

## Cryptocurrency Outlook: More Chasm Crossing

Stephen Perrenod

March, 2018

### Event

**Note:** This paper is an analysis of the technologies and trends surrounding blockchain and cryptocurrencies. It is not, and must not be considered as, financial, investment, or legal advice.

### Introduction

In this paper, we provide our views of the cryptocurrency economy in the next 9-15 months. The only thing more difficult than forecasting the near future is forecasting for longer time frames, and with the rapidly evolving cryptoeconomy, forecasting for a whole year is dangerous enough.

Make no mistake, cryptocurrencies are money. Despite the attempts of economists and money center bankers and central bankers to fight this reality, the leading cryptocurrencies are money in varying degrees. The major ones are not as significant as the US Dollar, Yen, or Euro, but they are used as media of exchange amounting to trillions of dollars per year, and have been retaining value and increasing value rapidly, despite high volatility.

Bankers are trying to incorporate cryptocurrencies into their existing systems. Central bankers are beginning to plan versions of cryptocurrencies tethered to their national fiat currencies. Economists, with their linear models, are struggling to understand the technology and its power.

### Money in the internet

Some have called Bitcoin and cryptocurrencies the Internet of Money. We say it is “money in the internet”. Technology and the internet are changing everything, why shouldn’t they change money as well? Amazon and PayPal changed the way we spend it, now cryptos are changing the way it is created and distributed.

With cryptocurrencies (‘cryptos’) the money is literally stored in the internet, as a distributed ledger with many copies, spread across a large number of internet-connected computers. The creation usually comes about through

consensus algorithms and cryptographic hash mining processes, the details of which vary from crypto to crypto.

The boundaries have shifted. Fiat currencies are created and distributed by nation-states through their central banks and banking systems, and have cross-border movement. Cryptos are created by consensus algorithms and “mining” and they have no national borders. Borders exist, but they are between different cryptos. These are more like borders within free trade areas than like the DMZ between North and South Korea.

Each crypto is the currency for its own little economy, its own community, and collectively there is an overall cryptocurrency economy. Individuals can choose to participate in as many of these communities as they wish, and can exchange cryptos one for the other, as well as for fiat. These economies are no longer all small; Bitcoin has a market cap (money supply) of about \$160 billion but that turns over nearly twice per month, so the annual size of the economy is several trillions of dollars.

### Money 3.0

We also refer to cryptos as Money 3.0 ([see this Money 3.0 article.](#)). In that article, we noted that Money 1.0 was in the form of metallic coins, and Money 2.0 is fiat paper and digitized money, with centralized ledgers. Money 2.0 is actually created in conjunction with debt, and has no asset backing. These have been the primary models over the last couple of millennia, with Money 2.0 achieving total dominance after World War II. But progress is accelerating, and we are in a new millennium.

There are three essential properties of money. It must serve as:

- ✦ A unit of account
- ✦ A store of value
- ✦ A medium of exchange

Money is whatever can be used as a socially agreed upon unit of account and medium of exchange. It also should retain its value, not depreciate quickly, so that it can be used next month and next year as well. Notice we say socially. Societies agree upon what is used as money, and nation-states in recent centuries have taken the lead in that definition, telling society what it wants.

Money 3.0 is asset-based, not debt-based. The asset is unique digital information stored in the internet, and accessed by the owner’s wallet, which stores keys to crypto, not the money itself.

If money is a socially agreed upon unit of account and medium of exchange that has some value, then cryptos are money. Different cryptos may do a better job at storing value, or may be more efficient as mediums of exchange, but they have these attributes in varying degrees.

The major criticisms are around scalability, including the rate of transaction processing over blockchains and the cost of those transactions. Scalability is the same criticism that was raised

about the internet, but it has managed to scale many orders of magnitudes over several decades, and cryptos will scale as well.

### 2017 key metrics











Let's set the stage by looking at what happened in 2017.

#### Prices

Bitcoin crossed the chasm, in terms of price and awareness, along with a number of other alt-coins such as Ethereum, Ripple, and Bitcoin Cash.

On January 1<sup>st</sup> of 2017 the price of Bitcoin was below \$1000 at \$963. The daily transaction volume was only \$83 million, and it was the only crypto with a market cap over \$1 billion. On that date, its supply was 16.1 million BTC and the market cap was \$15.5 billion.

The top 5 coins were Bitcoin, Ethereum, Ripple, Litecoin, Monero, and they had a collective market cap of around \$17 billion.

▲ #	Name	Symbol	Market Cap	Price
1	 Bitcoin	BTC	\$15,482,057,105	\$963.06
2	 Ethereum	ETH	\$722,829,967	\$8.26
3	 Ripple	XRP	\$237,638,345	\$0.006540
4	 Litecoin	LTC	\$214,726,272	\$4.37
5	 Monero	XMR	\$185,582,499	\$13.58
6	 Ethereum Classic	ETC	\$127,129,044	\$1.45
7	 Dash	DASH	\$78,695,538	\$11.26
8	 MaidSafeCoin	MAID	\$44,886,080	\$0.099184
9	 Augur	REP	\$41,714,289	\$3.79
10	 Steem	STEEM	\$39,078,093	\$0.170216











*Leading cryptos at start of 2017. Source: coinmarketcap.com*

At the end of the year, on December 31<sup>st</sup>, the Bitcoin price was \$13,170 and the supply 4% or so larger at 16.8 million units. The daily volume was well over two orders of magnitude larger

at \$13.6 billion, and the market cap was up 14 times at \$221 billion. Both the number of transactions and volume of transaction grew tremendously. On that day, the market cap of all cryptocurrencies was over \$500 billion.

The top 5 coins at the end of the year were Bitcoin, Ripple, Ether, Bitcoin Cash, and Cardano. Litecoin had dropped to #6 and Monero fell out of the top 10. Bitcoin Cash, which forked on August 1<sup>st</sup>, was the most valuable of many hard forks of Bitcoin (see our [Bitcoin Forks So 2017](#) blog entry on the topic of forks).

Each one of the Top 5 coins had market caps on 12/31/17 larger than the Bitcoin market cap alone on 1/1/17. A portfolio based on the Top 5 might be considered by some as the new FAANG for crypto, however we do not provide investment advice here at OrionX.

#	Name	Symbol	Market Cap	Price
1	 Bitcoin	BTC	\$220,903,949,498	\$13,170.18
2	 Ripple	XRP	\$82,199,880,481	\$2.12
3	 Ethereum	ETH	\$69,767,510,695	\$721.66
4	 Bitcoin Cash	BCH	\$41,526,715,510	\$2,459.32
5	 Cardano	ADA	\$18,030,140,406	\$0.695418
6	 Litecoin	LTC	\$12,000,947,760	\$220.00
7	 IOTA	MIOTA	\$9,564,670,064	\$3.44
8	 NEM	XEM	\$8,389,826,956	\$0.932203
9	 Dash	DASH	\$7,850,364,658	\$1,008.33
10	 Stellar	XLM	\$5,756,694,225	\$0.322342

*Leading cryptos at end of 2017. Source: Coinmarketcap.com*

Bitcoin increased in price over 13 times during the year. Ethereum increased by over 87 times. Ripple increased over 300 times.

### Adoption (wallet addresses)

The number of wallet addresses for BTC rose from 11 million to 21.5 million, nearly doubling, and shows no sign of tapering off. This number is still small, only 0.003 per capita for the globe. The number of addresses for Ethereum skyrocketed from under 1 million to over 17 million and at the end of the year was increasing by over 1 million per week.

**Our first prediction is that the number of Ethereum addresses will be greater than the number of BTC wallet addresses at the end of 2018.**

### Transaction volume

During 2017 the number of transactions in Bitcoin has been relatively flat, around ¼ million per day. Transactions became much more valuable, of course, on average. Ethereum transactions grew from under 40,000 to nearly a million, roughly 25-fold.

This illustrates the difference between store of value, and medium of exchange. In absolute terms Bitcoin has been the greatest store of value (per coin adjusted for supply), whereas Ethereum has been more effective as a medium of exchange based on transaction growth, lower cost for transactions, and wallet address growth.

Now it appears that Ethereum is poised to give Bitcoin a run for market cap leadership.

**Another major prediction is that the market cap of Ethereum will exceed that of Bitcoin by the end of 2018.** We revisit this below.

### ICOs

ICOs (initial coin offerings) raised over \$5 billion in 2017, across more than seven hundred offerings. The largest three were Filecoin at \$257 million, Tezos at \$232 million, and EOS at \$185 million. Although the overall total was less than 2% of the IPO dollar volume, ICOs generated tremendous press because of the very rapid growth as compared to less than \$1 billion raised in 2016. There was also a lot of increased attention and regulation from national authorities in a number of jurisdictions.

## Ten themes and predictions for the mid-term

It is still very early days in the cryptocurrency ecosystem, thus significant and unpredictable developments are common and expected. In the following discussion, our time horizon is 9-15 months and the main purpose is to examine the underlying forces that shape the technology and the market. The specific predictions point to those forces and how they can manifest themselves in the cryptocurrency ecosystem.

### 1. Cryptocurrency market caps will grow

Despite the recent pull back to around \$400 billion, the market cap for all cryptos will be higher than at the end of 2017 and will approach \$1 trillion by the end of 2018. Historically market valuations have grown over 100% per year, although with large fluctuations. Bitcoin and the current top 10 cryptos will mostly be more valuable than today.

Ethereum will surpass Bitcoin in market cap (65% probability). This will occur as financial services providers and other enterprises roll out solutions during the year. The Ethereum Enterprise Alliance now has over 200 members including major technology companies such as Cisco, HP Enterprise, Intel, and Microsoft and a number of major banks and financial services companies. It has over a dozen working groups. It is inevitable that major solutions will come out of these organizations.

The Hyperledger Consortium, created by the Linux Foundation has eight project areas. Their premier membership includes the top three Japanese computer companies, and Cisco, Intel, and IBM are also premier members. There are 185 total members. The Hyperledger Consortium is addressing solutions across finance, healthcare, manufacturing, logistics and other industries.

Hyperledger Sawtooth 1.0 released late January of 2018, is a modular platform for building and running distributed ledgers. It integrates with Ethereum and supports a number of common scripting languages for developing smart contracts.

We believe that platform developments and industry cooperation in the Ethereum ecosystem will drive increasing interest in, and value for, the Ethereum coin.

The overall cryptocurrency ecosystem will continue to garner more interest, and increasing regulation will actually open the taps for greater Wall Street investment.

### 2. Scaling technology will enhance transactions rates, lower costs

Better scaling, leading to more efficient transactions and lower fees, is an area that will see considerable improvement due to off-chain technologies such as Lightning for Bitcoin. There are also alternative mining approaches such as sharding, where different sets of miners work on selective blocks only (e.g. with 10 shards, a given miner works on every tenth block).

Transaction fees for Bitcoin rose above \$40 at the end of 2017 but as of early 2018 have come back down to around \$4. Segwit appears to have contributed considerably to lowering of

average fees. The largest U.S. exchange, Coinbase completed Segwit implementation by the end of February.

With Lightning Network now in advanced prototype stage, better scaling is on the horizon. Apps supporting Lightning are starting to appear, but it is currently a “hot wire”, unsafe for average users. Lightning allows for channels between two or more parties for off-chain transactions. These ultimately get registered to the blockchain. The intent is to make Bitcoin much more scalable and useful for payments.

Ethereum fees rose to \$4 in late 2017 but are now under a dollar. Ethereum has several proposed variants of off-chain solutions, including both payment-oriented solutions and much more general scaling solutions. The latter category includes Truebit for off-chain smart contract execution, and Plasma, that uses a tree hierarchy of block chains. Several of these alternatives will (optimistically) launch in 2018.

Litecoin fees average a quarter of a dollar, Bitcoin Cash is one “bit” (an eighth of a dollar). Ripple is half a cent. Thus, fees are reasonable for many purposes already with alternative coins.

In addition, there are cryptos without fees. RailBlocks is one crypto that is promoted as a fee-less crypto. It is one of the first DAG (directed acyclic graph) based cryptos, and uses a balance-weighted consensus method. IOTA is another that is DAG-based and fee-less.

And in an interesting move, PayPal has recently filed a patent that looks as if it creates secondary wallets dynamically, in order to pass keys on the fly in conjunction with transactions. The solution is aimed toward addressing greater volume and more rapid confirmations.

### 3. ICOs will be under tighter control

Initial Coin Offering dollar volumes will continue grow, in part because deals will be much better regulated. This will make investors more comfortable, as weaker deals and fraudulent offerings are weeded out, leading to increased investment capital, and often larger deal sizes.

A recent report suggested nearly half of last year’s ICOs are already failures (or frauds).

However, the front tranche of deal sizes could drop on average, as there will be less early stage money flowing into ICOs and more funds are reserved against achieved milestones for these new business endeavors. There is a trend toward more staging of the investment, such that tokens will be released to a company and developers only after certain product or marketing milestones are achieved.

The SEC in the U.S. is clearly in a mood, since mid-2017, to regulate many ICOs as securities, rather than as utility tokens. They are chartered with looking out for investors’ interests and have produced a [list of questions](#) investors should have in mind before committing funds to a cryptocurrency or ICO. (As always for such speculative offerings, you should only invest funds you can afford to lose, and for which you expect to wait several years for a return on your investment).

China, on the other hand, as of early 2018 has banned all ICOs. This is not surprising, really, given their heavy-handed regulation of the internet. Chinese active in the community suggest the ban may not be permanent. Blockchain development is actually part of the latest five-year plan of the Communist Party.

Enlightened regulation makes it safer for large investment houses, beyond leading-edge VCs, to enter the market. Funds for ICO investment that spread money across multiple ICOs are being established.

With the [SAFT](#) (Simple Agreement for Future Tokens) approach, one separates the security aspect from the utility aspect. A SAFT offering is viewed as a security, generally available to accredited investors only, that has a right to future tokens. Tokens on the other hand, must have a utilitarian purpose, a use within a given cryptoeconomy, rather than being purely for speculation.

We expect the first ICO with over a billion dollar investment in tokens will happen during 2018. It looks like Telegram, a messaging service very popular with the crypto community, could raise over a billion dollars with its ICO. Telegram is presently reviewing its offering with the SEC. A presale is being reported as raising over \$600 million.

#### 4. What will bankers do? Try to control blockchains.

Bankers have faced a dilemma around blockchain. Should they resist it, embrace it, or a bit of both? [Jamie Dimon of JP Morgan called Bitcoin a fraud](#) and later backed off. After all, his bank was a launch member for the Enterprise Ethereum Alliance and has other blockchain endeavors. Many other banks are members. Goldman Sachs, among others, is setting up a cryptocurrency trading desk.

Bank of America identified cryptocurrencies as a risk to its business in its most recent annual report filing. JP Morgan has noted that blockchains can disintermediate payment services that they currently provide.

The ICO game has been in other hands, including VCs. Investment banks will want in, if their governments and bank regulators will allow it. Some Swiss and German banks are starting to provide ICO services.

The favored solutions of financial services companies for now are being built around permissioned blockchains and for non-consumer use, such as for facilitating exchanges between banks themselves. Ripple, as a permissioned blockchain solution, has made significant headway as a payment solution for currency exchange and international remittances. One example is a B2B payments solution between the US and the UK being developed for American Express.

Bankers don't even like to talk about Bitcoin, because they know they cannot control it; they would much prefer discussing blockchain. In 2018 we will see increasing investment in blockchain technologies and the solutions being implemented by financial services companies,



in a manner that is mostly transparent to consumers. These ‘walled gardens’ will allow them to leverage the technology’s potential for efficiencies realized from automation while retaining control consistent with existing banking systems.

Central banks are reflexively opposed to Bitcoin and cryptocurrencies. After all, Bitcoin doesn’t need a central bank – money creation and distribution rules are built into the consensus algorithms. It is thus an existential threat. According to the general manager of the Bank for International Settlements (BIS), which is the central bankers’ central bank, "Cryptocurrencies piggyback on the institutional infrastructure that serves the wider financial system, gaining a semblance of legitimacy from their links to it". He said that policy intervention would be justified.

They are concerned that cryptocurrency could fuel speculative bubbles and undermine their national fiat currencies. For example, Thailand has asked its banks not to get involved in cryptocurrencies; Vietnam has banned them entirely.

Despite this, central banks are also looking closely at the potential for cryptocurrencies, and will be focused on solutions for clearing funds between banks, one of their core functions. National cryptocurrencies are also possible in the near term for some weak currencies; Venezuela, in the throes of hyperinflation, has announced a petroleum-in-the-ground-backed cryptocurrency scheduled to roll out within a few months. Their parliamentary opposition says it is not a real crypto, just a token for forward sales of petroleum.

India, Russia and Estonia are other nations looking at digital national currencies. Will they be true cryptocurrencies? Perhaps, but certainly they will not be open source, permissionless blockchains. They will be centrally controlled and issued as indicated in the BIS graphic below.

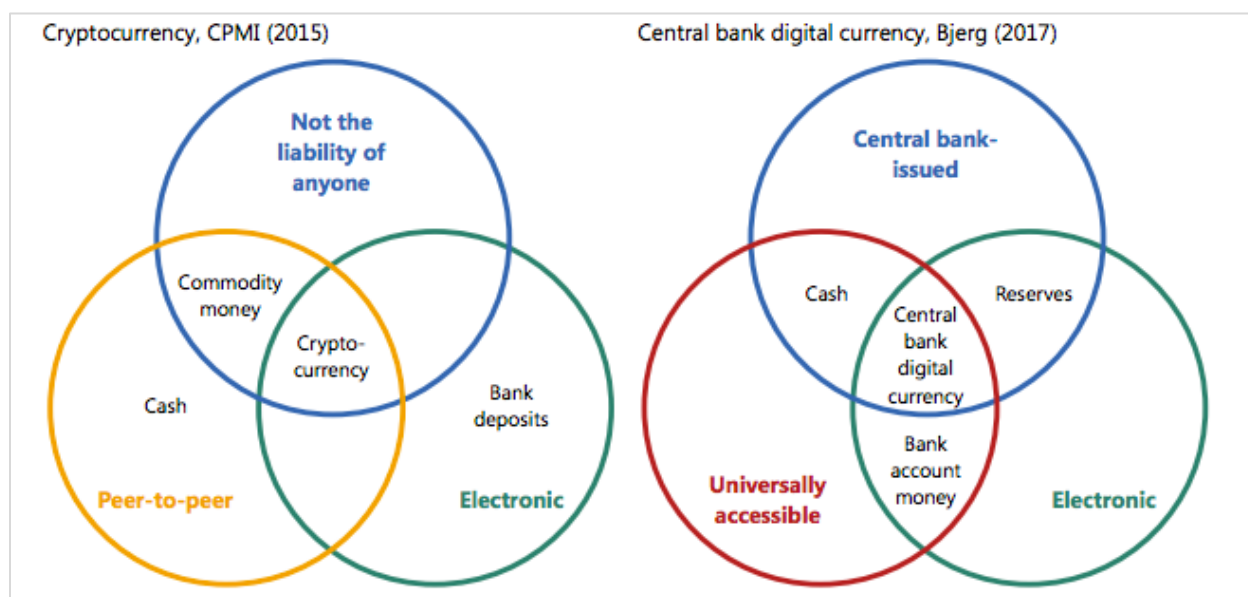


Image credit: Bank for International Settlements

See the difference? The whole point of Bitcoin is as a peer-to-peer asset-based form of money. Central bankers would strip those attributes out and make them central bank-issued 'liabilities'. And peer-to-peer is weakened into what they call 'universal accessibility'. Well fiat is universally accessible, once you have some, but perhaps such a digital currency would be more easily accessible to the unbanked.

Will central banks start to look at cryptocurrencies as reserves? Countries looking to diversify their reserves have typically focused on major fiat currencies and gold. SDRs are restricted to a handful of nations; cryptocurrency can be another possibility.

Investment in any significant way in cryptocurrency as reserves is very unlikely in 2018, but central banks will increase their pilots, prototypes and market studies. They will also seek to coordinate regulation as they try to push toward the right-hand side of the figure above.

## 5. Fraud and theft will still be prevalent

The most famous fraud was Mt. Gox. Mt. Gox's former CEO, Frenchman Mark Karpeles, was arrested in Japan in August 2015. Mt. Gox at one time was the world's largest bitcoin exchange, and had 850,000 Bitcoins go missing in 2014, 200,000 of which were later 'found'. At the time, the value was around \$473 million. The present value of 650,000 Bitcoins is over \$7 billion. Last year he pled not guilty to embezzlement charges and his trial in Japan is ongoing.

There have also been frauds in the mining business, such as ZenMiner and GAW Miners, who were selling fake mining contracts to the tune of \$20 million.

There are many ICOs which will turn out to have been essentially fraudulent if not outright frauds. PlexCorp has had assets frozen by the SEC due to fraudulent marketing in a scheme that raise \$15 million. The SEC also charged a real estate company, and a diamond company, both owned by the same individual, with selling unregistered and non-existent coins.

Bitfinex is a Hong-Kong registered exchange that suffered a major theft. Of \$70 million stolen, around 2/3 was recovered for many customers. The popular exchange Poloniex was hacked in 2014, but the loss was covered.

Coincheck in Tokyo suffered a \$530 million theft by hackers in January of this year. Over a quarter million investors were affected. The theft is thought to be the largest to date and centered around NEM, an alt-coin popular in Japan. The exchange is promising retribution of around 80% of losses from its own funds.

Frauds and thefts will continue to grow in dollar terms. A new record for largest single theft will be set, but may still be less than largest bank raid of fiat currency to date of nearly \$1 billion.

Most of the hacks are against hot wallets controlled by exchanges and many involve phishing attacks to gather passwords. Crypto hashes seem to remain secure, so the advice is to keep most of your funds in your own private wallet.

Due diligence is called for, as always, when doing business with an exchange or investing in an ICO.

Here, for your enjoyment, is a list of the top [10 bitcoin “villains”](#).

## 6. Forks will diminish in importance

The era of Bitcoin forks is largely behind us as we wrote [here](#). Last year was a big year for Bitcoin forks, with Bitcoin Cash, Bitcoin Gold, and around 18 other hard forks in late 2017 and early 2018. (Soft forks are upgrades that do not cause a persistent split in the chain).

Technology enhancements promoted in these forks are across several main categories:

- ✦ Bigger blocks for scaling, shorter block times
- ✦ Off chain or side-chain transactions (Segwit for signature, and more generally Lightning, etc.) for scaling
- ✦ Different hashing algorithms for easier mining
- ✦ More anonymity, security
- ✦ Enhanced programmability, smart contracts
- ✦ Increased money supply

If you owned bitcoin prior to block 478558, you in principle own all 20 of the forked coins, including the most valuable one Bitcoin Cash, and mostly in a one-one ratio. Putting your hands on them is trickier.

That is a question as to what support particular private wallets or public exchanges provide. There are guides on the internet and YouTube as to how to retrieve although it seems more trouble and risk than justified in most cases.

For now, it seems we have reached a point of exhaustion for the principal good ideas and the newest forks are more likely to be dodgy, or frauds, or duplicating others, or of limited potential. The most obvious technical improvements have already been applied in various forks, and the desires of different communities have been addressed. Future forks will produce tokens of limited value.

Proposals taking advantage of off-chain or side chain technologies will be the focus of scaling progress in the near future. These do not fork the main blockchain.

## 7. Dapps will blossom wildly

Dapps are decentralized applications. These are open source, decentralized applications governed by protocols and with tokenized incentives. Applications on the blockchain that are in wide use are still relatively few, setting aside the popularity of Cryptokitties. We expect to see many more working real-world dapps released in 2018.

The Internet today is primarily in the hands of large corporations. Dapps on blockchains could provide the world with a path to a much more decentralized Internet 3.0. This would be an open peer-to-peer internet, with net neutrality and more.

Technically, Bitcoin itself is a dapp built as open source, running on a decentralized blockchain and adhering to a set of protocols. More typically, the term “Dapps” is used to refer to applications other than coins or tokens that are implemented on a blockchain and that make use of tokens.

Ethereum is a very popular platform for dapps, since it allows for smart contracts to be programmed on the Ethereum Virtual Machine. Here is a [list of over 1000](#) projects built on Ethereum, many of which are pretty simple, such as games. But you have to start somewhere. And over 400 of these are live today. As an example of something more sophisticated, here’s a wizard for creating tokens and crowdsale contracts in 5 steps: <https://wizard.oracles.org/>

Some other examples include Golem (calling itself “Air BnB for computers”), for utility access to computer power. Brass Golem is the first use case for Golem, allowing users to rent out their computer power for computer image rendering.

Another example is Augur, a prediction market. Everex is being built for cross-border payments. The Rudimentary is designed to provide equity crowdfunding for artists. And let’s not forget ERC20 – the standard for token issuance in ICOs is itself a dapp on Ethereum.

We expect to see an explosion of Dapps during 2018, including many real-world working examples.

Want to create your own? [Here’s a good place to start!](#)

## 8. Social media and identity are ripe for change (P2P or B2C?)

One out of three people across the globe is a social media user. Today social media are highly centralized and controlled by a few large companies. Identity and social media will be major areas for Dapp development this year.

The problem to solve is that these massive social media and internet companies own the data you provide and they monetize it for their own benefit. Large companies have dominated since they have all the servers and software algorithms, but today’s desktops and smart mobiles are very powerful devices. Blockchain-based social media will allow users to own their personal data and decide who can access it, and to determine whether there is a price or licensing requirement for access. It will allow users to be compensated in cryptocurrency if the social media network likes their content to a sufficient degree.

There are a number of existing “social media on blockchain” startups, including Steemit for blogging. If users like your posts you can be rewarded with Steem dollars. Akasha is another publishing, blogging platform. It sits atop Ethereum. Narrative is another, describing itself as a content economy rewarding creators and moderators. They intend to redistribute 85% of revenue to the user base. Governance will reside in the community, including a user-elected tribunal as final authority.

SocialX is a photo-sharing and messaging network that will reward content creators. For example, “Superlikes” will have associated cryptocurrency. It is intended to have governance reside in the community,

Blockstack is more ambitious, looking to overthrow the existing paradigm for the internet and to ensure greater net neutrality. It is a platform for a peer-to-peer internet including domain name servers on a blockchain, with identity, storage and token services. The core software has support for identity and Bitcoin and Ethereum wallets. It is accessible from a browser, and provides a development platform for dapps. It presently has over a dozen apps, many focused on token portfolios. It already includes a home sharing app, a music distribution app whereby artists get paid directly, and a health records management app, for example.

This whole area is exploding in 2018. We will see multiple social media blockchain unicorns. Already, Steem dollars have a market cap close to a billion dollars.

Facebook and Twitter are facing increasing criticism for centralized control and various missteps. They are ripe for disruption, as is Google’s core search business.

Facebook could react by implementing its own token, in fact they would be remiss not to. Google could as well.

This push for blockchain in the social media arena could well favor Ethereum over Bitcoin because of its advanced smart contract capabilities.

This battle can be framed as P2P vs. B2C.

## 9. Distributed exchanges will improve rapidly

The vast bulk of crypto exchange happens today on centralized exchanges. This is not aligned with the original spirit of Bitcoin, envisaged as a peer-to-peer currency by Satoshi.

A number of distributed exchanges (dexs) are under development and some are in operation at present. They provide a cross-border, more anonymous way of making crypto exchanges, and they implement the exchange process from your private wallet to the buyer’s private wallet. This is similar to the escrow process used in buying and selling real estate in that ownership passes directly from seller to buyer.

In contrast, a centralized exchange keeps your crypto in their exchange wallets and then keeps track of how much of that belongs to your account. This is similar to your brokerage account where most stocks are held in ‘street name’, i.e. your broker’s name. Thefts from crypto exchange wallets have been a serious problem the last several years, as discussed above.

Distributed exchanges are a solution to provide efficient movement between private wallets, and are seeing a lot of activity lately. They offer a safe way for individuals to exchange between coins or to buy or sell, perhaps at lower cost, via relayers.

Here are some current ones: Bitsquare, Bitshares, NXT, CounterParty and Waves. Waves uses Proof of Stake for mining native coins. A number of these solutions require usage of their own coins. The other approach is known as 'cross chain atomic swap'; the first such swap happened in 2017. CounterParty implements smart contracts on the Bitcoin blockchain and like all of these solutions, provides decentralized escrow services.

Some dexs under development include BarterDex, EasyDex, LoopRing, RadarRelay, and PAX. PAX adds additional functionality to Barter Dex (which uses atomic coin swaps) and will allow fiat national currencies to be exchanged with cryptos and for positions to be held for a period of time. LoopRing expects to launch trading in the first half of this year; their coin is listed on at least two exchanges. The Radar Relay team has built a RESTful API that implements the 0x spec. The 0x spec is an open protocol to support trading of ERC20 tokens on the Ethereum blockchain, and is designed to support the implementation of decentralized exchanges.

This is neither an exhaustive list, nor a recommendation for any of these platforms, but it is indicative of the high degree of innovation in the area of distributed exchanges and the current level of moderate sophistication.

The centralized exchanges will respond. We will see hybrid examples arise. Existing centralized exchanges will provide the facility for direct exchange from an individual's wallet, mimicking the peer-to-peer experience. That is, they will automate the process for movement of crypto from a private wallet to an exchange wallet, combined with the exchange from crypto A to crypto B (or to fiat), and with the resulting funds retained at the central exchange, or possibly sent to another private wallet for the newly purchased cryptocurrency, or to the user's bank account in case of fiat. They already have the banking information typically and will only have to have customers record their public key addresses for the wallets in question.

Since centralized exchanges are regulated by national governments and must enforce KYC (know your customer), they will only provide this service for existing customers, but it will help them to maintain and grow their customer base.

## 10. Government regulation will be a force for stability

Government responses to cryptocurrency across the globe have varied and will continue to vary, but in the free world there will be focus on stabilization, tracking, and on taxation for exchanges, money transfers, ICOs, futures, and ETFs. Government response and the banking system response have considerable impact, e.g. the restrictions on credit card purchases imposed by several large U.S. and U.K. banks in Feb. 2018.

China's regulation in the cryptocurrency domain is very severe. China's tough talk and actions on cryptocurrency have caused repeated pullbacks in the prices of Bitcoin and other cryptos.

Cryptocurrency exchanges in China are being shut down; this includes their access to WeChat, the most popular messaging app in China. Even crypto mining is being repressed.

Of course, given that China has been important as a buying community, these regulatory restrictions have had significant market impacts. In response Chinese mining companies have been looking to move mining to Europe, Canada and other locales where they can still mine at reasonable cost.

"Blockchain's advocates for absolute decentralization have no solid ground, because (blockchain) itself is a software developed in a centralized way," - Zhang (head of technology unit at China's Securities Regulatory Commission)

China's attempts to try to centralize blockchain, while not surprising from a highly centralized and authoritarian government, are doomed to fail, since blockchain is designed around decentralization. It's an empty threat, they can of course create their own national cryptocurrency but the above statement is nonsensical. Blockchains can run anywhere there is an IP address. China can be part of the crypto world, or cut themselves off from the world.

In the West and in Japan and Korea, regulation has been more targeted, and in three main areas.

One is on regulating ICOs and forcing them into the security offering framework in the typical case that the ICOs in fact represent equity in a business as opposed to true utility tokens. Recently the SEC sent requests for information to over 80 ICO issuers. They have a substantial task force around ICO regulation and clearly intend to regulate ICOs broadly as security offerings.

A second area is enforcement of KYC/AML for exchanges, to allow governments to track money transfers, and exchange reporting for taxation purposes. FINCEN in the U.S. has made it clear that they will enforce existing regulations with respect to cryptocurrency transfers.

A third area is in classifying cryptocurrency as an asset, subject to income taxation when mined, and to capital gains realization when sold. The IRS has classified cryptocurrencies as assets for the purpose of income and capital gains. Recently a U.S. court ruled that cryptocurrencies can be considered commodities. The CFTC has an interest with the recent introduction of Bitcoin futures.

The effect in the U.S. has been to increasingly limit ICO investments to accredited (wealthier) investors. This may have helped push more ICOs toward doing a portion of their offering in airdrops (small amounts of free coin for signing up to their social media sites). Airdrops are a way of offering cryptos freely in exchange for market recognition.

Exchanges are becoming more regulated globally and that is generally healthy for the cryptocurrency economy, given the number of frauds and hacks that have occurred.

We believe the Chinese will look to establish their own national cryptocurrency, centrally controlled and for use in their Silk Road and other trading initiatives. They are looking for ways to avoid the use of the USD in their trading, and to diversify away from dollars as their principal reserve holdings.

A number of other countries including Venezuela and Cambodia have announced national cryptos. As previously mentioned, India, Russia, and others are studying this possibility. We expect to see more of this, especially in less developed nations with weaker currencies and with nations looking to avoid sanctions.

### Conclusions

Despite price volatility, Bitcoin forks, technology disputes, increased and inconsistent government regulation, ICO scams, other scams, and thefts, the state of cryptocurrency is stronger than ever.

Technology issues around scaling, fees, security, and usability are all actively being addressed. Solutions are being implemented at a rather rapid pace, considering all of the various factions with differing objectives and the limited number of expert developers.

The market cap of all cryptos exceeded half a trillion dollars during 2017. Six coins had over \$12 billion market cap or more at the end of the year. Litecoin was a dozen billions, Bitcoin over 200 billions.

We believe cryptocurrency is “money in the internet” and digital global money, Money 3.0. As such, it is poised to be one of the two or three most important internet developments going forward, of greater significance than 5G for example, and perhaps comparable to artificial intelligence and IoT in its impact. It will also be of great use in both IoT solutions and AI solutions. As the internet has, cryptocurrency and blockchain can touch every industry, every consumer, every user, for applications where value is exchanged or recorded or even perceived.

Copyright notice: This document may not be reproduced or transmitted in any form or by any means without prior written permission from the publisher. All trademarks and registered trademarks of the products and corporations mentioned are the property of the respective holders. The information contained in this publication has been obtained from sources believed to be reliable. OrionX does not warrant the completeness, accuracy, or adequacy of this report and bears no liability for errors, omissions, inadequacies, or interpretations of the information contained herein. Opinions reflect the judgment of OrionX at the time of publication and are subject to change without notice.