BLOCKTOWER

Understanding Cryptocurrency (updated May 2018)

Ari Paul

CIO, Managing Partner

BlockTower Capital

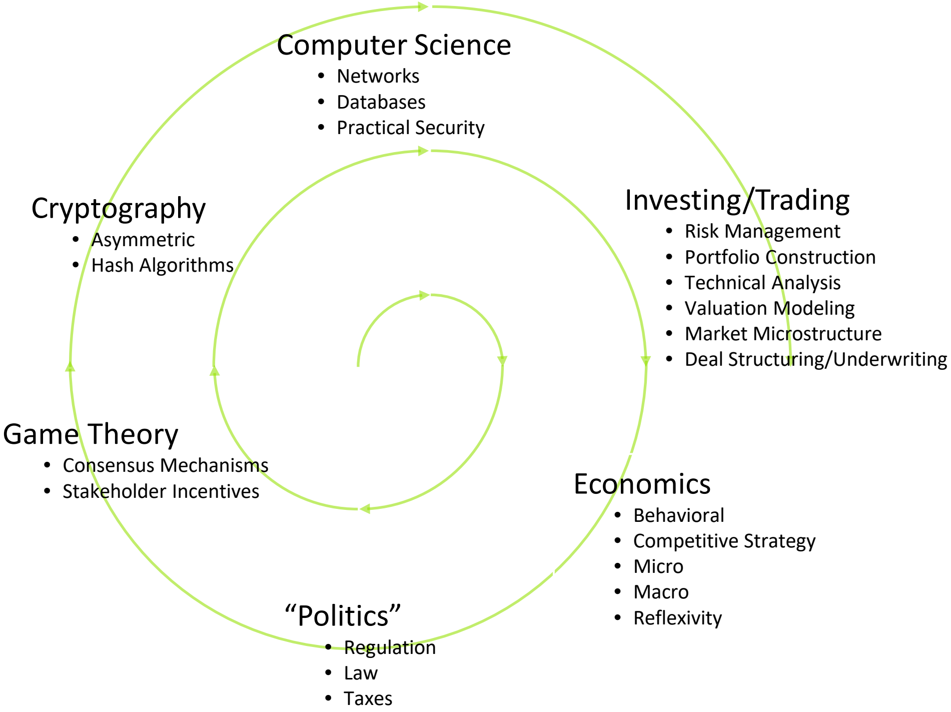
What is cryptocurrency?

Cryptocurrency is at the intersection of game theory, cryptography, computer science, economics, venture capital, and public markets.

Don’t be scared. These are the puzzle pieces. Individually, they don’t look like much, but after we assemble them, we’ll see the big picture as a holistic whole.

The Spiral

Learning about cryptocurrency must take the form of a spiral. You have to start somewhere, but each individual topic is hard to apply to cryptocurrency in isolation. Learn a little about one topic, then move on to the next until you complete the spiral, then keep learning and diving deeper with each rotation. The pieces will gradually come together.



Computer Science

- Networks
- Databases
- Practical Security

Investing/Trading

- Risk Management
- Portfolio Construction
- Technical Analysis
- Valuation Modeling
- Market Microstructure
- Deal Structuring/Underwriting

Economics

- Behavioral
- Competitive Strategy
- Micro
- Macro
- Reflexivity

"Politics"

- Regulation
- Law
- Taxes

Game Theory

- Consensus Mechanisms
- Stakeholder Incentives

Cryptography

- Asymmetric
- Hash Algorithms

Obsolete Technology

Financial technology appeared strangely stagnant in 2008.

Compared to instant and free communication via email, transferring electronic money was incredibly slow:

- 4 days to transfer money between bank accounts via ACH?
- 6+ hours and a $15+ fee to transfer money domestically via Wire Transfer?
- 24+ hours and $35+ fee for international Wire Transfers?
- 24+ hours and a $35+ fee to transfer cash to another country via Western union?

Obsolete Technology

Capital Markets Were Archaic Too

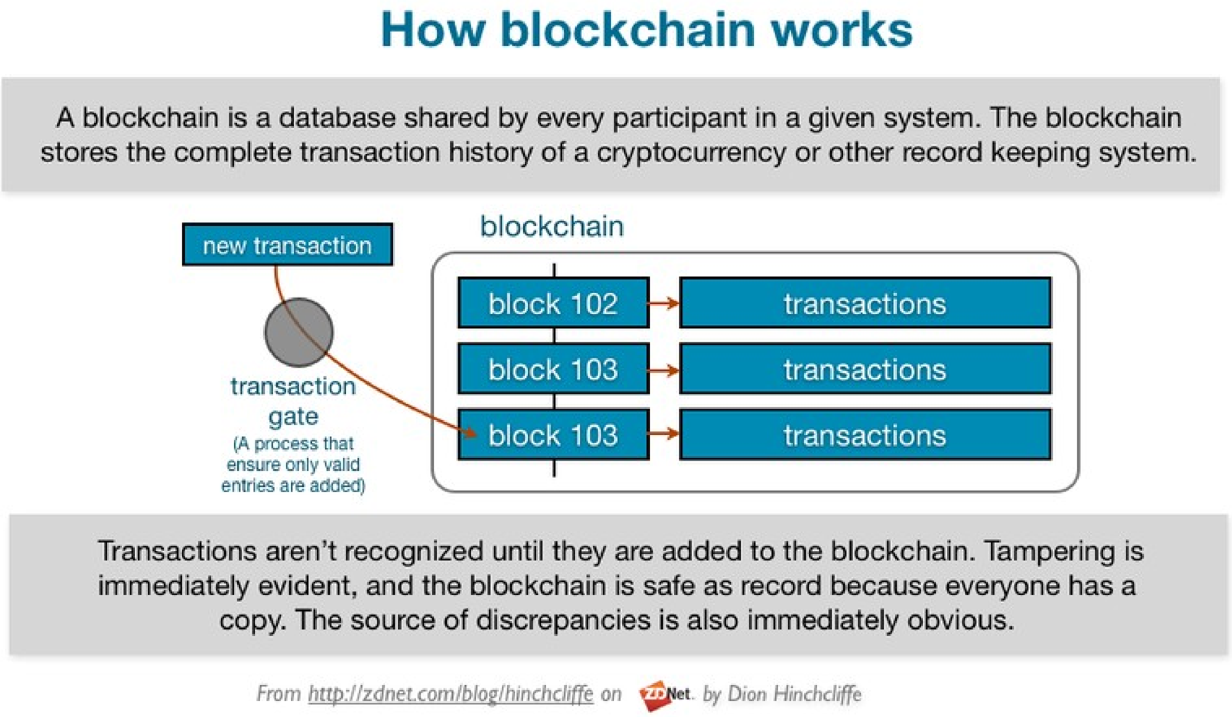
- 3 days to settle a stock trade?
- 24+ hours to settle a treasury trade?
- Cascading treasury “failure to delivers”?
- Traders shortselling more equity in a company than actually exists?

What Made Cryptocurrency Possible?

Cryptocurrency as an idea is 50+ years old. To make it work required 3 innovations:

- "Proof of work" mining – an economic system that incentivizes selfish rational actors to participate productively in a network using cryptographic functions.
- Public key cryptography – asymmetric encryption that enables secure digital signatures.
- The permission-less blockchain – a new type of database, a distributed public ledger.

What’s a Blockchain?



How blockchain works

A blockchain is a database shared by every participant in a given system. The blockchain stores the complete transaction history of a cryptocurrency or other record keeping system.

Transactions aren’t recognized until they are added to the blockchain. Tampering is immediately evident, and the blockchain is safe as record because everyone has a copy. The source of discrepancies is also immediately obvious.

From http://zdnet.com/blog/hinchcliffe on ZDNet. by Dion Hinchcliffe

What’s a blockchain? ...a little jargon.

A blockchain is a special type of database. It is a *distributed* database that maintains a *continuously-growing list* of records that are *secure from tamper and revision.*

» *Distributed:* identical copies of the database are maintained on many separate computers; no single entity is trusted with keeping the definitive copy of the blockchain.

» *Continuously-growing list:* every new transaction is appended to the list of previous transactions. Nothing is ever changed or deleted. This lets every viewer of the blockchain confirm that every transaction is valid, because we can examine each transaction’s link to its predecessors.

» *Secure from tamper and revision:* each addition to the blockchain contains a *hash* of previous transactions; if previous transactions are edited, we would instantly spot that the *hash* is no longer correct.

» *Hash: a one-way function* (i.e. a function that can be easily performed in one direction but is practically impossible to perform in the other) that is used to map data (like all previous blockchain transactions) to a fixed size string. As a simple example, I can use an algorithm to create a hash of this entire presentation that maps to a short text string like: gJakdIkleBNeJKa. Anyone could use the *hash* function to confirm that the presentation has not been tampered with because the *hash* is correct, but they would not be able to recreate the presentation from the *hash*.

What’s a cryptocurrency?

A cryptocurrency is a tradeable *intrinsic token* of a blockchain. An *intrinsic token* is a token that is native to the blockchain. The most famous cryptocurrency is Bitcoin (BTC).

An *intrinsic token* can be thought of as a ticket at an amusement park that can be spent at various rides or exchanged with other patrons. Within the bitcoin network, bitcoins are spent to pay for monetary transmission (currently about $2 per monetary transfer). Within the ethereum network, Ether (ETH) pays for decentralized computing power.

In contrast, an *asset-backed token* may be added by a third party to any blockchain to represent ownership in an asset like gold, US dollars, or real estate.

Cryptocurrency Use Cases and Valuation

For now, nearly all cryptocurrencies fall into one of the following buckets, and each bucket requires a unique valuation approach. The current buckets are:

1. Censorship resistant store of value – “digital gold” or “swiss bank on your phone”

2. Utility token – “amusement park tickets” or “paid API keys”

3. Tokenized security – a cryptocurrency version of a traditional asset ownership interest

Store of Value

Valuation Method: Addressable Market

Offshore bank accounts hold roughly $20 trillion (*source: Tax Justice Network*). Much of this is held in judgement resistant trusts and complex corporate structures provided by large global banks.

Why do law abiding billionaires and large US corporations pay JP Morgan fees to offshore wealth?

Amazon can't allow their entire global business operation to be shut down by a single judge in one legal jurisdiction freezing all their assets.

This is a *floor* for the addressable market. Lower friction and reduced costs raise demand.

Utility Tokens

Valuation Framework: “Hot potatoes.”

Example: Someone can create an open source version of Ebay. If it’s open source, how does the creator get paid? They code the program so that buyers are only able to make purchases using a custom token sold by the developer. A user of the open-source-ebay would first have to convert US dollars or Bitcoin into EbayToken by buying it on an exchange or from the developer. This potentially transmits demand for the open source network into demand for the utility token.

Problem: Utility tokens are “hot potatoes” that no one wants to hold. A relatively low token value can support a high network value if they can be transferred quickly. In other words, if a user can instantly convert US dollars into EbayTokens, and sellers can convert EbayTokens into USD immediately, will EbayTokens reflect the value of the network?

Tokenized Security

Valuation Framework: Traditional

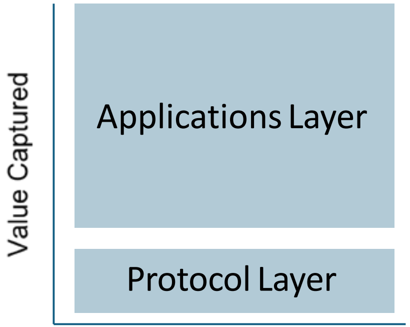
Any asset can be "tokenized" just as any asset can be securitized. For example, real estate mortgages can be traded on a stock exchange via REITs. Exchange listing of real estate mortgages retains their economic properties but may effect valuation at the margin via changing the liquidity profile and reducing regulatory costs.

These same real estate mortgages can also be "tokenized", with ownership recorded on a blockchain, potentially further increasing liquidity and further reducing regulatory costs.

To value a traditional asset token, look at the underlying economic ownership and then adjust for liquidity and regulatory effects.

Where is value captured?

The Internet

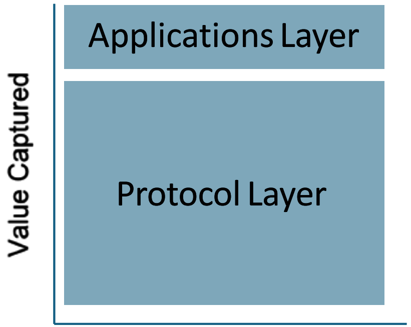


Value Captured

Applications Layer

Protocol Layer

Blockchains



Value Captured

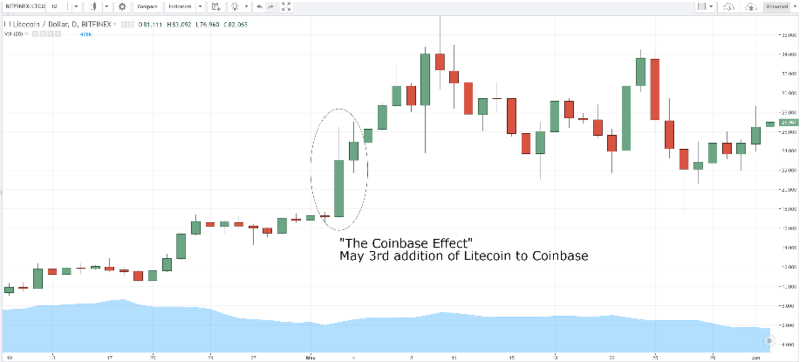
Applications Layer

Protocol Layer

With the internet, most value was captured at the Applications Layer. For cryptocurrencies, the majority of value may be captured at the protocol level…maybe. (Source: Joel Monegro, USV)

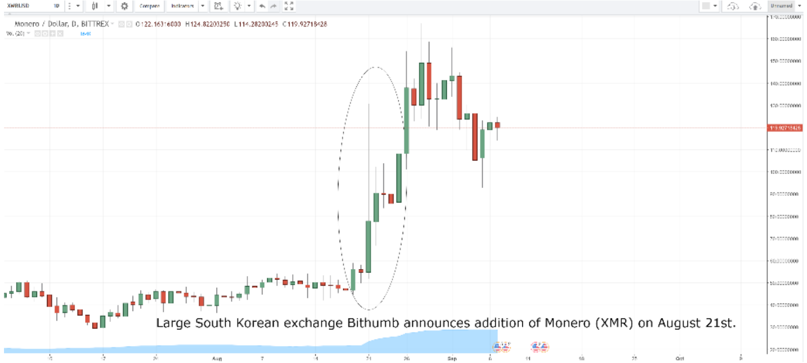
The “Accessibility Discount”

Litecoin (LTC)’s addition to Coinbase on May 3rd produced an immediate 30% rally. True effect likely greater as the information was partially priced in ahead of the announcement.



"The Coinbase Effect"
May 3rd addition of Litecoin to Coinbase

Monero (XMR)’s planned addition to Bithumb announced on August 21st produced an immediate 100% rally.

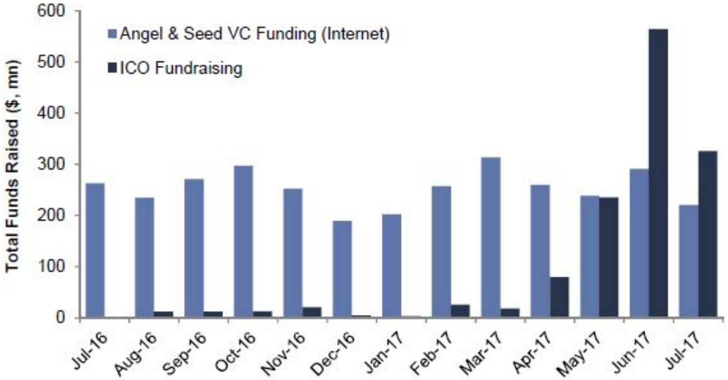


Large South Korean exchange Bithumb announces addition of Monero (XMR) on August 21st.

ICOs

ICOs (initial coin offerings) have exploded in popularity, with more being launched each *week* in August 2017 than were launched in all of 2014. One reason is accessibility. Ethereum's ERC20 format provided a standardized way to both issue and invest in new cryptocurrencies.

Exhibit 8: The pace of ICO fundraising has now surpassed Angel & Seed stage Internet VC funding globally
Total Funds Raised by month ($, millions)



Note: ICO fundraising as of July 18th, 2017, per Coin Schedule. Angel & Seed VC funding data as of July 31st, 2017 and does not include "crowdfunding" rounds.

Source: CoinSchedule, CB Insights, Goldman Sachs Global Investment Research.

But this may just be the start from an ease of access perspective. Where's my iphone app for ICOs?

Institutional Constraints

Total cryptocurrency market capitalization is $400 billion today. There is an immense amount of capital desperately seeking assets with high expected return and low correlation to the existing portfolio. CalPERS (the California Public Employee Retirement's System) is a pension that controls $290 billion alone.

What needs to happen for tens (hundreds?) of billions of institutional capital flow into cryptocurrency?

- **Third party qualified custodial services**
- **"Institutional quality" investment vehicles with disintermediated (e.g. insured) operational risk**
- **Credible fund managers with 2+ year track records**
- **Well constructed and low fee passive indices**

BLOCKTOWER

Thanks For Joining Us!

Ari Paul

CIO, Managing Partner

BlockTower Capital

https://www.blocktower.com/

https://thecryptocurrencyinvestor.com/

@aridavidpaul on Twitter