

Introduction to Blockchain and Cryptocurrencies

Michael Josem – 21 February, 2019

Michael Josem

○ Current:

- Head of Customer Growth at Jobhawk, an app-based marketplace for construction labour
- Freelance marketing, communications and public relations. Past Clients have included CoinPoker & SimpleToken
- Current crypto portfolio: 2 ETH

○ Past:

- A decade in online gaming, serving as Head of Public Relations, Innovation Manager and Senior Security Manager for various brands including PokerStars, Full Tilt, 138.com, etc.

What do we know today?

- Who owns any cryptocurrencies?

At the outset

- I'm not a financial advisor, and nothing here should be construed as financial advice. I'm not making any financial predictions or offering any investment advice here.
- My skill here is in translating from the complicated technical speak into normal words.

NOT
financial
advice

Agenda



WHAT IS BLOCKCHAIN?



WHAT IS A
CRYPTOCURRENCY?



WHAT IS A SMART
CONTRACT?



WHAT ARE SOME
OPPORTUNITIES FOR
INSURANCE?

What is blockchain?

- “Distributed Ledger Technology”
- Basically, a shared list
- Bitcoin is a subset of blockchain

Key features of blockchain

- Distributed publicly but centralised ledger
- A consensus algorithm
- A currency or token that has value and is tradeable

The implications of this

- Any peer can view the entire ledger (transparency vs privacy)
- The ledger cannot be changed (no trusting of any central authority to fix errors)
- Rewards for participating (encourages centralisation)
- “Mining” to verify and process transactions (huge volume of processing power)

A simple metaphor

- A shared spreadsheet where anyone can append, but no one can edit, running simultaneously on many processors around the world.

What is cryptocurrency?



asia murphy, bsd evangelist @am_anatjala · 16 Aug 2018

i still don't get bitcoin

22 120 505



generative adversarial poster

@Theophite

Follow

Replying to @am_anatjala

imagine if keeping your car idling 24/7
produced solved Sudokus you could trade for
heroin

11:49 PM - 16 Aug 2018

4,148 Retweets 16,832 Likes



101 4.1K 17K

What is cryptocurrency?

- What was currency?
- What is currency?

How is cryptocurrency different from currency?

- Recorded on the blockchain
- Something that people value
- No centralised operator – distribution is determined by the programming
- In some ways, replicates some features gold-backed money

Cryptocurrency Attributes

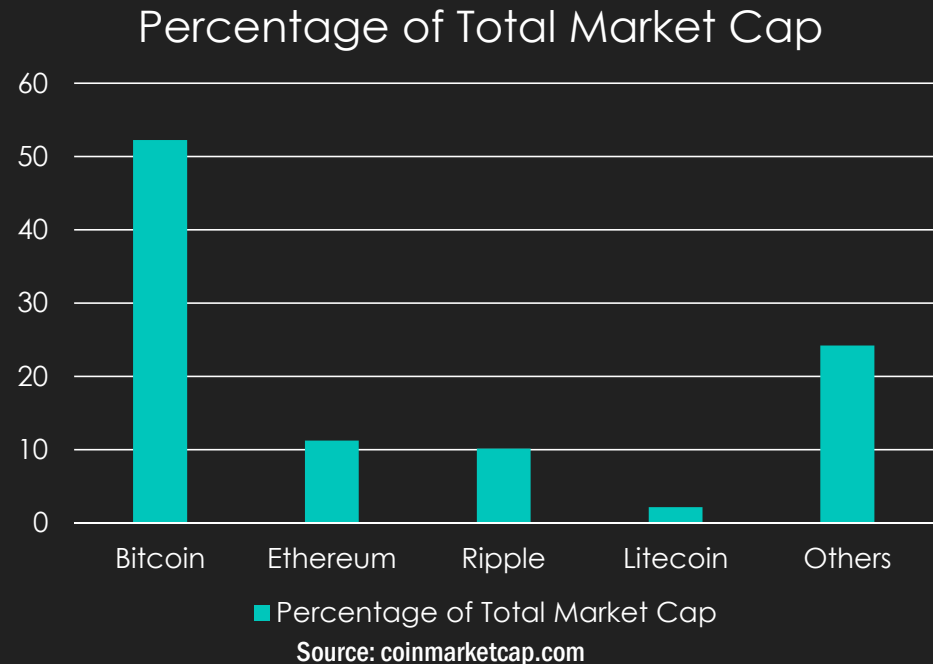
- **No central authority: useful for transactions that banks and Governments would prohibit**
 - Ethical uses: circumvent capital controls (China; Latin America)
 - Unethical uses: circumvent capital controls (Iran; North Korea; illegal goods & services)
- **No middleman storage**
 - Benefits: you have 100% control of your money
 - Weaknesses: security and usage is entirely on you
- **Supply set by programming**
 - Benefits: Semi-Predictable inflation
 - Cost: No fractional banking

Cryptocurrency Attributes

- Entirely Electronic
 - Benefit: You can hide and send it easily (much of the time)
 - Weakness: You need electricity to send it
- Immutable
 - Benefits: No chargebacks
 - Cost: No fixing mistakes or theft
- Transactions happen on the blockchain
 - Benefits: All the above
 - Weaknesses: Variable transaction fees, congestion, real-world centralisation

The biggest – by far - Bitcoin

- Bitcoin was the first meaningful cryptocurrency in 2008
- Pseudonymous creator, Satoshi Nakamoto
- “Hard” limit of 21 million
- Until early 2017, accounted for 85%+ of cryptocurrency value. Around 50% for the last 6 months or so.
- Each transaction is published with to/from wallet address recorded.
- Technical reasons limit it to around 7 transactions per second.



What is a smart contract?

- In our blockchain (append-only spreadsheet running on lots of processors) you can run programs
- These programs can be setup to do stuff (eg, move cryptocurrency around)

Hypothetical examples

- If a flight is delayed X minutes, pay compensation
- If it rains in Douglas on Y consecutive days, pay money to event organizer
- “Insurance” on any event with a clear authoritative electronic oracle

A Giant Warning Label

- The words "hack" and "theft" make human, normative presumptions about how you're supposed to use the code. But the code doesn't care. The code can't be "hacked." It can only be used; its use has no normative implications.

-Matt Levine, Bloomberg.com

A Giant Warning Label

- The legal system has safeguards so that investors usually get what they expect. If you invest in a company, you are in a sense signing up for a certificate of incorporation and bylaws, which are written in lawyerly language. But you also get a prospectus that explains the terms of your investment in relatively plain English. The terms of that investment tend to be constrained by law, underwriter due diligence, public policy and tradition. Even if you invest in a company whose bylaws say that the board of directors can sacrifice you to a demon on the first full moon of a leap year, it's unlikely that that term would be enforced.

-Matt Levine, Bloomberg.com

A Giant Warning Label

- If you invest your Ether in a smart contract, you'd better be sure that the contract says (and does) what you think it says (and does). The contract is the thing itself, and the only thing that counts; explanations and expectations might be helpful but carry no weight. It is a world of bright lines and sharp edges; you can see why it would appeal to libertarians and techno-utopians, but it might be a bit unforgiving for a wider range of investors.

-Matt Levine, Bloomberg.com

Hypothetical examples

- If a flight is delayed X minutes, pay compensation
- If it rains in Douglas on Y consecutive days, pay money to event organizer
- “Insurance” on any event with a clear authoritative electronic oracle

Potential Opportunities for Insurance

- Asset listing/recording (But can be done without blockchain)
- Automated settlement (But assessing & adjusting claims! Electronic oracle!)
- Cross-jurisdictional agreements (But if you don't trust them...)
- Providing insurance to sector