PRESENTED BY **Huobi**.pro

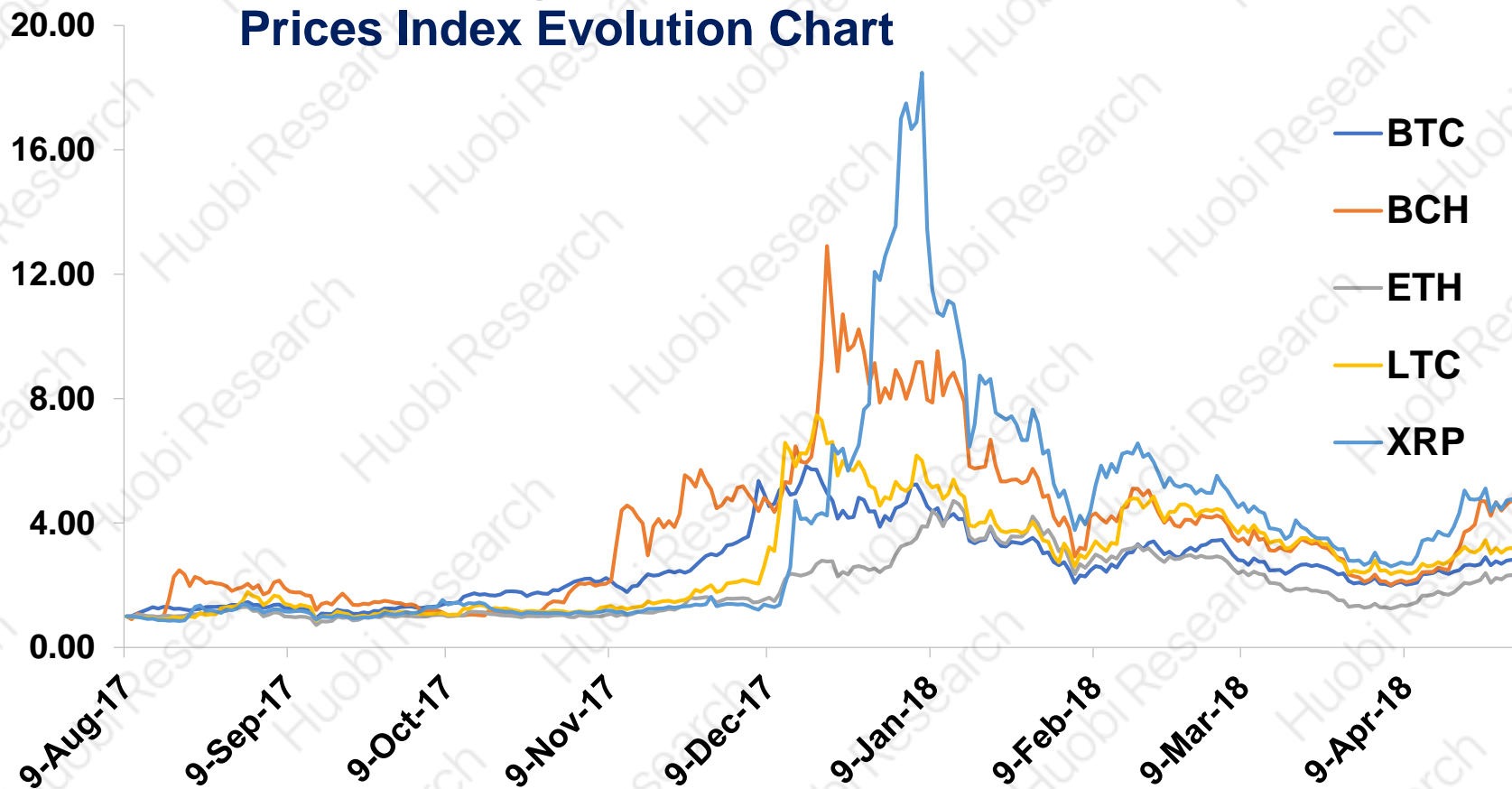**BF** | **BLOCKCHAIN FESTIVAL**
VIETNAM

**I**

# Digital Assets

# Global digital asset market outlook in 2018H1: Correction as major theme

### Top 5 Digital Assets
### Prices Index Evolution Chart



Legend:
- BTC
- BCH
- ETH
- LTC
- XRP

- *2017, digital asset market total market capitalization increased **30 times** from $17.74 billion to **$559.76 billion**.*

- *2018H1, massive retracement was triggered, Top 5 digital assets price **70% below all time high,** roughly same price level as October 2017.*

Source: Coin Market Cap, Huobi Research

# Search activity in digital asset descend sharply in 2018H1: Bitcoin declining the most

## Search Index of Digital Assets



Legend:
- Bitcoin
- Etheruem
- Litecoin
- Ripple
- Cryptocurrency
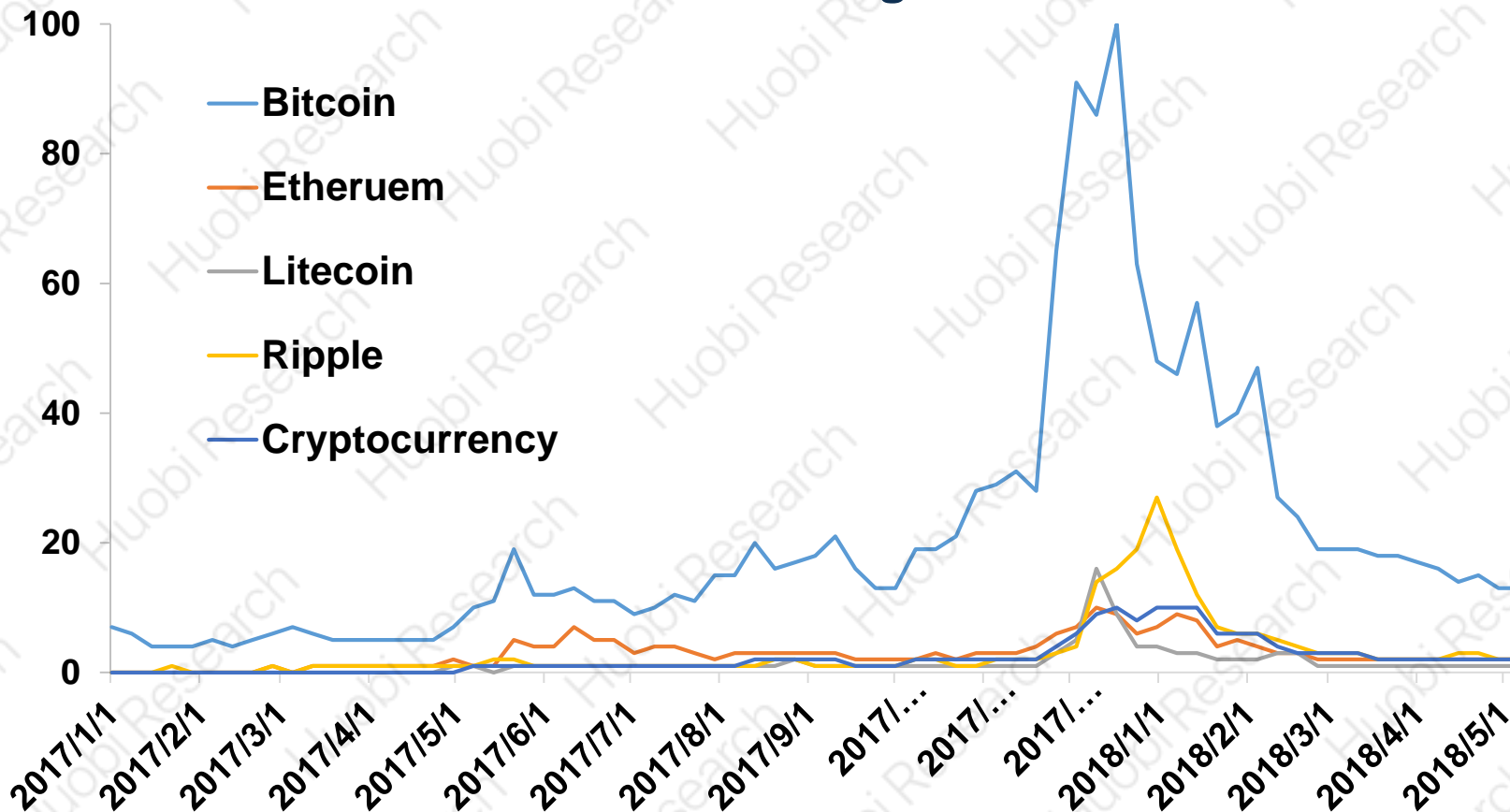
- *2017, Bitcoin was the main eye catcher, google search activities towards digital assets steadily accumulated and reached peak in December.*

- *2018H1,* **public attention on digital assets fall down quickly**. *By end of April, search index of Bitcoin only* **12%** *of peak.*

Source: Google Trends, Huobi Research

# Bitcoin Market Activity Overview in 2018H1: Trending below 2017 Average

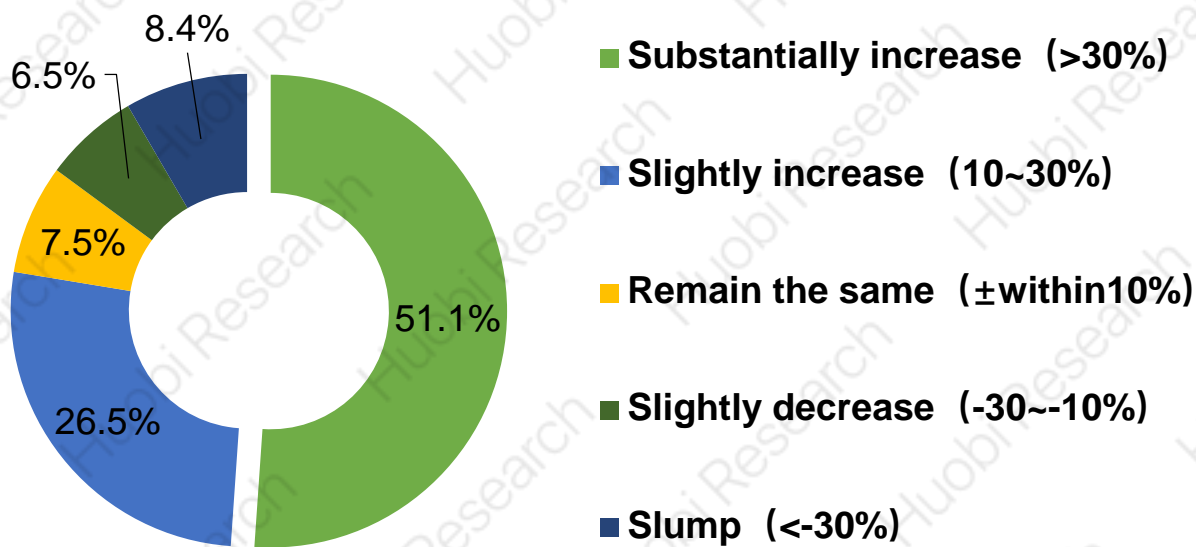## Number of Bitcoin Daily Active Addresses

### (in thousands)
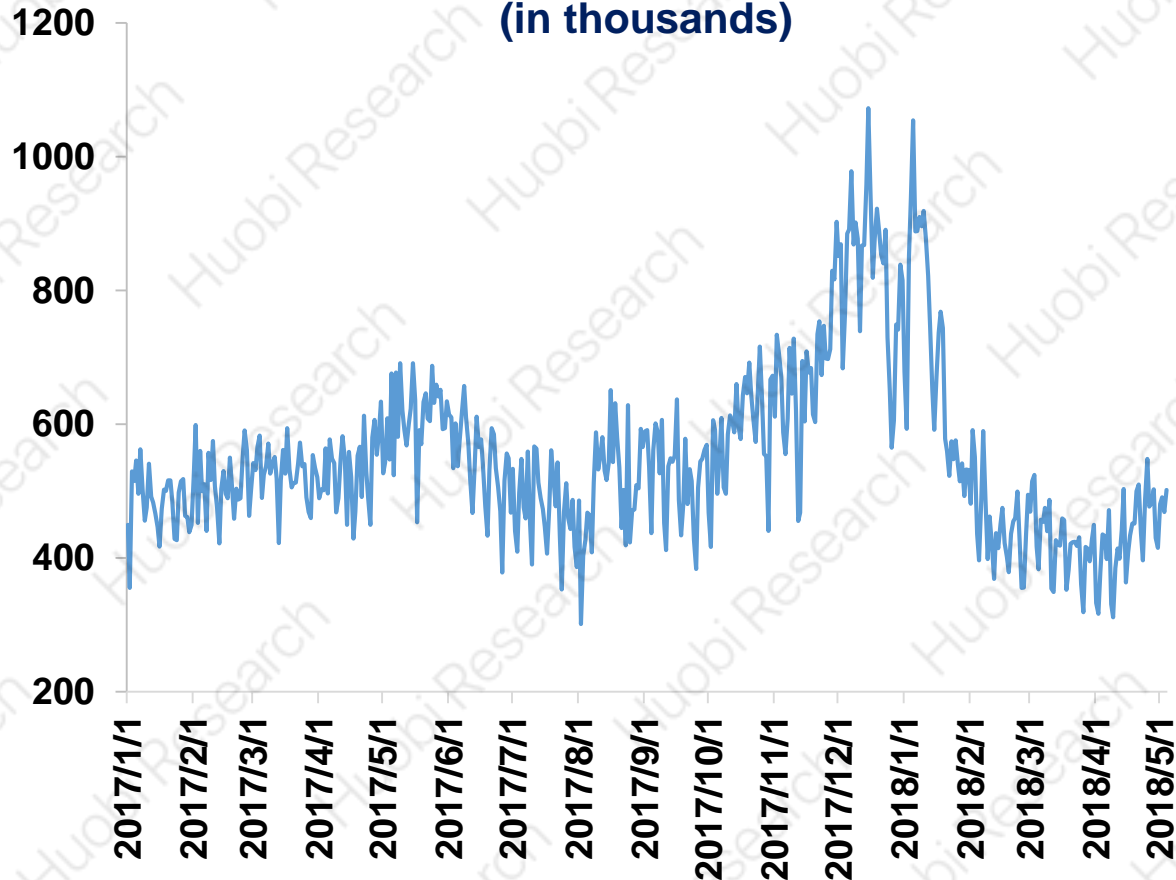


## Bitcoin Daily Transaction Volume
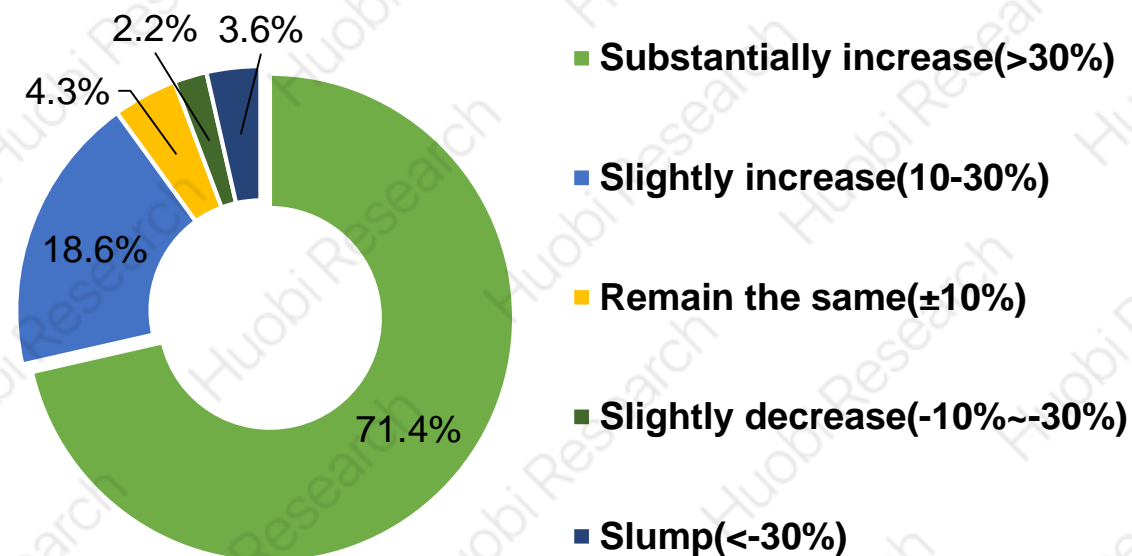
### (in thousands)



Source: Qundl, Huobi Research
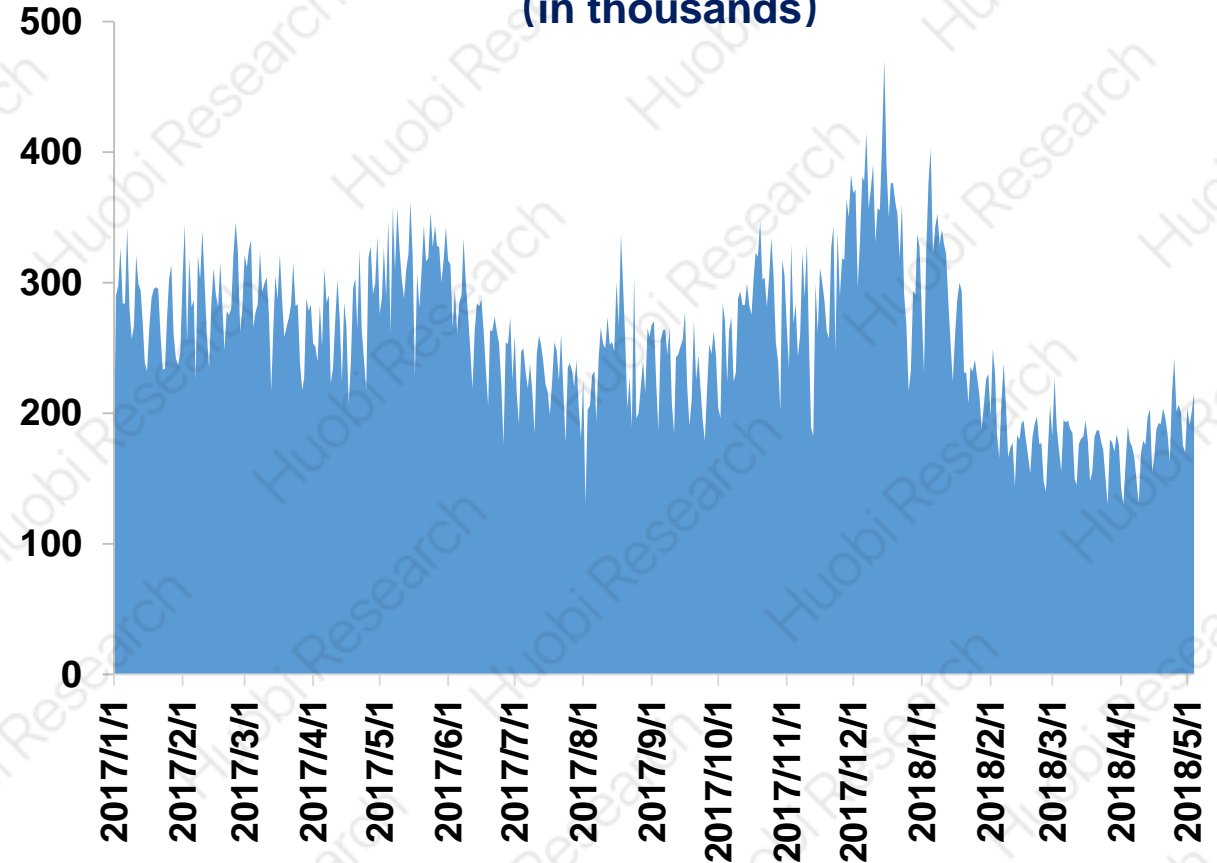
Huobi Investor Sentiment Survey: Market still bullish towards 2018H2

Investor Market Expectation—March 2018

Investor Market Expectation—April 2018

8.4%
6.5%
7.5%
26.5%
51.1%

- Substantially increase （>30%）
- Slightly increase （10~30%）
- Remain the same （±within10%）
- Slightly decrease （-30~-10%）
- Slump （<-30%）

2.2%  3.6%
4.3%
18.6%
71.4%

- Substantially increase(>30%)
- Slightly increase(10-30%)
- Remain the same(±10%)
- Slightly decrease(-10%~-30%)
- Slump(<-30%)

Higher proportion of correspondents expressed optimistic attitude towards market in 2018H2.

Source: Huobi Research

# Token Sales Market in 2018H1: Cools Down, yet capital raised still large compared to 2017

## Capital raised in token sales
## (in million dollars)
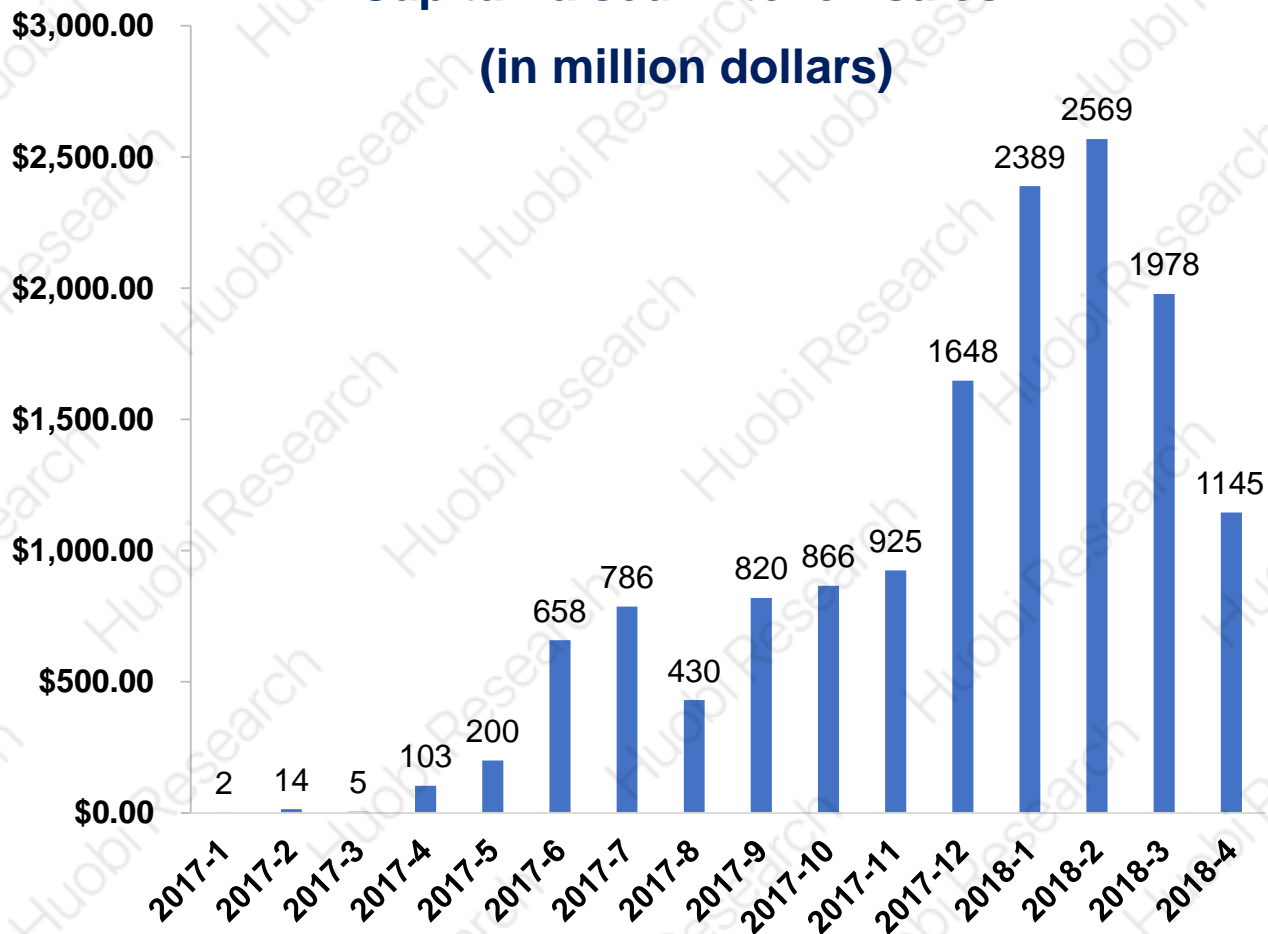


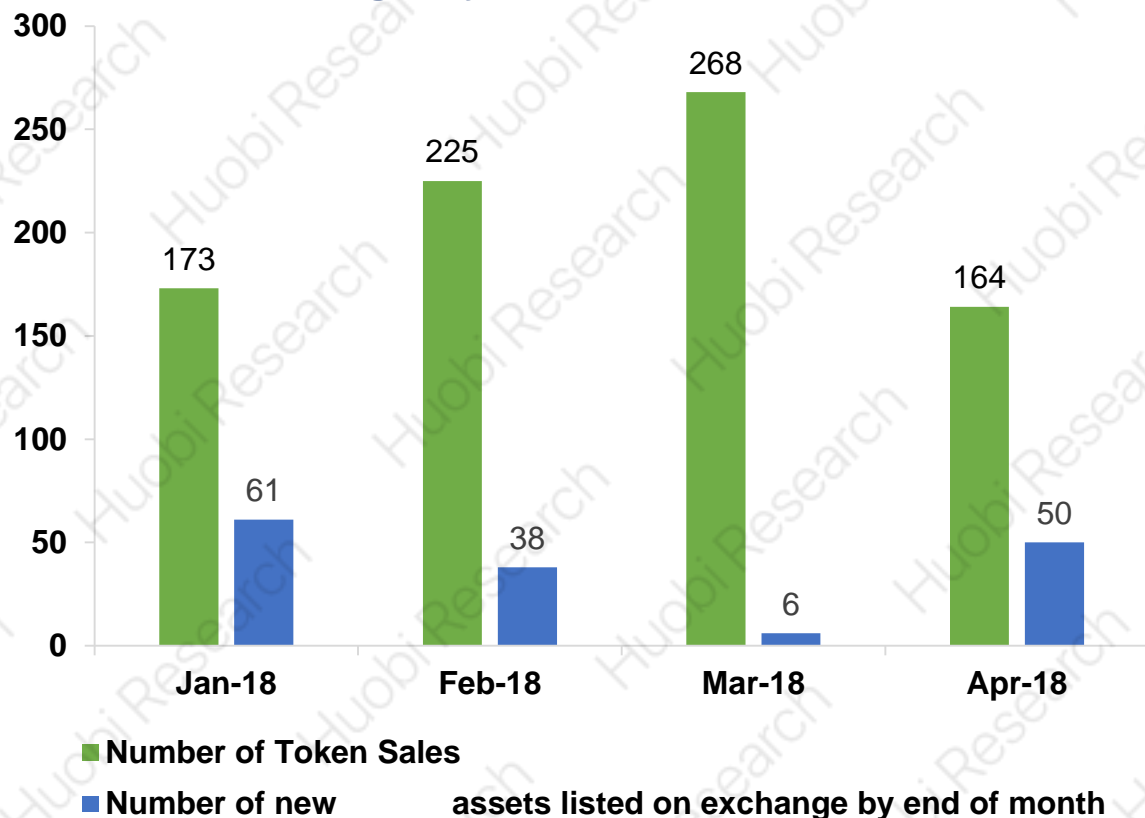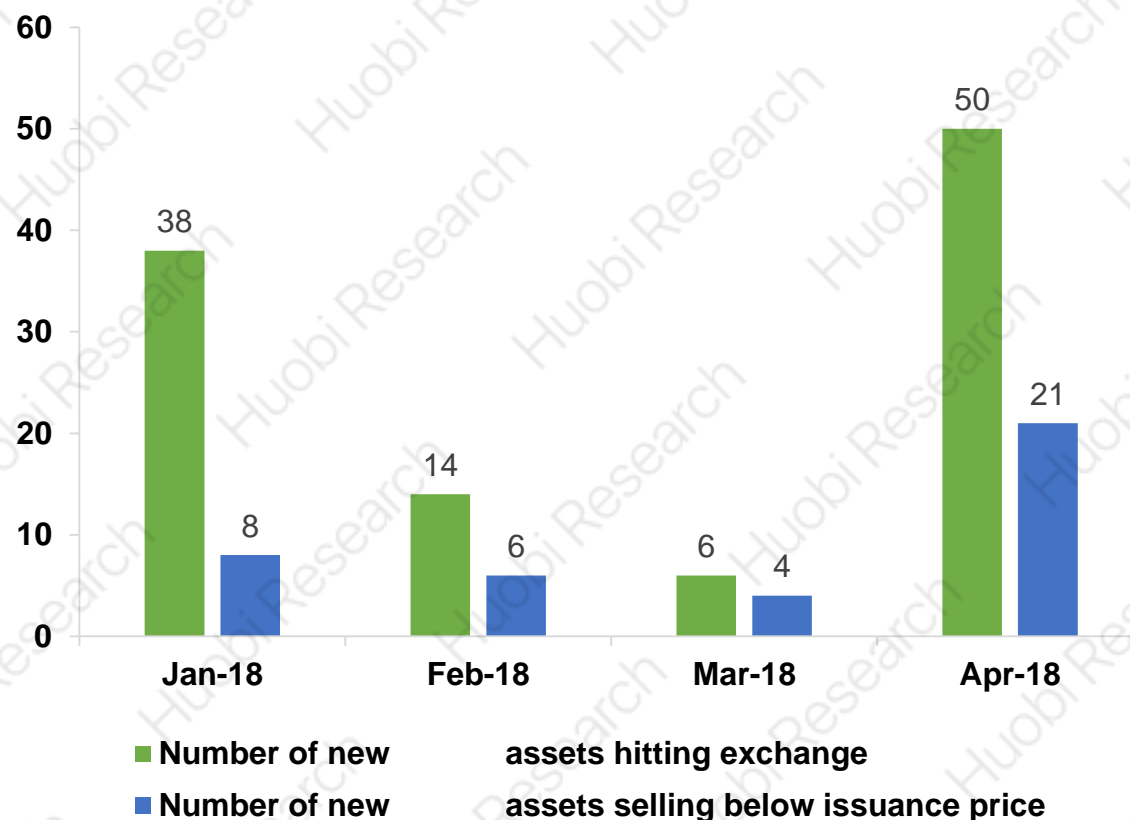## 2017 Top 10 token sales in terms of capital raised

Bancor    COMSA    Filecoin    KIN    Polkadot

Q    SIRIN LABS    TenX    tz

| Name | Project catagory | Funding time | Capital raised |
|------|------------------|--------------|----------------|
| 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 | Cryptoasset Trading | 2017.6 | $153,000,000 |
| Polkadot | Cross-Chain facility | 2017.10 | $145,171,723 |
| Qash | Crytoasset Trading | 2017.11 | $106,400,000 |
| Status | Social network | 2017.6 | $107,664,907 |
| Kin | Decentralized Exchage | 2017.9 | $98,500,326 |
| Cosma | Cross-Chain Payment | 2017.11 | $95,614,242 |
| TenX | Payment, Clearance | 2017.7 | $80,000,000 |
| **Total** | | | **$1,431,735,907** |

Source: Huobi Research

# Token Sales Market 2018H1: Selling below issuance price becomes common, liquidity shrinks

## Number of new digital assets listing on exchange by end of token sales month

## Number of new digital assets price falling below issuance price



■ Number of Token Sales
■ Number of new          assets listed on exchange by end of month

■ Number of new          assets hitting exchange
■ Number of new          assets selling below issuance price

Source: Huobi Research

# Digital asset crowd funding: New trend is emerging

## Token sales are remodeling：DAICO



DAO

* Leverages wisdom of crowds
* Does not fully trust single centralized team
* Funding can be spread over time

DAICO

ICO

* Based around single project
* No 51% attack risk

*Better utilization of investor funds and improved relationship* between investors and developers, funding spread over time or milestones.

*If either party i.e., investors or developers are not happy with the progress of the project development, they can **vote to deactivate the DAICO***.

Source: Huobi Research

## Digital asset crowd funding: New trend is emerging

### Raise capital in the form of securities: United States as an example

**Reg A+ Regulated Token Sales**

**Reg D Regulated Token Sales**

- *Raise up to 50 million dollars in 12 month*

- *Solicitation to public investors permitted*

- *Applicable to public investors*

- *Shares tradable immediately after sale*

- *Unlimited capital raising amount*

- *Solicitation not allowed, private disclosure*

- *Only open to accredited investors*

- *12 month restricted sale period*

Source: Huobi Research

# Looking back: Compared to previous 2 bull market, what's different this time?

## First Bull market:
## BTC came into public eye

**Bitcoin price 2011.4 to 2011.6**



$35
$30
$25
$20
$15
$10
$5
$0
2011/1/10    2011/6/10    2011/11/10

## Second Bull market:
## P2P cash consensus

**Bitcoin price 2013.1 to 2013.12**



$1,400
$1,200
$1,000
$800
$600
$400
$200
$0
2012/11/6    2013/11/6    2014/11/6

## Third Bull market:
## Smart contract consensus

**Bitcoin price 2017.1 to 2017.12**



$25,000
$20,000
$15,000
$10,000
$5,000
$0
2017/1/1    2017/7/1    2018/1/1

Source: Huobi Research

# Looking back: Compared to previous 2 bull market, what's different this time?

**Bitcoin dominance**

**87.32%** vs **40.99%**

**BTC/ETH Market Cap**

**13x** vs **96x**
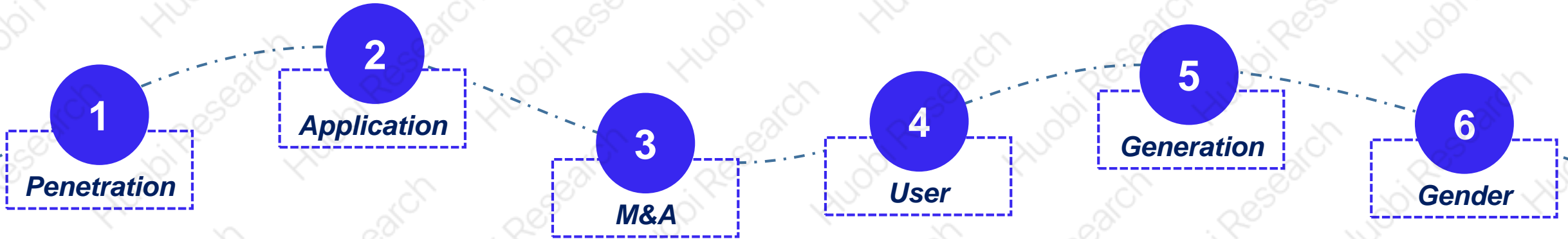
**No. of Digital Assets 17/18**

**637** vs **1335**

**BTC/ETH Addr No. Increase**

**1x** vs **18x**

*We are moving from **consensus on peer to peer cash like bitcoin**, to **consensus on blockchain and smart contract themselves**. That is, the things supporting the market from behind is becoming people's belief in the ability of blockchain to revolutionize our living world.*

Source: Huobi Research

## Looking ahead: What would be the rationales driving the market?

**1** Penetration

**2** Application

**3** M&A

**4** User

**5** Generation

**6** Gender

*In long term,*

- *Paradigm shift from **"investment-driven"** towards **"invest + application" driven**.*

- *Various **use cases and demands will be tokenized on-chain** and reflected in market cap.*

- *Token-Fiat currency transaction will decline, **Token-Token exchanges expected to grow***

# Rational 1. Penetration：Digital Assets finance VS Traditional finance
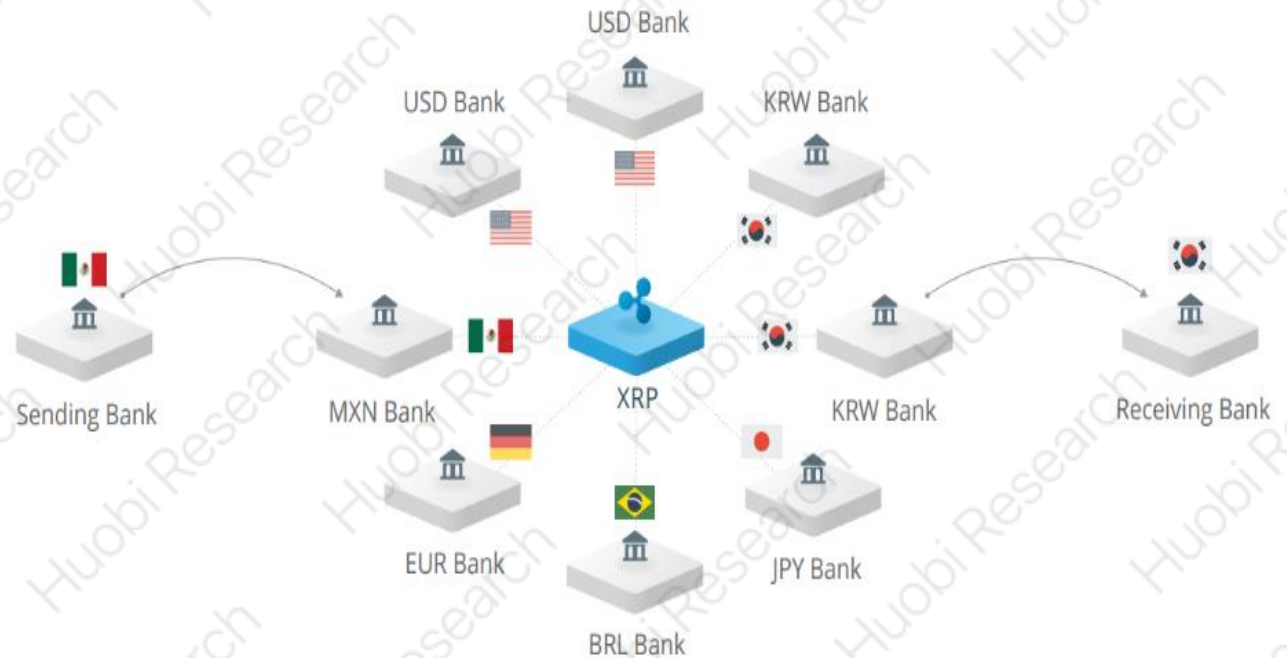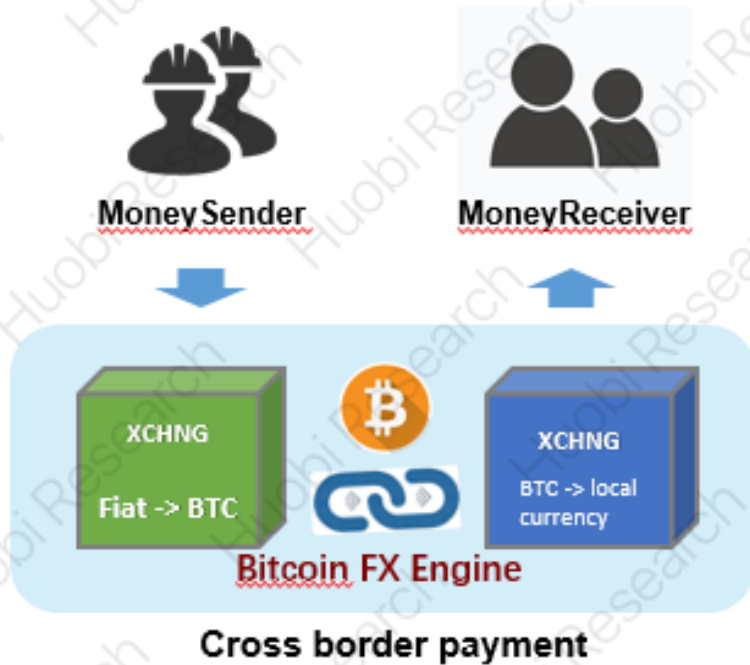


- ***Promote financial inclusion*** *in under developed areas, realize true peer to peer finance in a trustless environment*

- *Distributed ledger and smart contracts can be adopted in clearing and other financial back office,* ***reducing the cost of operation***

# Rationale 2. Application: Only "use case + blockchain" could set the market on fire

## "Blockchain + use case" : Bottom to top



**"CryptoKitty"** as example:

**Premature way of playing**

- *Seek appropriate use cases for technology*

- *Target digital assets community, highly speculative*

## "Use case + blockchain" : Top to bottom



- *Apply technology to real use cases*

- *Target general public, optimize user experiences*

# Rationale 3. Merger & Acquisitions: Blockchain acquiring internet killer applications

- *IPO in Traditional Financial Market VS Token sales in Crypto Market*

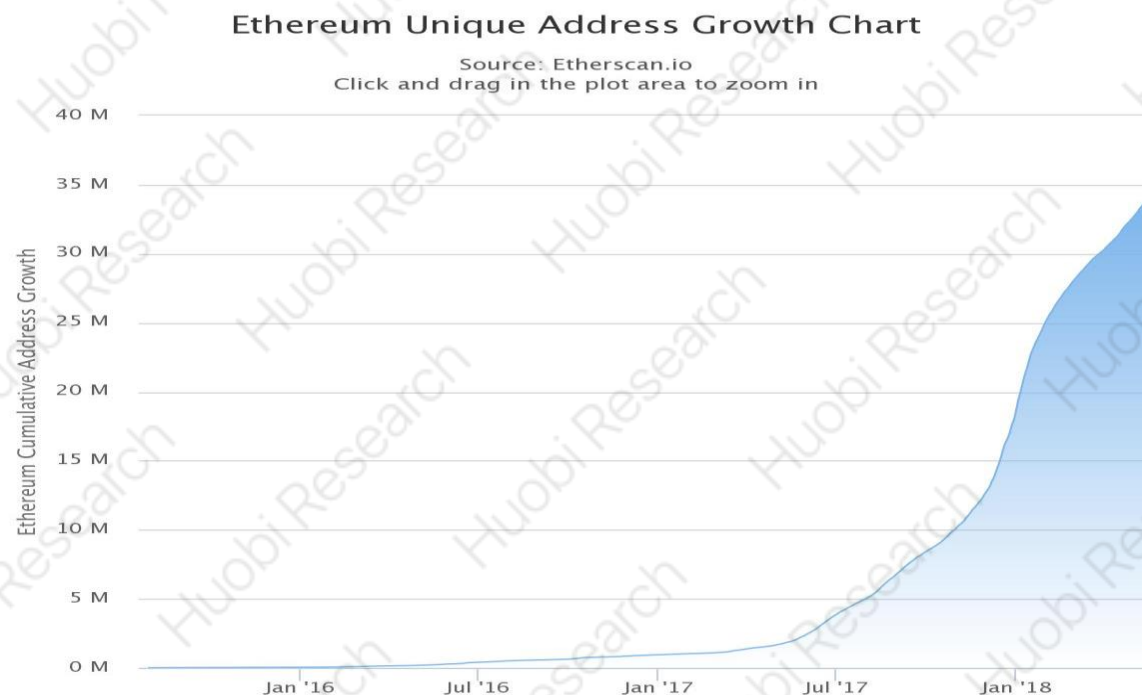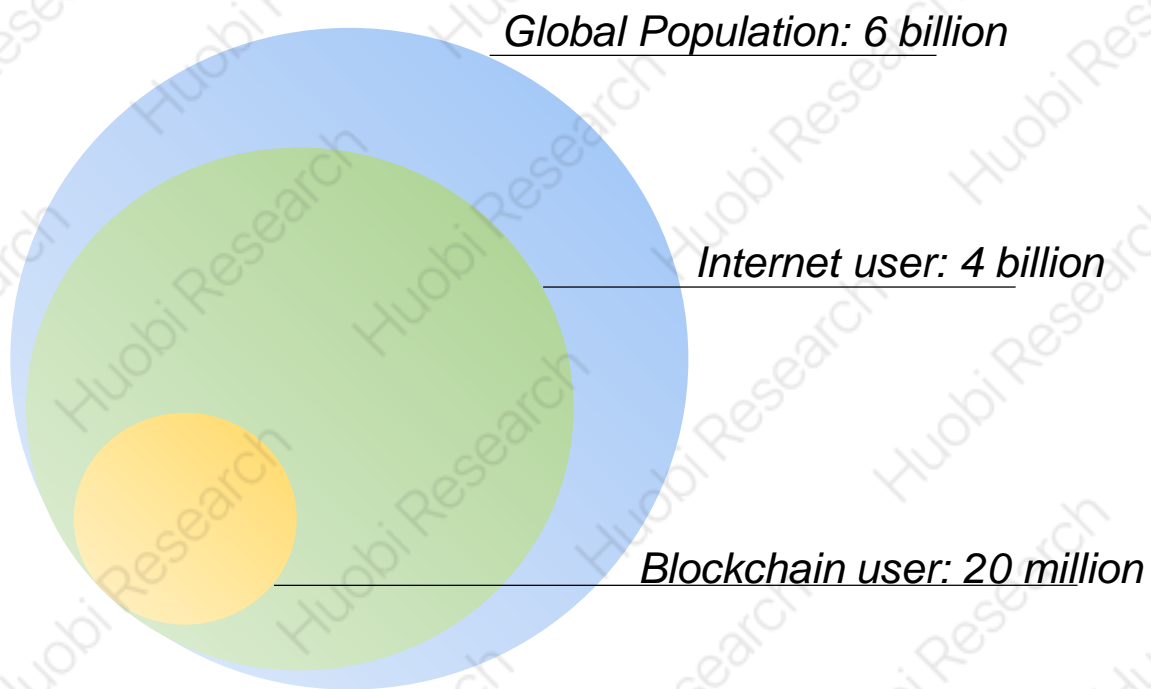- *M&A in Tradition Financial Market VS ?*

*Our thoughts:*

- *Great numbers of blockchain platforms, to supplement its own Dapp eco-system, would start to acquire quality internet applications.*

- *New exit strategies may be created by moving internet start-ups on chain.*
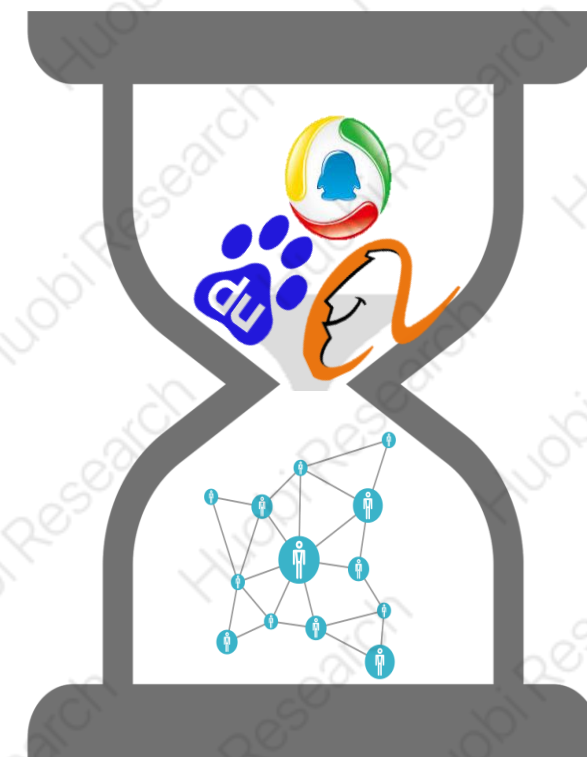
# Rationale 4. User: blockchain user base will keep growing, pushing up market activity
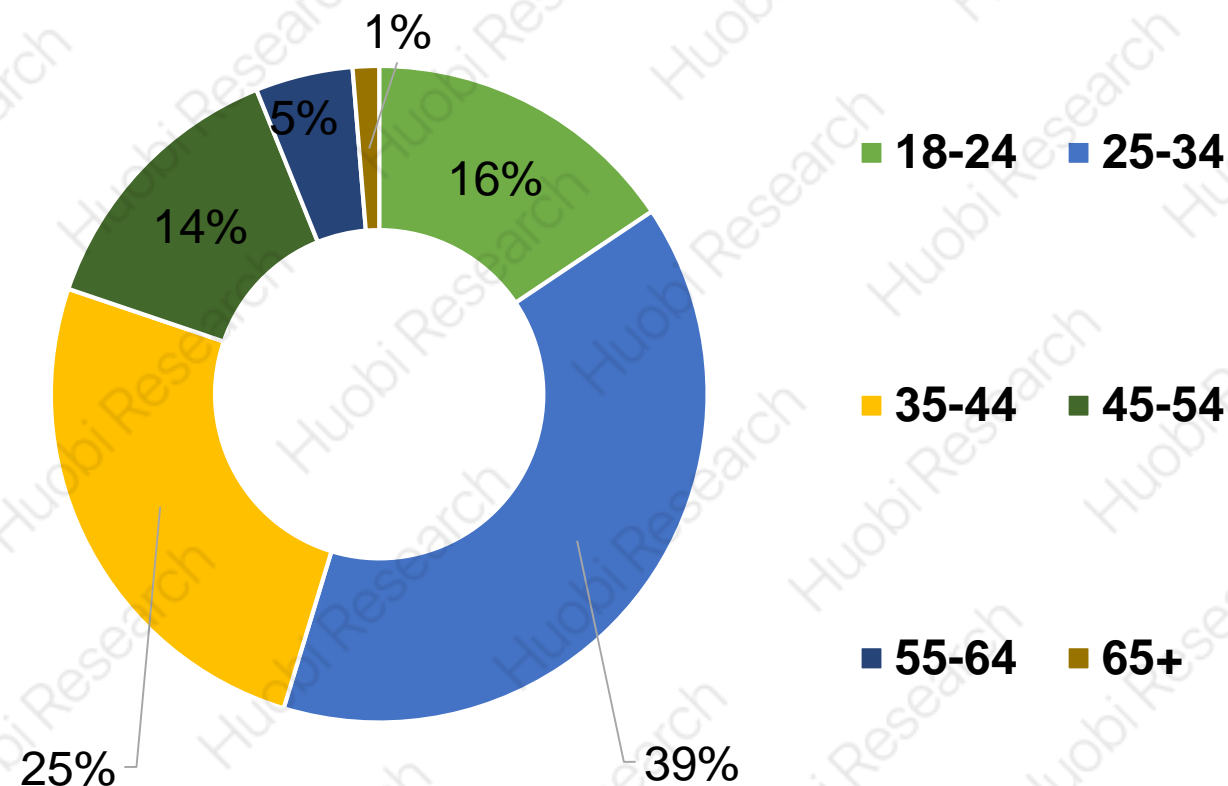
- *Ethereum unique addresses roughly 34 million, actual user about 20 million, **0.3 % of world population** and **0.5% of internet user base**, still great potential.*

*Global Population: 6 billion*

*Internet user: 4 billion*

*Blockchain user: 20 million*

### Ethereum Unique Address Growth Chart

Source: Etherscan.io
Click and drag in the plot area to zoom in



Source: Huobi Research

# Rationale 5. Generation: from younger generation to the masses

- *According to our research, most of the participants in Bitcoin community **are between 24-34 years old, 39% of total.***

- *55% of the participants in total are under 35 years old，**decreased from 60% in 2015 announced by CoinDesk, digital assets are gradually accepting by masses.***

## Age Structure of Bitcoin Community



Legend:
- 18-24
- 25-34
- 35-44
- 45-54
- 55-64
- 65+

Values: 1%, 16%, 5%, 14%, 25%, 39%

Source: Huobi Research

# Rationale 6. Gender: From male to female

- *According to our research, currently, about* ***17% of the bitcoin community participants are females****, the left* ***83% are males****. Gender divide exists.*

- *However, proportion of female participants are higher than before, according to Coindesk, 2015, only 10% are female.*

Source: Huobi Research

## Gender structure of Bitcoin Community



17%

83%

■ **Female**

■ **Male**

II
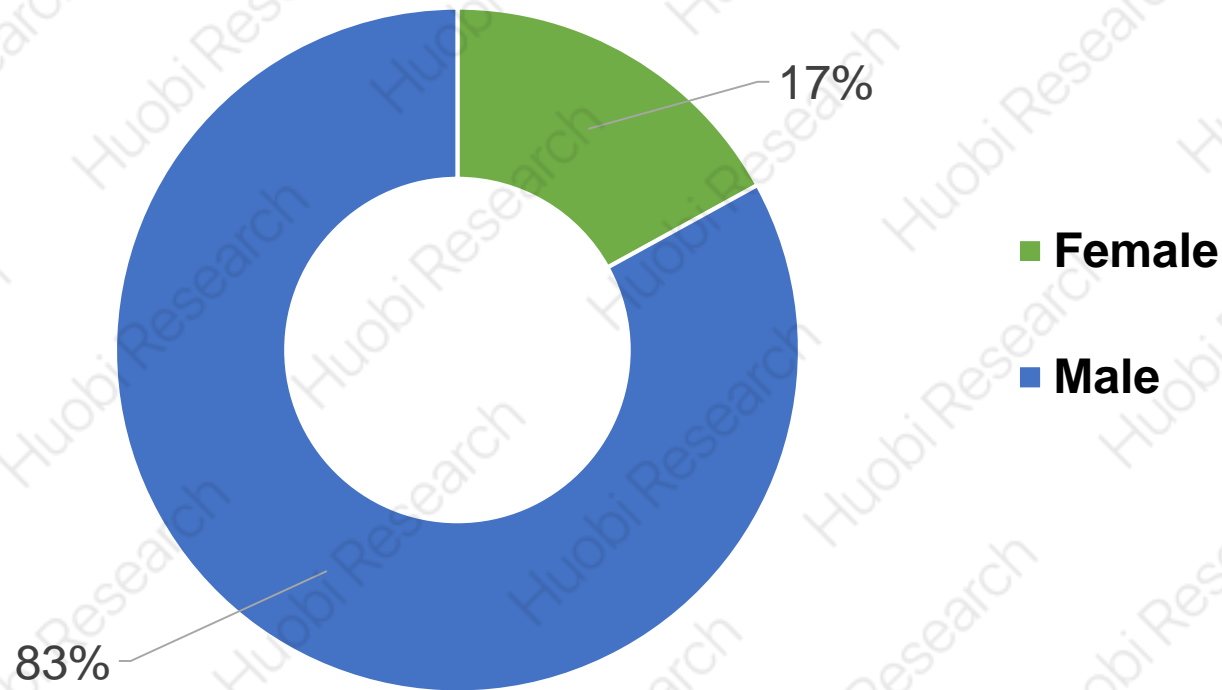
Regulation

# Global digital asset regulation outlook

- *Whether digital assets are permitted to be used as **payment tool***

- *Whether **digital assets exchanges** are permitted to operate*

- *Whether **token sales** is permitted*

- *Whether **investments in digital assets** are permitted*



Source: Huobi Research
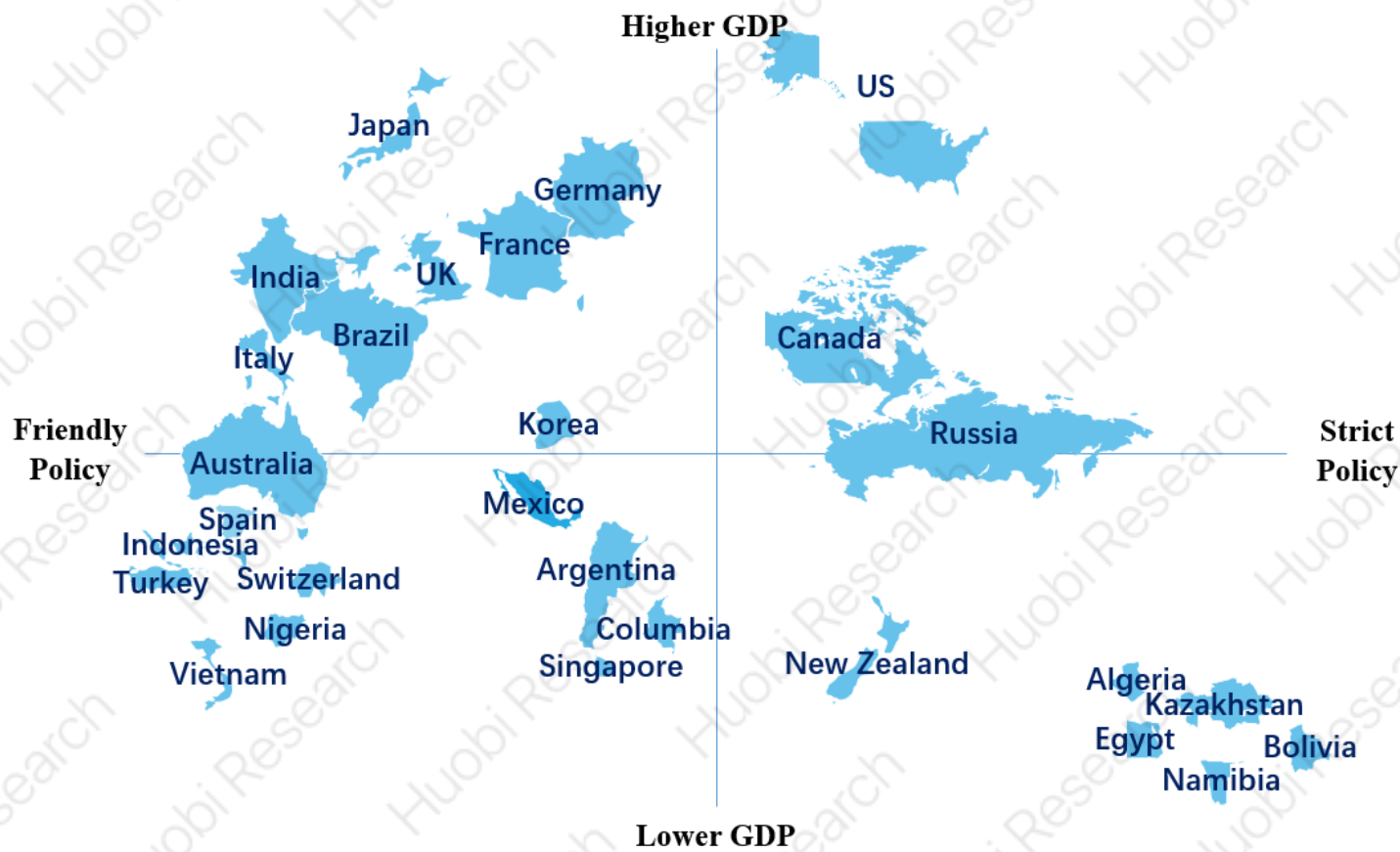
**Trend 1:** **The US may become a good regulation example and be followed by other countries**

**Classified supervision:"utility token"and"security token"**

- *Internal Revenue Service (IRS) takes digital assets **as commodities rather than currencies***

- *Different states apply different policies, mostly apply **license scheme**, yet security tokens need to be traded on SEC registered national exchanges, which currently most digital exchanges don't belong*

- *Namely, digital asset crowd funding is permitted, yet regulation, especially **regulations to potential security tokens are strengthening***

Source: Huobi Research

**Trend 2:** Both centralized regulators and self-regulatory organizations will play important roles

## Centralized regulation: license scheme

## Self-regulatory organization

- On April 1, 2017, the "Payment Service Amendment Act" took effect, Bitcoin was recognized as **legal tender**

- *Digital* **assets exchanges be authorized** by the Ministry of Finance of Japan (MFJ) and Financial Services Agency (FSA)

- No relevant laws concerning the legal status of digital assets, yet payment not prohibited.

- Exchanges only required to register as E-commerce platform, **South Korean Blockchain Association** published "Digital Assets Exchange Self-regulation Control Project" **to impose more requirements.**

Source: Huobi Research

III

Industry

# 5 Major Segments of Blockchain Industry

| Hardware and Infrastructure | Provides, integrates hash power and hardware support for the blockchain systems |
| Platforms | Provides development platform, underlying architecture for blockchain applications |
| Middle Layer | Make blockchain easier to deploy and be used to serve applications developers and users |
| Service | Provide professional services for industry participants, mobilize the circulation of capital and information |
| Application | Apply blockchain technology to various industries and use cases to serve end users |

# Hardware and Infrastructure: Oligopoly starts to appear among the hardware producers

**Chip manufacturers (including OEM)**

NVIDIA   AMD   HISILICON

**Mining Hardware Producers**

BITMAIN   EBANG   Canaan

**Mining Pool**

ANTPOOL   ViaBTC   f2pool

**ASIC Mining** vs **GPUs Mining**

**Future Trends**

1. Leading effect in hardware producers will be more apparent

2. GPUs mining will coexist with ASIC mining

3. Opportunities arise in low-energy mining

# Platforms: It was and will continue to be the segment with severest competition
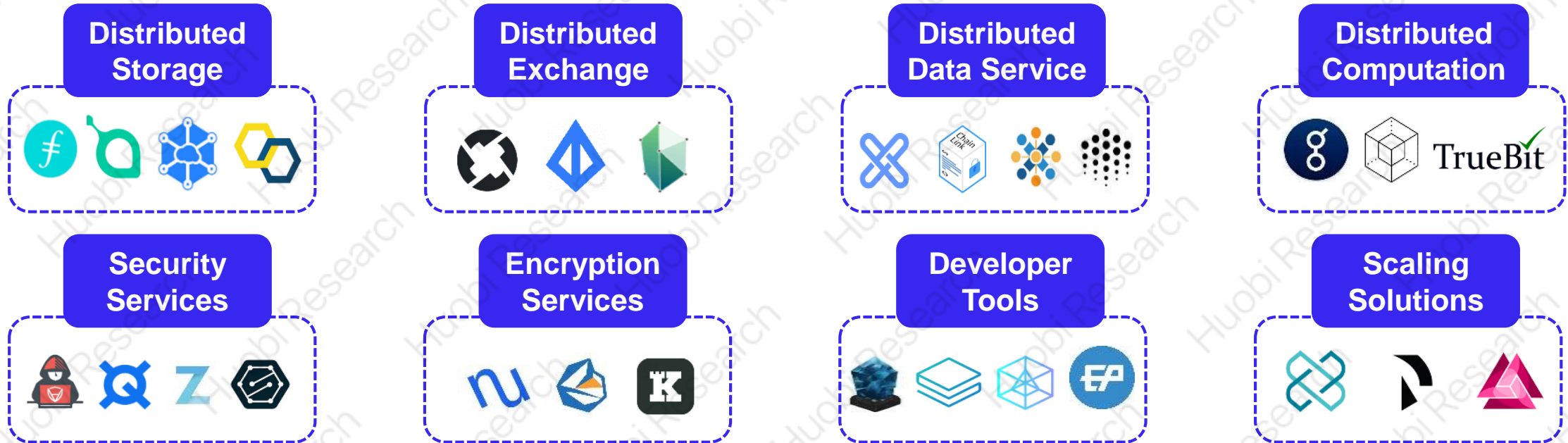
**General Platform**

**Vertical Platform**

**Future Trends**

1. *Cross-chain interoperability becomes an important criterion*

2. *Performance no longer the only criterion, "developer-friendly" will become demanded*

3. *Opportunities in blockchain platforms for specific sectors will appear*

# Middle layer: where great opportunities lie, "sweet spot" in blockchain

**Distributed Storage**

**Distributed Exchange**

**Distributed Data Service**

**Distributed Computation**

**Security Services**

**Encryption Services**

**Developer Tools**

**Scaling Solutions**

**Future Trends**

## *Virtuous Circle:*

1. *The emergence and maturity of middle layer would accelerate the landing of Dapps*

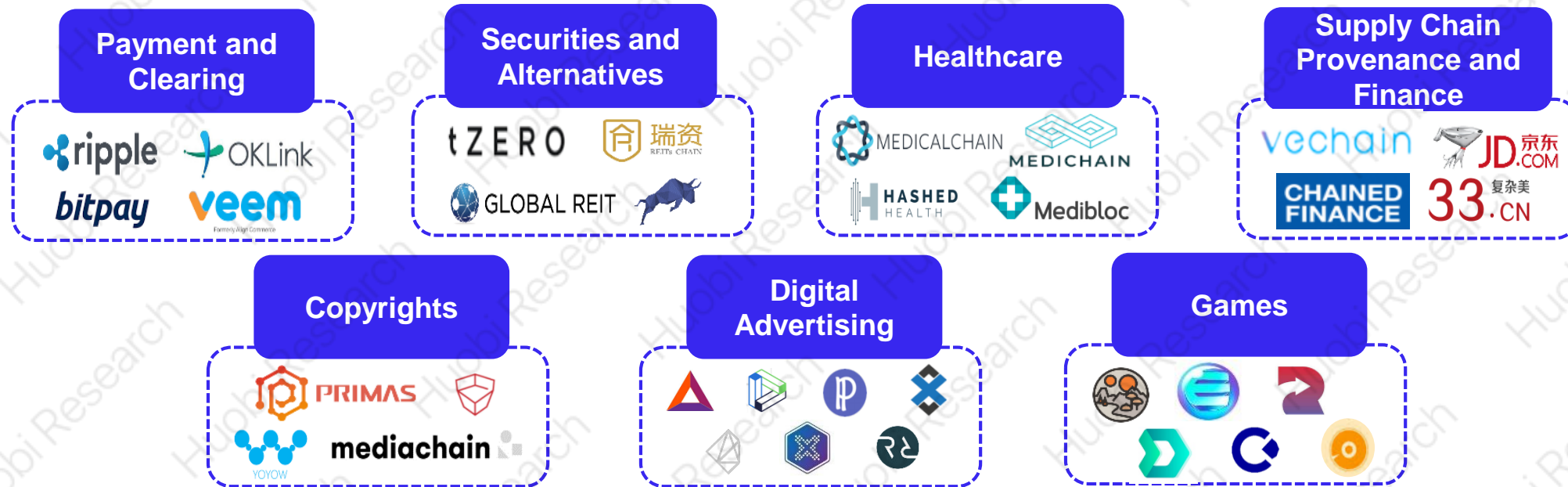2. *The development of Dapps in verticals would in turn induce new demands*

# Service layer: where integration like the internet happens

**Digital Assets Exchange**

Huobi  BINANCE
OKEX  gate.io  NEX
BITTREX  bithumb  IDEX
POLONIEX  BITFINEX

**Media and Communities**

coindesk  BITCOIN MAGAZINE
金色财经  巴比特 服务于区块链创新者
币世界 BiShiJie.com  链得得
火讯财经 HUOXUN.COM  火星财经

**Market Quotes and Information Service**

AICoin www.aicoin.com
非小号
MyToken  CoinGecko

**Digital Assets Wallet**

imToken  Huobi Wallet
KCASH  qbao

**Future Trends**

1. *Decentralized and centralized digital assets exchange will co-exist*

2. *Market quotes and information providers can potentially provide* **one-stop trading** *services*

3. *Wallets may become* **the entrance for distributed applications** *in longer run*

**Application layer:** Adoptions of blockchain technology start to arise in some sectors

**Payment and Clearing**

**Securities and Alternatives**

**Healthcare**

**Supply Chain Provenance and Finance**

**Copyrights**

**Digital Advertising**

**Games**

*Common Features of the sectors needing blockchain:*

1. *There are inefficient communications and high costs of trusts*

2. *There are strong demands for data validation and consensus*

3. *There are needs for massive data sharing and high-computing power*

**IV**

# Technology

# Moving from centralized coordination to decentralized cooperation

## Centralized coordination

## Decentralized cooperation

VS
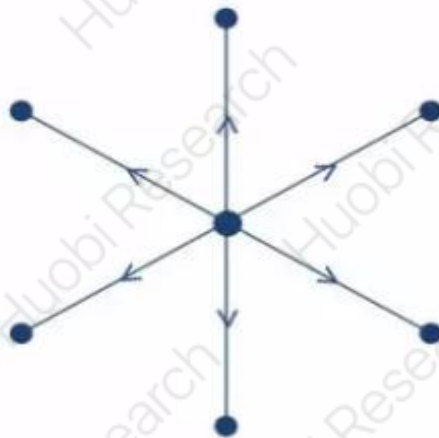
- *Needs a trustworthy third party (Center)*

- *Issue of costs, privacy, and trusts*

- *Open, distributed and equal network environment*

- *Enables cooperation on a large-scale*

# We are now on the third stage: Building a public & decentralized economy
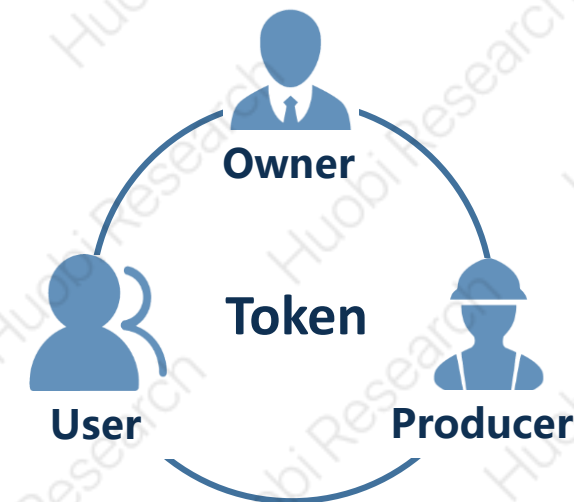
## 1.0 P2P Network
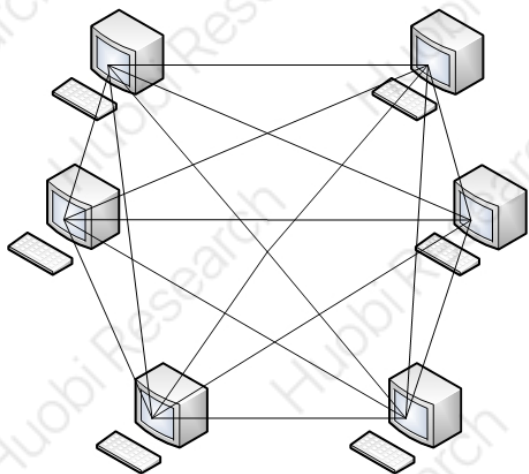


- *P2p communication & transmission*
- *Example of application:* **BitTorrent**

## 2.0 Distributed ledger



- *Records transactions in a cryptographic, distributed way*
- *Example of application:* **Bitcoin**

## 3.0 Distributed economy



Owner

Token

User          Producer

- *Replace employment relationship with "action-reward" mechanism*
- *Example of application:* **Dapps**

# Current Technology Bottlenecks in Blockchains

**Scalability**

- **Current bottleneck**
  - *Slow transactions validation*
  - *Weak transaction handle capability*

- **New Solutions**

*Improvement on consensus mechanism*

*Improvement on transaction validation*

**Privacy**

- **Blockchain characteristics**
  - *Transparant, traceable, verifiable;*
  - *Not completely anonymous*

- **New Solutions**

*CoinJoin, ring signature, zero-knowledge, invisable internet*

**Inter-operability**

- **Current Problems**
  - *Assets are not transferrable*
  - *No communications and interactions*

- **New Solutions**

*Notary schemes, relay, sidechain, distributed private key, hash locking*

# Scalability: scalability is the fundamental of high-scaled applications

## Consensus Mechanism Improvement

■ *PoS*

*No computation, replace miners with validators*

**COSMOS**    **Cardano**    **Thunderella**

■ *dPoS*

*Delegates selected from voting records transactions*

**EOS**    **BitShares**    **Steemit**

■ *pBFT/dBFT*

*Improves BFT protocol with PoS/dPoS*

**NEO**    **HyperLedger**

## Transaction Validation Improvement

■ *Sidechain and state-channels*

*Off-chain: Transaction processing & smart contract running*

*Main chain: Only a settlement layer*

■ *Sharding*

*Divides transactions into groups (shards)*

■ *Sub-chain and layered structure*

*Smart contract running & ledger clearing in different layers*

**MOAC**

# Privacy: How to take advantages of good features of public chain while maintain the privacy

## CoinJoin

**DASH**

- *Combines multiple payments from multiple spenders into one single transaction;*
- *Initiators choose master nodes randomly, thus mix transactions among them*

## Ring Signature

- *Actual transaction senders (signer) are combined with non-signers to form a ring, thus mask the origin of the transactions*

**Monero**

**Privacy**

## Zero-Knowledge

**Zcash**

- *Conceal transaction information: sender, receiver and amount;*
- *Only those with private keys have full access to the information*

## Invisible Internet

- *Combined with Onion Router Project;*
- *User information such as IP addresses is concealed, hard to trace*

**Verge**

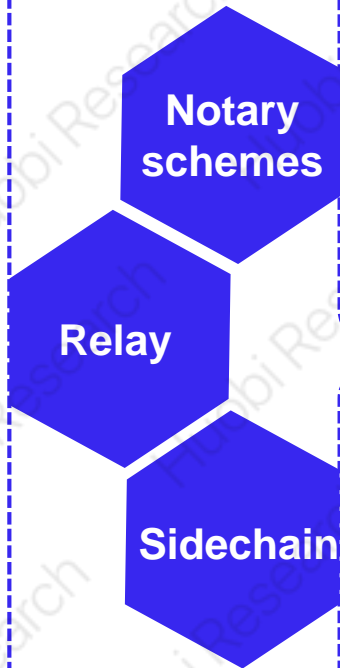# Interoperability: key for communication between isolated blockchain eco-systems 1/2
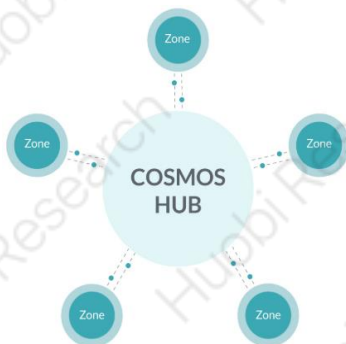


**Cosmos:**
- *Hub + Zones: "IBC" Protocol*
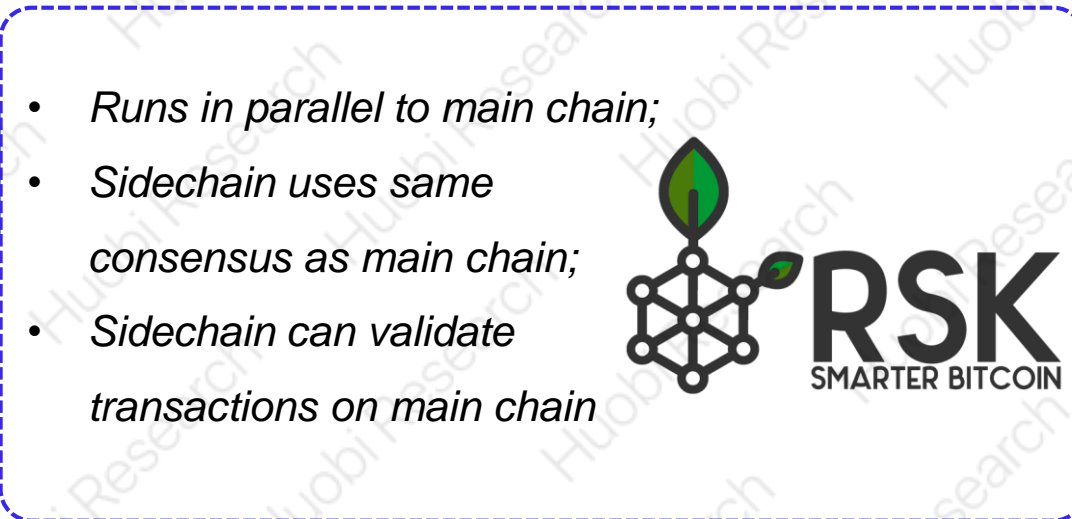- *Free token transfer via Hub*
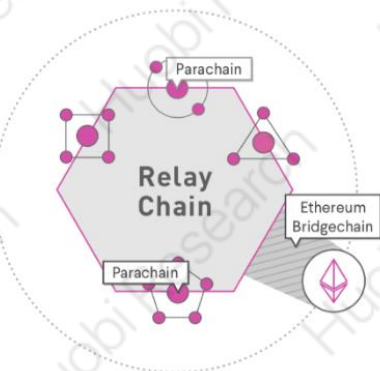
**Polkadot:**
- *Relay Chain + Para Chain*
- *Free cross communication*
- *Bridge to other chains*

**Notary schemes**

**Relay**
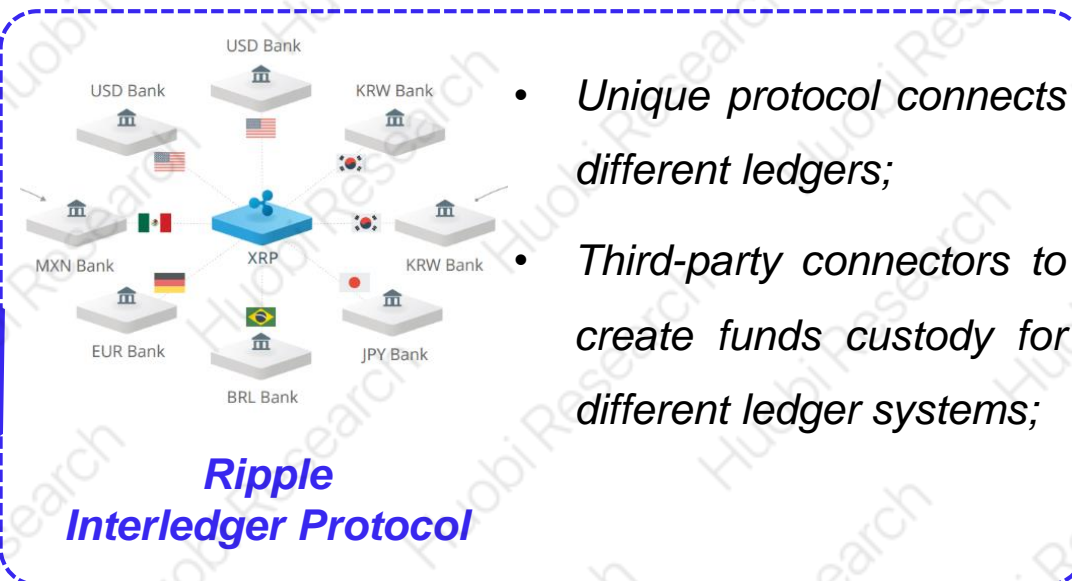
**Sidechain**



- *Unique protocol connects different ledgers;*
- *Third-party connectors to create funds custody for different ledger systems;*

**Ripple
Interledger Protocol**

- *Runs in parallel to main chain;*
- *Sidechain uses same consensus as main chain;*
- *Sidechain can validate transactions on main chain*


RSK SMARTER BITCOIN

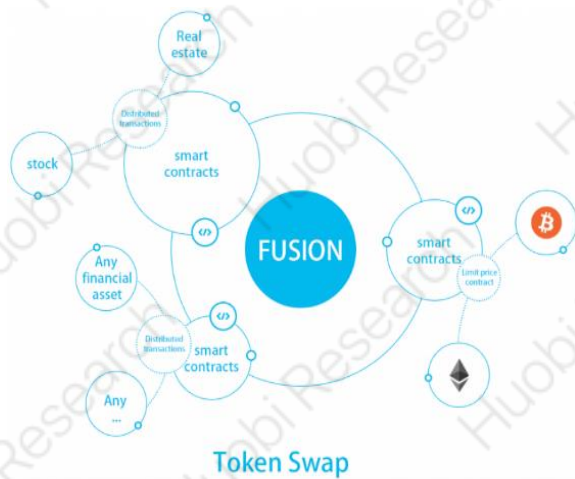# Interoperability: key for communication between isolated blockchain eco-systems 2/2
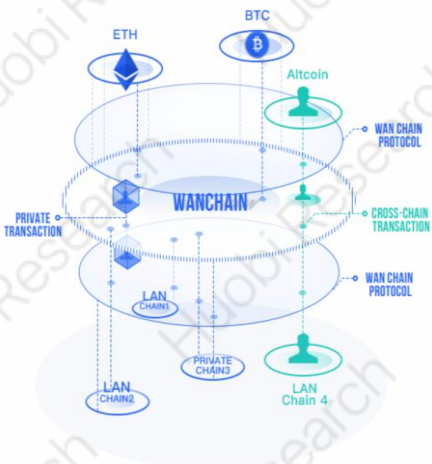


## WanChain

- *Multi-party computation + ring signatures;*
- *Cross-chain locked account*
- *Assets on original chain pegged on WanChain assets*

## Fusion

- *Distributed private key mngt*
- *Map digital assets onto Fusion chain – lock in;*
- *Ceases smart contract and releases mapping – lock out*
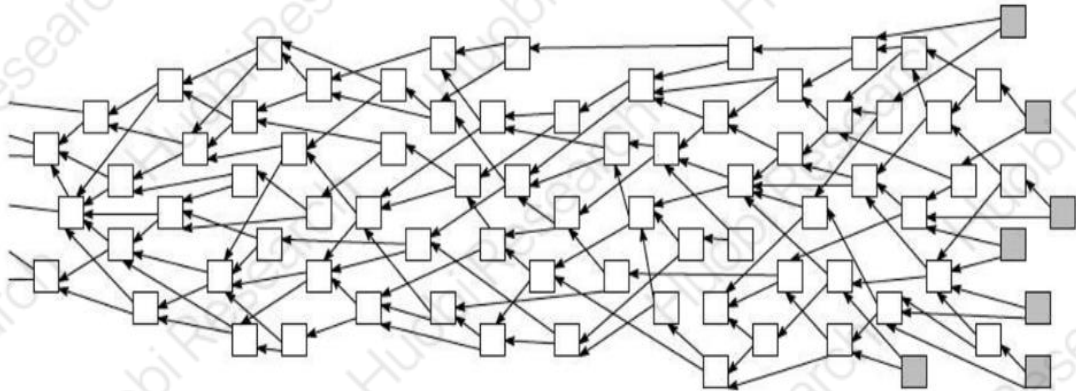
**Distributed private key**

**Hash locking**

*Between Bitcoin and Litecoin (homogeneous blockchain)*

- *Establishing off-chain payment channels between different blockchains;*
- *A path made up of multiple payment channels*

RAIDEN NETWORK

# Emergence of Innovated Distributed Ledger Technology Other Than Blockchain

## Directed Acyclic Graph (DAG)

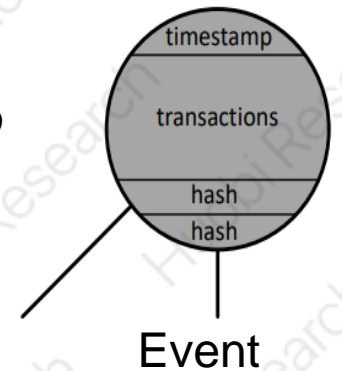

## Hashgraph



(a)   (b)   (c)   (d)

- *Asynchronous book keeping*

- *No blocks, each node confirms the data unit themselves.*

- *Different units are correlated through tx hashes, forming a data structure in one direction without cycles.*
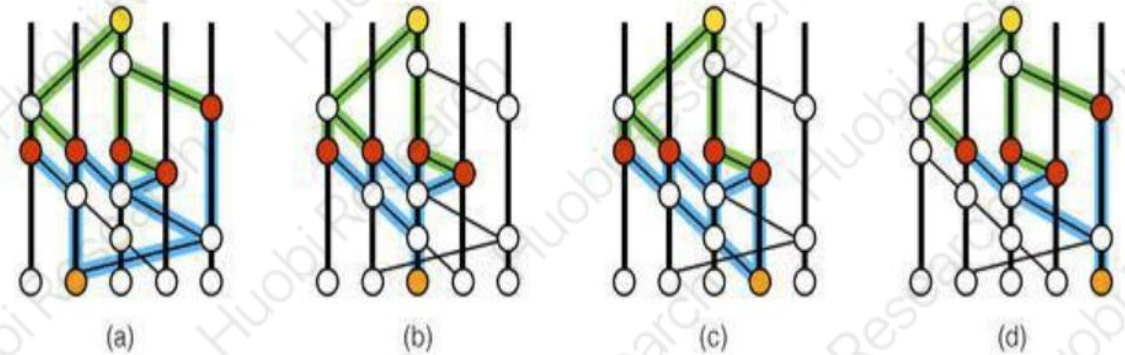
- *Transmission through Gossip of events using gossip about gossip protocol*

- *Virtual voting*

timestamp
transactions
hash
hash

Event

# Closing Thoughts...

- *How much will the platform layer improve for the next few months?*

- *Will the number of blockchain user exceed 50 million?*

- *Will some of the new public blockchains Outbeat Ethereum?*

- *Will Nasdaq launch its digital asset exchange faster than expected?*

# Follow Us on Social Media



Wechat
Official Account

Twitter
@Huobi_Research

Email：huobiresearch@huobi.com

Medium: Huobi Research
https://medium.com/@huobiresearch

Facebook: Huobi Research
https://www.facebook.com/Huobi-Research-655657764773922