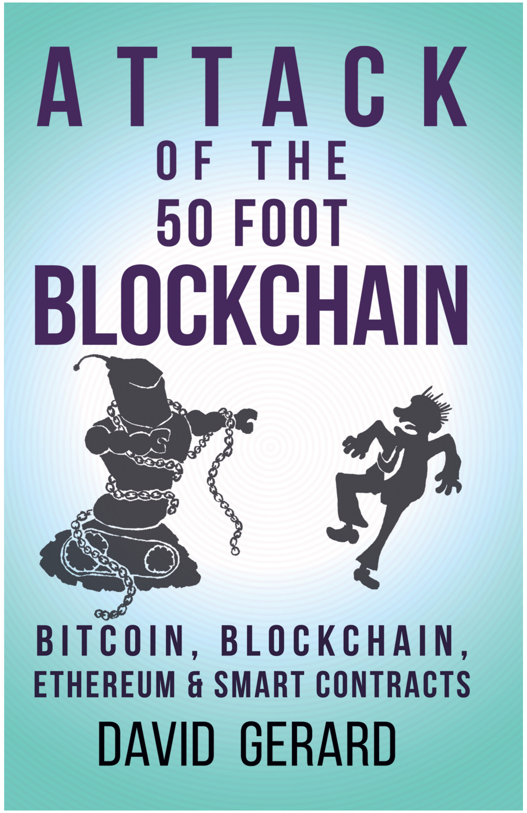
Cryptocurrency, blockchains and markets

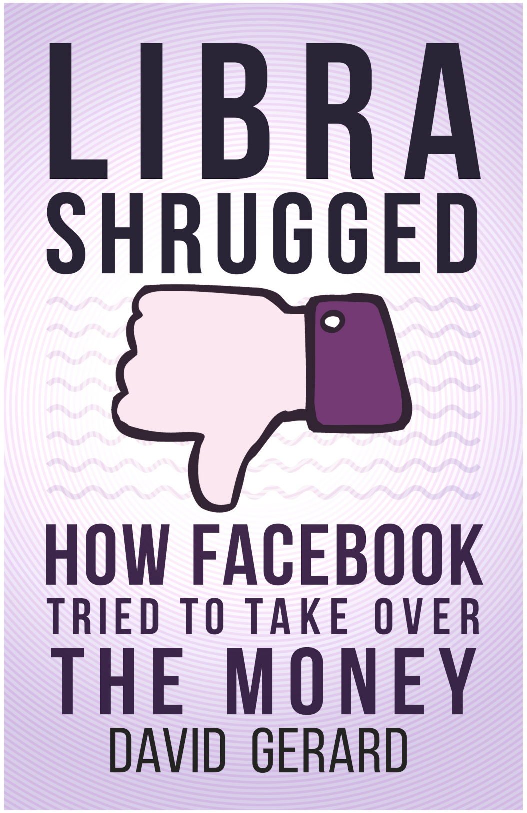
The market in magical Internet money — and how to take due caution

David Gerard



David Gerard

- Music journalist, moved to IT
- Started following Bitcoin in 2011
- *Attack of the 50 Foot Blockchain* 2017, *Libra Shrugged* 2020
- News site: davidgerard.co.uk/blockchain/



What actually is all this stuff?

Today’s talk:

1. The fabulous promises of cryptocurrency and blockchain!
2. What a blockchain actually is — *append-only ledgers*
3. Bitcoin — *the origin of “blockchain” hype*
4. Cryptocurrency in finance — *trader beware!*
5. Enterprise blockchain — *“but what are the use cases?”*

1. The fabulous promises of cryptocurrency and the “blockchain”!

The fabulous promises of crypto!

- Trustless!
- Decentralised!
- Fast and free!
- Uncensorable and irreversible!
- Immune to bad actors!
- Secured by math!

The fabulous promises of crypto*!

** apologies to any cryptographers in the audience*

- Trustless! — *against who?*
  (actually means "a computer doesn't have to trust another computer in particular mathematically defined circumstances", not the squashy English word)
- Decentralised! — *against what threat?*
- Fast and free! — *except when it's neither*
- Uncensorable and irreversible! — *do you actually want this?*
- Immune to bad actors! — *except in practice*
- Secured by math! — *everything that goes wrong except the cryptography itself is redefined as "user error"*

2. What on earth is a “blockchain”?

What on earth is a “blockchain”?

- The first question *everyone* asks
- An old data structure – Merkle tree (1979)
- adopted by Bitcoin (2009)
- The good part is simple!
- The bad part is silly

A 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 protect against errors?

Check digits

- The last digit of a credit card isn’t in fact part of the card number:

  4012 8888 8888 1881

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

Hashes – extended check digits

- A *hash* is a 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

So we know each record is correct

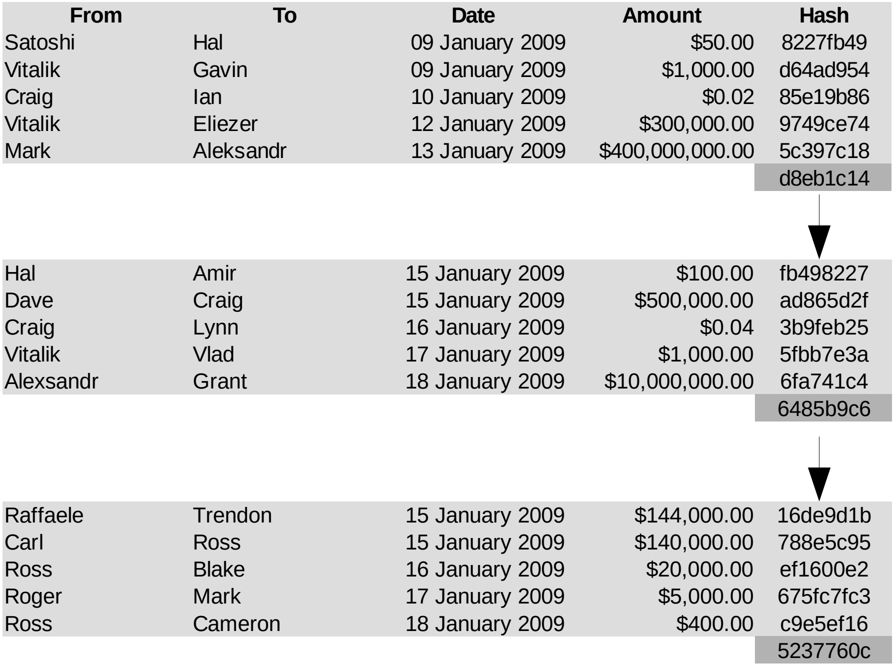
Let’s hash all the hashes!

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, then 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



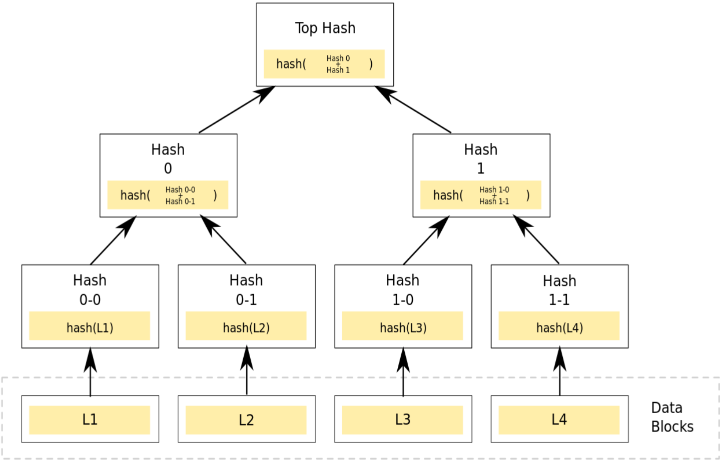
From	To	Date	Amount	Hash
Satoshi	Hal	09 January 2009	$50.00	8227fb49
Vitalik	Gavin	09 January 2009	$1,000.00	d64ad954
Craig	Ian	10 January 2009	$0.02	85e19b86
Vitalik	Eliezer	12 January 2009	$300,000.00	9749ce74
Mark	Aleksandr	13 January 2009	$400,000,000.00	5c397c18
				d8eb1c14

Hal	Amir	15 January 2009	$100.00	fb498227
Dave	Craig	15 January 2009	$500,000.00	ad865d2f
Craig	Lynn	16 January 2009	$0.04	3b9feb25
Vitalik	Vlad	17 January 2009	$1,000.00	5fbb7e3a
Alexsandr	Grant	18 January 2009	$10,000,000.00	6fa741c4
				6485b9c6

Raffaele	Trendon	15 January 2009	$144,000.00	16de9d1b
Carl	Ross	15 January 2009	$140,000.00	788e5c95
Ross	Blake	16 January 2009	$20,000.00	ef1600e2
Roger	Mark	17 January 2009	$5,000.00	675fc7fc3
Ross	Cameron	18 January 2009	$400.00	c9e5ef16
				5237760c

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)
- This is obviously useful for some things



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

3. Bitcoin

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: a 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*

(History: see David Golumbia “The Politics of Bitcoin” 2016)

The fabulous promises of Bitcoin!

— these may look familiar

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

The actual pitch

The actual pitch for Bitcoin has always been:

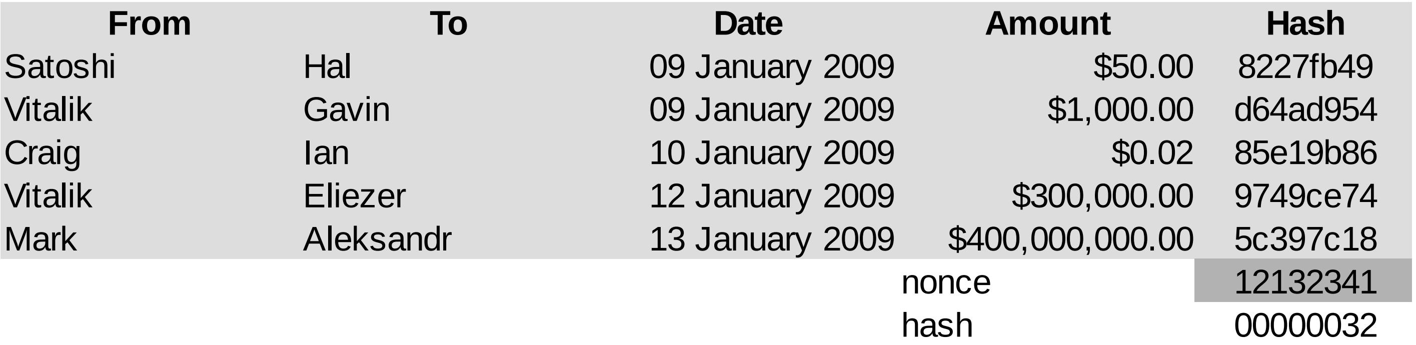
- You can get rich for free!
- This is a very popular product!
- You never even have to deliver
- All the tech, handwaving etc. is to obfuscate the fundamental pitch

How bitcoins are issued

- 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 (the “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 resulting 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*

  – *120,000,000,000,000,000,000,000 (1.2×10^{23}) guesses every 10 minutes, with just one 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 Thailand, 134 terawatts in 2021
  – source: Digiconomist.net Bitcoin Historic Sustainability Performance
- 0.5% of world electricity consumption (26,444 terawatts in 2021)
  – source: IEA Electricity Market Report, January 2022
  – literally wasted guessing numbers
- Predominantly fossil fuels
- Still only does 7 transactions/second
  – average 2200 kWh per transaction, 1000kg CO_2

What we get out of “Proof of Work”

- We waste all this power to get a completely decentralised system!
- You may wonder if this is worth 0.5% of the world’s entire power consumption
- So what does Bitcoin give us for this?
  – at least in theory

How the promises worked out

- Bitcoin “mining” has economies of scale
  — *so it recentralises*
- so, Bitcoin had recentralised by early 2014
- Four mining pools issue most of the bitcoins
- “Decentralisation” is fake

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
- Bitcoin is just like gold! … if you could create new gold mines by cut’n’paste
- Other coins (“altcoins”) don’t do much better

Altcoins

- Ethereum is the second most popular crypto
- Allows “smart contracts”, i.e. small computer programs — which might run tokens themselves (for ICOs, DAOs or DeFi)
- Ethereum is Proof-of-Work, like Bitcoin
- Some chains use “Proof-of-Stake”
  — thems what has, gets
- Centralisation still happens
- Decentralisation is a legal fiction,
  not an operational reality

  — *can’t sue me, bro*

4. Cryptocurrency in finance

Cryptocurrency in finance

- Markets don’t care about cryptocurrency ideology
- So all the crypto-assets are traded in the same markets – just a pile of “cryptos”
- Bitcoin, Ethereum, altcoins
- ICO/DAO/DeFi Tokens – centrally issued, run over Ethereum or a similar blockchain
- Centralised coins – *e.g.*, Ripple (XRP)

The crypto markets are risky!

- No real use cases for cryptocurrencies
- Negligible crypto economy – no circular flow of income
- So, not a pool of capital you can invest and grow — just commodities you can sell on
- Trading is zero-sum – winners and losers
- Very volatile – +/- 5-10% any given day

Conventional markets

In normal security and commodity markets, you can presume:

- Regulated, with sensible rules
- So you can get on with business
- Regulation gives some efficiency
- You can trust the exchange won’t mess you around
- You can trust the exchange is competent

Crypto markets

You can't trust any of those are the case in crypto!

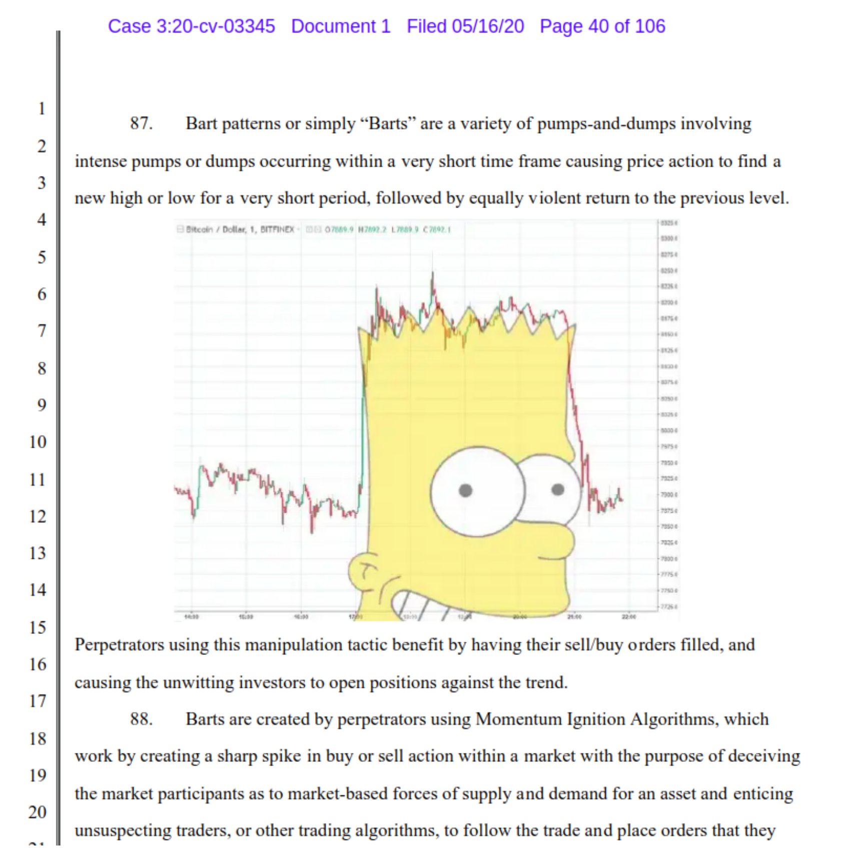
- Unregulated trading environment
  – *"Wild West"*
- Can't trust exchange won't mess you around
- Exchanges in regulated jurisdictions have vastly less volume than the unregulated casinos
- Can't trust exchange competence!
  – *is it just a website run from someone's flat?*
  – *Margin calls, tech problems, wiped out – so sorry!*

Banned in regulated trading:

- Wash trades *– Bitfinex, GDAX*
- Painting the tape *– Mt. Gox – 2013 bubble*
- Spoofing *– Bitfinex, GDAX*
- Front-running *– Yobit, all of DeFi*
- Insiders trading on exchange *– Bitfinex*
- Crashing a market to burn margin traders *– “Bart” pattern*

“Bart” pattern

- A “Bart” happens when you rig the price on an exchange to win a much larger margin bet elsewhere
- *e.g.* dump on Coinbase to win bet on BitMex
- This happens *all the time* in crypto
- Common in other thinly-traded and ill-regulated commodity markets



Case 3:20-cv-03345 Document 1 Filed 05/16/20 Page 40 of 106

87. Bart patterns or simply “Barts” are a variety of pumps-and-dumps involving intense pumps or dumps occurring within a very short time frame causing price action to find a new high or low for a very short period, followed by equally violent return to the previous level.

Bitcoin / Dollar, 1, BITFINEX O7089.9 H7092.2 L7089.9 C7092.1

Perpetrators using this manipulation tactic benefit by having their sell/buy orders filled, and causing the unwitting investors to open positions against the trend.

88. Barts are created by perpetrators using Momentum Ignition Algorithms, which work by creating a sharp spike in buy or sell action within a market with the purpose of deceiving the market participants as to market-based forces of supply and demand for an asset and enticing unsuspecting traders, or other trading algorithms, to follow the trade and place orders that they

ICOs, DAOs, DeFi

- Initial Coin Offerings — unregistered penny stocks — heyday was 2017-2018
- DAOs — nowadays, a fancy word for any collective enterprise — pretending to be more
- DeFi — Decentralised Finance — set up fancy trades between minor altcoins
  — get skinned by the experienced traders who prey on the gambling addicts
  — get front-run by the Ethereum miners
- DeFi is so scammy, they invented a new term, “rug pull”

ICO/DAO/DeFi tokens

- Print private currency, claim use case
  - “Utility tokens”
- Real market: speculators
- Regulators are paying attention
  - *SEC admin orders, arrests*
- Treat as highly speculative!

Stablecoins

- Tether — main source of liquidity in crypto
- Incredibly dodgy and incompetent, fined repeatedly
  — 13 employees on $80b assets?!
  — New York, CFTC fines just in 2021
- USDC — slightly less dodgy
- But none of these have ever been properly audited

NFTs

- Literally just a crypto-token with a web address in it
  — Like a piece of paper with “THE MONA LISA” written on it, and I tell you I sold you the Mona Lisa
- Market is *mostly* wash-trading, hoping for a sucker
- Heavily promoted by celebrity agencies
- No evidence of real consumer market

KYC / AML

- “Know Your Customer”
- Nightmarish for retail traders
  – *closed accounts common, esp. in the UK*
- Bit better for institutions
  – *talk to your bank first!*

When trading cryptos:

- Trading is zero-sum
- Extremely risky environment
- You can make a fortune, though
- Or lose a fortune
  — vastly more likely
- ***Trade carefully!***

5. Blockchain in the enterprise

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 the tech 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.

Example: Healthcare webinar

- Big 4 accountant
- How you could use Blockchain in Healthcare
- Magical bits done by “Smart Contracts”
- Request for specifics fobbed off –
“It’s like predicting Facebook in 1993!”
- But they’ll take your money now

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
- 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 in business

- “Smart contract” 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
  — 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

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”
  – common in “blockchain” case studies
- Not a blockchain at all – just the ledger
- Name is for marketing
  – definitely worked!

Real-life example: git

- stores computer program code
- each ledger entry is a program code change
- full history of all changes
- can maintain and merge branches
- does everything good bit of blockchain does
- nobody calls it a blockchain, but works comparably

Conclusion

- 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 a blockchain*
- “Could” is a word meaning “doesn’t”
- “Potentially” is a word meaning “doesn’t”
- “Incentivises” is a word meaning “doesn’t”
- 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