



## **Where blockchain stands today**

*An OSV report*

### **Essentials**

#### **The ICO (Initial Coin Offerings) rush**

Blockchain based startups are taking advantage of the mature crowd funding model to raise capital without giving up on equity and termed it as ICO (Initial coin offerings) or token sale .The pace of ICO offerings continues to quicken. CoinDesk, estimated that blockchain companies raised \$327 million since the beginning of this year. The same publication calculates that ICOs are now outpacing traditional VC investment in

the Blockchain space. Non blockchain companies like KIK messenger is taking advantage of the phenomenon and offering token sale to create their own ecosystem and virtual currency.

## **Increasing cryptocurrency market cap**

During a period of volatility, the market capitalization of cryptocurrencies has risen significantly. The most notable development is that the total valuation of Ether (the currency used by Ethereum) is now approaching that of Bitcoin. Based on the current circulating supply, the top three as of June 15th:

- Bitcoin (BTC): \$40 billion -- Bitcoin is the original blockchain based cryptocurrency designed by the pseudonymous Satoshi Nakamoto. While no organization is in charge, new development is organized under the banner of BitcoinCore. The organizations whose employees contribute the most to BitcoinCore are Chaincode Labs, Blockstream and MIT.
- Ethereum (ETH): \$33 billion -- Ethereum went live in 2015. It is designed as an extension of the blockchain idea to support more powerful smart contracts. It is sometimes described as a "world computer" which supports building Dapps (decentralized applications). Its development is led by the Ethereum Foundation.
- Ripple (XRP): \$10 billion -- The Ripple Consensus Ledger is designed and built by the startup RIpplE to provide cross-border inter-bank transfers. The company Ripple is also behind the Interledger protocol which specifies the movement of payments

across disconnected blockchains and other ledger technologies.

## **Blockchain Confidentiality**

The popular blockchains (Bitcoin or Ethereum) lack privacy as they are designed to be more transparent. Zcash is a relatively new cryptocurrency which includes privacy preserving properties that make its use anonymous. Zcash tokens were not pre-mined and they did not hold an ICO. Instead the creators have implemented a scheme whereby 10% of all tokens that will ever be created are transferred to the Founders' Reward fund. This is scheduled to happen over the first four years of Zcash operation. Monero is a competing public blockchain that promises untraceable transactions. Enterprise blockchain technology from Chain, Blockstream and Corda also offer various forms of confidential transactions.

## **Venture Capital Investment Thesis**

Current crypto-active venture firms such as Andreessen Horowitz, Union Square Ventures, RRE Ventures and others are actively observing the phenomenon. These VCs have developed a "fat protocol" thesis where they believe "thin" internet protocols have limited financial value, and rather, "fat protocols" such as blockchain can be bundled with applications at the protocol layer and create significant value. Both Union Square Ventures and Andreessen have deployed capital through hedge funds such as Poly Chain Capital, which exclusively invests in token offerings.

# Notable

## Open Source

Bitcoin has been developed as open source since 2009. Many other blockchains have always been developed as open source, including Ethereum. Furthermore, the open source business model has been adopted by many of the Blockchain startups (e.g. Bloq, "Red Hat for Blockchain"). Over the past 18 months, we have seen other significant closed source blockchain projects shift to open source:

- In Feb 2016, IBM contributed their existing blockchain project (Open BlockChain) to the newly formed Hyperledger Foundation where it was renamed as Fabric. Note that the Hyperledger consortium was itself announced in December 2015.
- Blockchain startup Chain switched to an open source model. In April of 2016, it announced that the specification (ChainOS) was being made open. In October of 2016, Chain released ChainCore code as Open Source.
- R3 released their Corda distributed ledger platform as open source in November of 2016. Just recently, the status of Corda was upgraded to that of a public beta.

## Blockchain or not?

Some in the ecosystem have been using the term, "Distributed Ledger Technology" (DLT) to encompass a wider variety of mechanisms for achieving decentralized, replicated, shared data across peer nodes. A blockchain would be one example of DLT. Some examples of DLT that are not blockchains:

- R3 Corda -- A distributed ledger for Financial Services, "inspired by blockchain." Due to privacy and scalability concerns, all nodes don't see details of all transactions. The company has stated, "No blockchain because we don't need one."
- IOTA Token -- A transaction and data layer for the IoT to support M2M (machine-to-machine) transactions. Important properties include that it is lightweight (in storage and bandwidth requirements) and there are no fees. Transactions are stored in a directed acyclic graph (DAG), that IOTA refers to as a Tangle, instead of a blockchain.

## **Proliferation of alliances and consortia.**

During the recent industry conference in NY, the Swiss Crypto Valley association tweeted out that, "There may be over 100 #blockchain consortia by the end of 2017 #consensus2017," which is likely an undercount. There are a confusing variety of competing and cooperating blockchain associations, often with overlapping membership, including:

- Hyperledger Foundation -- 142 members under the Linux Foundation banner and IBM exerts the most influence. Supports a number of different permissioned blockchain technologies, but Fabric is the most prominent.
- Enterprise Ethereum Alliance -- Young and quickly growing alliance with 116 members. Microsoft is prominent. Focused on delivering tools for enterprises to create permissioned blockchains using the Ethereum technology.

- Blockchain Alliance -- New York-based alliance of large companies, mostly in the Bitcoin ecosystem. The alliance is mostly concerned with policy issues and regulation.
- R3 Consortium -- 84 member consortium led by DLT startup R3. Membership is mostly banks and financial institutions which take part in R3-led experimental projects and receive early access to market research and Corda DLT technology.
- IC3 -- The Initiative for Cryptocurrencies and Contracts was formed at Cornell University, and also includes blockchain and financial industry members. Smaller consortium focused on advancing new blockchain technology advancement.

## **Off-chain Transactions**

Public blockchains only scale to support a limited number of transactions and fees are too expensive to support micropayments. In response, "Layer 2" protocols such as Lightning Network payment channels are being tested. Channels allow direct transfer of Bitcoin or other cryptocurrency without directly recording on the blockchain -- a blockchain transaction is only required to open or close a channel.

Sidechains can sometimes serve a similar purpose. A sidechain is a companion blockchain where asset values are pegged to the main chain. Asset value may be moved back and forth. Sidechains may have differing consensus rules in order to allow more throughput or shorter confirmation times.

## **Interoperability Between Blockchains**

Blockchain technology is not a single protocol, so how can they interconnect? Due to the proliferation of blockchain technologies, there are multiple efforts underway to enable communication between blockchains.

- Interledger (ILP) -- A protocol proposed by Ripple; currently a W3C Community Group. ILP allows monetary value to be routed across ledgers. Chain recently demonstrated the ability to use Interledger to transfer assets between their blockchain and both Bitcoin and Ethereum.
- Sidechains -- Enable Bitcoins and other ledger assets to be transferred between compatible blockchains. The startup Blockstream has developed the Elements open source Projects and the Liquid commercial implementation. The Drivechain proposal is a competing sidechain design.
- Cosmos -- Proposed by Tendermint which recently conducted a \$17 million ICO to support the project. Generalizes Sidechains with a hub design.

## **Secure Hardware Enclaves**

Secure hardware, including HSMs, Intel's SGX or Arm's TrustZone, can be employed in order to improve blockchain security. The earliest hardware applications have been to create offline wallets, based on STMicro chips, for securing cryptocurrency keys. Startups and researchers are now developing applications to provide blockchain node and endpoint security as well as trusted sources of external data. In 2017, the use of Intel SGX hardware, in particular, is gaining momentum.

## **Enterprise Blockchain-as-a-Service**

There is not as much competition for cloud-based Blockchain service offerings as one might expect. However, the current competition is led by IBM and Microsoft.

- IBM Hyperledger Fabric on Bluemix -- IBM's service was announced in April of 2016. The service is cross marketed with Watson and IoT. There is a GUI for deployment and monitoring.
- Microsoft Azure BaaS -- A rudimentary Microsoft BaaS offering was first announced in November of 2015. It includes support for multiple blockchain technologies, but is weighted in favor of Ethereum. Capabilities are growing under the banner of "Project Bletchley" which includes capabilities for global network deployment and incorporation of outside data using a mechanism they call "cryptlets."

## **From Lending Club to Upgrade**

Renaud Laplanche, the former longtime CEO of Lending Club, recently launched a new consumer lending startup called Upgrade. Upgrade will be using the blockchain protocol to enhance data integrity by creating time-stamped, immutable transaction records. Lending Club is arguably the most well-known marketplace lender founded in 2006 and went public in 2014. Laplanche was forced to resign from his role in 2016 after it was informed certain Lending Club loans had falsified dates. His latest venture, Upgrade, has raised \$60 million in funding.

## **UK Financial Conduct Authority testing the Blockchain**

The UK Financial Conduct Authority (FCA) has unveiled a number of blockchain and digital currency projects to its regulatory 'sandbox' in a bid to promote product testing and consumer safety. Nine blockchain startups (out of a total of 24) are involved in the fintech sandbox. Within the sandbox, startups test new services and products under the supervision of regulators.

## **New Leadership Addition at Chain**

Blockchain startup Chain (Note: Orange is an investor) hired Goldman Sachs veteran, Tom Jessop, as President. Jessop served formerly a managing director at Goldman Sachs focused on principal strategic investment and technology business development. Chain recently announced that their blockchain ledger is powering Citi and NASDAQ's payment processing and reconciliation.

## **New Funding for R3**

Blockchain consortium R3 raised a \$107 million Series A round to accelerate commercial applications of blockchain technology. Leading investors include SBI Group, Bank of America Merrill Lynch, HSBC, Intel and Temasek.

## **Brave held an ICO**

Brave software is developing a new web browser with a value proposition centered around speed and privacy. The browser blocks ads as well as tracking tokens. The company had also integrated a Bitcoin wallet into the browser as a means of both contributing to content providers, who would otherwise lose ad revenue and also for users to share in the payment of a future, privacy-

preserving ad network that they intended to create. The company was developing its own token for use in a blockchain-based ad ecosystem. They recently raised \$31M in via token sale.

## Numbers

# \$327M

Through June 9th 2017, blockchain entrepreneurs have raised \$327m through ICO offerings in 2017, a figure that now exceeds the \$295m raised through VC funding, according to CoinDesk data.

# \$100B+

Aggregated market cap of all listed virtual currencies surpassed \$100B, with bitcoin being dominant with 38% market share.(source:coinmarketcap.com)

# 1238+

The number of blockchain based startup in the world(Source: blockchainangels.eu)

## Quotable

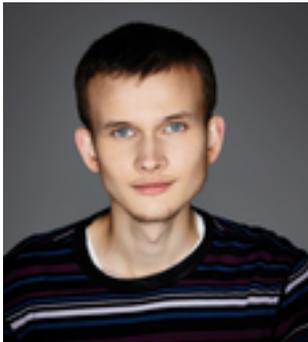


**“I can't emphasize enough how radical a change this is to the past. Historically the only way to make money from a protocol was to create software that implemented it and then try to sell this software (or more recently to host it)... With tokens, however, the creators of a protocol can monetize it directly and will in fact benefit more as others build businesses on top of that protocol. ”**  
— *Albert Wenger, Partner, Union Square Ventures*



**“Bitcoin is a remarkable cryptographic achievement and the ability to create something that is not duplicable in the digital world has enormous value.”**

— *Eric Schmidt, Executive Chairman, Alphabet.*



**“Some consortiums are created just because it seems to be trendy, and there is a risk to spend a few million dollars and come up with a technology which is much worse than the one built by a group of hackers who sit somewhere in the basement, There are advantages but there are risks as well.”**

— *Vitalik Buterin, Founder, Ethereum Foundation.*

**Companies**

**Civic**



Palo Alto based startup trying to secure user identities by using a blockchain while facilitating on-demand low cost KYC for businesses.

## Enterprise Ethereum Alliance



Notable alliance comprised of 116 diversified firms including Microsoft, Toyota, Merck and others, with a mission to build enterprise grade ethereum smart contracts that are secure and scalable.

## Skuchain



Mountain view based startup, creating a “commerce cloud” to enable frictionless interactions and offer transparency among trade partners in the supply chain domain.

Prepared by:

**Orange Silicon Valley**

SG/OSV

+1 (415) 243 1500

