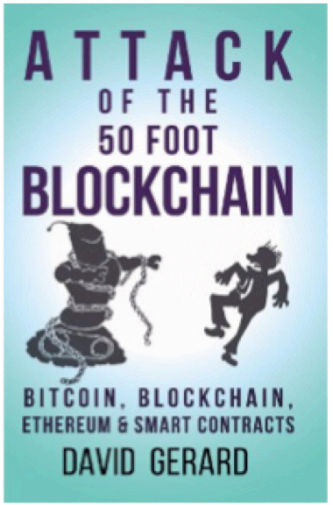
What is Blockchain – a primer for market researchers

David Gerard

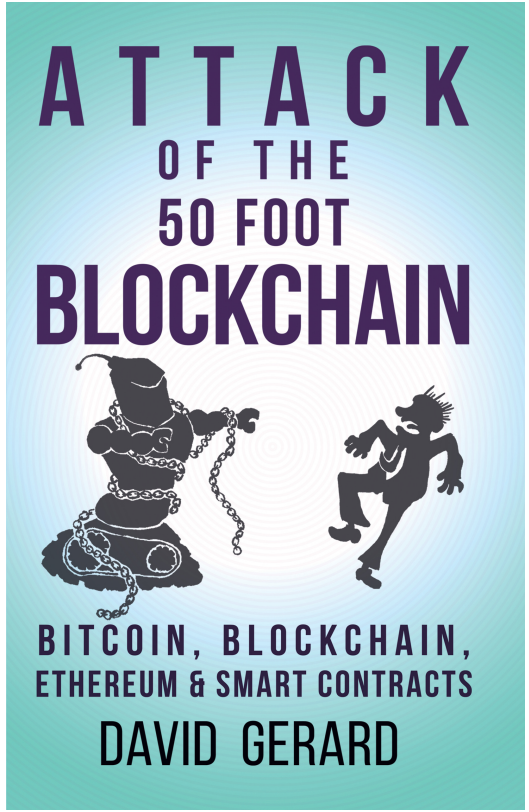
Author and Crypto Journalist



What can the Blockchain do for me?

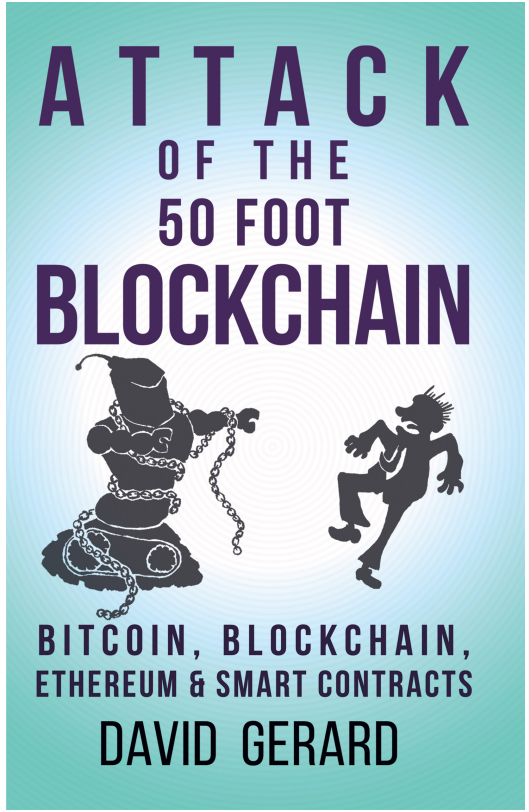
The basics of Blockchain —
what, why, cautions to take

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 — *append-only ledgers*
2. Bitcoin — *the origin of “blockchain” hype*
3. Blockchain in business — *“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!
- Very fast to calculate – *data→hash*
- Utterly unfeasible to reverse! – *hash → data*
  – *very hard to fake!*
- *We'll mention hashes again later ...*

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

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)
- So … where did all the magical promises for “Blockchain” come from?

2. Bitcoin

2. Why 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

- Not a payment system, but a political project
- Founded in ideology — *extremist libertarianism*
- No central authority at all — *no trust requirement*
- A completely rigid gold standard! — *digital version*
- Credit is bad too —*use the actual “gold” as money*

The fabulous promises of Bitcoin!

- Decentralised! Trustless!
- Fast and free!
- Uncensorable and irreversible!
- No “just printing money”!
- Will destroy banks and governments!
  – *they really claimed this*

How the promises worked out

- Bitcoin had recentralised by early 2014
- Bitcoin “mining” has economies of scale
  — *so it recentralises*
- Four mining pools issue most of the bitcoins
- One company makes 80% of the mining chips
- Bitcoin uses 0.1-0.5% of *all the electricity in the world*
  — *for 7 transactions per second worldwide*

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

- 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
- Other coins (“altcoins”) don’t do much better

3. Blockchain for business

What organisations want

- Any organisation — business, non-profit, government — 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*
- “Blockchain” is a particular collection of marketing promises
  — *not any particular technology*

The fabulous promises of Blockchain!

- Literally the Bitcoin promises
  — *just change the buzzword!*
- Decentralised, fast and free!
  — *“against who” is not clear — no sensible threat model*
- Uncensorable, irreversible, immutable, incorruptible!
  — *nobody say “GDPR”*
- Smart Contracts for added magic!
  — *the hard bit is always done by “smart contracts”*
  — *which literally means “with a computer program”*

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.

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
  — *lots of these from IBM*
  — *all actually centralised systems (Walmart, Maersk)*

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?

GDPR and blockchains

- GDPR requires *any* collection of personal data to be *redactable*
- **Never** put personal data into a blockchain!
- Blockchain-for-marketing pitches claim using a blockchain will help *comply* with GDPR
- This is completely false

How to reverse a hash

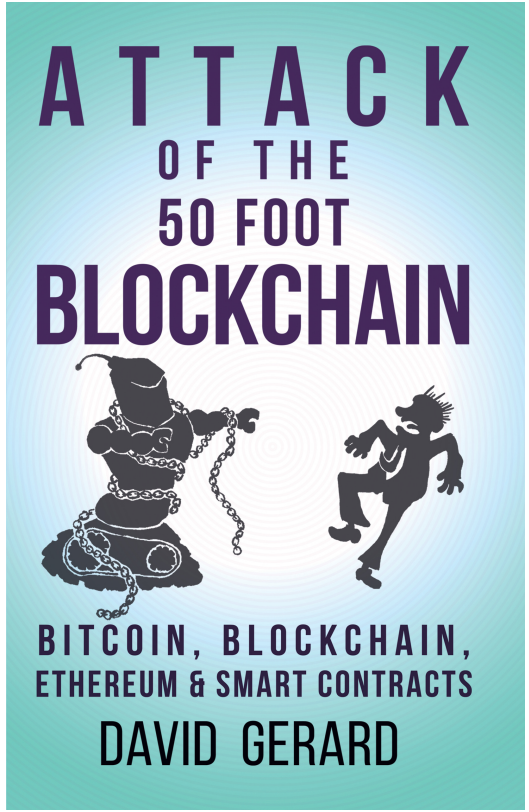
- Hashes are irreversible …
  … unless you have a table of someone else's hashes

Issues to consider

- Magic doesn’t happen
  — *if it sounds too good to be true, it probably is*
- **Never** put personal data into a blockchain!
  — *even hashed personal data*
  — *don’t let even slightly personal data within a mile of it*
- If it sounds too good to be true …
- … it probably is

Any questions?

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



Q & A

David Gerard

Ray Poynter

NewMR 2018 Sponsors

Gold

conjoint.ly

WATCH ME THINK

P2 SAMPLE
POWERFULLY PROGRAMMATIC

Confirmit.

INFOTOOLS

netquest

QuestionPro
Communities

Further

Silver

HAPPY THINKING PEOPLE
THE PEOPLE UNDERSTANDING COMPANY

TALK EYE

M ESH
The Experience Agency

AMAI 25 AÑOS
INTELIGENCIA APLICADA A DECISIONES

UNIVERSITY OF GEORGIA

MRII
MARKET RESEARCH INSTITUTE INTERNATIONAL

LiGHTSPEED

Communication

keen as mustard.
marketing for data, research & insight

#NewMR