The basics of Blockchain and Bitcoin

David Gerard



David Gerard

- Music journalist, moved to IT
- Started following Bitcoin in 2011
- Started *Attack of the 50 Foot Blockchain* in late 2016
  – *well-timed for the bubble!*



The basics of Blockchain

What actually is all this stuff?

1. The blockchain data structure – *the good bit*
2. Bitcoin – *how it works, how it doesn’t work*
3. Business blockchain – *“but what are the use cases?”*

1. What on earth is a “blockchain”?

Simple accounting ledger

- Just a list of transactions

From	To	Date	Amount
Satoshi	Hal	09 January 2009	$50.00
Vitalik	Gavin	09 January 2009	$1,000.00
Craig	Ian	10 January 2009	$0.02
Vitalik	Eliezer	12 January 2009	$300,000.00
Mark	Aleksandr	13 January 2009	$400,000,000.00

- But – how can we ensure against errors?

Check digits

- Last digit of a credit card:

4012 8888 8888 1881

- Calculated from the other digits – a *checksum*
- If it’s wrong, it’s not a valid card number!

Hashes – extended check digits

- Much longer checksum, from any data
- *e.g.*, 8743b52063cd84097a65d1633f5c74f5
- If the hash is the same, the data is the same!
  - *128-bit hash → one in 2^{128} or 3.4×10^{34} chance of clash*
- Very fast to calculate – *data→hash*
- Utterly unfeasible to reverse! – *hash → data*
  - *very hard to fake!*

Simple ledger with hashes

- Let’s attach a hash to every record!

From	To	Date	Amount	Hash
Satoshi	Hal	09 January 2009	$50.00	8227fb49
Vitalik	Gavin	09 January 2009	$1,000.00	d64ad954
Craig	Ian	10 January 2009	$0.02	85e19b86
Vitalik	Eliezer	12 January 2009	$300,000.00	9749ce74
Mark	Aleksandr	13 January 2009	$400,000,000.00	5c397c18

So we know each record is correct

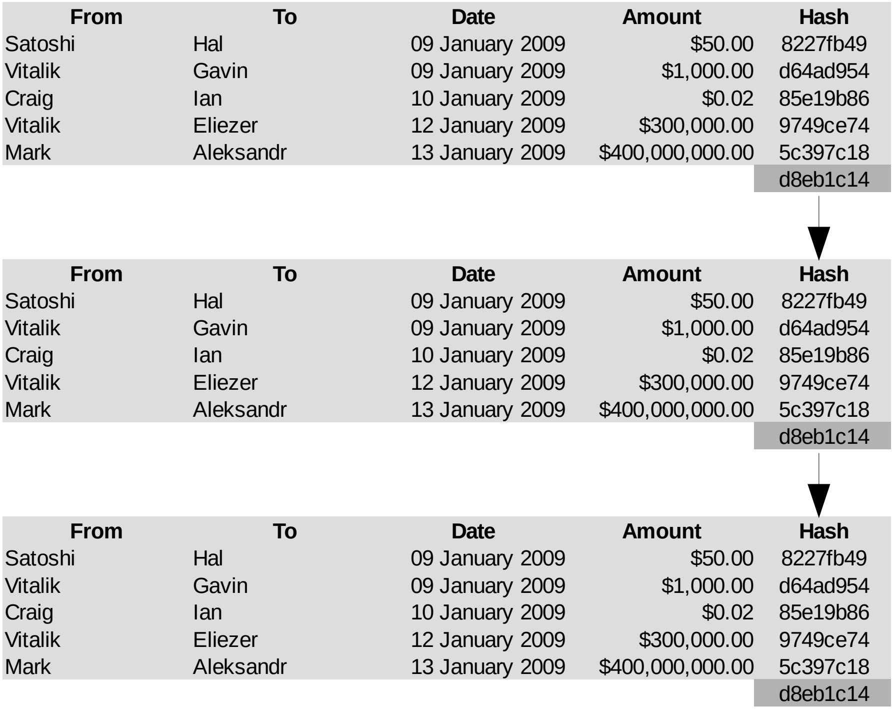
Let’s hash all the hashes!

From	To	Date	Amount	Hash
Satoshi	Hal	09 January 2009	$50.00	8227fb49
Vitalik	Gavin	09 January 2009	$1,000.00	d64ad954
Craig	Ian	10 January 2009	$0.02	85e19b86
Vitalik	Eliezer	12 January 2009	$300,000.00	9749ce74
Mark	Aleksandr	13 January 2009	$400,000,000.00	5c397c18
				d8eb1c14

- So if we know that last hash – we know that the whole block has to come to that hash!
- Saves rehashing whole block for each new entry

Let’s chain the blocks!

- Each block’s hash is also hashed with the next block
- This gives us a hash of the whole chain



From	To	Date	Amount	Hash
Satoshi	Hal	09 January 2009	$50.00	8227fb49
Vitalik	Gavin	09 January 2009	$1,000.00	d64ad954
Craig	Ian	10 January 2009	$0.02	85e19b86
Vitalik	Eliezer	12 January 2009	$300,000.00	9749ce74
Mark	Aleksandr	13 January 2009	$400,000,000.00	5c397c18
				d8eb1c14

From	To	Date	Amount	Hash
Satoshi	Hal	09 January 2009	$50.00	8227fb49
Vitalik	Gavin	09 January 2009	$1,000.00	d64ad954
Craig	Ian	10 January 2009	$0.02	85e19b86
Vitalik	Eliezer	12 January 2009	$300,000.00	9749ce74
Mark	Aleksandr	13 January 2009	$400,000,000.00	5c397c18
				d8eb1c14

From	To	Date	Amount	Hash
Satoshi	Hal	09 January 2009	$50.00	8227fb49
Vitalik	Gavin	09 January 2009	$1,000.00	d64ad954
Craig	Ian	10 January 2009	$0.02	85e19b86
Vitalik	Eliezer	12 January 2009	$300,000.00	9749ce74
Mark	Aleksandr	13 January 2009	$400,000,000.00	5c397c18
				d8eb1c14

Tamper-evident append-only ledger!

- Distribute the ledger
- You can quickly verify the hashes of your copy
- But – it’d be impossibly slow to fake
- This hash-of-hashes construct is called a Merkle Tree (1979)
- Used in Bitcoin (2009)

2. Bitcoin

2. Bitcoin

- Digital cash would be a useful thing
- We could use this hard-to-fake ledger for our new digital cash!
- But – who gets to add new entries?
- Obvious answer: central authority (bank)
- But ...

Bitcoin’s founders had odd requirements

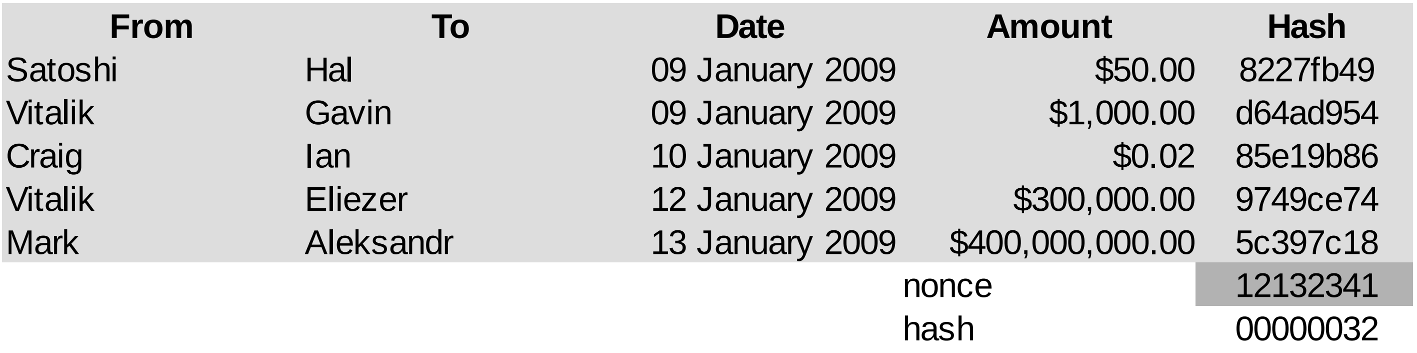
- Founded in ideology *– very strong libertarianism*
- No central authority at all – *no trust requirement*
- Can’t just print money – *monetary policy = evil!*
- A completely rigid gold standard! *– digital version*
- Credit is bad too – *use the actual “gold” as money*

How bitcoins are issued

- 21 million Bitcoins total, released slowly
- New bitcoins issued every ~10 minutes
- How to do this with no central authority?
- *Make it a lottery!*

How Bitcoin mining works

- Get a block of transactions
- Guess a random number (“nonce”), add to end
- Take the hash!



From	To	Date	Amount	Hash
Satoshi	Hal	09 January 2009	$50.00	8227fb49
Vitalik	Gavin	09 January 2009	$1,000.00	d64ad954
Craig	Ian	10 January 2009	$0.02	85e19b86
Vitalik	Eliezer	12 January 2009	$300,000.00	9749ce74
Mark	Aleksandr	13 January 2009	$400,000,000.00	5c397c18
			nonce	12132341
			hash	00000032

How Bitcoin mining works

- If the hash is a small enough number –
  you win the bitcoins!
- If you don’t – guess again
- Literally – just guessing numbers very fast
  – no “complex calculations”, just simple ones fast

  – 14,000,000,000,000,000,000,000 guesses every 10 minutes, 1 winner

“Proof of Work” – Proof of Waste

- If too many people win – make it harder!
- Ends up in Red Queen’s race
  – adding more power to stay in the same place
- As much power as Ireland – 0.1% of world
  – literally wasted guessing numbers
- Only does 7 transactions/second *– same since 2009*
- So … what does all this get us?

The fabulous promises of Bitcoin!

- Decentralised! Trustless!
- Fast and free!
- Uncensorable and irreversible!
- No QE, *a.k.a.* just printing money!
- Will destroy banks and governments!
– they really claimed this

How the promises worked out

- Bitcoin had recentralised by early 2014
- Proof of Work has economies of scale
  – so it recentralises
- Four mining pools issue most of the bitcoins

How the promises worked out

- Bitcoin was fast and near-free up to mid-2015
- … when the transactions reached capacity
- Bitcoin transactions have been slow, unpredictable and expensive since
- Peaked at $55 average fee in Dec 2017

How the promises worked out

- Uncensorable! Irreversible!
- Turns out not to be what users want
  - *consumers like chargebacks, increases confidence*
- Errors, fraud, thefts not easily reversible
  - *irreversibility is a fraudster's charter*
- Brittle!
  - *one mistake and you've lost your coins*

How the promises worked out

- No QE, rigid issuance – imitation gold standard
- But we gave up gold standard for good reason
- Deflationary currency → no reason to spend
- Even when a merchant adopted Bitcoin, bitcoiners didn’t spend – they held
- Only black markets – *e.g.*, darknet drugs
  – even they don’t like Bitcoin – too slow, too volatile

How the promises worked out

- You can’t “just print” bitcoins
- BUT – anyone can copy the code
  – and they did – 1000+ altcoins
- Market treats all these as one pool, “cryptos”
- Bitcoin is just like gold! … if you could create new gold mines by cut’n’paste

How the promises worked out

- Has so far not destroyed banks, governments
- Ideas of regulatory response at odds with how regulators treat other innovations in finance
- Some enthusiasts are at odds with the world
  - *Majority of crypto fans are fine – reality-based*
  - *But the odd ones are very loud*

Can altcoins do better?

- Bitcoin was the first paper/string mock-up, pressed into service
- Others can be a bit faster with proof-of-work
  - *Ethereum runs 16 transactions/second*
  - *already having transaction clogs – CryptoKitties!*
- Experimental new work – unfinished or not fully tested
  - *IOTA, Hashgraph, etc*
- But so far, no new solutions

3. Business Blockchain

What organisations want

- Any organisation – business, non-profit, gov – has bureaucracy – the machinery they run on
- Can we make this work better?
- … with ***blockchains?***

“Blockchain”

- Bitcoin losing lustre by early 2014
- So, market to business as “Blockchain technology”
- *a.k.a.* “Distributed Ledger Technology” (DLT)
  – do shared Excel sheets count?
- But – the promises are still Bitcoin promises!
  – else, shared Excel sheets would count

The fabulous promises of Blockchain!

- Literally the Bitcoin promises
  – just change the buzzword!
- Decentralised, fast and free!
- Uncensorable, irreversible, immutable, incorruptible!
  – nobody say “GDPR”
- Smart Contracts for added magic!

The fabulous promises of Blockchain!

Actual promises from one large vendor:

- “an enterprise-class, cross-industry open standard for distributed ledgers that can transform the way business transactions are conducted globally”

- “highly secure blockchain services and frameworks that address regulatory compliance across financial services, government, and healthcare”

The fabulous promises of Blockchain!

- Last two – “is” statements that are really “could”
  - *“could” is a word meaning “doesn’t”*
- No existing software does all those things
- Blockchain marketing promises things that *literally don’t exist yet*
  - *e.g. patient-controlled healthcare data*
- If it sounds too good to be true … it is.

Permissioned blockchains

- Usual case in business
  – all participants known, authorised
- Don’t want your back office on the public Net
- Don’t use Proof of Work (it’s silly)
- This is also called a “database”
- Even if shared – someone runs it, controls access

Smart Contracts

- Small computer programs
- Run automatically when something happens
- Immutable, like the blockchain
  – this is your market integrity
- VERY hard to get right –
  must deploy perfect program
  – all computer programs have bugs

Smart Contracts

- Ethereum was written to run smart contracts
- Gavin Wood – 2nd lead Ethereum developer
  – wrote the Ethereum protocol doc
- Wood’s startup Parity lost $160m in Nov 2017 to a programming error
- Up in smoke, irretrievable

Smart contracts on permissioned blockchains

- “Smart contract” in a closed system just means “computer program”
- Salesman: “The magic bit is done with … smart contracts!”
- Translation: “We could do it on a … computer!”
- Will be much like any other new large IT system

Blockchains in the real world

- Almost none in production use
- World Food Programme
  – single-user private Ethereum – i.e., a database
- Press releases
  – a majority from IBM
- Pilot programmes
  – “BOJ and ECB joint research project on distributed ledger technology”
  – didn’t go well

More realistic pitch: fix your data!

- Blockchain will clean up your data!
- Will clean up your formats!
- Will fix up years of accumulated cruft!
- For free! ← *maybe not*

Fund that boring back office cleanup!

- “The word ‘blockchain’ has managed to make that boring back-office coordination work sexy, which means that it might actually get done.”
  – Matt Levine, Bloomberg, 11 July 2016
- Works, too! – e.g. Walmart supply chain pilot
- So – use “blockchain” to lock in funding!
- (You don’t have to actually use a blockchain)

6 questions for your salesperson

The obvious skeptical questions:

1. Are they mixing up “might” and “is”? Does their software do *all* the stuff they said?

2. Will the system scale to the size of your data? How?

3. How do you deal with human error in the “immutable” blockchain or smart contracts?

6 questions for your salesperson

4. If this is to work with people you trust less than the ones you deal with now – what’s your threat model?

5. If it’s to work with people you can already trust – why blockchain?

6. What does this get you that a centralised database can’t?

The good bit: The data structure

- The append-only tamper-evident ledger!

From	To	Date	Amount	Hash
Satoshi	Hal	09 January 2009	$50.00	8227fb49
Vitalik	Gavin	09 January 2009	$1,000.00	d64ad954
Craig	Ian	10 January 2009	$0.02	85e19b86
Vitalik	Eliezer	12 January 2009	$300,000.00	9749ce74
Mark	Aleksandr	13 January 2009	$400,000,000.00	5c397c18
				d8eb1c14

  – *the good bit is the 40yo data structure*

Real-life example: KSI Blockchain

- Estonia’s “blockchain revolution”
- First released 2007
- Widely touted as “blockchain success story”
- Not a blockchain at all – just the ledger
- Name is for marketing
  – definitely worked!

Issues to consider

- Magic doesn't happen
  – *if it sounds too good to be true, it probably is*
- Talk to your programmers and sysadmins
- You may have a use case for the Merkle tree ledger
- Even if it's marketed as "blockchain" or "DLT"

What we’ve covered today

- How the good bit works – the Merkle tree
- How the silly bit works – Bitcoin proof of work
- Business blockchain – beware magical promises

Any questions?

- David Gerard
- dgerard@gmail.com
- www.davidgerard.co.uk/blockchain/
- Twitter: @davidgerard