OrionX.net

Event

The OrionX Constellation
Blockchain

Cryptocurrency Outlook 2019: Still Early Days

Stephen Perrenod
March 2019

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 crypto-economy, forecasting for a whole year is dangerous enough. We begin with definitions and a glossary of terms.

Definitions

To get started we provide a few key definitions of Bitcoin, Blockchain, Consensus Algorithms and other related terms.

Bitcoin: The original decentralized cryptocurrency, whose supply is increased through regulated "mining" via a cryptographic hashing process that validates transactions, and that is stored in blockchain form in the Internet. Bitcoin introduces triple entry accounting because transactions are recorded on the blockchain as well as in the sender's and receiver's wallets. *Bitcoin's software layers include its blockchain and the Nakamoto consensus algorithm, as well as the BTC cryptocurrency.*

Our one sentence definition is:

> *Bitcoin is cryptographically encapsulated energy, is mined in the Internet with the hardest and most pre-determined monetary policy ever implemented, and is stored within a public triple entry distributed ledger that spans the Internet.*

Blockchain: A record or ledger of transactions stored in blocks. Blocks are time stamped and linked to one another in sequential fashion. The links require cryptographic hashing. Blockchains may be open, public, and permissionless such as Bitcoin's blockchain, or permissioned blockchains that may be private or semi-private, requiring access privileges.

Consensus Algorithms: The rules by which transactions are validated, and more broadly, the monetary policy that creates new coin supply. Proof of Work (PoW) is the best known and is also referred to as mining. Mining encapsulates value in relation to the difficulty of the cryptographic hashing process and the rate at which supply is created. There are many others, such as Proof of Stake (and other algorithms that do not require consensus), but non-PoW coins all require a degree of centralization with a corresponding decrease in security which, nevertheless, may be acceptable for specific use cases including a desire for greater liquidity.

Cryptocurrency: There are over 2000 cryptocurrencies that have been created. After Bitcoin the first created were forks of the Bitcoin blockchain and were also mined cryptos.

OrionX Constellation™ reports cover 5 Es: industry milestones (Events), historical view of a technology segment (Evolution), main vendors in a market segment (Environment), customer decision criteria (Evaluation), and how vendors in a segment score (Excellence) based on the OrionX methodology, which considers market presence and trends, customer needs and readiness, and product capabilities and roadmap.

Since then a large variety of consensus algorithms have been tried, and many cryptos are simply issued, rather than mined. While this provides rapid liquidity and can boost transaction throughput, it undercuts security, decentralization, and store of value attributes.

Distributed Ledger Technology (DLT): A record of transactions that is stored across many servers, which can include multiple organizations, or even in the public space (Internet). A blockchain is a particular type of distributed ledger.

Initial Coin Offering (ICO): Creation of a new coin or token, with some defined market or use case, and promotion of same to raise funds for development and marketing. Colloquially, a way to raise money when you have a small development team and no working product. Many ICOs have involved pre-mining and airdrops (giving away a portion of coins in order to build interest and jumpstart the blockchain).

Security Token: A token tied to real assets such as real estate, commodities, or company shares, and subject to financial securities laws.

Smart Contract: Analogous to program trading, but more broadly applicable, rules or business logic that allow for more complex automated transactions to occur on top of a blockchain according to pre-specified triggers

Stablecoin: A cryptocurrency whose value is pegged to a particular fiat currency, or commodity, or basket of fiat or commodities.

Trustless: A sufficiently distributed blockchain provides decentralized and immutable validation and tracking of transactions without the need to trust a centralized authority. Also known as distributed trust; instead of being placed in counterparties, trust is placed in algorithms and the knowledge that mining is sufficiently decentralized.

Additional references:

- Here is an OrionX overview presentation on Blockchain and Cryptocurrencies: *https://www.slideshare.net/Shahin.Khan*
- In this presentation, titled Top Cryptocurrency Supercomputers, we looked at cryptocurrency mining pools around the globe: *https://www.slideshare.net/perrenod/top-cryptosupers-20181112v3*

And now, on to our outlook.

Ethereum and Smart Contracts

Our biggest mistake last year was being impressed by the rapid growth in Ethereum's market value in 2017, and even predicting the possibility of a 'flippening': the elusive ethereal unicorn of achieving a market cap value greater than Bitcoin. See our prior outlook at: *http://orionx.net/wp-content/uploads/2018/03/Blockchain-Event-Outlook-20180326.pdf*.

In the Great Crypto Crash of 2018, Ethereum *fell* harder than Bitcoin in percentage terms. Its market cap fell from $70 billion on the last day of 2017 to $14 billion on the last day of 2018, an 80% drop. Bitcoin fell from $224 billion market cap (coins outstanding x price per coin) to $67 billion in the same interval, a 70% drop.

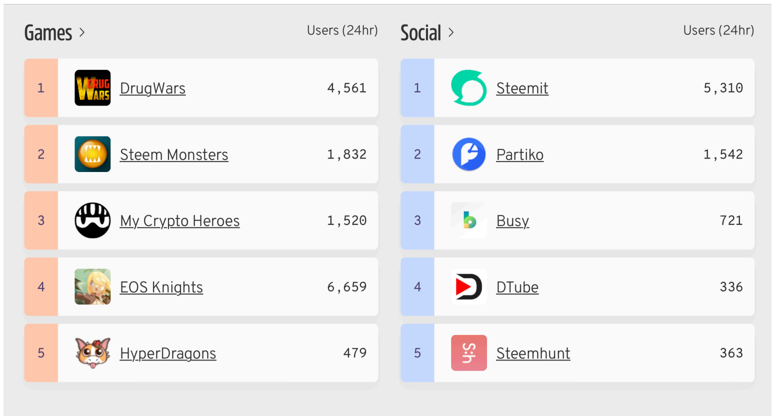
But what happened to Bitcoin was largely similar to what happened to Ethereum, a market correction that ended a bubble that peaked in late 2017 and early 2018, as a response to the drying up of the ICO market and a slowing of new people entering the cryptocurrency markets. The ICO market was fueled by excessive speculation into literally a couple thousand different "altcoins" of little value during 2016 and 2017. Few altcoins had the ability to deliver real utility, and many were outright frauds. The “investments” in those altcoins were largely made with payments in the top two cryptocurrencies as well as fiat.

Regulators at the SEC in the US and in other countries increasingly tightened restrictions on ICO issuance in the name of investor protection. The SEC initiated several enforcement actions against ICO promoters. As restrictions tightened and the large majority of ICO prices sank below their initial offering values, the market quickly dried up in 2018.

The problem was one of utility, especially for the Ethereum ecosystem, which is built on the promise of ‘smart apps’, or dapps (distributed apps) that require the blockchain. A large fraction of ICOs were issued as tokens on Ethereum. The state of dapp development overall remains immature at best.

After Cryptokitties, it seems little of note happened. Cryptokitties, if you haven’t heard, is a game allowing you to raise a virtual kitten, the Tamagotchi of the blockchain era. A flurry of popularity for this single dapp exposed scaling issues for Ethereum.

A recent rundown on the state of the dapp market (*https://medium.com/fluence-network/dapp-survey-results-2019-a04373db6452*) notes that most began development during 2018. Half of apps are developed with small teams of less than 6 developers, only 20% with teams of more than 10 people. Games, gambling, tools, collectibles, social apps and exchanges are the top categories for dapps.



	Games ›	Users (24hr)		Social ›	Users (24hr)
1	DrugWars	4,561	1	Steemit	5,310
2	Steem Monsters	1,832	2	Partiko	1,542
3	My Crypto Heroes	1,520	3	Busy	721
4	EOS Knights	6,659	4	DTube	336
5	HyperDragons	479	5	Steemhunt	363

Figure 1: Highest usage dapps

Ethereum has captured 87% of the dapps, with EOS second at 19% and Tron third (some are developed on multiple blockchains). A plurality use centralized cloud backends and databases. The biggest problem is usage, which is low, and even then, there is reported presence of bot users designed to inflate usage statistics. Only 12% of projects report more than 500 daily active users! TRON’s acquisition of BitTorrent may provide a large potential new user community.

Games and social were the two leading dapp categories as of Q1-2019. You can monitor developments and usage at stateofthedapps.com (*http://stateofthedapps.com/*)

One of the biggest criticisms of Ethereum is the need to rely significantly on its main blockchain which has proven to be too slow and expensive for the types of apps that it has attracted. But right now, usability and number of users are of the greatest concern for developers. Another criticism has been the delays in Ethereum’s roadmap, but the long-awaited Constantinople release and the St. Petersburg release finally went live at the end of

February. Constantinople hardens the money supply by cutting block reward from 3 ETH to 2 ETH. St. Petersburg rolls back a feature in Constantinople that was found to have a major security hole and that delayed the roll out for several weeks. Ethereum's plan to eventually move to Proof of Stake, instead of its current Proof of Work algorithm, generates considerable ongoing controversy. A ProgPOW proposal seeks to favor GPUs over ASICs even more than Ethereum presently does.

Bitcoin and Lightning

Despite the bear market in valuation in 2018, Bitcoin chugged along to new heights in terms of security. Total hash power reached 43 exahashes, far more than any other mined coin. Although there are a handful of large mining pools (*http://orionx.net/2018/11/cryptosuper500-cryptocurrency-mining-list-blog/*) mining continued to become more decentralized.

Bitcoin demonstrated high practical value in Argentina and Venezuela due to political crises leading to collapsing fiat currencies. While Argentina's inflation rate is high at 48%, Venezuela's Bolivar reached an 80,000% inflation rate by year end 2018 (*https://www.forbes.com/sites/stevehanke/2019/01/01/venezuelas-hyperinflation-hits-80000-per-year-in-2018/#38c734484572*).

Criticism of bitcoin's energy consumption continues from time to time, but it is less than 1/2000 of the world's total consumption (*http://orionx.net/2018/07/will-bitcoin-consume-all-electricity/*). And 75% is estimated to come from low cost renewables including hydropower, geothermal power, and wind power. Bitcoin is well suited for off-peak usage of renewable sources.

Bitcoin has been forked many times (*https://unhashed.com/bitcoin-cryptocurrency-forks-list/*) in the past, always resulting in lesser coins. There was some forking drama around Bitcoin Cash. It was a hard fork in 2017 (*http://orionx.net/2018/01/bitcoin-forks-2017/*) off the Bitcoin blockchain, a pretender to the throne that only achieved a fraction of the valuation of (the original) Bitcoin. It and other Bitcoin-named cryptocurrencies are evidence that higher security in terms of aggregate hashrate receives higher value in the market, since these clones have similar monetary policies to Bitcoin core and continue the existing Bitcoin chain.

Bitcoin Cash itself forked again in late 2018 due to infighting among its proponents, resulting in a new Bitcoin Cash and a Bitcoin SV. The two resulting coins ended up with even less total value, combined they represent only 5% of Bitcoin's value at present. A hashwar between the respective sponsors helped aggravate the general cryptocurrency crash, as the two sides spent Bitcoin and Bitcoin Cash from their reserves. "Bitcoin Core", the client software for Bitcoin, or "Bitcoin Legacy" are sometimes used to refer to Bitcoin. Neither the core nor legacy designation is necessary.

Bitcoin is criticized for its limited transaction rate and for high fees. And yet Bitcoin exceeded PayPal in transaction volume in 2018, by a factor of 2, at $1.3 trillion versus $600 billion. And fees have dropped to well below $1, which means it is much cheaper than Visa and MasterCard for a $50 transaction.

The Lightning Network (*http://orionx.net/2019/01/will-lightning-electrify-bitcoin/*) a second layer payments solution, was the biggest development for Bitcoin and perhaps cryptocurrencies in general during 2018. Lightning implements second layer payment channels and these can be established with other cryptocurrencies, not only Bitcoin. It took off, scaling to 15000 payment channels at the beginning of 2019.

Lightning is a network of payment channels that allow for tiny or moderate sized transactions to be batched up before final recording to the blockchain. It allows two users without a direct payment channel connection to send payments over its network. It is limited only by the number and topology of the channels and the carrying capacity of Bitcoin loaded into those channels. It implements simple smart contract features to enforce honest payments.

The Lightning Network provides the answer to critics who say Bitcoin cannot scale and has transaction fees that are too high. It has the potential to outperform Visa and MasterCard on both scores while also allowing very small payments they won't even touch.

Cloud providers such as Amazon and Microsoft and web caching provider Akamai have widely distributed infrastructure so might consider becoming major players in the Lightning Network.

Schnorr signatures are the next big thing for Bitcoin and will provide provable security and non-malleability and also provide the building block for multi-signature and smart contract capability. The intent is to implement Schnorr capability as a soft fork. Schnorr's linearity property supports key aggregation from multiple parties, providing improved privacy of multisig transactions and enabling smart contracts with Taproot.

Security Tokens

As ICO regulations have tightened, the industry has received increased attention in two areas, security tokens and stable coins. Security tokens provide to the token holder a share of an asset or of a pool of assets, or of a debt or equity offering. A promising use case is in tokenizing real estate, providing greater liquidity and opening participation and profit-sharing to a wider audience. Even sports franchise tokenization is envisioned; diehard fans would love to own part of their favorite team.

REITs generally involve baskets of properties, while tokens could more readily facilitate ownership of individual properties, including time shares for vacation properties. How the SEC will view this area, and what kind of guidelines they will develop remains to be seen.

A portion of the St. Regis hotel in Aspen has already been tokenized in an $18 million offering. QuantmRE last December launched what is said to be an SEC-compliant token (*https://bravenewcoin.com/insights/quantmre-launches-security-token-tied-to-u-s-real-estate-assets*) available to accredited investors, for residential real estate. The largest STO (security token offering) yet was announced on March 1st of this year by Vertalo and Securrency. Working with Inveniam Capital they aim to tokenize four US properties with a total value of $260 million, including a water pipeline project in North Dakota.

In the non-real estate arena, Bitbond is a peer-to-peer lending market based in Germany offering small business loans denominated in Bitcoin. They are issuing an interest-bearing security token for business expansion purposes. (Disclosure: The author is a small-scale lender on their platform).

Many more STOs are sure to follow during this year. Whether these asset tokens will be secure enough is one major concern, and certainly SEC actions and opinions related to security tokens will be key.

Stablecoins

Stablecoins are designed to offer something much less volatile than Bitcoin or other cryptocurrencies, and thus serve as an on-ramp from fiat to cryptocurrency, or a way to park money between crypto trades on exchanges. Stablecoins are generally tethered to a major fiat currency, typically the dollar or Euro or Yen, but they are sometimes tied to gold or a currency or commodity basket.

The best known and largest stablecoin by capitalization is Tether (USDT), a top 10 crypto with a $2 billion market cap. It also has a very high velocity, with a daily turnover of $8 billion as of late February.

Big banks are now jumping in to the game. Several banks are issuing their own stable coins, tied to the US dollar or Japanese yen. Like other stablecoins, these are centralized solutions built on permissioned blockchains.

Banks who have announced such coins include Signature bank, JP Morgan, Citibank, Mizuho Bank, and Mitsubishi UFJ Group. While the JP Morgan coin is targeted toward institutional clients, and the Mitsubishi MUFG Coin initially so as well, Mizuho will role out a J-Coin tethered to the Yen and intended for broad retail use, reportedly motivated by the upcoming Olympics games to be held in Japan in 2020 and the popularity of digital payment systems in other countries. The large banks entering the cryptocurrency space is another sign of the market maturing. However, Citibank just shut their Citicoin project down this month.

Signature Bank appears to have been the first to launch, with a blockchain based payment system and digital dollar Signet built on Ethereum. They had already obtained approval from NY State banking authorities.

IBM has a stable coin project based on Stellar, and have recently announced that six banks around the globe are participating, including in Brazil, South Korea, and the Phillipines. These will be tied to their respective national fiat currencies.

Enterprise Blockchains: Distributed Ledger Technology

The Enterprise Blockchain race is on, with IBM in the lead, and Microsoft, Oracle and Fujitsu not far behind. Supply chains and logistics are major targets for enterprise blockchain technology, but there are many additional areas being targeted from health care to government records.

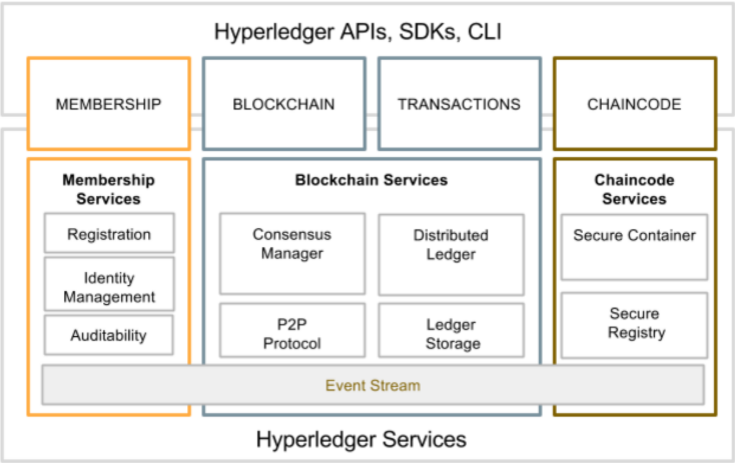


Figure 2: Hyperledger is a prominent example of Enterprise Blockchains, which can be considered as the Intranets of the Blockchain world.

Enterprise blockchains are typically permissioned semi-private implementations available within a company, or a consortium of companies, engaged in mutual commerce. The former are called private blockchains and the latter, federated blockchains.

Hyperledger is an open source effort for cross-industry blockchain technology, hosted by the Linux Foundation and with members from finance, manufacturing, logistics and technology industries. Premier members in the technology space include Cisco, Fujitsu, Hitachi, IBM, Intel, NEC, and SAP. Other large members include Accenture, Airbus, American Express, Baidu, and Damler. There are nearly 200 general members.

Projects include blockchain platforms, distributed ledgers for decentralized identity, smart contracts, and supply chain tracking. Hyperledger's Sawtooth platform, contributed by Intel, uses Proof of Elapsed Time and random secure 'leader' selection in its consensus algorithm. Sawtooth has been tested in seafood supply chain history and in bond securities settlement applications.

IBM and Digital Asset contributed the plug-and-play Fabric framework for consortium blockchains with permission levels. Fabric has no native currency but allows users to define assets and use them with Fabric Composer. Chaincode adds business logic for smart contracts. Oracle has added a tools layer on Fabric. IBM use cases include crude oil transactions, pharmaceutical procurements, and trade finance.

Microsoft was first to put blockchain in the cloud, offering a service on Microsoft Azure. It is building bridges from blockchain to its platforms including SQL data base, and even to Salesforce and SAP. The impetus is to bring a single view of data, sharable among participants, and including unstructured data in the mix.

Microsoft Azure supports R3's Corda for maritime insurance application in conjunction with Maersk, the largest container ship and supply vessel operator in the world. Buhler, a major supplier of food processing machines for grains, provides another use case with a blockchain project to reduce waste and energy usage in the supply chain while increasing food safety. In addition to Corda, Azure offers Ethereum, and Hyperledger environments.

Alibaba, Baidu, Huawei and Tencent are all entering the Blockchain-as-a-Service (BaaS) space, so things will become more and more interesting. Bank of America analyst Kash Rangan expects a $7 billion BaaS market.

Cryptocurrency Phones

A cryptocurrency phone, also known as a blockchain smartphone, has specific security for encrypting messages and voice traffic and support for mobile cryptocurrency wallets, providing an embedded cold storage wallet. The HTC Exodus 1 was announced in October 2018 by the Taiwanese company and can be purchased with Bitcoin or fiat. It has a secure enclave separated from the OS for cold storage.

This is supposedly similar to storing your cryptocurrency on a hardware wallet (special USB device) that is detachable from a computer.

Sirin Labs, out of Israel, claims to have the first blockchain phone, also introduced in 2018, and named for the deceased cryptographer Hal Finney. Hal received the first Bitcoin ever transferred. The Finney phone is said to have enough blockchain capability that it can support automated internal exchange between tokens (which ones are supported is not clear). It appears that like Sirin Labs is going into the banking business or has a partnership with an exchange. Available in pebble gray or coal black, it has a small second screen for the cold wallet. Sirin has a dapp store with a handful of applications at present.

The Electroneum M1 uses the phone to mine its own ETON token. Initial rollout is planned for South Africa.

The big name that has entered this space is Samsung, with their Galaxy S10 that supports Bitcoin, Ethereum, and Enjin. It also has dapp support, including one that comes embedded and allows users to earn Cosmo tokens in exchange for beauty reviews.

Expect to see a number of additional cryptocurrency phone offerings introduced this year. Apple fans will probably have to wait until 2020. It is also expected that additional blockchain related features will be introduced to help secure users' online identities and data. This could be a step toward liberating users from highly centralized social media platforms.

Messenger Coins

Speaking of centralized social media platforms, Facebook, with its messaging application WhatsApp, and also Telegram, Signal, Line and others are looking to offer currencies on their networks. We expect major developments in this space during 2019. The NY Times reports that Facebook has 50 blockchain engineers. However, it is conceivable that these coins will not be true cryptocurrencies.

Some of these cryptos are already named. Gram is the planned coin for Telegram. And Link has been announced by Line, which is big in Japan, Taiwan, and Thailand.

Most of these may end up being stablecoins, tied to various national fiat currencies. Facebook is reportedly looking at a currency basket to set token value. They plan initial rollout for users of WhatsApp in India.

They all must face the governance problem. They will want to control issuance and then what do you have, but a centrally controlled stablecoin. This is far from the original Bitcoin ethos of a decentralized coin that is mined, not issued, and not tied to fiat currency.

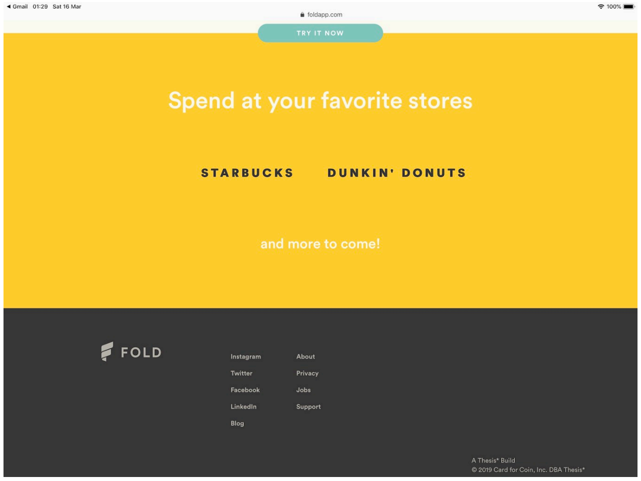
The applications could be numerous, however. One application is for users of a messenger app to send funds to one another within their network, and in some countries a single messenger application may address a very large fraction of the populace. Another use case is for retail payments and yet another is for advertisers to offer rewards or discounts.

The smartest thing a messaging platform could do would be to leverage the Lightning Network for their payments architecture. Time and again, open standards win out. This could bring a large user community into the Bitcoin ecosystem.

Expect this area of messenger coins to be a major source of attention toward cryptocurrencies, and it should certainly help drive adoption substantially. To impact the overall market more, one would want to see these coins available for trade on exchanges as well.

Coffee? The Retail Killer App

Bakkt has announced that they will provide a Bitcoin processing option for Starbucks, who have taken an equity position in the payment solutions firm. Microsoft Azure may be the cloud back end. Starbucks will not handle Bitcoin directly. We await further details. Fees for Bitcoin are down considerably, and if Bakkt uses Lightning Network in their solution the fees could be tiny.



Spend at your favorite stores

STARBUCKS DUNKIN' DONUTS

and more to come!

A Thesis* Build
© 2019 Card for Coin, Inc. DBA Thesis*

Fold is another such solution, using Lightning, that can allow customers to purchase coffee and more at Starbucks and Dunkin' Donuts. Fold actually places the orders on users' behalf, and they plan to add Whole Foods and Uber capabilities later this year.

These solutions need to be all about ease of use and consistency to drive adoption.

Last Year's Predictions and Score

Below we indicate our major predictions and whether those were correct or not. We did not do so badly, scoring 6 Yes outcomes, 3 No outcomes and 1 Maybe. We were most wrong about dapps taking off, as mentioned above.

1) Cryptocurrency Market Caps will grow – No
2) Scaling technology will enhance transactions rates, lower costs - Yes
3) ICOs will be under tighter control - Yes
4) What will bankers do? Try to control blockchains. - Yes
5) Fraud and theft will still be prevalent - Yes
6) Forks will diminish in importance - Yes
7) Dapps will blossom wildly - No
8) Social media and identity are ripe for change (P2P or B2C?) – Yes
9) Distributed exchanges will improve rapidly - No
10) Government regulation will be a force for stability - Maybe

Conclusions

While the themes change somewhat, cryptocurrency adoption continues to grow. Bitcoin retained leadership, with more than half of all cryptocurrency value, through the Great Crypto Crash of 2018.

The market may have positioned itself for greater stability, with security tokens edging aside initial coin offerings, and the Lightning Network and other second layer solutions bringing more scalability and usability to Bitcoin and other coins.

Enterprise blockchains continue to find more and more use cases. The banks are entering in a rather big way for both institutional and retail usage with stable coins tied to national currencies, and social media platforms with messenger coins are looking to do the same.

Cryptocurrency phones are a big potential leap forward in the user interface for secure wallets, and will make everyday purchases such as buying coffee and groceries much easier, allowing onboarding of new, casual users.

Please visit OrionX.net/research for additional information and related reports.

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.