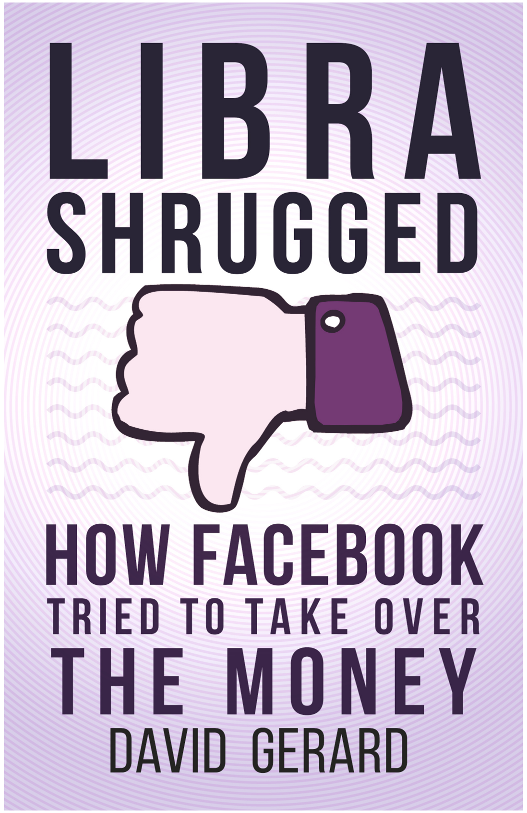
The Blockchain: Magic (probably) doesn't happen

How to sell a hash tree as a tech revolution

David Gerard



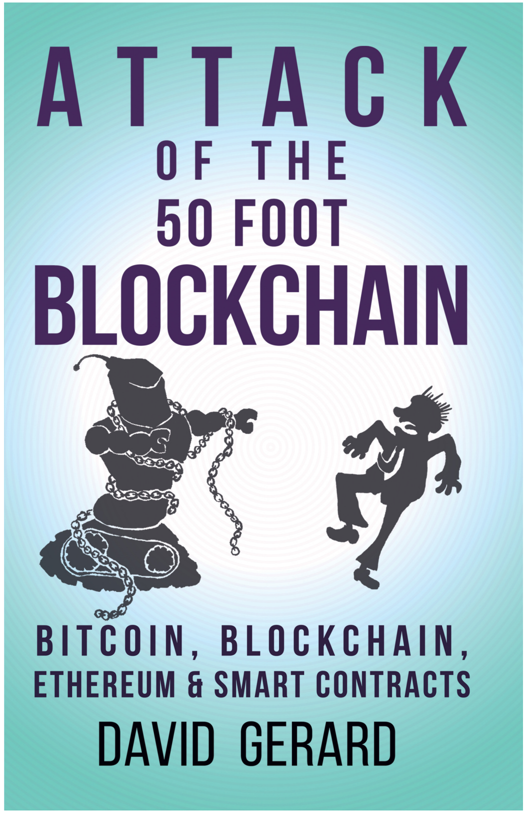
LIBRA SHRUGGED

HOW FACEBOOK TRIED TO TAKE OVER THE MONEY

DAVID GERARD

David Gerard

- Started as music journalist
- Moved to IT, Unix sysadmin
- Started following Bitcoin in 2011
- *Attack of the 50 Foot Blockchain* released 2017
  - *well-timed for the bubble!*



1. What on earth is a “blockchain”?

Simple accounting ledger

- Just a log 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?

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
- But — what if we have a *lot* of entries?
- What if someone tampers with the ledger — adds or removes an entry?

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

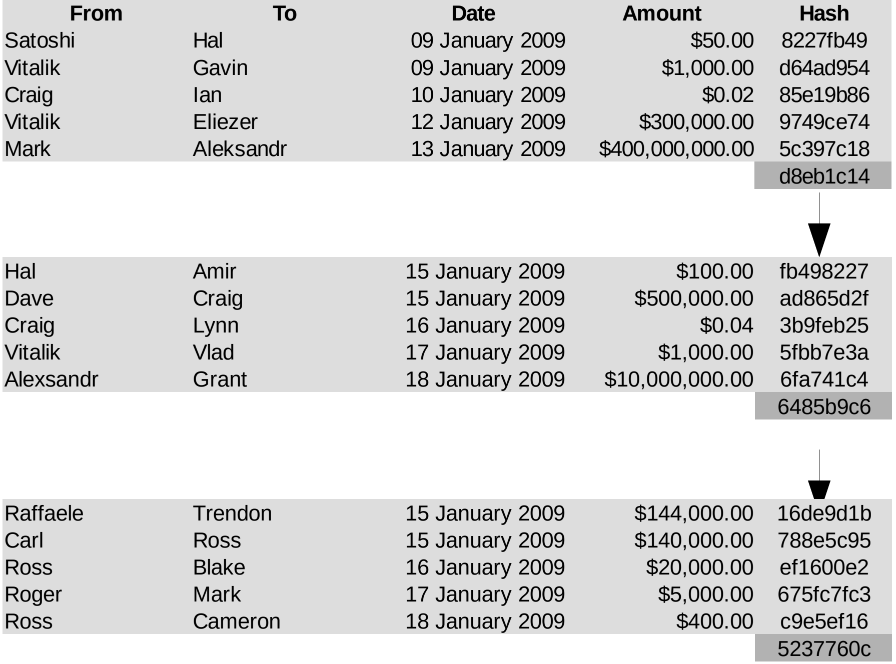
- So if we know that last hash — we know that the whole block has to come to that hash!
- Saves rehashing the whole block for each new entry

Tamper-evident append-only ledger!

- If you distribute the ledger, you can quickly verify the hashes of your copy
- And — it’d be impossibly slow to fake
- This hash-of-hashes construct is called a Merkle Tree (1979)
- A hash of hashes of data has the same cryptographic guarantees as just a hash, but is faster to amend

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 of blocks
- It’s … a blockchain!
- So … where’s all the magic I’ve heard about come from?



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

2. Bitcoin

Bitcoin

- Digital cash would be a useful thing
- We could use this hard-to-fake Merkle tree 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 — *extremist libertarianism — see “The Politics of Bitcoin” by David Golumbia (2016)*
- 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*

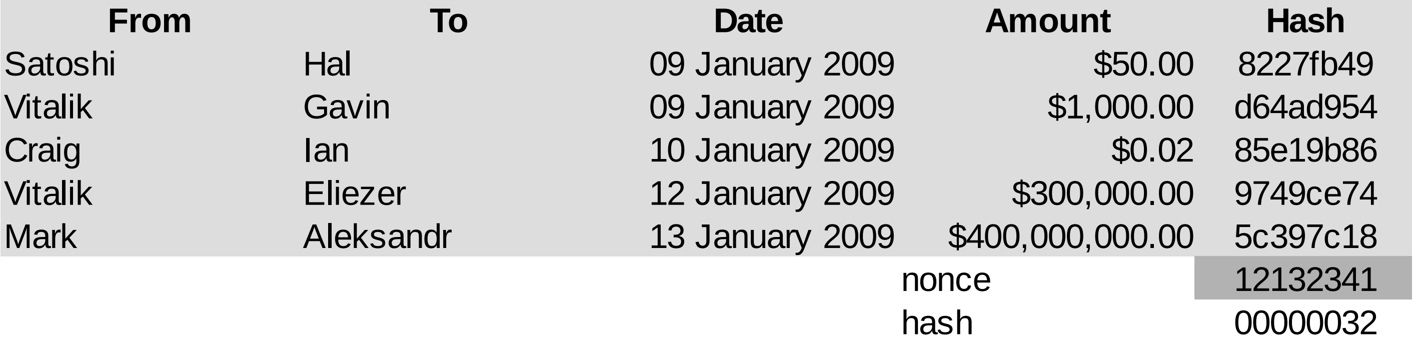
— All this is weird pseudo-economics that has never worked in the real world, ever

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*

  — 77,000,000,000,000,000,000,000 guesses every 10 minutes, 1 winner

“Proof of Work” — Proof of Waste

- If too many people win — make it harder!
- Ends up in a Red Queen’s race
  — *more and more power to stay in the same place*
- As much power as Ireland or Austria — 0.1-0.5% of world
  — *literally wasted guessing numbers*
- Still only does 7 transactions/second — *same since 2009*
- Bitcoin is anti-efficient
- So … what does all this get us?

The fabulous promises of Bitcoin!

- Decentralised! Trustless!
- Fast and free!
- Uncensorable and irreversible!
- No “just printing money” — limited supply!

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
- Bitcoin was fast and near-free up to mid-2015

  … then the transaction capacity filled
- Bitcoin transactions have been slow, unpredictable and expensive since
- Peaked at ~$55 average fee in Dec 2017

How the promises worked out

- Uncensorable! Irreversible!
- This turns out not to be what users want

  — *consumers like chargebacks, they increase 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

Can altcoins do better?

- Bitcoin was the first paper/string mock-up,
  pressed into service
- Other proof-of-work coins have similar throughput
  — *Ethereum runs 16 transactions/second*
  — *already having transaction clogs — ICOs, CryptoKitties, DeFi*
- Experimental new work — unfinished or not fully battle-tested
  — *IOTA, Hashgraph, Cardano, etc*
- Users hop from coin to coin as old ones clog

3. Enterprise Blockchain

What organisations want

- Any organisation has bureaucracy — the machinery they run on
  - *business, non-profit, government*
- 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!

- “Blockchain” is a particular collection of marketing promises
  — *“blockchain” is NOT any particular technology*
- 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!
  — *though anything run by a company has a touchable entity that’s responsible*
- Smart Contracts for added magic!
  — *the hard bit is always done by “smart contracts”*
  — *which literally means “with a computer program”*

Permissioned blockchains

- Usual case in business
  — all participants known, authorised
- Don’t want your back office on the hostile Internet
- Don’t use Proof of Work (it’s silly)
- This is also called a “database”
- Even if shared — someone runs it, controls access
- No magical “blockchain” results

Blockchains in the real world

- Almost none in production use
- Main smart contract use case: ICO tokens
  — *and excuses why something needs a blockchain*
  — *with handwaving about blockchain economics*
- Press releases, pilot programmes

  — *a majority from IBM*

Real world blockchain projects

- World Food Programme
  — *single-user private Ethereum — i.e., a database*
- Wal-Mart/IBM supply chain trials
  — *all nodes on IBM Cloud, administered by Wal-Mart*
  — *doesn’t exist yet*
- Maersk/IBM trials
  — *as centralised as Wal-Mart trials*
  — *vendors openly wondering what the “blockchain” bit is supposed to achieve*
- Voatz military absentee voting trial
  — *collect votes, log them on private Hyperledger cluster*
  — *use Blockchain to transmit votes from their app, print out a paper ballot*

Initial Coin Offerings

1. State a problem
— doesn't have to be a real problem

2. Tokens can solve it!
— add some weird Bitcoin economic reasoning

3. There are no other steps

But the fabulous potential!

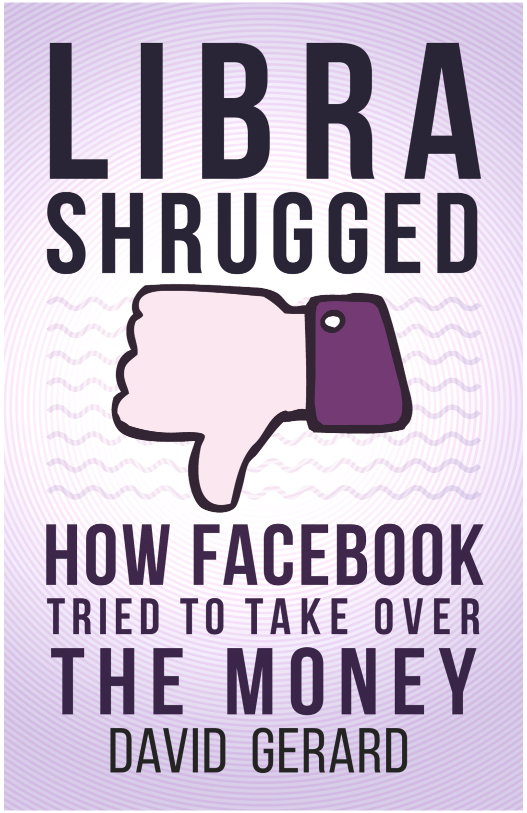
- Nonsense claims claiming magical technology
- Different technologies, same scams:
  “get rich for free”
  — *altcoins, ICOs, blockchain projects, DeFi ...*
- Remember: Magic doesn’t happen
- The space has lots of good, sincere people …
  and a ton of repeat scammers

Issues to consider

- Magic doesn’t happen
  — if it sounds too good to be true, it probably is
- Whenever someone promises magic,
  it’s a big green light for scammers
- The blockchain space is full of scammers
  — and naive suckers
  — and suckers who think they’re the scammer
- If it sounds too good to be true …
- … it probably is

Questions, please!

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



LIBRA SHRUGGED

HOW FACEBOOK TRIED TO TAKE OVER THE MONEY

DAVID GERARD