Cryptocurrency Summary
Julien Cohen  ·  www.julcoh.com
1/7/2018

[Donations welcome]

ETH: 0x4e03Bf5CCE3ee4Ddae4d3d6aAD46ca4f198AeD6
BTC: 1GqWMZRRygRJJWYYTWHKAVoRcgyQHjgBMZ
XMR: 42Y1S1kBoPk381kc7hA68zaiC78BxMoCADjLrfCtdWiE7ejhZc49s1t9i7P2EmTnHsLDiKoSUjogCbLVHXRjxjrCT4WG8ic
XRB: xrb_1bpzh745s9kzk8ymfnks3jtdi65ayumdstokzd4yw40hu3fopxmiojcxntcu

Background
This document is purely informational. At the time of writing there are over 1000 cryptocurrencies ("cryptos") in a highly volatile, high risk market. Many of the smaller “altcoins” require significant technical knowledge to store and transact safely. I advise you to carefully scrutinize each crypto’s flavor of blockchain, potential utility, team of developers, and guiding philosophy, before making any investment\(^1\) decisions. With that out of the way, what follows are brief, extremely high-level summaries of some cryptos which have my interest, listed in current market cap order. But first, some info:

Each crypto is a different implementation of a **blockchain** network. Originally developed as decentralized digital cash, these technologies have evolved into much broader platforms, powering the future of decentralized applications across every industry in the global economy. Without getting into the weeds,\(^2\) most cryptos work on similar principles:

**Distributed Ledgers**  
Each node on a blockchain network has a copy of every transaction, which enables a network of trust which eliminates fraud.\(^3\)

**Decentralized**  
“Miners” comprise the infrastructure of a blockchain network.\(^4\) They are monetarily incentivized to add computing power to the network, simultaneously securing and processing each transaction.\(^5\)

**Peer-to-peer**  
Cryptos act like digital cash-- they require no third party to transact and are relatively untraceable. Unlike cash, you can back them up.

**Global**  
Transactions are processed cheaply and instantly, anywhere on Earth. Using cryptos, an African peasant and a San Francisco engineer have the same access to capital, markets, and network services.

**Secure**  
Blockchains are predicated on the same cryptographic technology that secures your sensitive data and government secrets. They have passed seven years of real-world penetration testing with no failures.\(^6\)

---

\(^1\) “Investment” is a misnomer. Cryptos are traded like securities, but grant you no equity (like trading currency).

\(^2\) The weeds for Bitcoin: [basic intro (1:36)], [non-technical explanation (5:24)], [Bitcoin 101 – Andreas Antonopoulos (23:51)]

\(^3\) It is impossible to double-spend or create a fake transaction, as each ledger is confirmed against every other ledger.

\(^4\) Some utility token blockchains use DAG networks or similar non-linear networks which don’t require mining.

\(^5\) In practice, these are giant warehouses full of specialized computers constantly processing transactions. Miners locate to the cheapest electricity source, and the bulk of mining currently occurs in China.

\(^6\) Centralized second-layer exchange websites have been hacked, but the core technology is untouched.
**Bitcoin (BTC)**

The first cryptocurrency. As with first movers in any technology, there are associated pros and cons. Bitcoin has by far the strongest brand recognition and deepest market penetration, and it is the only crypto which can be used directly as a currency at over 100,000 physical and web stores around the world. In Venezuela and Zimbabwe, where geopolitical events have created hyperinflation in the centralized fiat currency, citizens have moved to Bitcoin as a de facto transaction standard.\(^7\)

However, Bitcoin unveiled a number of issues that have been solved by subsequent cryptos. It is experiencing significant scaling issues, resulting in high fees and long confirmation times. The argument over potential solutions created a rift in the Bitcoin developer community, who “forked” the network into two separate blockchains amidst drama and politicking in October 2017. Potential solutions to these issues abound, with some already in place, and others nearing deployment.

Bitcoin currently has the highest market cap, and since it is easy to buy with fiat currency, the price of many smaller cryptos (“altcoins”) are loosely pegged to its price. This will change in the coming year(s).

**Ethereum (ETH)**

Where Bitcoin is a currency, Ethereum is a platform, designed as a foundational protocol on which to develop decentralized applications (“Dapps”). Anyone can write code and deploy their program on the global network for extremely low fees. Just like Twitter wouldn’t exist without the open platform of the internet, the next world-changing Dapp can’t exist without Ethereum.

Current Dapps include a global market for idle computing power and storage, peer-to-peer real estate transactions (no trusted third party for escrow), identity networks for governments and corporations (think digital Social Security card), and monetization strategies for the Internet which replace advertising. Think back 10 years to the advent of smartphones, and then to our culture today--Ethereum could have a similar network effect on humanity.

Ethereum is currently the #2 market cap crypto below Bitcoin, and many believe it will surpass it in 2018. It has a large, active group of developers working to solve scaling issues,\(^8\) maintain security, and create entirely new programming conventions. If successful, platforms like Ethereum may well be the foundation of the decentralized internet of the future.

**Ripple (XRP)**

Ripple is significantly more centralized than most crypto networks, designed as a backbone for the global banking and financial technology (“fintech”) industries. It is a network for exchanging between fiat currencies and other asset classes instantly and cheaply, especially when transacting cross-border and between separate institutions. It uses large banks and remittance companies as “anchors” to allow trading between any asset on the network, and big names like Bank of America, American Express, RBC, and UBS are partners. The utility of this network is global and massive in scale.

It is extremely important to note that not all cryptos have the same number of tokens. Ripple has 100 Billion tokens compared to Bitcoin’s 21 Million. Do not directly compare price between cryptos. XRP

---

\(^7\) This effect has been termed bitcoinization.

\(^8\) The Ethereum roadmap shows moving from a Proof of Work (PoW) to Proof of Stake (PoS) consensus model.
will likely never reach $1k or $10k\textsuperscript{9}, but the price will rise commensurate with its utility as a financial tool.

In some sense, Ripple is anathema to the original philosophical vision of this technology space. And while I agree with the cyberpunk notion of decentralized currencies, separation of money and state, this is the natural progression of the crypto world. The internet was an incredible decentralized wild west of Usenet groups and listservs before Eternal September and the dot-com boom, but its maturation affected every part of global society.

**Cardano (ADA)**
Cardano's main claim to fame: it is the only crypto developed using academic methodologies by a global collective of engineers and researchers, built on a foundation of industry-leading, peer-reviewed cryptographic research. The network was designed from first-principles to allow scalability, system upgrades, and to balance the privacy of its users with the security needs of regulators.

One part of this ecosystem is the Cardano Foundation, a Swiss non-profit founded to work proactively with governments and regulatory bodies to institute legal frameworks around the crypto industry. Detractors of Cardano claim that it doesn’t do anything innovative, but supporters see the academic backing and focus on regulation development as uniquely valuable.

**Stellar Lumens (XLM)**
Stellar Lumens and Ripple were founded by the same person. They initially shared the same code, but today the two are distinct in their technical back-end as well as their guiding philosophy and development goals. Ripple is closed-source, for-profit, deflationary, and intended for use by large financial institutions. Stellar is open-source, non-profit, inflationary, and intended to promote international wealth distribution. As such, they are not direct competitors.

IBM is a major partner to Stellar. Their network is already processing live transactions in 12 currency corridors across the South Pacific, with plans to process 60% of all cross-border payments in the South Pacific’s retail foreign exchange corridor by Q2 2018.

Beyond its utility as a financial tool, the Stellar network may become a competitor to Ethereum as a platform for application development and Initial Coin Offerings ("ICOs"). The theoretical maximum throughput for the network is higher, and it takes less computational power to run. The Stellar development team is highly active, has written extensive documentation for third-party developers, and has an impressive list of advisors, including Patrick Collison (Stripe), Sam Altman (Y Combinator), and other giants in the software development community.

**Iota (IOT)**
Iota was developed as the infrastructure backbone for the Internet of Things (IoT), sometimes called the machine economy. As the world of inanimate objects is networked together, their need to communicate grows exponentially. Fridges, thermostats, self-driving cars, printers, planes, and industrial sensors all need a secure protocol with which to transact information.

Iota uses a “Tangle” instead of a traditional blockchain, and this is the main innovation driving the crypto’s value. Each device that sends a transaction confirms two other transactions in the Tangle. This

\textsuperscript{9} At $2.62 per token, Ripple already commands a $100B market cap.
removes the need for miners, and enables unique features like zero fees and infinite scalability. The supply of tokens is fixed forever at $2.8 \times 10^{15}$, a staggeringly large number (almost three thousand trillion), and the price you see reported is technically “MIOT”, or the price for a million tokens.

**Monero (XMR)**
The most successful privacy-focused cryptocurrency. In Bitcoin and most other cryptos, anyone can examine the public ledger and trace specific coins through the network. If your identity can be attached to a public address on that network, an accurate picture of your transaction history can be built-- who, what, and when. Monero builds anonymity into the system using strong cryptographic principles, which makes it functionally impossible to trace coins, attach names to wallets, or extract metadata from transactions. The development team actively publishes in the cryptography research community.

Anonymous transactions are not new-- we call it cash. Only in the past two decades has anonymity grown scarce in the first-world with the rise of credit cards and ubiquitous digital records. Personal data is becoming the most valuable resource on Earth, and there are many legitimate reasons for law-abiding citizens to want digital privacy, but it is true that with anonymity comes bad actors-- Monero is the currency of choice for the majority of black market (“darknet”) transactions. Similarly, US Dollars are the main vehicle for the $320B annual drug trade. An investment here should be based on the underlying cryptographic research and technology behind this coin, as well as competitors like Zcash.

**RaiBlocks (XRB)**
Zero fees and instantaneous transfer make RaiBlocks extremely attractive for exchange of value, in many senses outperforming Bitcoin at its original intended purpose. This crypto has seen an explosion in price and exposure over the past month, and it may become the network of choice for transferring value within and between crypto exchanges.

Just in the first week of 2018: the CEO of Ledger (makers of the most popular hardware wallet on the market) waived the $50k code review fee to get RaiBlocks on his product, and XRB got listed on Binance and KuCoin, two of the largest altcoin exchanges globally. This is one to watch for 2018.

**VeChain (VEN)**
Developed as a single answer to the problem of supply-chain logistics, VeChain is knocking on the door of a fast-growing $8 trillion industry. Every shipping container and packaged product in the world requires constant tracking and verification. A smart economy for logistics built on the blockchain promises greater efficiency and lower cost through the entire process flow.

Don’t take my word for it-- VeChain has investment from PwC (5th largest US corporation), Groupe Renault, Kuehne & Nagel (world’s largest freight company), and DIG (China’s largest wine importer). The Chinese government has mandated VeChain to serve as blockchain technology partner to the city of Gui’an, a special economic zone and testbed for China’s smart city of the future. This crypto has some of the strongest commercial partnerships in the industry, and a large active development team.

---

10 After a January 2017 update.
11 Monero uses ring signatures while Zcash uses ZK-SNARKs to create anonymity. Both have pros and cons.
12 Note: all signs point to this crypto being renamed “Nano” in the coming weeks: nano.co.