Global Blockchain Industry Overview and Prospects (2018 H1)

Huobi

Huobi Research

May 2018

【Authors】

Hubery YUAN
Bonna ZHU
Xiao XIAO
Dazhi GUO

huobiresearch@huobi.com

Global Blockchain Industry Overview and Prospects (2018 H1)

May 2018

Summary:

Crypto assets experienced its third bull market in 2017. This time Bitcoin was no longer the only eye catcher, and a great number of ERC20 tokens were created and flourished. **A paradigm shift in the crypto assets market, from consensus on peer to peer cash like Bitcoin to consensus on smart contracts, is forming.** Entering 2018, the market started to cool down, until mid-April, along with **the super nodes election campaign from some projects using DPoS consensus,** the crypto market stabilized and started to rebound in a short run. According to our sentiment survey, **global investors are still optimistic toward the market in the second half of 2018,** with 71.4% of the responders believe the market cap will increase more than 30%.

Crypto asset crowdfunding exploded in 2017. **The funding amount was 23 times that of 2016.** In 2018, up to 67% of the new crypto assets we followed were selling below issuance prices, however, a few projects still delivered great performances, such as Zilliqa, Tomochain, Bluzelle etc. **We expect more capital to center around quality projects. In addition, the first DAICO was successfully completed in 18H1.** New funding models are expected to be more popular in the future. Besides, **projects in the US will tilt to regulated funding, following Reg A+ and Reg D.**

There will be 6 rationales for crypto market. **Penetration:** Crypto finance will penetrate traditional finance; **Application:** Only *Use cases* + *Blockchain* could set the market on fire; **M&A:** Acquisition of high-quality internet applications through crypto assets will happen; **Users:** Blockchain user base will keep growing, pushing up market activity; **Generation:** Average age of users will move up; **Gender:** More females are expected to enter the market.

Regulations: **US SEC announced that most of the ERC 20 tokens may be securities** and started to strengthen the regulation using securities market framework. We expect more countries to follow US as an example. Meanwhile, self-regulatory organizations were set up in Japan and Korea. Future picture will become a **combination of centralized regulation and self-regulatory**. However, joint regulation won’t come out in short run.

We divide the blockchain industry into five sectors: **Infrastructure, Platform, Middle layer, Application and Services**. In 2017, main competition fell in Platform sector. **Attentions should still be majorly paid on Platform layer and Middle layer in 18H2.**

Technology: Current blockchain networks cannot support commercial applications at large scale. **Scalability, privacy, and interoperability** are still bottlenecks. A lot of new solutions emerged, and some distributed ledger technology other than blockchain also appeared, such as **DAG and hashgraph.** Technology improvement will even accelerate in near future.

Content

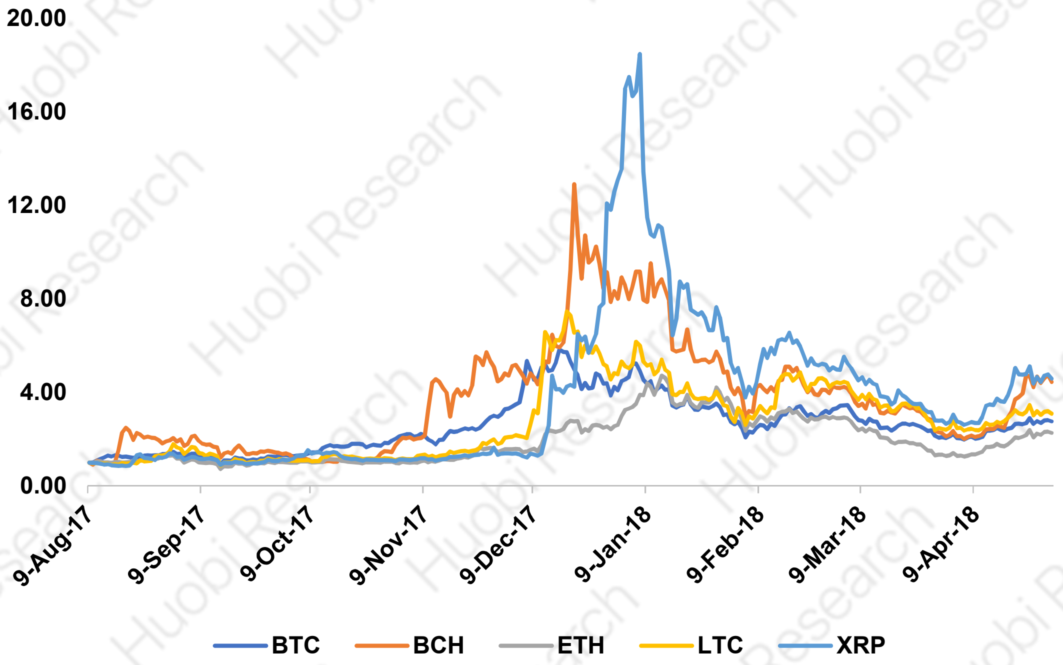
Part I. Crypto assets market overview and prospects

The emergence of crypto assets market dates back to 2009, when the first decentralized crypto asset Bitcoin came into being. According to Coin Market Cap, till now, there are over 1,600 different crypto assets actively traded on the global market, and there are even more around us in the daily lives.

1.1 Market turning to bearish, waiting to regain bullish momentum

In year 2017, crypto assets market experienced explosive growth, total market capitalization of the crypto assets market increased 30 times from $17.74 billion to $559.76 billion, exceeding return of any other asset class in the world. However, entering 2018, market directions changed, and massive retracement was triggered. By the end of April, the market prices of Top 5 crypto assets, Bitcoin, Ethereum, Ripple, Bitcoin Cash, and Litecoin dropped to 70% below all-time high and were roughly at the same level as in 2017 October.

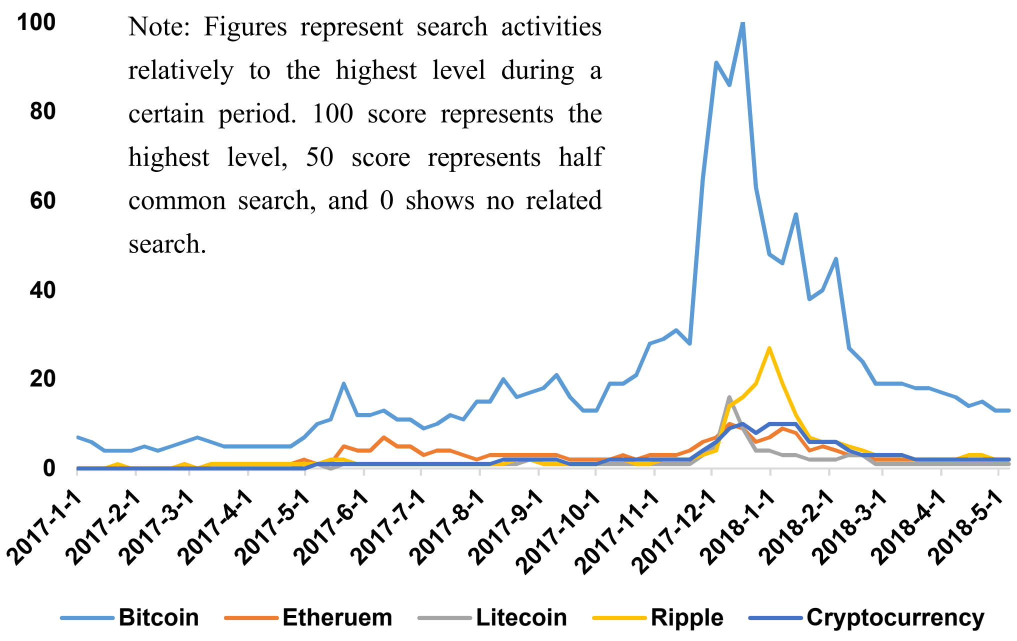
Graph 1: Top 5 crypto assets prices index evolution



Source: Huobi Research

Besides, crypto assets market activities also suffered from a corresponding decrease:

Graph 2: Search index of crypto assets

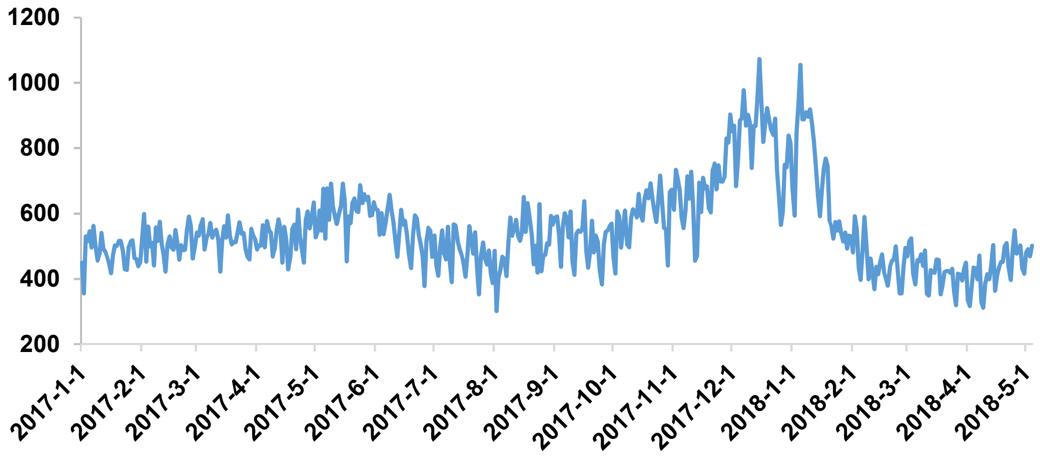


Note: Figures represent search activities relatively to the highest level during a certain period. 100 score represents the highest level, 50 score represents half common search, and 0 shows no related search.

Source: Google Trends， Huobi Research

Bitcoin attracted most of the public attention. In 2017, search activities towards crypto assets steadily accumulated and reached peak in December. Entering 2018, search activities towards crypto assets fell dramatically, with attention to Bitcoin experiencing the most significant decline. By the end of April, search index of Bitcoin was only 12% of its peak level in December 2017.

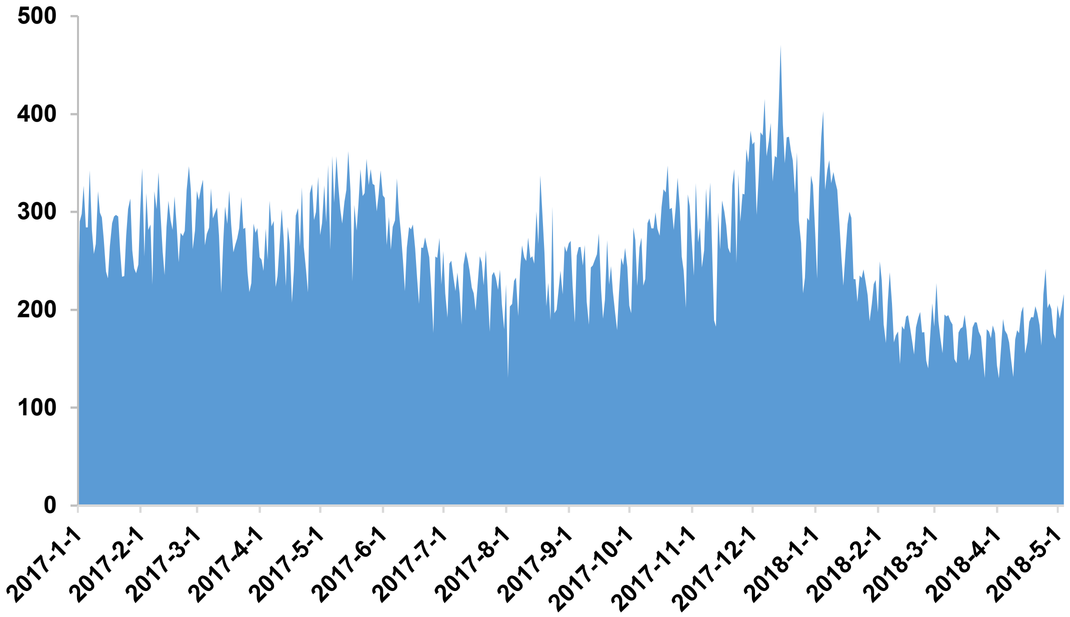
Graph 3: Number of active Bitcoin address (in thousands)



Source: Quandl, Huobi Research

In 2017, number of active Bitcoin addresses was relatively stable, except for the considerable increase in November and December 2017. However, since the beginning of 2018, Bitcoin activity declined significantly. On 9th of April 2018, the number of active Bitcoin addresses reached its bottom, which was roughly 71% below the peak on 15th December 2017.

Graph 4: Bitcoin daily trading volume (Excluding top100 active Bitcoin addresses, in 000s)



Source: Quandl, Huobi Research

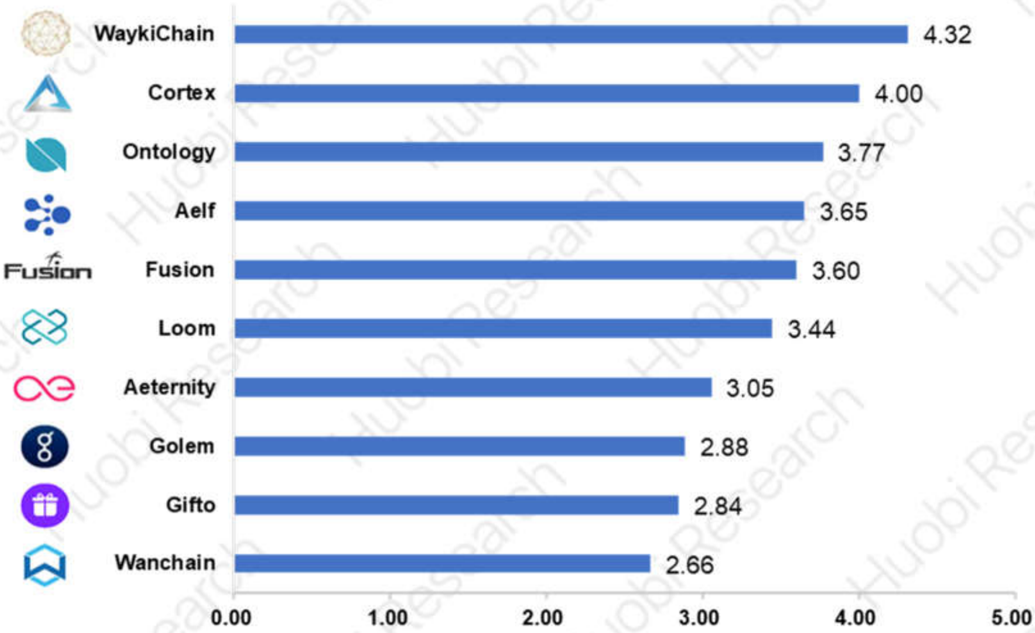
Corresponding to the increase in public attention and wallet activity, Bitcoin transaction volume also increased steadily in 2017. On 15th December 2017, the number of Bitcoin daily transactions reached all-time high, surpassing 470k trades per day. However, entering 2018, as the market cooled down, Bitcoin transaction volume also plunged, reaching its lowest level at 130k trades per day, roughly 73% below the peak.

Entering Q2 2018, as US and Japan tax season ended, investor sentiment started to recover, and market began to warm up：

➢ **Super nodes elections stimulated the market in a short run**

Since April, some projects with DPoS consensus, such as EOS, CMT, and TRX, launched super nodes election campaigns. The crypto market was thus stimulated and started to rebound in a short run. Huobi Research tracked the top 100 crypto assets, and ranked the ten best performers during April:

Graph 5: Ten best performers among top 100 crypto assets in April

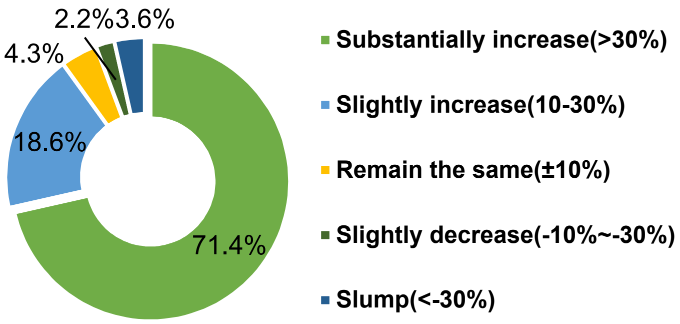


Source: Huobi Research

- **Market is still optimistic about the second half of 2018**

Despite the bearish market since the beginning of 2018, investor expectations towards the second half of 2018 remain optimistic. According to our monthly sentiment survey of global individual and institutional investors, 90% participants believed that the total market capitalization of all crypto assets will increase, with 71.4% believed that it will increase more than 30%.

Graph 6: Investors' expectation for the next 6 months



Source: Huobi Research Sentiment Survey

1.2 Crypto asset crowdfunding cooled down, yet still hot compared to last year

Crypto asset crowdfunding represents a popular way of crowdfunding in crypto assets. During the crowdfunding process, a certain amount of funding shares will be sold to investors in the form of crypto assets in exchange for major crypto assets such as Bitcoin, mostly Ethereum and NEO, etc.

2017 was a big year for crypto asset crowdfunding. Significant amount of new crypto assets was created and capital raised also increased dramatically. According to Token Data statistics, there were 435 out of 913 token sales succeeded in hitting soft cap, nearly half success rate. The successful token sales in total raised over 5.6 billion US dollars, surpassing the previous year figure of 0.24 billion dollars. Some of the projects even raised over 0.1 billion dollars, including blockchain infrastructure project “Filecoin” that raised 0.257 billion dollars, public blockchain project “Tezos” that raised 0.232 billion dollars, and cross-chain project “Polkadot” that raised 0.145 billion dollars, etc.

Graph 7: Top 10 new crypto assets in 2017 in terms of funding amount

Name	Project type	Funding time	Funding amount
Filecoin	Distributed storage	2017.9	$257,000,000
Tezos	Public blockchain	2017.7	$230,498,884
Sirin Labs	Hardware	2017.12	$157,885,825
Bancor	Crypto asset trading	2017.6	$153,000,000
Polkadot	Cross chain facility	2017.10	$145,171,723
Qash	Crypto asset trading	2017.11	$106,400,000
Status	Social network	2017.6	$107,664,907
Kin	Decentralized market	2017.9	$98,500,326
Cosma	Cross chain payment	2017.11	$95,614,242

TenX	Payment and clearance	2017.7	$80,000,000
Total			**$1,431,735,907**

Source: ICO Drops, Huobi Research

2017 was also a year in which new crypto assets greatly appreciated in value. Some of the top projects appreciated hundreds or even over a thousand times in value. Among those projects, by the end of April 2018, Spectrecoin was the top performer, who appreciated 741.42 times in value since its crowdfunding. If using all-time high price, then it reached as high as 8,288.18 times of the initial price. One of the other all-star projects, Qtum, also appreciated 347.97 times in value using all-time high price.

Graph 8：10 best performing new crypto assets in 2018

	Project Name	**Funding Time**	**Issue Price**	**Current Price**	**Price Change**	**Highest Price Change**
	Spectrecoin	2017-1	$0.001	$0.60	741.42x	8,288.18x
	Particl	2017-4	$0.134	$16.70	124.87x	384.10x
	Neblio	2017-8	$0.178	$15.06	84.83x	365.40x
	Populous	2017-6	$0.301	$24.50	81.35x	251.25x
	Qtum	2017-4	$0.307	$22.64	73.71x	347.97x
	Augmentors	2017-2	$0.015	$0.96	64.00x	140.00x
	OmiseGo	2017-6	$0.326	$17.55	53.83x	76.13x
	Icon	2017-9	$0.106	$4.59	43.30x	107.83x
	Tron	2017-9	$0.002	$0.085	42.80x	99.20x
	Zrx	2017-8	$0.048	$1.23	25.63x	52.71x

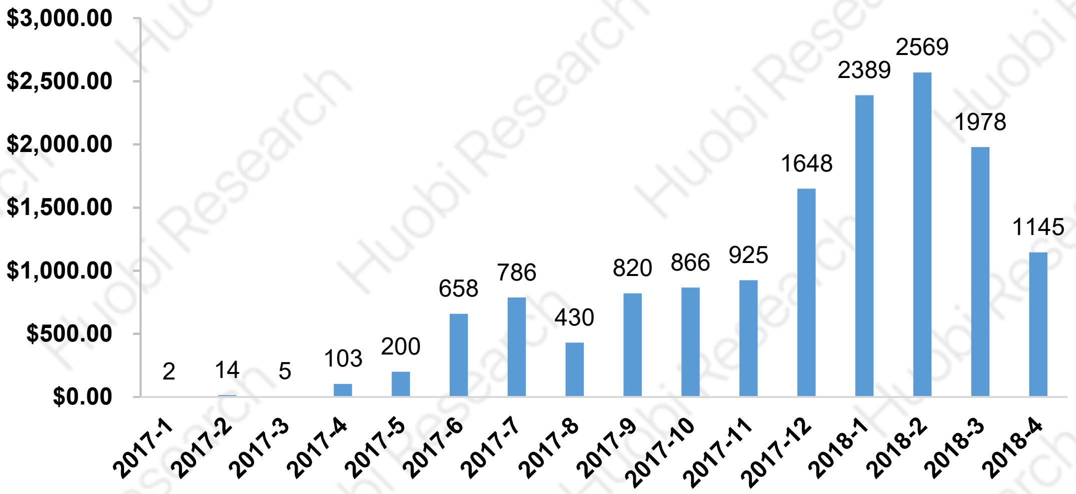
Source: ICO Drops, Huobi Research, as of April 2018

Entering 2018, crypto asset crowdfunding market started to cool down:

- **Funding amount declines on a monthly basis, yet still larger than 2017**

Huobi Research follows token sales on the market. Entering 2018, the amount of capital raised in token sales started to decline on a month-on-month basis. During April, the amount of capital raised was only 1.145 billion dollars, roughly 55% below the 2.569 billion dollars at the peak during February. However, overall, the amount of capital raised was still very large, already exceeding that of 2017 on an entire year basis.

Graph 9：Amount of capital raised in token sales, from 2017.1 to 2018.4



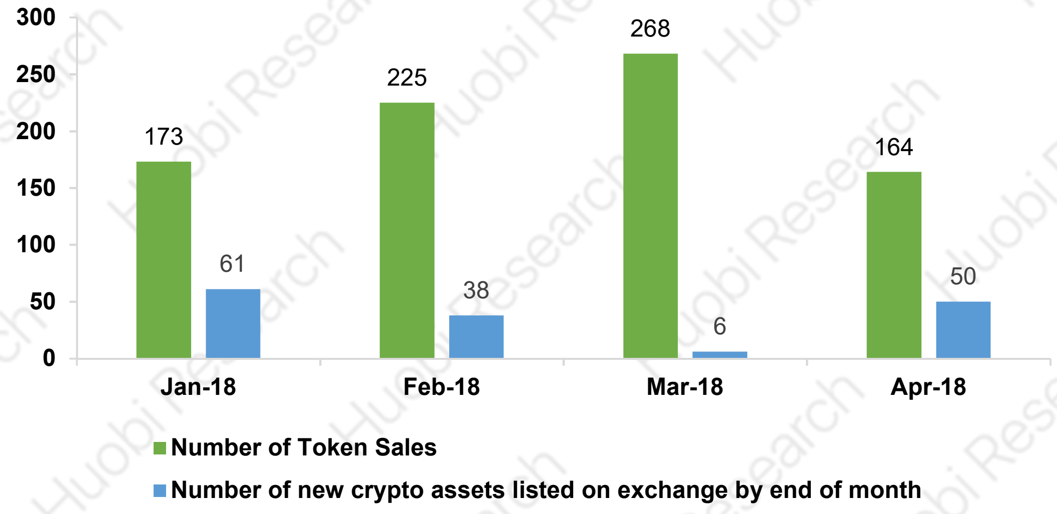
Source: Token Data, Huobi Research

In 2018, due to some top projects, the amount of capital raised in token sales was still very large. Telegram raised 0.85 billion dollars in February and March respectively through token sales. Also, EOS continued to raise capital from public. According to Token Data statistics, by the end of April, EOS has raised about 3.3 billion dollars. After removing effects from those top projects, in 2018, capital raised in token sales showed even more drastic decline on a month-on-month basis.

➢ **Regulation strengthen, liquidity shrinks**

Huobi Research closely follows new crypto assets listing on exchanges. In 2018, starting from January to April, the proportions of new crypto assets successfully listing on exchange by the end of token sales month were 35.62%, 16.89%, 2.23% and 30.49% respectively. During February and March, the proportion decreased significantly, mainly due to the tightened restriction imposed by global regulatory authorities. The bearish market condition also made many project teams delay their plan of listing on exchanges. Until the mid-to-end of April, market showed recovery signs, and the number of new crypto assets listing on exchanges started to bounce back. Market liquidity improved.

Graph 10: Number of new crypto assets listing on exchanges by the end of token sales month

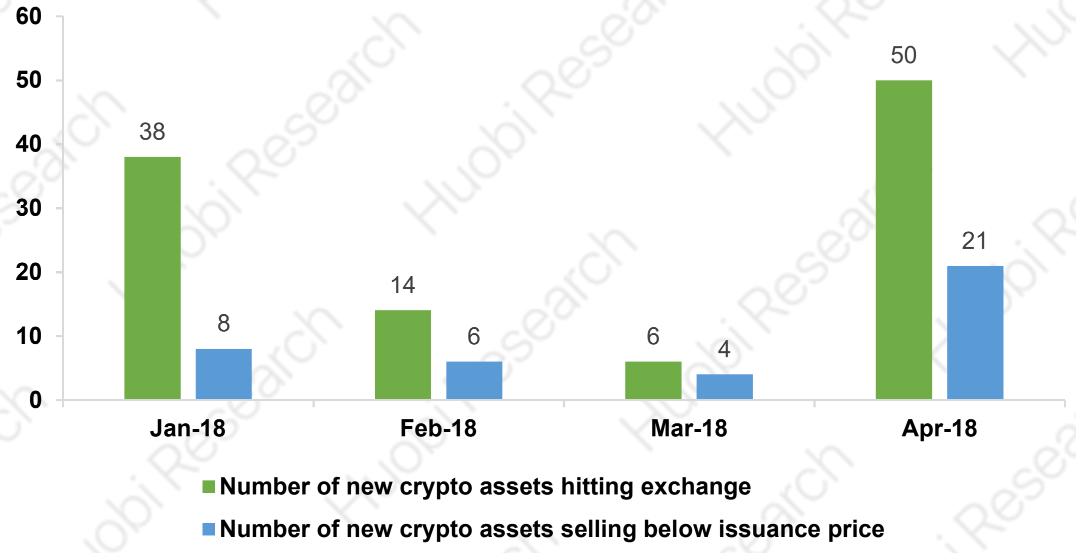


Source: www.icodata.io, Huobi Research

- **Market plunged, selling below issuance, yet top projects still perform well**

In 2018, as regulation towards token sale strengthened and Ethereum price declined, the performances of new crypto assets were facing significant challenges. From January to April, the proportions of crypto assets selling below issuance prices were 21.05%, 42.86%, 66.67% and 42.00%, accelerating fast.

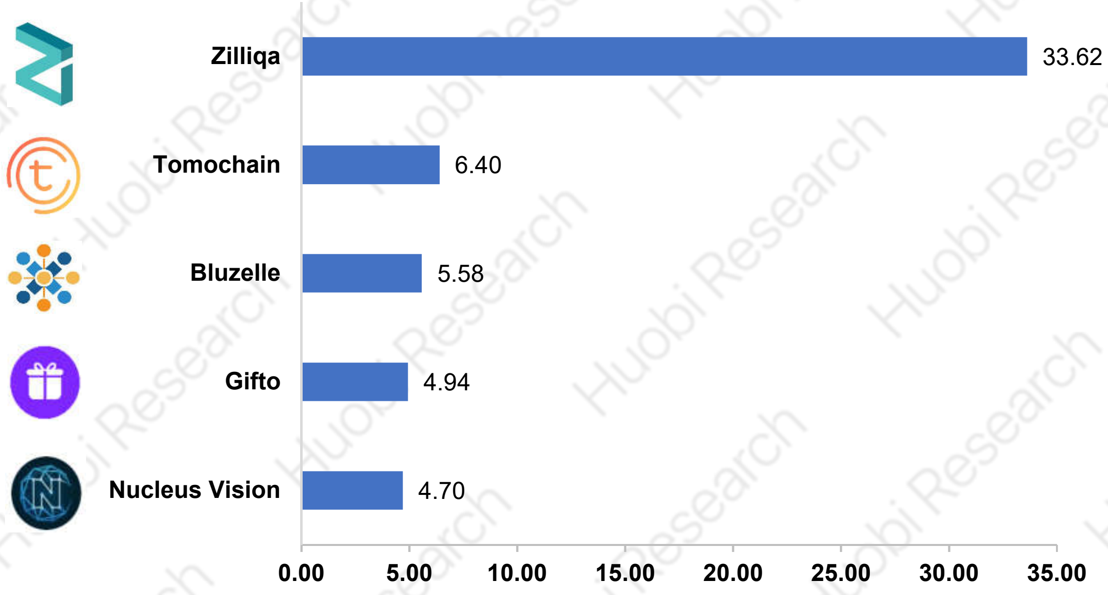
Graph 11: Number of new crypto assets selling below issuance prices



Source: www.icodata.io, Huobi Research

Although the number of new crypto assets selling below their issuance prices increased during the first half of 2018, some of the top projects remained exceptional. Five best performing new crypto assets are Zilliqa, Tomochain, Bluzelle, Gifto and Nucleus Vision. By the end of April, these projects appreciated 33.62, 6.40, 5.58, 4.94 and 4.70 times in value respectively compared to their token sale prices.

Graph 12：Five best performing new crypto assets in 2018 (Times of value appreciation)



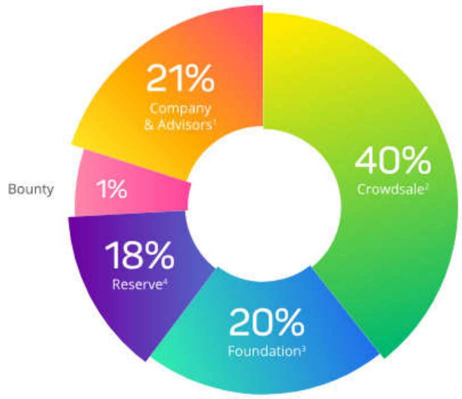
Source: Huobi Research, as of April 2018

We believe that the token sales market returning to normal is an inevitable trend. In the future, we may not easily witness projects with hundreds, thousands of times of return, but we would be more and more likely to see capital flow to quality projects, especially to compliant and legitimate ones, new logics in this market is about to come:

➢ Crypto asset crowdfunding 2.0: DAICO

The limitations of traditional crypto asset crowdfunding lie in information asymmetry, as well as the lack of control on entrepreneurs by investors. Information asymmetry here is reflected in the fact that most of the crowdfunding are "white paper" fund raising, with entrepreneurs having all the information while investors knowing little, making it hard to distinguish between true and false; Investors lacking control on entrepreneurs is reflected in the fact that currently there is no such rules nor laws to regulate use of funds, project executions and information disclosure, etc. Under such circumstances, scams often happen, leading to enormous losses for investors.

Graph13: Token distribution of the Abyss



Source: The Abyss, Huobi Research

January 2018, Ethereum founder Vitalik Buterin proposed a new way of crypto asset crowdfunding, DAICO, which combines DAO (Decentralized Autonomous Organizations) with traditional crowdfunding. A layer of smart contract would be created to control the release of funds. Under this model, entrepreneurs don't get access to all the funds raised in token sales, instead, the use of funds depends on whether the team demonstrates its ability to execute its plan and is decided through a voting mechanism; Also, if investors are unhappy with the project's progress, they have the right to vote to terminate the smart contracts, shut down the entire DAICO, and get the residual funds back based on the proportions of their tokens on hand.

Decentralized game distributor "The Abyss" is the first crypto asset project that used DAICO to raise funds. The project initiated token sales in April 18, 2018 and completed it in May. The project raised 18,511 ETH and 199,901 BNB, roughly about 15.36 million dollars. According to the token sales agreement, the Abyss token distributed to the company would be locked for 2 years through DAICO smart contract, and the token distributed to the foundation would be locked for 1 year.

- **Raise capital in the form of securities**

On contrary to innovative model like DAICO, there are a group of blockchain projects gradually turning to tradition IPO to raise capital. Whether token sales are qualified as issuances of securities has been a large dispute for a long time. As unregistered securities offering is considered illegal, in the past, most of the blockchain projects define their tokens as "Utility Tokens" to avoid regulation and registration.

Entering 2018, as the US SEC started its investigations on different token sales and relevant parties, more and more blockchain projects are abandoning the immature compliance method of “Utility Token” to be completely compliant. Currently, to raise capital in a more compliant way, many blockchain projects are accepting the following exemption provisions from security registration:

Reg A+ offering

As a part of JOBS ACT 2012, it was implemented in 2015 and serves as IPO rules for mini start-ups. It allows mid-to-small firms registered in the US and Canada to raise at most 50 million US dollars in a 12-month period without lock-up period, and public solicitation is also permitted. It doesn’t require securities registration, but the tokens must be listed on registered national securities exchanges.

Reg D offering

It is a part of private placement provisions issued by SEC that consists of three guidance rules: Rule 504, Rule 506(b) and Rule(c). Most of the token sales are using the latter two guidance rules. Rule 506(b) doesn’t cap on capital funding, yet general solicitation is prohibited, and the tokens should mostly be sold to accredited investors. There is also no limit on the number of accredited investors, but the number of un-accredited investors should be less than 35. Rule(c) doesn’t cap on capital funding either, and general solicitation is permitted too, yet only accredited investors are allowed to participate. There is a 12-month lock-up period under Reg D offering, and the tokens must be listed on registered national securities exchanges.

Reg S offering

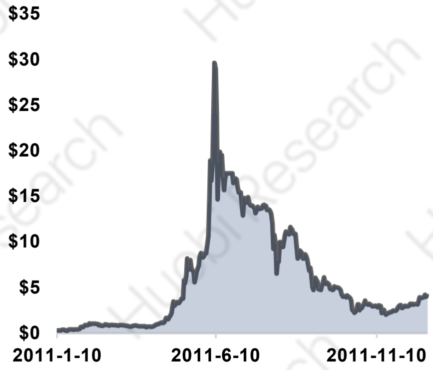
It is the off-shore security offering rules in the US. It allows start-ups to raise capital from foreign investors without registration, provided that token sales are made in an entire “off-shore” environment.

Source: SEC, Huobi Research

1.3 Looking back: What’s different in this bull market compared to previous ones?

Since the origin of Bitcoin, till now, we have experienced three bull markets, with the latest one substantially different from the previous two:

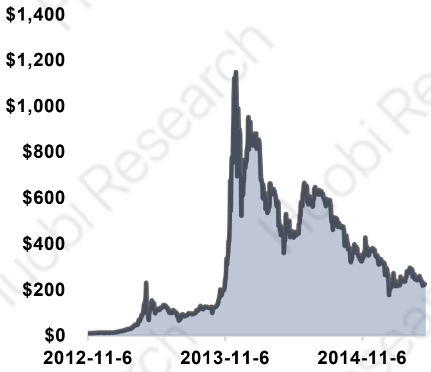
Graph 14: First time: Apr-Jun 2011, come and go in a hurry



During the 60-day bull market, Bitcoin price jumped 38 times from $0.75 to $30. Compared to $0.06 when first came into being, Bitcoin price has increased 492 times. The short bull run was triggered by the launch of Bitcoin/Sterling exchange in March. Later, media pieces from TIME and Forbes, etc. also promoted Bitcoin investment. However, the well-known hack of Mt.Gox exchange soon happened, bringing Bitcoin price down by 92%.

Source: Coindesk, Huobi Research

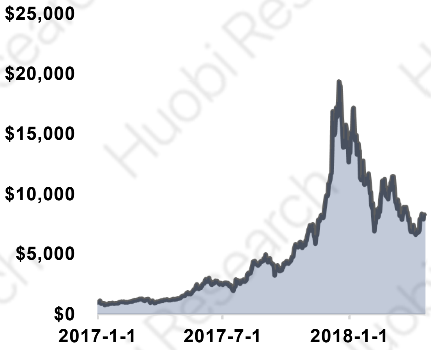
Graph 15: Second time: Jan-Dec 2013, consensus on peer to peer cash like Bitcoin



The second bull market lasted for one year, and Bitcoin price increased 82 times from $13 to $1,147. This time, Bitcoin peak price was already 20 thousand times of its initial price. The cause of this bull market was the credit crisis of traditional financial institution resulted from the debt crisis in Cyprus. Later 2013, some countries in Europe announced their friendly policy towards Bitcoin, boosting the market even further. However, in January 2015, the price went down again by 82% to a $210 low.

Source: Coindesk, Huobi Research

Graph 16: Third time: Jan-Dec 2017, consensus on blockchain and smart contracts



The third bull market also lasted for about one year. Bitcoin price went from $789 to $19,343, amid a slight fall from $4,950 to $3,226 due to China restricting crypto asset crowdfunding on September 4th. This time, Bitcoin peak price was almost 320 thousand times of the initial price and the booming token sales market was the major cause for this bull run. Similar to what happened in the past, market collapsed in 2018, with Bitcoin price falling by 69% down to $6,000 in February.

Source: Coindesk, Huobi Research

Seasonality do exist in Bitcoin and the crypto assets market, which is to some extent the result of block rewards cutting in half every four years. The Bitcoin bull run in 2013 was directly related with block rewards cutting in half in 2012, and the 2017 bull market was also a result of such change in 2016. However, the bull market in 2017 was no longer a solo show of Bitcoin, the real market driver upgraded from consensus on peer to peer cash like Bitcoin to consensus on blockchain technology especially smart contracts, from the beginning to the end of 2017:

- **Percentage of Bitcoin dominance:** 87.32% down to 40.99%;
- **Market cap increase of Bitcoin VS Ethereum:** 13 times VS 96 times;
- **Number of different crypto assets:** increased from 617 to 1,335, by 116%;
- **Increase in number of addresses in Bitcoin VS Ethereum:** 1 times vs 18 times.

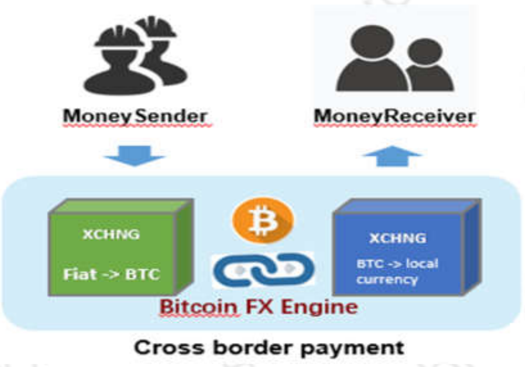
Source: Coin Market Cap, Huobi Research

1.4 Looking forward: how will the market evolve and what are new drivers?

What will drive the crypto assets market in the future? Will there be new rationales in this market? Huobi Research summarized six important potential rationales about future crypto assets market:

➢ **Penetration: Crypto finance penetrates traditional finance**

Graph17：cross-border payment via crypto



Source：Huobi Research

The biggest impact of crypto assets on traditional finance lies in the payment sector, especially cross-border payment, and the way firms conduct businesses. Using crypto asset like Bitcoin as payment tool can significantly reduce the time and middle-men cost; Also, distributed ledger and smart contracts can be widely adopted in clearing and other financial back office, helping to reduce the cost of operation and compliance. Also, in traditional finance, many people may be neglected and don’t have the chance to enjoy the financial services they deserve, with the introduction of blockchain and its deriving crypto finance, everyone now has an opportunity. We firmly believe, due to the nature of anonymity, boundarilessness and programmability, the crypto finance will impact traditional finance in various ways and the day for crypto finance will arrive.

➢ Application: Only "*Use cases* + *Blockchain*" could set the market on fire

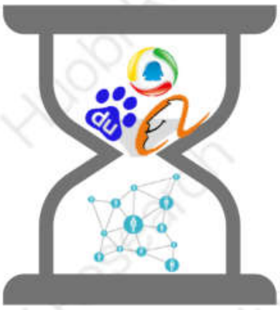
Graph18: Use cases and blockchain

Source: Huobi Research

Huobi research closely tracked DApps built on Ethereum. The ones with top DAUs, except for decentralized exchange such as EtherDelta and IDEX, are mainly blockchain games. However, as current blockchain technology is still in the early stage, most of the blockchain applications are premature and limited in functions. To attract users, game designers had to add speculative features into their applications. These we call "blockchain + use cases", where developers look for the use cases to fit in blockchain technology and is not the real future. Huobi Research believes, "use cases + blockchain" is the right way to embrace blockchain. We need to find common needs and real use cases, then add blockchain as a fundamental technology to optimize user experiences. Though blockchain technology is still far away from being mature, we still have many use cases that can be tokenized, or we can firstly move some of the parts in great need of consensus and transparency on chain. In short, only use blockchain when it is needed.

➢ M&A: Blockchain acquiring internet

Graph19: Blockchain acquiring internet

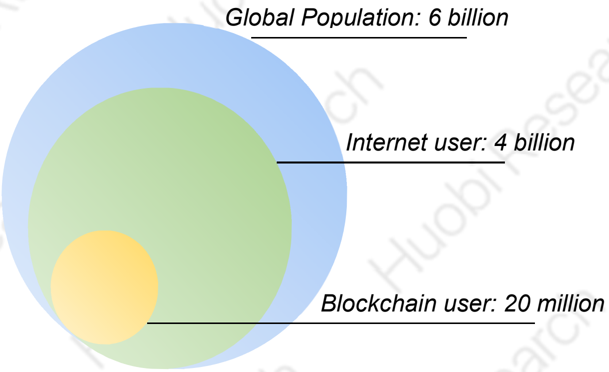


Source: Huobi Research

In traditional financial market, M&A is one of the main two drivers of market cap besides IPO. In a distributed crypto market, the function of crypto asset crowdfunding is similar to an IPO that creates new crypto assets. With the maturity of blockchain infrastructures, we expect to see M&A techniques being applied in the blockchain area in the future as well. A great number of blockchain platforms, to supplement their own Dapp eco-systems, would start to acquire high-quality internet applications. Meanwhile, moving internet start-ups on chain may become a new exit strategy.

➢ **Users: blockchain user base will keep growing, pushing up market activity**

Graph20: Blockchain user number

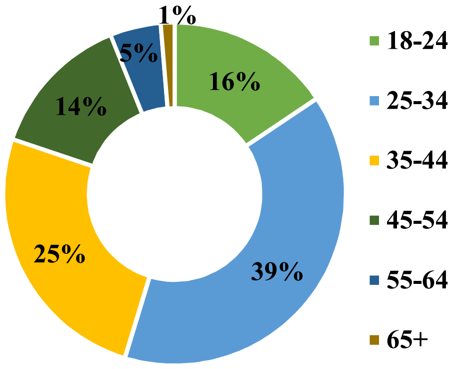


Source: Huobi Research

Currently, there are over 24 million and 32 million wallet addresses for Bitcoin and Ethereum respectively. Total number of blockchain users is expected to be around 20 million worldwide, less than 0.3% of global population. According to *We Are Social* and *Hootsuite*, there are over 4 billion internet users globally in 2017, with only 0.5% penetration of blockchain. Huobi Research believes that the growing of user base will stimulate the market activity and accelerate the development of community, thus driving up the crypto market. In addition, as more and more institutional investors regard crypto assets as a new asset class to diversify their portfolios, market depth and capacity will be significantly enlarged.

➢ **Generation: from younger generation to the masses**

Graph21: Age distribution of BTC community



Source: Huobi Research

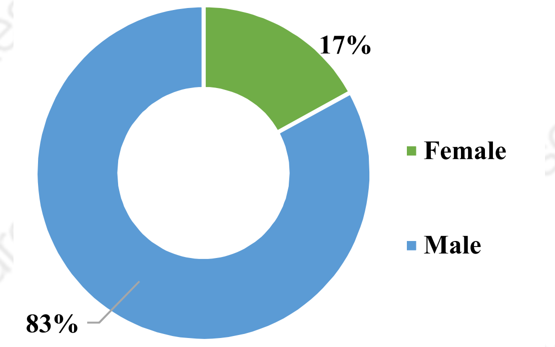
According to research conducted by Huobi Research, 39% of the users in Bitcoin community are between 25 and 34 years old, which is also the largest age group. Also, 55% of the users in total are under 35 years old，decreased from 60% in 2015 announced by CoinDesk. We believe: crypto assets will get more and more widely accepted by the masses in the future, rather than only being a pure concept among the younger generation.

More middle-aged with higher risk tolerance will treat crypto assets as a new asset allocation vehicle, and Dapps targeting at users with various ages will also appear.

- **Gender: From male to female**

According to research conducted by Huobi Research, currently, about 17% of the Bitcoin community users are females, a 7% of increase from 10% in 2015 announced by CoinDesk. More and more females are entering the blockchain and crypto area. On the one hand, this will lead the market towards a more rational direction, since female investors are more cautious and prefer sustainable and longer-term growth. On the other hand, females have higher spending incentives, which could create new directions for Dapp developers.

Graph22: Gender of Bitcoin community



Source: Huobi Research

To summarize, in long term, we believe there are three big trends in this area:

First, the crypto market will experience a paradigm shift from investment-driven towards “invest + application” driven. Currently, market cap of crypto assets is majorly an expectation of the future, in other words, the “investment” feature is very strong. In the future, with the maturity of the Dapp eco-system, “usage” needs will increase.

Second, various use cases and demands will be tokenized and put on chain, and their value will be reflected in the market capitalization of all crypto assets. The increase of market cap resulting from such on-chain movement may exceed our expectation.

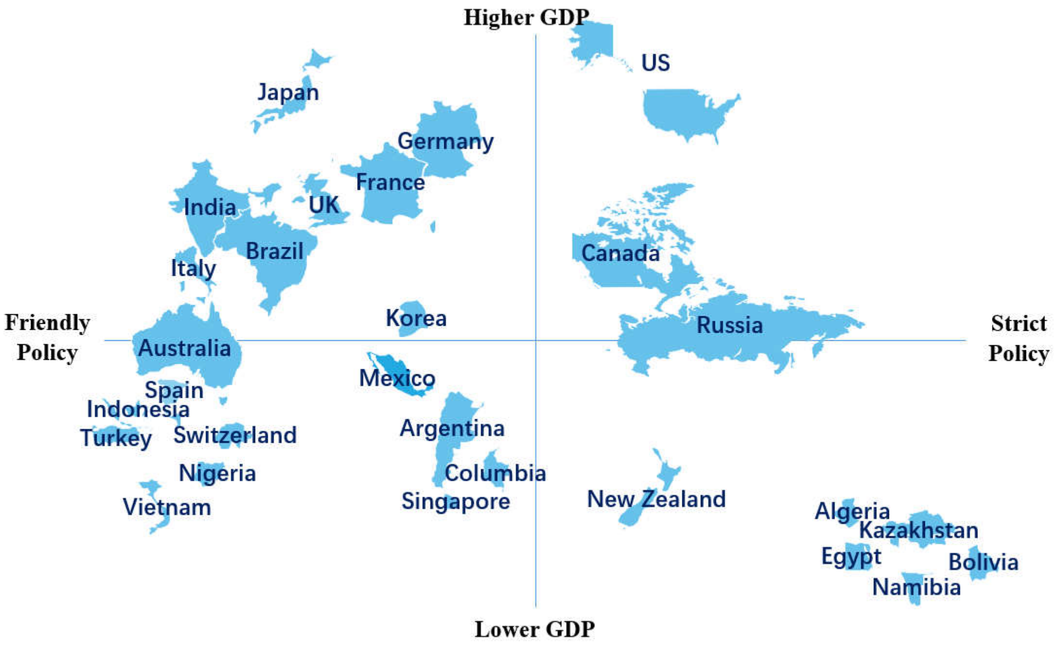
Third, transactions between tokens and fiat currencies will be less and less, while the peg between tokens themselves are expected to become stronger. That is, interactions among Dapps and different blockchain eco-systems will lead to more frequent exchanges between tokens.

Part II. Crypto Market Regulation Overview and Prospects

2.1 Global Blockchain and Crypto Market Regulation Prospects

2017 was a big year for blockchain technology, and crypto assets spread all over the world. However, regulation was also forming as market chaos emerged. Huobi Research summarized the whole picture of global regulation based on 2016 GDP and related policies updated to mid-2018:

Graph 23: Overview of crypto assets and crowdfunding policies in major countries and regions



Source: Huobi Research

As crypto assets received more and more attention last year, regulatory authorities all over the world have also been preparing to engage. In late 2017 and early 2018, several countries began to formulate related regulatory frameworks. Huobi Research believes that there are three important trends to pay attention to in the future:

- **The US may become a good regulation example and be followed by other countries:** Entering 2018, the US SEC are strengthening its role as a regulator in the crypto market and are imposing more strict compliance rules concerning licenses, security offering registration and taxation etc., all of which are very similar to the ones in traditional securities market. Later, other countries such as

Germany and Netherland also started to define crypto assets as securities. In April 2018, the CEO of NASDAQ announced that they would extend their business into crypto asset exchange when appropriate, which may further push the release of clearer policies, such as the definition of "Security Token" and "Utility Token". Huobi Research believes that more countries or regions may follow the US and impose regulations similar to that in securities market on crypto assets.

- **Both centralized regulators and self-regulatory organizations will play important roles:** Crypto assets are still in the early stage and with a high level of sophistication, and centralized guidance and regulation are very necessary. Japan is a very typical country in legalizing crypto assets through legislation and it authorizes crypto asset exchanges through licenses, while the US is typical in managing crypto assets differently based on the characteristics of tokens, for example, "Security Token" or "Utility Token". Meanwhile, self-regulatory organizations serve as supplements for centralized regulators, especially when mature compliance rules are not yet in place. For example, after the Coincheck incident broke out, 16 registered crypto asset exchanges formed Japan Crypto Asset Business Association (JCBA) and announced to set investor safety standards for the crypto market. Also, Korean Blockchain Association (KBA) was established in December 2017, and currently 23 crypto asset exchanges have joined the association and are dedicated to set up related market standards.

- **Efforts to improve regulation systems by leading countries and regions will speed up the formation of global joint regulation among country unions.** On the G20 summit in March 2018, each country shared their independent attitude towards crypto market regulations, yet didn't come to an agreement concerning how to regulate the market. Before the summit, Germany and France once sent their proposal of joint regulation to the host country, trying to push regulation towards cryptos onto the level of Europe Union. However, there is still a relatively long way to go, but we do can expect joint regulation to come in the longer future.

2.2 Crypto Market Regulations of Major Countries and Regions in the World

Huobi Research tracks the blockchain and crypto market regulatory policies of major countries and regions in the world, and systematically evaluates their regulations on four perspectives:

- **Whether crypto assets are permitted to be used as payment tool**
- **Whether crypto asset exchanges are permitted to operate**
- **Whether crypto asset crowdfunding is permitted**
- **Whether investments in crypto assets are permitted**

Meanwhile, we introduced a “Supervision Strictness Index” (SSI) as the output of the above evaluation, varying from one star to four stars. The more stars, the tighter the policies, and the more conservative and unacceptable attitude toward crypto assets is; vice versa.

(1) North America

The United States： From loose to tight; Emphasizes the securities nature of crypto assets. SSI： ★★★

Whether crypto assets are permitted to be used as payment tool

The Internal Revenue Service (IRS) has taken crypto assets as commodities instead of currencies since 2014, according to IRS Notice 2014-21. Investors need to pay corresponding taxes on long-term and short-term capital gains. In general, the US government doesn’t recognize the monetary attributes of crypto assets, but it doesn’t prohibit merchants from accepting crypto assets as payments.

Whether crypto asset exchanges are permitted to operate

Historically, it’s the state governments who regulate crypto assets service companies, and the policies differ among states. However, most of them implement the license scheme. For example, Coinbase, an US crypto asset exchange, obtained Bitlicense in New York State.

On March 7, 2018, the Securities Exchange Committee (SEC) issued a public statement requiring that crypto asset exchanges offering transaction services concerning crypto assets that meet the definition of securities be registered through SEC or be exempted. The well-known US exchanges such as Coinbase, Bittrex, and Poloniex are currently not on the list of registered exchanges. Such incident shows tightening regulations in the US, and exchanges offering transaction services concerning security tokens may face lawsuits.

Whether crypto asset crowdfunding is permitted

At the end of 2017, crypto asset crowdfunding attracted attentions from the US SEC. In January 2018, the US SEC investigated the crypto assets held by AriseBank, a Texas crypto assets bank, and suspended the company’s ongoing $600 million crypto asset crowdfunding; In February 2018, Jay Clayton, chairman of the US SEC, stated at the Congress’s Crypto Assets Hearing that most of the ERC 20 tokens may be securities. Namely, crypto asset crowdfunding is permitted, but funding under the name of “Utility Token” when raising securities is not compliant any more. The crypto asset crowdfunding will be regulated by the US SEC, and the regulation will be strengthened in the future.

Whether investments in crypto assets are permitted

Since the US government defines crypto assets as commodities, it does not prohibit crypto assets investments. However, from a taxation perspective, related regulations are gradually strengthening.

At the end of 2017, the IRS asked Coinbase, one of the largest crypto asset exchanges in the US, to hand over its customer records from 2013 to 2015. According to the IRS statistics, only fewer than 900 people paid tax on Bitcoin investment from 2013 to 2015, while over 14,000 users traded Bitcoin. On January 31, 2018, Coinbase sent the official 1099-K tax form to its US users. In addition, at the end of 2017, the US President Trump signed a new taxation act, stating that all crypto asset transactions be taxable, including crypto-to-crypto trades.

(2) Asia

Japan: Overall regulation is still loose, yet the laws for crypto asset crowdfunding are about to come out. SSI： ★★

Whether crypto assets are permitted to be used as payment tool

On April 1, 2017, the "Payment Service Amendment Act" signed by the Japanese Cabinet took into effect, and crypto assets such as Bitcoin are recognized as legal payment tools. Since then, Bitcoin payments have been widely promoted and approximately contributed 0.3% of Japanese GDP.

Whether crypto asset exchanges are permitted to operate

Japan is one of the few earliest countries to conduct license scheme on crypto asset exchanges at national level. On April 1, 2017, the "Payment Service Amendment Act" signed by the Japanese Cabinet took into effect. This Act established a series of standards and rules, requiring domestic crypto asset exchanges be authorized by the Ministry of Finance of Japan (MFJ) and Financial Services Agency (FSA), and that exchanges must submit registration documents to the FSA by the end of September 2018. As of today, 16 crypto asset exchanges have been authorized in Japan.

After the NEM token stolen incident on Japanese exchange CoinCheck in January 2018, the FSA started to investigate crypto asset exchanges in Japan. In March, the FSA announced the punishment of several exchanges such as Coincheck, GMO Coin, and Mr. Exchange, and asked some other exchanges to rectify their business within time limit. Under such circumstances, till now, 8 crypto asset exchanges that filed for registration have withdrawal their applications. Although the supervision has been strengthened, the overall attitude of regulators remains supportive and encouraging.

Whether crypto asset crowdfunding is permitted

There is no established regulation towards crypto asset crowdfunding in Japan, and the Payment Services Amendment Act, which came into effect on April 1, 2017, is not sufficient to clarify whether relevant funding behaviors are legal or not.

Since 2018, the FSA began to monitor all kinds of crypto asset crowdfunding towards Japanese investors. In February, the FSA issued a warning to Blockchain Laboratory, a crypto asset crowdfunding organization based in Macau, stating that its operations were not officially licensed and requesting it to stop offering services to Japanese investors. Relevant laws and regulations are expected to come out soon.

Whether investments in crypto assets are permitted

Japan permits crypto assets investments, but investors will face different levels of taxation. In February 2018, the National Tax Agency of Japan introduced a comprehensive tax plan for crypto assets, stating that the return on crypto asset investments belong to personal "miscellaneous income". Taxes were also filed at progressive rates, ranging from 15% to 55%. If capital gains exceed 40 million JPY (about 365,000 USD), the maximum tax rate of 55% will be levied on the excess amount, which is much higher than the 20% capital gain tax rate on stocks and foreign exchanges.

South Korea: Policies strengthened; AML is the key issue. SSI: ★ ★ ★

Whether crypto assets are permitted to be used as payment tool

South Korea does not have relevant laws recognizing the legal status of crypto assets as payment tools, but payment using crypto assets such as Bitcoin is not prohibited.

Whether crypto asset exchanges are permitted to operate

South Korea allows the domestic exchanges to operate under the e-commerce law. Companies can register as e-commerce platforms to offer crypto asset exchange services. Meanwhile, though South Korean Blockchain Association released the "Crypto asset exchange Self-Regulation Control Project", announced the crypto asset exchange self-regulatory framework in April 2018, and set certain qualifications and operational requirements for crypto asset exchanges to comply overall, the barrier of setting a crypto asset exchange is still relatively low.

With the rapid development of the crypto market, South Korean government is gradually strengthening their supervision on the exchanges: In early 2018, South Korean Financial Services Commission (FSC) announced that crypto asset exchanges should implement real-name rules. After that, banks began to refuse to open new virtual accounts for small exchanges, and only provide statutory deposit services to the four major crypto asset exchanges. At the same time, South Korean government announced that it would impose a 22% corporate tax as well as a 2.2% local income tax on the crypto asset exchanges.

Whether crypto asset crowdfunding is permitted

Crypto asset crowdfunding is completely prohibited in South Korea. At the beginning of September 2017, South Korean FSC revealed that it would penalize crypto asset crowdfunding projects, including South Korean projects raising funds overseas. Then at the end of September, South Korean FSC completely banned crypto asset crowdfunding, and there were no substantially changes as for now.

Whether investments in crypto assets are permitted

South Korea allows the public to invest in crypto assets and has not yet imposed taxes on relevant investment return. Entering 2018, related regulations have been strengthened: On January 23, the South Korea FSC issued a series of measures to prohibit anonymous transactions on South Korean exchanges, and minors and foreigners are prohibited from trading crypto assets as well.

Singapore: No major change on policies; Overall regulation is expected to be further friendly. SSI: ★

Whether crypto assets are permitted to be used as payment tool

As early as in 2014, the Inland Revenue Authority of Singapore (IRAS) indicated that crypto assets such as Bitcoin were not currencies but commodities. Using crypto assets in payment would be considered as "barter transactions" where VAT is applicable. In November 2017, the Monetary Authority of Singapore (MAS) issued the second consultation draft of the "Payment Services Act (draft)", hoping to simplify the cumbersome supervision of all payment services through a separate bill. In the future, crypto assets such as Bitcoin may be considered as official payment tools, and corresponding licenses may be issued.

Whether crypto asset exchanges are permitted to operate

Singapore allows the founding and operation of crypto asset exchanges. On November 14, 2017, MAS issued the "A Guide to Digital Token Offerings", stating that crypto assets intermediaries in Singapore, including crypto asset exchanges, must obtain a license for offering services concerning crypto assets that are defined as capital market products, securities or futures. Otherwise, if crypto assets intermediaries only offer crypto-crypto trades that has nothing to do with capital market products, securities or futures, license or authorization from MAS is not required, but anti money laundering regulation still needs to be met.

Whether crypto asset crowdfunding is permitted

On November 14, 2017, the MAS issued the "A Guide to Digital Token Offerings", which accepted crypto asset crowdfunding and defined the scope of related supervision. When the tokens belong to capital market products defined by "Securities and Futures Act (Cap. 289)", the issuance of tokens will be regulated and authorized by the MAS. If the crypto assets do not belong to capital market products, they do not need to be supervised by the MAS, and only need to comply with conventional requirements such as anti-money laundering.

Whether investments in crypto assets are permitted

Singapore has a friendly attitude towards crypto asset investments, and it does not levy tax on investment income. However, Singapore government has repeatedly issued statements to warn investors on the potential risks of such investments.

Hong Kong：No substantial change, enforcement is strengthened. SSI: ★★★

Whether crypto assets are permitted to be used as payment tool

Hong Kong has not legally recognized crypto assets as payment tools, but it has not prohibited the use of crypto assets such as Bitcoin for payment.

Whether crypto asset exchanges are permitted to operate

Hong Kong allows the establishment of crypto asset exchanges. However, if an exchange provides transaction services concerning security tokens, it needs to be registered through the Hong Kong Securities and Futures Commission (HKSFC) or obtain related licenses according to "Statement about Initial Crypto asset crowdfunding" issued on September 5, 2017.

On February 9, 2018, HKSFC issued the "SFC warns of crypto asset risks" and sent out letters to 7 crypto asset exchanges in Hong Kong or connected with Hong Kong, warning that they should not offer transaction services concerning crypto assets that are "securities" without licenses.

Whether crypto asset crowdfunding is permitted

Crypto asset crowdfunding is not banned in HK. On September 5, 2017, HKSFC issued the "Statement about Initial Crypto asset crowdfunding", stating that some of the crypto assets may fall into the "Securities" defined in "Securities and Futures Ordinance". For such "Securities", if they are targeting at Hong Kong public, not only dealers, advisory institutions and institutional investors in the primary market need to possess related licenses, but also secondary market participants (including exchanges) must be authorized by HKSFC or register with HKSFC

On March 19, 2018, HKSFC suspended the crowdfunding of Black Cell Technology Limited due to their unauthorized sales of "Security Tokens" to HK public investors.

Whether investments in crypto assets are permitted

Hong Kong allows the public to invest in crypto assets, and there is no taxation on corresponding investment return. However, HKSFC also issued several statements to warn investors against the risks of crypto assets investments.

（3）Europe

Russia: From strict to loose, regulations turning clear and definite. SSI: ★★★

Whether crypto assets are permitted to be used as payment tool

On February 28, 2014, the Prosecutor General of Russia issued a statement banning the use of Bitcoin and crypto asset trading in Russia. After that, although the ban on crypto assets in Russia was slightly loosened, the overall attitude from government remains highly tensioned.

In 2018, Russia’s attitude toward crypto assets changed dramatically. In January, the Russian Ministry of Finance proposed the draft of the “On Digital Financial Assets”. In March, the Russian State Duma’s Speaker Vyacheslav Volodin and the Parliament’s Legislative Council Chairman Pavel Krasheninnikov proposed several amendments, allowing crypto assets to be used but not enforced as payment instruments under conditions and terms stipulated by law, crypto assets quantity and user information be collected, and digital signature using private keys be as valid as the written statement and signature. This marks Russia’s first step toward legalizing crypto assets.

Whether crypto asset exchanges are permitted to operate

Since Russia completely banned crypto assets like Bitcoin in 2014, the Central Bank of the Russian Federation issued a statement in September 2017 reiterating that it will not approve any formal exchange for crypto assets trading at this stage, nor will it approve the use of such technology as an infrastructure, that is, the Russian government does not allow any crypto asset exchange to operate within its territory.

Entering 2018, Russia’s attitude towards crypto asset exchanges changed tremendously. The draft “On Digital Financial Assets” proposed by the Russian Ministry of Finance stipulates that Russia allows the opening of crypto asset exchange, but exchanges need to operate under the framework of federal law on the securities market in Russia and need to be registered at the Central Bank of the Russian Federation.

Whether crypto asset crowdfunding is permitted

In September 2017, the Central Bank of the Russian Federation issued a statement calling for caution against crypto asset crowdfunding with high risks.

In 2018, the Russian Ministry of Finance introduced a draft of the "On Digital

Financial Assets", which clarified the legal status of crypto asset crowdfunding and stipulated that individuals or legal entities may issue tokens, yet a series of documents and signatures will be required, in order to ensure the integrity of information disclosure and reliability.

Whether investments in crypto assets are permitted

In 2018, the Russian Ministry of Finance submitted the draft "On Digital Financial Assets". Based on the draft, unaccredited investors (defined by federal law on the securities market in Russia) are only allowed to possess up to 50,000 rubles worth of crypto assets, and crypto assets can only be kept in a special account offered by exchanges. However, accredited investors are allowed to open up digital wallet accounts in the name of accredited investors. Former crypto asset restriction is gradually letting loose.

United Kingdom: Policies still unclear, yet no restriction either. SSI: ★

Whether crypto assets are permitted to be used as payment tool

There are no relevant laws that clarify the attributes of crypto assets in the United Kingdom, yet using crypto assets in payment is allowed and there is no prohibition.

Whether crypto asset exchanges are permitted to operate

Crypto asset exchanges are allowed to operate in UK. Exchanges like Bitstamp, CoinEgg and HitBTC are all registered here, however, currently these exchanges are limited to “crypto-to-crypto” trading. If exchanges are involved with fiat currency or crypto asset related derivatives, for example futures and CFDs, then they are regulated and supervised by Financial Conduct Authority (FCA) and should meet anti-money laundering rules. The policy has not changed as of now.

Whether crypto asset crowdfunding is permitted

The UK government does not ban crypto asset crowdfunding and conducts regulations on a case by case basis. However, because of the risks associated with such activities, FCA in September 2017 sounded a warning. In February 2018, FCA announced that they would conduct an in-depth study on crypto asset crowdfunding from a legal perspective before judging the necessity of further regulatory actions. In the future, we expect UK government to introduce new relevant policies.

Whether investments in crypto assets are permitted

There is no restriction to crypto asset investments in UK, at the same time, investment income is not yet taxable for the time being, the policy has not changed as of now.

Switzerland: Friendly overall, constantly improving policy. SSI: ★

Whether crypto assets are permitted to be used as payment tool

Using crypto assets in payments is not forbidden throughout Switzerland and does not involve taxes. In some cases, payments via crypto assets will be regulated under Anti-Money Laundering Act. Zug has now become a famous "crypto assets valley" in the world, local government already announced in 2016 that citizens could use crypto assets to pay for government services. In September 2017, the municipality of Chiasso also stated that it would accept crypto asset for taxation and the payment should not exceed 250 Swiss francs (about 265 dollars).

Whether crypto asset exchanges are permitted to operate

Switzerland is relatively open to the operation of crypto asset exchanges. Currently, there is no specific license plate concerning crypto asset exchanges. Most of the crypto asset exchanges registered in Switzerland possess Financial Services Standards Association (VQF) membership, which includes crypto assets operation among its business scope.

Whether crypto asset crowdfunding is permitted

Switzerland holds a positive attitude towards crypto asset crowdfunding and regulations are gradually improving. In September 2017, the Swiss Financial Market Supervision Authority issued a guide on the issuance of tokens, pointing out that Switzerland has not yet established a complete regulation for crypto asset crowdfunding, however according to the form of crypto asset crowdfunding, crypto asset crowdfunding needs to comply with current financial market regulations: When crypto assets raised are used as means of payment, such activity will be regulated under the Anti-Money Laundering Act; when such activity may be defined as deposit-taking, the issuer needs to possess banking license and to comply with the Banking Law; when crypto assets raised are similar to securities, the issuer needs to hold a security brokerage license; and when the funds raised are managed by external third parties, the regulations concerning collective investment scheme must also be met.

With a sharp increase in the number of crypto asset crowdfunding launched in Switzerland, FINMA published new guidelines in February 2018, which categorizes tokens into three types: payment tokens, utility tokens and asset tokens (asset tokens are analogous to equities). Among them, asset tokens are a form of securities, at the same time, only when the sole function of a utility token is to authorize the usage of specific applications or services will it not be regarded as securities.

Whether investments in crypto assets are permitted

There is no limit on crypto asset investments, meanwhile, investment income is not taxable so far.

Germany: Policies relatively clear and definite, and is improving. SSI: ★★

Whether crypto assets are permitted to be used as payment tool

Germany's attitude towards the use of crypto assets in payment is very positive. As early as August 19, 2013, the Federal Ministry of Finance in German announced that Bitcoin was categorized as a "unit of account" and could be used for payment.

On February 27, 2018, the Federal Ministry of Finance further issued a guidance document: When users pay with Bitcoin and other crypto assets, buyers and sellers are providing "supplementary services" for the conversion of legal currency and crypto assets, which, according to the 2015 EU Court VAT (VAT) ruling, doesn't impose any other taxes on both sides, except for VAT included in the price of goods.

Whether crypto asset exchanges are permitted to operate

Germany currently does not have a clear regulation policy concerning crypto asset exchanges, but relevant supervision may fall under the German Federal Financial Supervisory Authority (BaFin). Guidance on token sales issued by BaFin on March 28, 2018 requires that market participants who provide services related to tokens and token sales must carefully consider the classification and corresponding regulations when conducting related businesses. On January 29, 2018, Berlin crypto asset exchange "Crypto.exchange GmbH", was asked by BaFin to immediately stop the securities business due to its fraudulent actions.

Whether crypto asset crowdfunding is permitted

Germany maintains a conservative attitude towards crypto asset crowdfunding but has not banned such activity and is actively seeking to improve relevant regulations. On November 9, 2017, BaFin issued a public statement to remind investors of the high risks associated with token sales, and listed a series of risks, encouraging investors to conduct detailed due-diligence before participation.

With increasing numbers of token sales taking place in German, BaFin issued further guidance on March 28, 2018, clarifying that tokens issued belong to financial instruments, and would fall into the category of securities regulation. According to BaFin, tokens will be decided, on a case by case basis, whether it is a "financial instrument" as defined by the Securities Trading Act (WpHG), a “security” defined in Prospectus Rule (WpPG), or a “capital investment” defined by Capital Investment Rule (VermAnlG). Regulations will then be determined based on classification of a crypto asset. Besides, if the conditions are met, crypto asset crowdfunding also needs to follow other regulations within the scope of securities regulation at a national and EU levels such as Market Abuse Regulations (MAR).

Whether investments in crypto assets are permitted

At present, Germany does not restrict investment in crypto assets, but BaFin has issued announcements for several times, reminding investors of the high risks associated with such assets and encouraging investors to carefully study blockchain technologies before investing to fully understand the potential risks.

There are no clear policies and regulations concerning the taxation on crypto asset investments. However, given BaFin’s announcement that crypto assets fall into the category of securities, in the future, investment in crypto assets may follow regulations similar to traditional security investments.

（4）Oceania

Australia: Friendly environment, stable regulation. SSI:★

Whether crypto assets are permitted to be used as payment tool

Australian government is one of the few countries in the world that has liberalized the trading and circulation of crypto assets such as Bitcoin. On July 1 2017, the Australian government officially declared the legal status of Bitcoin as a means of payment and ended the double taxation on Bitcoin. Before that, consumers who use crypto assets as payment must pay GST (Goods and services tax) twice: one on the purchase of the crypto assets, and the other on its use in exchange for other goods and services.

Whether crypto asset exchanges are permitted to operate

Australia is carrying out a registration system for digital asset exchanges. At the end of 2017, The Australian senate has officially approved “Draft amendments to the AML/CTF Rules resulting from the Anti-Money Laundering and Counter-Terrorism Financing Amendment Act 2017”, which authorized AUSTRAC, the financial intelligence agency in Australia to regulate Bitcoin exchanges. Bitcoin exchanges in Australia are required to register with AUSTRAC and to meet AML/CTF obligations, including: adopting and maintaining an AML/CTF program to identify, mitigate and manage money laundering and terrorism financing risks; identifying and verifying the identities of their customers; reporting to AUSTRAC about suspicious matters and transactions of $10,000 or more; keeping certain records for seven years.

Above policies were officially put into effect on April 3, 2018, and a period of 6 months was implemented for exchanges to take compliant actions.

Whether crypto asset crowdfunding is permitted

Australia is open to crypto asset crowdfunding. On September 9, 2017, Australian Securities and Investments Commission (ASIC) published regulatory guideline. The guideline states: The legal character of crypto asset crowdfunding depends on the formation, operation of the crypto assets, as well as the rights associated with such crypto assets. That is, applicable laws may differ in different cases.

Whether investments in crypto assets are permitted

Australia permits crypto assets investment, but capital gains are taxable.

If people acquire crypto assets for investment purpose, then people have to pay capital gains when crypto assets appreciate. However, if people hold for 12 months or more, they may be entitled to discounts. If people acquire crypto assets for personal consumption purposes, then capital gain taxes are exempted under 10,000 Australian dollars.

New Zealand: Conservative still, strict regulation remains. SSI: ★ ★ ★

Whether crypto assets are permitted to be used as payment tool

The Reserve Bank of New Zealand is conservative in accepting crypto assets as a legal means of payment and thinks even though crypto assets expanded the way people conducts transactions, yet transaction volume in crypto assets is still small, and anonymity of crypto assets does not match traditional way of credit assessment, thus cannot replace tradition financial system.

Whether crypto asset exchanges are permitted to operate

The New Zealand government implements strict supervision on digital asset exchanges, the New Zealand Financial Market Administration (FMA) defines crypto assets as securities and sets out the legal obligations for providers of crypto assets related services, such as exchanges, wallets, and brokerage. According to FMA, such providers must comply with the following requirements: be registered on the Financial Service Providers Register (FSPR), pay the applicable fees and levies, and comply with the fair dealing provisions and with anti-money laundering obligations. The policy hasn't changed ever since.

Whether crypto asset crowdfunding is permitted

The Financial Markets Authority (FMA) announce that all tokens or crypto assets are securities under the FMC Act. In some cases, according to the characteristics and economic nature of crypto assets, they can be classified as financial products, such as debt securities, equity securities, managed investment products or derivatives. In other cases, if it is not a financial product, the issuer's company must abide by the "Fair Trading Act" under the "Financial Market Management Law". This law applies not only to domestic products, but also to crypto asset products from overseas. In addition, issuers of tokens are subject to other further regulations, such as anti-money laundering laws. At present, relevant policies have not changed.

Whether investments in crypto assets are permitted

The New Zealand government did not prohibit investors from participating in crypto assets investment, but the attitude is relatively conservative. Investors were warned of the risk of investing in crypto assets.

Part III. Blockchain industry overview and prospects

As a revolutionary technology, blockchain has also created a complete industry while empowering various industries. We divide the blockchain industry into five major segments:

- **Hardware and infrastructure layer:** Provides, integrates hash power and hardware support for the blockchain systems;
- **Platform layer:** Provides development platform, underlying architecture for blockchain applications;
- **Middle layer:** Makes blockchain applications easier to deploy and is used to serve developers and users;
- **Service layer:** Provides professional services for industry participants and mobilizes the circulation of capital and information;
- **Application layer:** Applies blockchain technology to various industries and use cases to serve end users.

3.1 Hardware and infrastructure layer

Provides, integrates hash power and hardware support for the blockchain systems：

- Mining hardware producer

Bitmain Canaan Ebang

- Mining pool

Antpool ViaBTC F2Pool

- Chip manufacturers (including OEM)

Nvidia AMD Hisilicon

➢ **Current situation and future trends：**

Currently, mining hardware is mainly compatible with blockchains using PoW consensus protocols such as Bitcoin. Professional mining hardware mostly use ASIC chips and usually possess a much higher computational efficiency than GPUs.

However, since ASIC chips are usually designed for a specific algorithm, thus can only be applied to one specific crypto asset or crypto assets with similar algorithms.

In addition, professional ASIC miners also caused the concentration of network hash power and consumption of large amount of electricity. We believe the future of this segment to be like:

- **The competitive landscape of professional ASIC miners has taken shape and leading effect is expected to be more apparent in the future:** At present, ASIC chips used in professional mining hardware are firstly designed by miner manufacturers, and then developed and manufactured by traditional chip manufacturers such as TSMC. In other words, while core R&D capability is controlled by the chip manufacturers, miner manufacturers possess abilities to design chip architectures, and this creates entry barriers for new comers. In addition, as demand for mining increases, the prices of ASIC chips also rise significantly, posing pressure on small-scale, low-cost mining hardware manufacturers. We expect the big players become even stronger in the future.
- **GPU mining will coexist with ASIC mining:** GPU mining hardware is proved to be more versatile than ASIC mining hardware and is compatible with multiple crypto assets. It is like a computer with enhanced graphics configuration and is more suitable for public individuals. In addition, GPUs are more computationally intensive in graphics algorithms. Besides, to prevent ASIC mining hardware from concentrating too much of the network hash power and posing 51% attack threat regardless of costs, more and more blockchains are expected to adopt consensus mechanisms against ASICs, such as PoS or PoW+PoS. However, since traditional manufacturers such as Nvidia and AMD control GPUs capabilities, any equipment that uses these GPUs can be crafted into mining hardware, thus we don't expect professional GPU mining hardware producers to emerge, and rather, GPUs mining is more likely to be long-tailed among users.
- **Future opportunities exist in low energy mining hardware:** Whether it is ASIC mining or GPUs mining, a large amount of electricity will be consumed, and the process of mining is merely repeating hash computing without generating too much value. In the future, low-energy mining such

as CDN mining may increase, bringing new opportunities for mining hardware producers.

3.2 Platform layer

Provides development platform, underlying architecture for blockchain applications

- General blockchain platforms

Ethereum EOS Cardano Stellar NEO Qtum Icon

Zilliqa Aeternity Ontology Wanchain Rchain IOST Aelf

Aion Nebulas Fusion Nuls TomoChain Moac DFinity

Polkadot Cosmos Tezos Emotiq Thunderealla Seele Algorand

- Blockchain platforms for specific use case

Tron Bytom Cybermiles Ulord IoTeX

➢ **Current situation and future trends:**

According to incomplete statistics by Huobi Research, currently there are at least dozens of blockchain platform projects, making this area extremely crowded. A blockchain platform is equivalent to an operating system and is the basis for blockchain applications. We can say, whoever captures the platform possesses a greater chance of becoming the future blockchain giant. Currently, leading effect in this field has begun. We still expect competition to increase in the short run, but at the same time, concentration degree will also gradually increase. In the future, we expect this segment to have the following trends:

- **Cross-chain interoperability becomes an important criterion：** As the underlying technology of blockchain gradually matures, the demand for cross-chain interaction has also increased, and more and more platforms with cross-chain capabilities are emerging. The main privileges of cross-chain are: 1) **Performance improvement:** cross-chain is one of the ways to solve the scalability issue of blockchain; 2) **Information interaction:** although blockchain removes the limitations of national boundaries, each independent blockchain itself is a separate island. Cross-chain information exchange allows data to be transmitted between different islands, forming a communication network for interconnection, interoperability, and mutual trust; 3) **Value transfer:** Each independent blockchain is a separate eco-system with value created inside. A blockchain with cross-chain capability is the hub linking different separate blockchains. Only by enabling interoperability between value and industries can we make blockchain a value transmit platform.

- **Performance is no longer the only criterion, while "developer-friendly" will become increasingly demanded:** In the past few years, people have made various attempts to improve transaction throughput of public blockchains, including lightening network, sharding, sidechains and improved consensus protocols etc. For now, a “developer-friendly” blockchain platform still doesn’t exist. Huobi Research believes that, in the future, such platforms will appear, and barriers for developers will continue to be lowered.

- **Opportunities in blockchain platforms for specific use cases will appear：** We know that the TCP/IP protocol defined the standard for the Internet. However, the world of blockchain is more complex. Different use cases and industries have different requirements in aspects such as consensus protocols etc. Huobi Research believes that, in the future, there won’t be a universal public blockchain, but rather, in each specific vertical, opportunities also exist. Currently, public blockchains for specific use cases have emerged. In the future, with the interaction of “blockchain + use case”, in each vertical there will be more business logic moving on chain.

3.3 Middle Layer

Makes blockchain applications easier to deploy and will be used to serve developers

- Distributed storage

Filecoin Siacoin Storj Genero Network

- Decentralized exchange

ZRX Loopring Kyber Network

- Decentralized data services

GXS ChainLink Bluzelle Ocean Protocol

- Distributed computation

Golem Enigma TrueBit

- Security services

Certik Quantstamp Zepplin Sentinal Protocol

- Privacy, encryption services

Nucypher Rockchain Keep Network

- Developers' tools

Lisk Stratis Arcblock Etherparty

- Scaling solutions

Loom Raiden Network Trinity

➢ Current situation and trends:

Since blockchain is essentially a technology solution and is compatible with various industry applications. The main purpose of the middle layer is to meet common needs of different verticals in applying blockchain technologies, such as distributed storage, decentralized data services, code auditing and encryption services etc. Those services can be regarded as outsourcing of blockchain technology. Huobi Research believes that the boom of above technology services for developers are certain, and will present a virtuous cycle of spiraling up:

- **Popularization of middle layer would accelerate the landing of distributed applications:** Middle layer lowers the threshold for blockchain and greatly accelerates the landing of distributed applications. For example, Dapps can directly use the existing distributed storage services provided by Filecoin etc.

rather than starting from scratch. This is the same as in the internet era, applications use existing cloud storage services such as Alibaba Cloud, Amazon AWS, etc. rather than building their own.

- **The maturity of distributed applications in verticals would in turn induce new demands：** With the popularization of Dapps, new opportunities will also emerge in this area. In the future, we may see demands for identity authentication for applications increase and creates potential opportunities.

3.4 Services layer

Helps funds and information to circulate, and provides professional services for participants in blockchain industry: (listed without particular order)

- Crypto Asset Exchange

Huobi Binance Bitfinex OKEX Bithumb

Gate.io Bittrex Poloniex IDEX Nex

- Media and Communities

Coindesk Bitcoin Magazine 8Btc Jinse Finance Bishijie

ChainDD Huoxing Finance Huoxun Finance

- Market Quotes and Information Providers

Coin Market Cap AICoin Mytoken Feixiaohao CoinGecko

- Crypto Assets Wallet

imToken KCASH qbao Huobi Wallet

Imtoken	Kcash	qbao	Huobi Wallet

➢ **Current situation and future trends:**

Services in blockchain industry include crypto asset exchanges, media and communities, market quotes and information providers, crypto assets wallets, etc. This layer accumulates all the information of the industry and serves as a hub of all transactions and funds. With the development of the industry, service layer has a very positive prospect. Meanwhile, due to the characteristics of this layer (where resources integration matters most like the internet), the leading effect in this layer will sustain and the bigger ones will continue to dominate.

- **Decentralized and centralized crypto asset exchanges will both exist:** The exchange of crypto assets is currently realized through off-chain match services provided by centralized crypto asset exchanges. Namely, transactions in crypto asset exchanges are not actually recorded on the blockchain. The liquidity is split and dispersed in different centralized crypto asset exchanges. With the development of blockchain technology, decentralized crypto asset exchanges, with all transactions matched on chain, will be more and more popular. However, due to the differences in transaction experience, decentralized crypto asset exchanges may target more on the users of distributed applications and provide simple and user-friendly services of token exchanges, while centralized crypto asset exchanges may target more on investment-oriented and transaction-driven users and provide the best trading experience.

- **Market quotes and information providers can provide one-stop trading services:** Due to the liquidity dispersion from currently centralized crypto asset exchanges, users need to register with different exchange platforms, which is a very cumbersome process. The market quotes and information providers, with its advantage in user bases, can provide one-stop trading services, allowing users to use one unique account to trade on different exchange platforms.

- **Crypto assets wallets may become the entrance to the world of Dapps in longer run:** Similar to the mobile internet world, where APPs serve as the windows for users to experience mobile internet, the Dapps will also become the main way for users to directly interact with the blockchain. Since the users need tokens to use Dapps, the importance of wallet, as a tool of managing different tokens, is evident. It could turn into the Dapp store and serve as the bridge between huge user flow and various Dapps in the coming era of blockchain 3.0.

3.5 Application layer

Serves end users across various industries. (listed without particular order)

Utilizing the technical advancements made possible by blockchain, entrepreneurs develop applications in areas where (1) there are inefficient communications and high costs of trusts, (2) there are strong demands for data validation and consensus, and (3) there are needs for massive data sharing and high-computing power.

Monetary market application such as payments and clearing:

In traditional finance, banks serve as the intermediaries for payment processing and clearance. A payment usually needs to go through origin bank, recipient bank, clearing houses, offshore correspondent bank, etc. The whole process takes many efforts, costs, and time. For small cross-border payments, high costs and long waiting time impose even more substantial burdens on the senders and receivers. Blockchain solves this pain point by: utilizing crypto assets as media of payment that have no border limitations, eliminating intermediaries, and utilizing distributed ledger to increase the efficiency of clearance. Here are some major projects in this sector:

ripple	OKLink	bitpay	veem	wyre	ABRA
Ripple	OKLink	BitBay	Veem	wyre	Abra

Huobi Research believes that there are two major trends in this segment in the future:

- **In short term, using crypto assets as media of exchange for cross-border payments is promising:** Several start-ups are focusing on using crypto assets to help users transfer funds across borders, such as Bitpay, Veem, Wyre providing B2B payment solutions and Abra delivering services to individual customers. For example, Bitpay can reduce the time window for cross-border payment from 4 business days to 1 business day and can cut the fee from 7% to 1%. Also, the amount received in fiat remains unchanged by using swaps to hedge against price volatility of crypto assets. Monthly transaction volume at Bitpay has exceeded 1 million USD. The clients include Lush and other leading FMCG brands. Huobi Research believes that using crypto assets as payment tool is heading into the stage of massive adoption.

- **In long-term, blockchain will revolutionize clearing industry by imposing new payment protocols:** New payment protocols will standardize the ledgers in the banks' back offices and pave the way for clearing data sharing, which increases the operating efficiency of the entire system. Currently, Ripple is the leading player who uses blockchain empowered protocols to provide payment solutions for major banks in the world. Ripple intends to replace SWIFT as the new standard in the new era. Similar projects include Stellar and OKLink who focus more on small and medium sized financial institutes. We think network based on blockchain technology can effectively decrease the middle-men costs and increase efficiency for clearing process and thus help small and medium sized institutions to fully realize the benefits brought by such services.

Applications for securities, commercial notes, and alternatives:

Currently, financial assets exchange needs the confirmation from centralized platforms. For example, in securities exchange, China Securities Depository and Clearing Corporation (CSDC) oversees all registration, clearing and settlement related activities. Overwhelming rules and policies and extensive auditing process are needed to maintain this centralized structure. The decentralization made possible by blockchain ensures a trustless environment where participants can freely exchange information. The consensus mechanism ensures that all information is valid, complete, and free from manipulation, thus the issue of information asymmetry will be eliminated. Here are some major projects:

Tzero Polymath Global Reit ReitsChain Shanghi Commercial Paper exchnge

Future trends in this area would be:

- **Major players from the US has pioneered the blockchain application in security market and more developed countries will follow:** In December 2015, the US SEC approved Tzero, a securities trading platform built by Overstock. Utilizing blockchain technology, this platform creates an environment where bonds, stocks, and crypto assets can be traded on an efficient and transparent way. In October 2017, Polymath came online and provided an integrated platform where security tokens can be issued and exchanged between parties. Huobi Research expects that as regulations for blockchain and crypto assets become clear in the future, more and more countries will deploy integrated blockchain solutions to securities market.

- **Central Bank of China pioneered blockchain-based commercial notes:** Central Bank of China deployed blockchain-based exchange of digital commercial notes in 2017. It became the pioneer among central banks to explore blockchain application in digitalized assets and securities.

- **As more types of assets are being tokenized, tokenized asset exchanges in more sectors are expected to appear:** Dating back to October 2015, NASDAQ partnered with blockchain startup Chain to build a private equity exchange platform called Linq. For REITs, start-ups such as Global REIT and Reitschain leverage the distributed ledger and distributed storage technology to tokenize real estate assets. In energy sector, Chinese start-up Energy-Blockchain started to issues structured financial products on blockchain based on the carbon emission. Huobi Research thinks that distributed assets exchange platforms in different sectors are fundamentally similar and mass adoption will boom as soon as any of the vertical integrated platforms prevails in the future.

Healthcare

Electric medical records, remote medical diagnosis, medical insurance are the main fields where blockchain technology can be adopted. Those use cases rely on distributed ledger, decentralized storage, and smart contracts to integrate the scattered healthcare data, enable the data owners to claim full control of their data, and empower entrepreneurs to leverage massive data to develop artificial intelligence.

Here are some of the major blockchain projects in healthcare industry:

MEDICALCHAIN	MEDICHAIN	MediShares	Medibloc	HASHED HEALTH
MedicalChain	MediChain	MediShares	Mediabloc	Hashed Health

Medicalchain and Medibloc are two major players developing solutions for electric medical records based on Blockchain technology. Combining Hyperledger and public/private key pair technology, Medicalchain allows data owners to decide who they want to release the medical records to, which specific parts of records they want to release, and how long they allow the third parties to access the data. On the other hand, Medibloc uses zero-knowledge proxy encryption and decentralized storage supported by IPFS to empower its users. Medishares revolutionizes medical insurance industry by proposing to have mutual reserve secured by smart contract. Mutual reserve pooled by users themselves eliminates tremendous overheads generated by the intermediaries and substantially speed up the claiming process.

We believe that blockchain applications that provide integrated health management services and facilitate the collaboration between primary and secondary care will boom soon:

- **Multi-dimensional and customized health management and disease prevention can be realized:** Combing IoT technology, wearable devices, electric medical records on blockchain, and machine learning, health management ecosystem can be built in a closed loop. The data access permissions can be capitalized under the structure of peer-to-peer storage, encryption, sub chain and main chain, and off-chain payments. Users can profit from lending the data collected by wearable devices to AI developers and research institutions, thus help with the training of artificial neuro networks, which is crucial for developing AI solutions for healthcare problems. Essentially, AI solutions trained by users' data will in turn benefit data owners by providing multi-dimensional health evaluations and customized treatment plans. Huobi

Research thinks that the successful platforms will have well-designed token models and incentivizing mechanisms that help to align the participants' behaviors and create a win-win for everyone in the network.

- **Hierarchical medical system will be further promoted:** Underdeveloped insurance coverage, isolated record keeping systems, and unprotected patients data usually hurdle the advancement of current healthcare system. Using blockchain and the underlying smart contracts, decentralized storage, and encryption technologies, entrepreneurs can tackle those hurdlers by coordinating the activities between different layers of healthcare, ensuring information integrity, and reducing the overheads.

Supply chain provenance and supply chain finance:

Blockchain applications in supply chain are mainly related to products provenance and ownership declaration, and supply chain financing. Several solutions are developed for products provenance and ownership declaration, including QR code and RFID chips. Those solutions focus on creating unique identity for each product and enclosing all the information, such as the sources, the logistics, and the ownership at a certain moment. However, all the information are usually stored in a centralized network and could suffer from malicious revises. With blockchain technology, all the product information can be stored on immutable and trustless decentralized network. Most importantly, smart contracts help to manage the ownerships and using rights in real time and thus boosting the efficiency of entire supply chain.

In terms of supply chain finance, banks and other participants in the industry can share ledger and credit history based on blockchain, which enables faster credit check. Products provenance and ownership declaration solutions will help banks to evaluate the collaterals put up by loan appliers and reduce the processing time. Conventionally, credit scores are used to reflect the creditworthiness and therefore the risk of default. However, for some young companies, although they have high quality supply chain assets, due to the lack of an established credit score, they still cannot get timely funds from banks. Blockchain can help them to form unique identities with many attributes and establish trust between parties if trust is needed.

For example, attributes such as “on-time deliver” and “on-time payment” can both be used as credit endorsements. Moreover, digitizing the supply chain assets such as account receivable/account payable, inventory, and commercial notes, can make the traditional assets splittable, which combined with the endorsement mechanism enables deep tier financing across the whole supply chain.

Here are some major projects in this sector:

Vechain	Bubi	JD.com	Chained Finance	Cainiao	33.CN

We expect that the trends of the two applications will be as follow:

- **Products provenance and ownership declaration meet the polarized demand of both established enterprises and small and medium sized companies:** Maersk, the world's largest container shipping company, partnered with Hyperledger, has completed a trial shipment crossing the Atlantic Ocean for the goods of Schneider Electric. By leveraging distributed ledger and smart contracts, Maersk saved the time and efforts for counting goods repeatedly and for cross-border legal documents. It completed the shipment in 2 weeks, comparing to 8 weeks in traditional way. China E-commerce giant, JD, has deployed blockchain-based product provenance platform and provide free service for brand owners in JD ecosystem. Vechain, another famous project, provides provenance services for leading luxury brands and art pieces. We believe that proof of authenticity services based on blockchain not only meets demands of established companies, but also meets demands in boutique operations filled with high value customers. Thus, the demand of those functionalities is polarized.

- **Core enterprises on supply chain will be the key driver of promoting blockchain supply chain finance:** Better cash flow and liquidity are the keys for supply chain. Core enterprises need to ensure the reliability of their supply chain and to receive materials from upper stream suppliers on time. Foxconn announced the establishment of the first blockchain-based supply chain financing platform, Chained Finance, and positioned it to help provide financing services for suppliers on its own supply chain. Hai Nan Airline partnered with 33.cn, a blockchain start-up in China, deployed blockchain-based supply chain commercial notes platform called “Hai Piao Hui” in 2017. JD, Alibaba, and Tencent have also set up their own blockchain supply chain financing platforms in 2018. Although the pain points of small and medium sized suppliers are bigger, however, since a successful supply chain financing platform involves various counterparties in the industry, it is not so easy for small suppliers to initiate the adoption of blockchain. Instead, blockchain will be promoted top down by core enterprises.

- **More innovative supply chain finance products based on supply chain provenance and ownership declaration will emerge in the future:** Utilizing smart contract, supply chain system can validate the change of ownership for goods, which can realize static and dynamic collaterals financing. If any disputes of ownership happens, mediation can be done easily by smart contract based on the records on chain.

Copy right and relevant transactions

With the development of Internet, especially mobile internet, digital content and copyrights trading have formed a relatively complete industry. However, plagiarism and infringement are holding the digital content industry from going further. In the meantime, copyright owners are making far less influence than those traffic-heavy content channels. Therefore, the profitability of content producers has been eroded and incentives and motivation of creativity have been reduced.

With Blockchain technology, content producers can now store, record and transmit their content and information with timestamps. In this way, the content cannot be tampered, and its protection can be assured. In addition, a distributed copyright trading network can also be built on blockchain, returning the profit from platform to content producer. Examples of projects in this sector are:

Primas Ink YoYoW Mediachain CNN Bitmark

In the future, blockchain technology is expected to continue to penetrate this field:

- **Urgent needs and mounting willingness to pay for quality contents are the**

cornerstones of blockchain copyright protection: There is a natural fit between the anti-tamper characteristic of blockchain and copyright protection. Currently, numerous players have entered this field, such as China's copyright confirmation and trading platform “Ink”, and the platform "Micro Video 360" jointly created by China Copyright Protection Center and Huaxia Mirco-Movie Culture and Media Centre integrating the service of micro video registration, confirmation, supervision, trading, sharing and clearance. The media giant Spotify also acquired a New York startup Mediachain in 2017 to help protect content producers’ copyright. In addition, with the popularization of intellectual property awareness, users are increasingly willing to pay for high-quality IP, which further creates a superior market environment for blockchain to step in.

- **Copyright trading based on blockchain will help maximize the value of long-tailed content and help create equality in the market:** In the traditional content industry, top IP's influence is apparent, however, many of the top IPs are mostly hype, with market prices much exceeding the fair value. Also, many mid-to-bottom level contents did not obtain the attentions due because of the lack of platform support, and their values are largely underestimated. We believe that with the decentralization technology brought by blockchain, the influence generated by the platform will be weakened, and IPs will be more reasonably priced with price gap effectively reduced.
- **Blockchain will empower integration between content industry and other sectors, promoting industrial upgrade:** Since June 2017, the US-based personalized artificial intelligence company ObEN has partnered with SNH48 to produce the world’s first virtual celebrity character based on the PAI public blockchain, allowing fans to interact with virtual celebrities online. And blockchain technology can be of great help in proving the authentication of the image on blockchain. Huobi Research believes that with blockchain technology in place, further integration of the content industry with other sectors such as social services, manufacturing, and high-tech industries will be more active.

Digital Advertising

The digital advertising industry has gone through the traditional purchase phase (ad slot placement), ad network purchase phase (media portfolio launch), and programmatic purchase phase (precise placement). Nowadays, with the popularization of programmatic purchase, the entry barrier for industry participants have been significantly lifted. Now, advertisers need to hire professional third parties for help. However, information and data inside the industry are fragmented and don’t circulate, resulting in the loss of mutual trust and unnecessary costs, such as advertising verification, data monitoring and ad block etc. Yet with blockchain that is transparent, irreversible, and traceable, above problems now can be solved and foundation for mutual consensus for digital advertising could be built. Relevant projects involved in digital advertising are as follows:

BAT DATA Prochain AdEx DATx AdChain RebelAI

We believe that:

- **blockchain will first enable low-frequency advertising cases:** Digital advertising has entered the stage of programmatic purchase, and real-time bidding transactions can be confirmed within millisecond speed. However, the current blockchain technology cannot achieve high transaction throughput. Major blockchains now only support dozens or hundreds of transactions per second, and all the Dapps are running on the same chain, utilizing the same resources. Such scalability bottleneck to some extent limits blockchain’s revolutionary impact on digital advertising. We expect blockchain to be firstly more used in use cases that don’t have requirements for high transaction throughput, such as content distribution, brand marketing etc.

- **Blockchain in digital advertising will gradually evolve from anti-fraud, disintermediation to advertising effectiveness management system:** In the traditional digital advertising field, attribution of advertising effectiveness has always been an important but complex issue. There are multiple stages from advertisement presentation to user conversion, which may involve multiple exposures. If payments are determined merely by clicks or conversion, the effects of some media may be overlooked. With traceability of blockchain, quantification issues can be resolved and blockchain can be upgraded to become an advertisers' comprehensive management and assessment system.

Games

As a field digitalized in nature and with massive users, the game industry is a natural fit for blockchain. Huobi Research believes that the change blockchain could make to the game industry does not lie in gaming experience nor the way to play games, but rather in establishing a more open, fair and trustworthy gaming environment for players. With the aid of blockchain, games that used to be black boxes and solely controlled by developers can now become transparent. Related projects in blockchain gaming industry are as follows:

Decentraland Enjin Refereum DMarket Bit.Game Etheremon

Besides, blockchain can potentially integrate with the game industry in the following aspects:

- **Player's virtual asset trading could be a major direction:** Ownership of virtual assets in traditional games, including game equipment, skins, and mounts belongs to game developers, also, the existence of such virtual assets depends on the survival of the game, and users cannot liquidate virtual assets into cash in a formal way. At the same time, virtual assets in traditional games are isolated, lacking interoperability. With blockchain, the circulation limitation of virtual assets is expected to change: By moving virtual assets on chain, users now can trade with each other using tokens, and counterparty risks could also be significantly reduced. At present, DMarket and Bit.Game are trying to build a blockchain-based virtual asset exchange. The land auction that can be carried out in the virtual game Decentraland is also an example of virtual assets transactions carried out through blockchain.

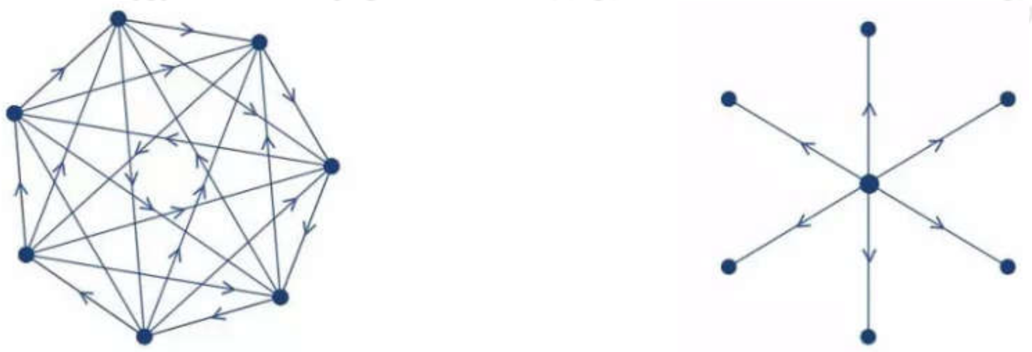
- **Blockchain is expected to transform the traditional game distribution model:** Traditionally, game developers mostly rely on large-scale game channels, including Steam platform, Tencent's Wegame platform, etc. in game distribution and promotion. However, distribution expenses under this circumstance are relatively high and small and medium sized developers usually bear extreme pressures. With blockchain, players and developers can now be gathered together in the same economic system. Developers can first purchase tokens, pledge into a smart contract reward pool, then players receive rewards in the form of tokens by forwarding, or completing certain tasks etc., thus developers can promote games in a more cost-efficient way. In 2018, distributed game distribution platform Refereum started its attempts in this area, and reached a cooperation with game streaming platform Twitch and game engine Unity.

Part IV. Blockchain technology overview and prospects

Our economy is built on trust. Nowadays, economic activity in almost any form needs a trustworthy third party. After introduction of a third party, uncertainty faced by counterparties in economic exchange is lowered. However, introducing a third party also brings troubles. First, there's cost and in some cases may be expensive. Second, there may be security problems such as sensitive data leakage. Third, it is still uncertain to what degree the third party can be trusted.

These are the reasons why we need blockchain and the pain points such technology aims to solve. The essence of blockchain is a tool that enables cooperation on a large-scale in an open, distributed and equal network environment, and is much different from traditional centralized coordination.

Graph 24: Distributed cooperation and traditional centralized coordination



Blockchain:

Distributed cooperation

Traditional third party:

Centralized coordination

Source: Huobi Research

4.1 We are in the stage of building an exciting open, distributed eco-system

The first real-world blockchain technology application stems from Satoshi Nakamoto, who in his paper "Bitcoin: A Peer-to-Peer Electronic Cash System" introduced Bitcoin and a brand-new way of transferring value to the rest of the world. Now the Bitcoin network has been running for 10 years, and Bitcoin is no longer the only crypto asst and blockchain application any more. Bitcoin going into mainstream also brought heated discussions about blockchain technology.

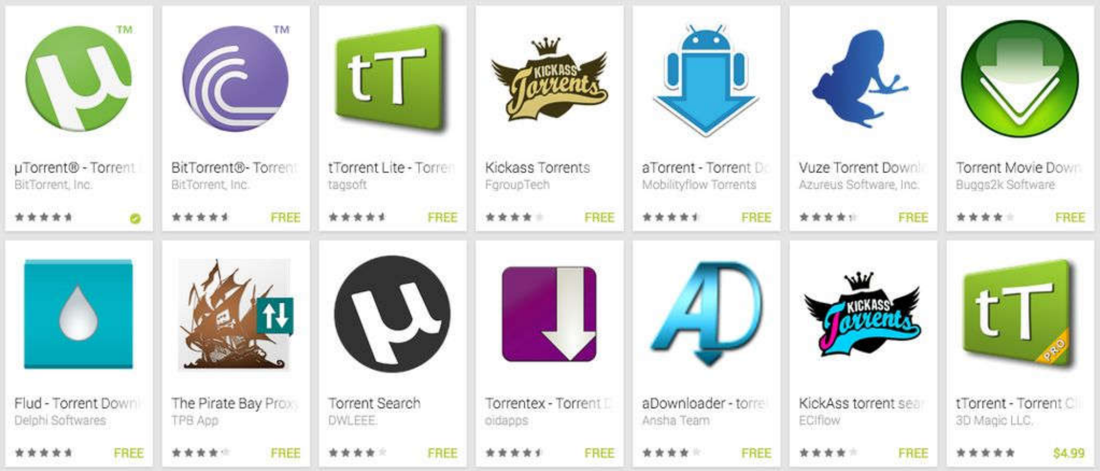
Incorporating the ideas from Xiao Feng, vice president of Wanxiang Holdings, initiator of Wanxiang Blockchain Labs and general partner at Fenbushi Capital, blockchain will go through three stages of development, and we are now at the most exciting part, which is building an open, distributed eco-system.

Layer (Stage) 1, Distributed communication network

The bottom layer and first stage of blockchain is a distributed network solving peer to peer communication and transmission problem. The core of such network lies in consistency, which in other words is reaching agreement among multiple nodes using a defined protocol under a circumstance that each could initiate, interact and broadcast information. The defined protocol in the blockchain setting is called consensus algorithm.

Distributed network technology has been in existence for decades, yet for most people, acquaintance with distributed network comes from peer to peer transmission applications like “BitTorrent”. The earliest peer to peer transmission application was a software named “Napster” developed in 1999 by a college student named Shawn. When a user launches the software, the computer itself would become a micro server offering upload and download services.

Graph 25: APPs of peer-to-peer transmission and downloading



Source: Huobi Research

Layer (Stage) 2, Distributed ledger

The second layer and stage of blockchain is a distributed ledger that records transactions in a cryptographic, distributed way, and it is very different from our traditional financial system. The biggest difference lies in the cost of running the system: While traditional financial system requires a whole set of complex and heavy facilities, a distributed ledger system only needs a set of rules defined by mathematical algorithms and coding. Specifically, under the traditional financial system, the bank would apply rigid KYC process to assess user creditability and would often require a trusted third party such as the central clearing house to record all of the transactions happened between different banks and parties. A distributed ledger system on the other hand, is open to everyone and records, synchronizes transactions as well as funding status onto everyone's ledger, thus eliminating the need for a trusted third party. During this stage, great numbers of peer to peer cashes such as Bitcoin, Litecoin, Monero, ZCash etc emerged, and all of above crypto assets are built on distributed ledgers.

Layer 3, Decentralized and open economic ecosystem

The third level and stage of blockchain, is a public, distributed and open economic eco-system with incentives. Very much different from the traditional shareholding system that incentivizes all of the participants through fixed employment relations, the blockchain eco-system incentivizes participants through a flexible "action-reward" relationship. In the blockchain eco-system, people are no longer bonded by one single, specific employer anymore. On the contrary, people could receive compensations from various sources as long as they complete pre-defined actions or works, such as solving hash functions, sharing resources or even uploading premium contents. Also, while the traditional shareholding system pays with fiat currency, the blockchain eco-system pays with tokens, or crypto assets that are programmable. That is, for the first time, rewards become a piece of code that could be executed autonomously and intelligently.

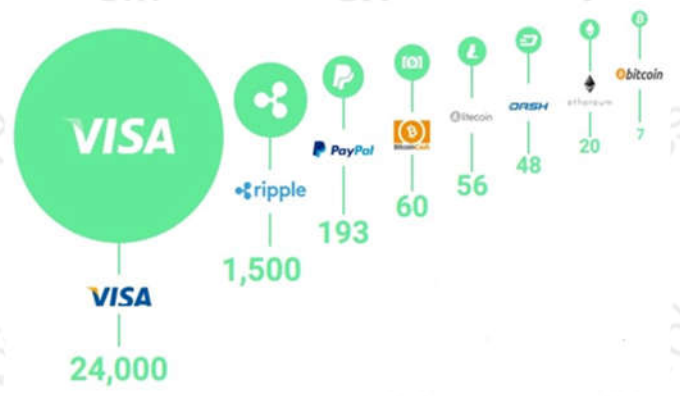
Now we are right in this stage. Blockchain technology, through changing the way people interact and cooperate with each other, is penetrating various use cases, and has triggered great amount of discussion in the research community and various industries. Currently, the blockchain technology is aiming to build a solid foundation and creating a basis for a scenario economic incentive-based business model.

4.2 Blockchain Technological Bottlenecks and Solutions

Although blockchain technology continues to make progress, its application still faces many challenges. At present, the performance and usability of blockchain cannot support commercial use at a large-scale. Scalability, privacy, and interoperability are still bottlenecks and major issues, yet new solutions are emerging:

- **Blockchain scaling solution developments**

Graph 26: Comparison of TPS performance



Source: Token data, Huobi Research

Scalability is still the most critical issue in the field of blockchain. Transaction throughput and latency are the two keys to large-scale commercial applications. At present, major blockchain networks can only process dozens of transactions per second, which is far less than VISA's capability to handle 24,000 transactions per second at peak. Also, confirming transactions on blockchain takes time. A typical block time for Bitcoin and Ethereum is 10 minutes and 14 seconds respectively, while for VISA service, it is almost instant. Currently, scaling solutions mainly focus on consensus mechanisms (distributed network level) and transaction verification mechanisms (distributed ledger level).

Firstly, consensus mechanisms:

In a public blockchain environment, traditional Proof-of-Work consensus faces energy waste and inefficiency problems. To scale transaction processing, Proof-of-Stake, Delegated Proof-of-Stake and Practical Byzantine Fault Tolerant were gradually developed and adopted.

Proof-of-Stake（PoS）

Cosmos　Cardano Ouroboros

Thunderella　Algorand

In terms of Proof-of-Stake consensus, besides Ouroboros from Cardano and Tindermint attempts from Cosmos, we’ve also seen the Algorand algorithm (a variant of PoS) proposed by MIT Turing Award winner — Micali； and the Snow White algorithm put forwarded by Professor Elaine Shi from Cornell University (used in Thunderella blockchain project).

Delegated Proof-of-Stake（DPOS）

Bitshares　Steemit　EOS

The most famous examples of blockchains that use Delegated Proof-of-Stake are Bitshares, Steemit, and EOS. Its principle is to allow delegates selected from voting to sign and record transactions.

Practical Byzantine Fault Tolerant（PBFT）

HyperLedger　NEO

Mostly used in consortium blockchains under trustless environment. Typical cases are Hyperledger and NEO, which upgraded their consensus mechanism to Delegated Byzantine Fault Tolerant.

Source: Huobi Research

Secondly, transaction verification mechanism:

From the perspective of transaction verification, there are currently the following scalability solutions: side-chain or state-channel, sharding, and sub chain or layered structure.

- **Sidechain and state-channels**

The essence of this solution is to put transaction processing or smart contract running off-chain. Through establishing off-chain channels, counterparties are able to complete multiple small-to-medium payments or to run smart contracts at low costs. Under such circumstances, the main chain only acts as a settlement layer to record the final state or functions as a court in the event of a dispute, thereby greatly alleviating the burden of the main chain.

Typical applications of side-chain include Lightning Network for Bitcoin, Raiden Network for Ethereum, Trinity for NEO, and Aelf and Asch Chains as “Main Chain+Sidechain” blockchains. Typical applications of state-channel include Aeternity, which is known as the “Ether Ethereum in Europe". At present, Lightning Network test net has been put online, with nearly 900 nodes and roughly 2400 network channels. Raiden network for Ethereum and Trinity for NEO are still under deployment. According to official statement, Aeternity is also expected to launch main net in June 2018.

- **Sharding**

Sharding technology divides a blockchain network into many separate, independent areas, called "shards", and each shard is assigned to a small group of nodes to maintain. Sharding mainly includes transaction sharding and state sharding. Transaction sharding refers to assigning different transactions to different shards, in this way, parallel processing becomes possible, thus leading to high transaction throughput. State sharding on the other hand, is allowing data and state to be stored in different pieces on different nodes. In other words, one single node is only responsible for saving a portion of the network ledger.

At present, most of the sharding solutions concentrate on transaction sharding. The most typical case is Zilliqa, whose test net 1.0, named “Red Shrimp” went on-line on March 31, 2018. State sharding is relatively difficult to achieve and usually involves cross-shard communications. Also, the amount of scalability that forgone when implementing state sharding may outweigh the benefits from storing states separately. Currently, Rchain, Emotiq, Zilliqa and Ethereum etc. are all exploring compatibility solutions in state-sharding as well as cross-shard communications.

- **Sub chain and layered structure**

In a traditional public blockchain network, a single node is not only in charge of transaction clearing, but also responsible for running all kinds of smart contracts, as well as storing various states.

The essence of a layered structure is the isolation of above two functions. Cardano is the most famous project that proposes such layered structure, which divides the blockchain network into “Control Layer” and “Settlement Layer”. The settlement layer is responsible for transaction confirmation and the flow of crypto assets, while the control layer will run smart contracts and will be programmed to recognize identity, assisting compliance. Currently, Cardano Settlement Layer is put on-line.

Sub chain comes from a “Mother-Child” structure, which divides a blockchain network into a main chain and numerous sub chains. In a “Mother-Child” structure, the main chain is responsible for transaction clearing, while each sub chain takes charge of smart contract and Dapp running. Also, each sub chain can define its own consensus mechanism, has unique execution modules, and is independently established, leading to parallel processing. Besides, sub chain periodically communicates and synchronizes with main chain. Typical cases include MOAC, Ontology, and Nuls, etc. On April 30 2018, MOAC officially put its main net on line, on March 30 2018, Ontology launched its test net, and one day right after, Nuls test net also went on line.

- **Privacy solution developments**

Under a public blockchain environment, the network ledger is open to anyone and all of the transactions are transparent. Such transparency could be fatal under the cases where privacy is required. Though major blockchain systems like Bitcoin network provides pseudonymity for its users, that is, transactions are marked by the hashes of public keys, which don’t directly show the user identity. However, we are still able to derive it from IP addresses, transaction records, block information, etc. So blockchain networks are not completely anonymous.

Then, how to take advantages of the good characteristics of blockchains (traceable, verifiable, etc.) while at the same time maintain the privacy (hide transaction information)? Currently, popular solutions include Ring Signature, Zero-Knowledge Proof, CoinJoin and Invisible Internet Project.

a. CoinJoin

Dash uses CoinJoin technology and combines multiple payments from multiple spenders into one single transaction to make it more difficult to trace; Meanwhile, in order to prevent master nodes from being attacked, Dash introduces Chaining and Blinding, which allows spenders to choose multiple master nodes randomly, thus mixes transactions among those master nodes successively. And transactions are sent via master nodes, instead of users themselves.

b. Ring Signature

Monero proposes an encryption scheme without centralized nodes, that is called Ring Signature. Whenever a transaction is initiated, the signer (actual sender) would be combined with non-signers to form a ring and help the actual sender mask the origin of a transaction to ensure that all inputs are indistinguishable from each other. Also, Monero utilizes Stealth Address technology to create automatic one-time addresses for all transactions.

c. Zero-Knowledge Proof

ZCash utilizes Zero-Knowledge Proof technology to automatically conceal transaction information such as sender, receiver and amount, etc. On the blockchain, only those with private keys have full access to the information. In other words, users have full control over their own transactions, making Zcash a decentralized network able to provide both full privacy and public blockchain compatibility.

d. Invisible Internet Project

Verge is an open-source, anonymous crypto asset based on Bitcoin technology. Through the Onion Router and Invisible Internet, user information such as IP addresses is concealed, making fast, anonymous transactions possible and transaction histories hard to trace.

Source: Huobi Research

However, currently most of the blockchain privacy solutions concentrate on transactions and payments, and haven’t touched on privacy issues in terms of smart contract, data storage, communication, etc. Since 2018, a group of blockchain projects aiming to fill in above gaps appeared, including Mainframe which is dedicated to realize peer-to-peer encrypted communication, Nucypher which focuses on providing distributed proxy encryption and decryption services, and Keep Network that strives to become the privacy layer for public blockchains and offer encrypted computations.

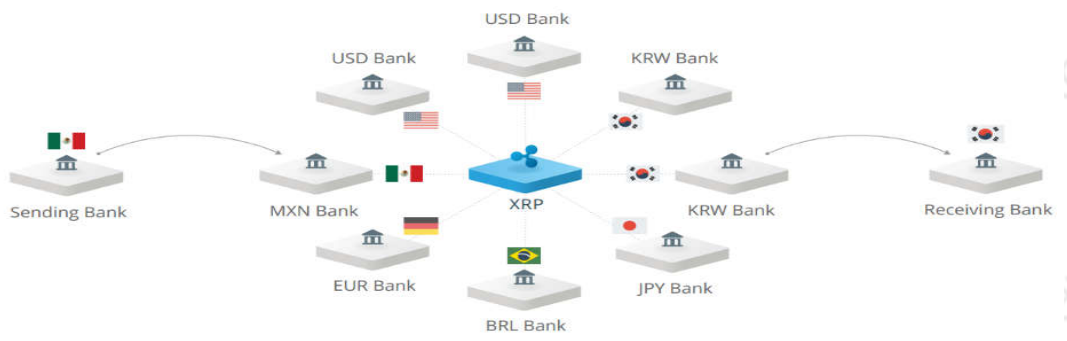
- **Interoperability solution developments**

Blockchain systems are divided into private blockchain, consortium blockchain and public blockchain. In terms of transaction throughput, scalability, and privacy considerations, private blockchains and consortium blockchains are more likely to be accepted by business entities and financial institutions, however: (1) assets in different private blockchains and consortium blockchains cannot be transferred between the networks freely; (2) Meanwhile, in current public blockchains, communications and interactions are even limited within a single eco-system, and cross-chain interoperability is still hard and costly. Therefore, various cross-chain technologies that could help connect different blockchains started to be explored. Currently, cross-chain technologies are still in research and trials, major cross-chain schemes include:

- **Notary schemes**

Ripple is a typical example, whose Interledger Protocol can connect different ledgers and let users transmit currencies freely by using third-party connectors or validators. The Interledger Protocol adopts cryptographic algorithm and uses third-party connectors to create funds custody for two different ledger systems. Also, a trusted person or group will hear and respond to incidents on each side of the ledger system. Once all parties reach agreement on cross ledger transactions, transactions can be confirmed.

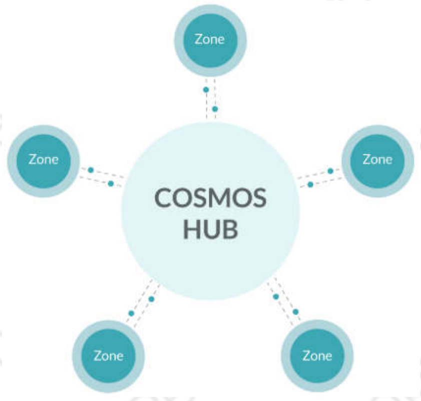
Graph 27：Ripple’s Interledger Protocol



Source: Ripple

- **Relay Technology**

Graph28：Cosmos “Hub—Zone” structure



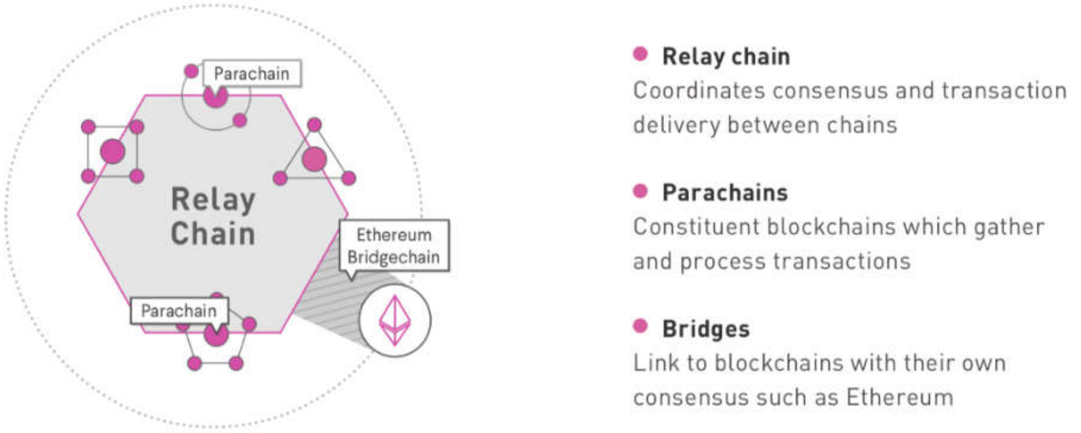
Source: Cosmos, Huobi Research

Cosmos and Polkadot are typical representatives. Cosmos has a cross-chain interaction which enables heterogeneous network brought by Tendermint. It uses its “Hub” as relay, and combines other “Zones” into a structure of internet of blockchains. Inside Cosmos, Hub and Zones can communicate through a protocol named “IBC” (Inter Blockchain Communication), and tokens can be transferred freely from one Zone to another through Hub.

In May 2018, Cosmos testnet entered the stage of “Gaia-5000”, where block rewards for validators can be tested.

Polkadot, on the other hand, is a heterogeneous multi-chain network. The network is made up of Polkadot, which is the relay chain and the core of the system, and large numbers of verifiable parallel dynamic data structures called para chains. Through Polkadot, different blockchains can communicate with each other and achieve scalability.

Graph 29：Polkadot “Relay-Parachain” heterogeneous multi-chain network


Parachain
Relay Chain
Ethereum Bridgechain
Parachain
● Relay chain
Coordinates consensus and transaction delivery between chains
● Parachains
Constituent blockchains which gather and process transactions
● Bridges
Link to blockchains with their own consensus such as Ethereum

Source: Polkadot Light Paper

- **Sidechain Technology**

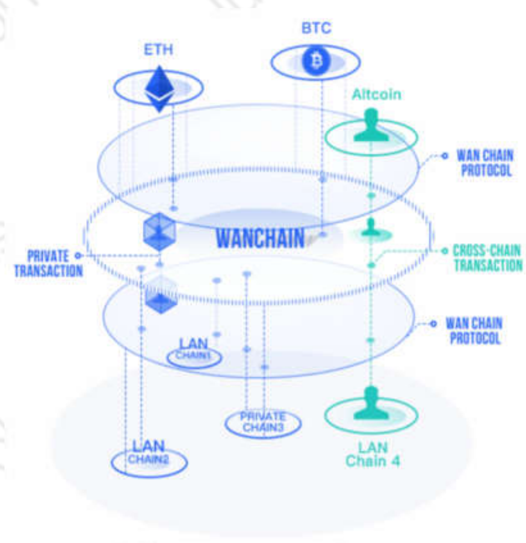
Sidechain is a blockchain that runs in parallel to the main blockchain. This structure extends functionality through interoperable blockchain networks. Assume chain B has all of the functionalities of chain A, then we call B is the sidechain of A, and A is the main chain of B. Main chain A does not necessarily know the existence of sidechain B, although sidechain B knows the existence of main chain A. A sidechain uses the same consensus protocol as the main chain, and the sidechains can also validate transactions happened on the main chain. Typical sidechain projects include Bitcoin sidechain Rootstock.

- **Hash locking technology**

Lightening network and Raiden network typically use hash locking technology. Lightening network is firstly used by Litecoin in cross chain payment, which is realized through establishing off-chain payment channels between different blockchains. In the cases that there is no peer to peer payment channel between two sides, as long as there is a path made up of multiple payment channels that can connect both sides, instant payment can also be achieved. It is hard to build Lightening network channels between heterogeneous blockchains, such as Bitcoin and Ethereum who use different communication protocols. Currently, the majority of cross-chain lightening networks exist between Litecoin and Bitcoin.

- **Distributed private key management technology**

Graph30 : Cross-chain transaction of Wanchain

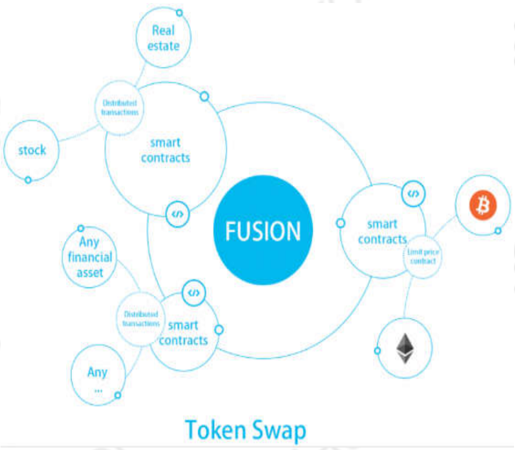


Source: Wanchain

Wanchain and Fusion are typical representatives. Wanchain uses secure multi-party computation and ring signature schemes, and achieves cross-chain transactions as well as interoperability of multiple blockchains. Specifically, for inflow transactions, users initiate cross-chain transaction requests, and the receivers are Wanchain's cross-chain locked account on the original chain. Then Wanchain's validator nodes verify the transactions and create a new smart contract token on Wanchain for users. For outflow transactions, the smart contract token created on Wainchain will be cleared and a transaction between the transferee address on original chain and Wanchain's cross-chain locked account will be made, thus the equivalent assets will be transferred back to the original chain.

Fusion uses distributed private key generation and management technology to map various crypto assets onto Fusion public blockchain, a process called lock-in. Then, those crypto assets could interact with each other, which realizes mortgages, loans, and insurance applications through Fusion smart contracts. The same is true for lock-out process, when smart contract ceases and releases mapping, crypto asset control rights are handed back to owners.

Graph 31: Fusion multi asset mapping



Source: Fusion

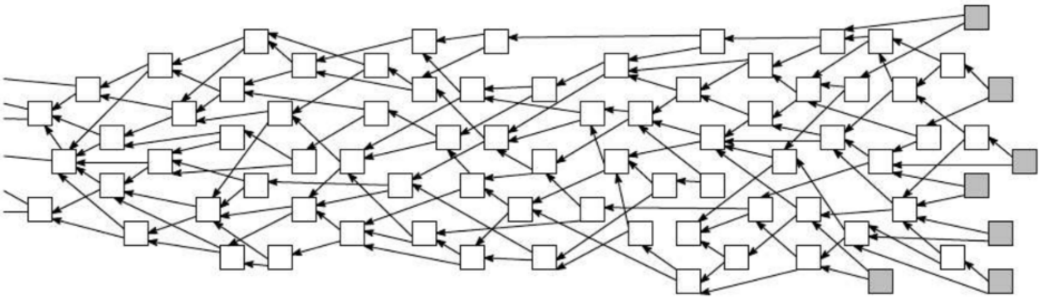
4.3 The Emergence of Distributed Ledger Technology Other Than Blockchain

Blockchain is not the only solution for distributed ledger system. Due to the trilemma of scalability, decentralization, and security we face in blockchain, more and more projects start to seek distributed ledger system solutions outside the blockchain. Currently, major distributed ledger systems beyond blockchains are:

- **Directed Acyclic Graph (DAG)**

DAG is a data structure concept from computer science. It is a graph that is directed and without cycles connecting the other edges. Unlike blockchain, there is no blocks in a DAG structure. Instead of confirming, recording data in blocks and chaining blocks one by one, in a DAG structure, each node confirms the data unit by themselves. Different units are correlated through transaction hashes, forming a data structure in one direction without cycles.

Graph 32: Structure of Directed Acyclic Graph (DAG)



Source: Wikipedia

Different from the synchronization process of a typical blockchain ledger, DAG enables asynchronous book keeping, thus supporting higher throughput and faster transactions. IOTA, ByteBall, Nano are traditional projects that use DAG, and there are more such as TrustNote, Hycon, CyberVein, etc. coming into the area.

Traditional DAG

IOTA

Innovated Tangle structure without mining and with all nodes participating in validating transactions. Every time a node initiates a transaction on the network, it must validate two previous transactions and complete a certain level of work (PoW), then wait for transactions to be validated by others. On May 3rd 2018, IOTA foundation announced the project Qubic, through which we can add smart contracts and oracles into IOTA network. This was considered as a big breakthrough for the IOTA project.

ByteBall.

Doesn't include PoW mining, and rather, ByteBall introduces main chain and witness into traditional DAG structure. Main chain is the shortest path validated by the witnesses in the disordered network and confirms all the transaction chronologically. Witnesses act as regulators in the network. They help organize the transactions according time stamps, and prevent the risk of double spending.

Nano

Formerly known as Raiblocks and changed its name into Nano in 2018. Nano created the structure of DAG Block-Lattic, instead of being single-threaded like traditional blockchain system, each account in Nano network forms an independent, separate chain that only records, maintains and updates own transactions, thus improving the network throughput. Specifically, a spender initiate a money transfer on his own chain, and conduct a certain amount of work to avoid spamming, at the same time, the receiver also records the transaction on his own chain and send it to validators. Validators will verify and broadcast the transaction to the whole

	network. If there is no conflict, the transaction will be confirmed, and if there is, a voting mechanism will be triggered.
Innovated DAG	
TrustNote	TrustNote improves the witness mechanism in ByteBall network by introducing two layers of consensus protocol. It adds a consensus layer named TrustME for witness, in which super nodes compete for witness rights. Apart from that, it also uses main chain in DAG structure to organize the transactions and to prevent double spending.
Hycon	Hycon is a Korean network based on DAG structure. It uses the SPECTRE consensus, adopts the voting algorithm between each two data units, and confirms the units pair by pair to prevent double spending in this asynchronous confirming model under DAG structure.
CyberVein	It adds an interactive smart contract layer into DAG structure, and adopts its own program language Vein and CyberVein Virtual Machine. In contrary to other DAG projects where nodes have to complete a certain amount of work before the validation process, CyberVein uses proof of contribution protocol, and rewards nodes based on their contributions to the network.

Source: Huobi Research

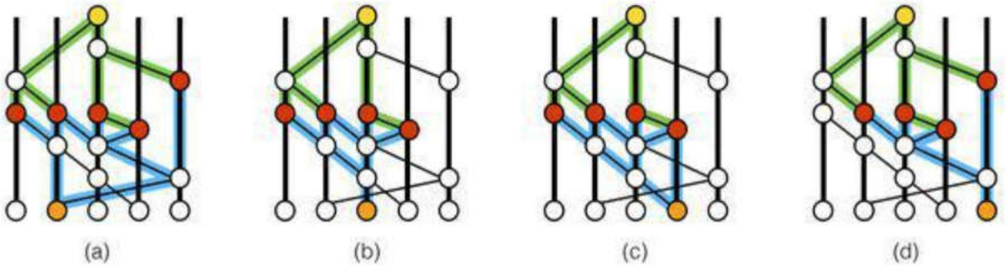
➢ Hashgraph

Hashgraph is a distributed ledger technology and data structure patented by Swirds company. Based on its innovative Gossip about Gossip protocol, each node sends his own transaction message to neighboring nodes and passes transaction messages from neighboring nodes to others. Each transaction message sent in the network includes the hash value of the transaction received from the former node and the hash value of the new transaction made by the current node.

In this way, each node in the network is aware of the message that his former node holds, thus knowing how his former node would vote. As the result, when the last node receives his message, the network reaches a consensus and confirms the transactions automatically, a process called Virtual Voting. By adopting such mechanism, hashgraph solves the complexity of sending message and latency of confirming transactions under BFT consensus.

Currently, hashgraph mainly targets at consortium blockchains in enterprise sector, and has already been able to handle 250 thousand transactions per second. However, whether hashgrapgh could be adopted in public blockchain environment is still waiting to be examined.

Graph 33: Gossip about Gossip under hashgraph structure



Source: Hashgraph

The features of hashgraph are:

- Hashgraph still uses Byzantine Fault Tolerant (BFT) algorithm, where the network can tolerate at most 1/3 of malicious nodes. If there are more than 1/3 malicious nodes in the network, the whole system would crash, and this could potentially be true under a permission-less blockchain environment.
- Unlike usual latency between transaction time and validation time under a blockchain environment, for example, using PoW consensus, if the priority of a transaction is not high enough or if it doesn't offer enough mining fee, the validator will record other transactions first. In hashgraph environment, the validation time is the same as transaction time. Once transaction initiates, the message will be transmitted through the entire network right away and get validated immediately.
- Mining doesn't exist in hashgraph, thus saving a lot of energy. Maintaining a public blockchain under traditional PoW is costly, and in a case where two different miners create two blocks at the same time, the system will automatically choose the longer chain, and abandon the other, causing a lot of waste.

Huobi Research of Blockchain Application

About us:

Huobi Research of Blockchain Application (Huobi Research) was founded in April 2016 and started research and explorations in various aspects in blockchain area since March 2018. We cover blockchain technology research, industry analysis, application innovation and economic model explorations etc. We aim to establish a research platform and to offer theoretical foundations as well as judgements of trends in blockchain to the public, ultimately promoting the development of the entire industry.

Contact us:

E-mail：	huobiresearch@huobi.com
Twitter:	Huobi_Research https://twitter.com/Huobi_Research
Medium:	Huobi Research https://medium.com/@huobiresearch
Facebook:	Huobi Research https://www.facebook.com/Huobi-Research-655657764773922
Website:	http://research.huobi.com/

Disclaimer:

1. Huobi Research does not have any form of association with blockchain projects or other third-parties mentioned in this report that could jeopardize the objectivity, independence and fairness of this report.
2. All outside information, data referenced in this report is from compliant and legitimate sources that we deem as reliable, and Huobi Research have conducted the due diligence concerning its authenticity, accuracy and completeness, but such due diligence does not provide any guarantee.
3. This report is only for reference purposes. Conclusions and viewpoints in the report do not constitute any form of investment advice on crypto assets. Huobi Research is not responsible for any losses resulting from the use of this report, unless stipulated by law. Under no circumstances should the readers give up their own investment analysis and judgements.
4. This report only reflects the opinions from Huobi Research on the day it was finalized. Future market condition changes may lead to updates of such judgements.
5. The report is copyrighted by Huobi Research, please cite the source when quote, and get approval from us when large amount of contents is referenced. Under no circumstances is reference, abridgment and modification contrary to original intention permitted.