Gold Mines in the Future:

Insights from Interviews with 20 Institutional Investors

Authors   [Huobi Research Institute] Mengchu Jiang, Siyu Chen, Dave Chan

Huobi Research

Abstract

It has become a consensus among all investors and practitioners that the crypto market is entering bear territory. Winter is the time to prepare for the sowing of seeds in spring. Huobi Research interviewed more than 20 representatives from outstanding global institutional investors, hoping to use their development status, investment philosophy and layout direction as a sample to understand their opinions on the current situation and trend of the industry, and additionally, to discover potential opportunities.

In the interviews, we learned that most institutional investors prefer to research more and act less. They pay more attention to infrastructure projects, with emphasis on ZK, new L1 chains and middleware. In terms of applications, DeFi, GameFi and social ranked in the top three. Among them, DeFi is the most favored direction for institutions, while GameFi and social remain controversial.

Their key areas of focus are as follows:

- ZK is one of the potential core drivers for the next cycle, which has long-term value. It occupies 2 core narrative levels: Scaling of Ethereum and privacy computation. ZK acceleration network and mining are the focus of institutional investment for a stable gaming structure.

- Institutions are more strategically focused on new L1 chains, rather than having seen certainty in return. They have expressed interest in two innovations that have emerged in the recent crop of new L1 chains, the Move programming language and parallel processing technology, and believe that their value may extend beyond a particular L1 chain itself.

- Middleware is second only to ZK and new L1chains in terms of the degree of attention. The most sought-after are decentralized identity, data protocols and wallets.

- Institutions tend to keep an eye on DeFi, but remain on the sidelines overall. For existing DeFi protocols, those with stable cash flow and independent of subsidies are likely to explode growth-wise again. For emerging DeFi protocols, institutions are currently focusing on protocols with relatively mature businesses in traditional areas but with fewer competitors on chain, which are mostly seen in the derivatives market.

- Social is controversial: everyone agrees that social is a necessary need with high potential. However, many organizations believe that existing SocialFi projects are still in the early stages of development, with unclear models and unsustainable

paradigms. If they rely only on tokenomics and packaging transformation of Web2 social, it will be difficult to acquire users from traditional giants.

- The controversy surrounding GameFi is prevalent: on the one hand, many institutions recognize that games can best attract incremental users, on the other hand, some institutions believe that current GameFi models are unsustainable.

We believe that the more promising tracks in the future are within the infrastructure category, including ZK, new L1chains, and middleware. While there is more uncertainty on the application side, DeFi is more likely to stand out, and potential opportunity falls in the derivatives sector. SocialFi is still some time away from breaking out because the prerequisites have not yet been completed. GameFi has potential growth opportunities, and those with better economic models stand a greater chance.

Table of Contents

1.Status quo of previous investments

Let's first recall the status quo of investments in the global crypto market. According to publicly available statistics by Odaily and PANews, there were 511 investment and financing events (excluding mutual funds and M&A) in the global crypto market in the second quarter of 2022, with a total disclosed amount of US$12.71 billion. Among all funding events, the number of deals with a funding size of more than US$100 million reached 28.

Compared to Q1 this year, there were 461 investment and funding events in the global crypto market, with a total disclosed value of US$9.2 billion. While the crypto secondary market environment worsened in Q2, there were signs of a rebound in funding activity. The number of investment and financing activities rose 11% YoY and the amount invested rose 38% YoY.
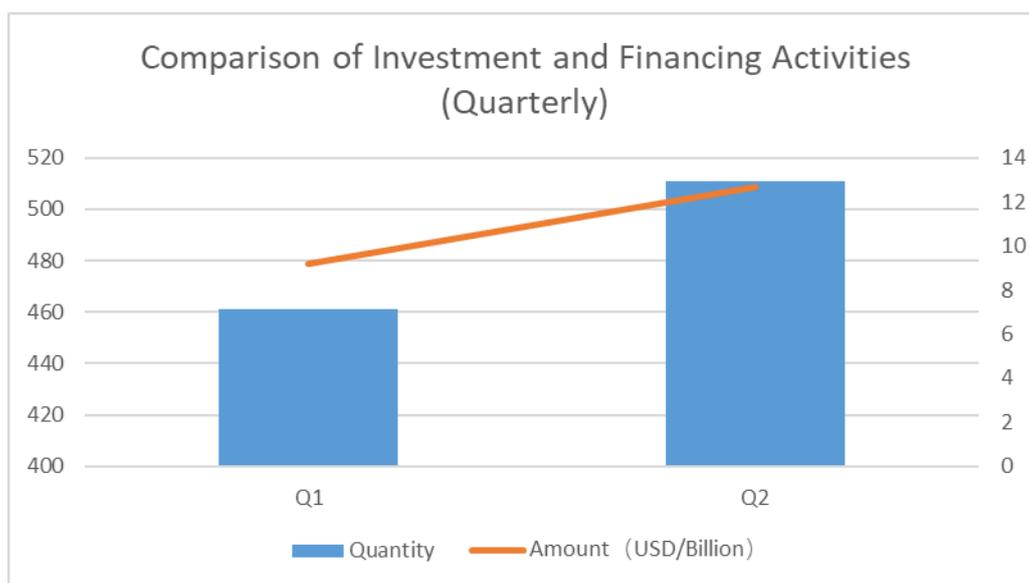

Figure 1: Comparison of investment and financing activities between Q1 and Q2 this year

On a monthly basis, however, we feel nothing but desolation. From April to July, the number and amount of investment and financing activities were monotonically decreasing. Total amount of investment and financing dropped by nearly 70%, and the

number of events dropped by 16% in 4 months. The cold state of the market matches the psychological state of the investors we interviewed.

The reason for the divergence between quarterly and monthly figures may be that the secondary market rebounded from January to March, driving the investment and financing market, and the majority of fundraising news was disclosed in April. The collapse of Terra and Three Arrows Capital (3AC), on the other hand, severely undermined market confidence and escalated the risk aversion of more investors, so the number and amount of investment and fundraising declined from May to July.
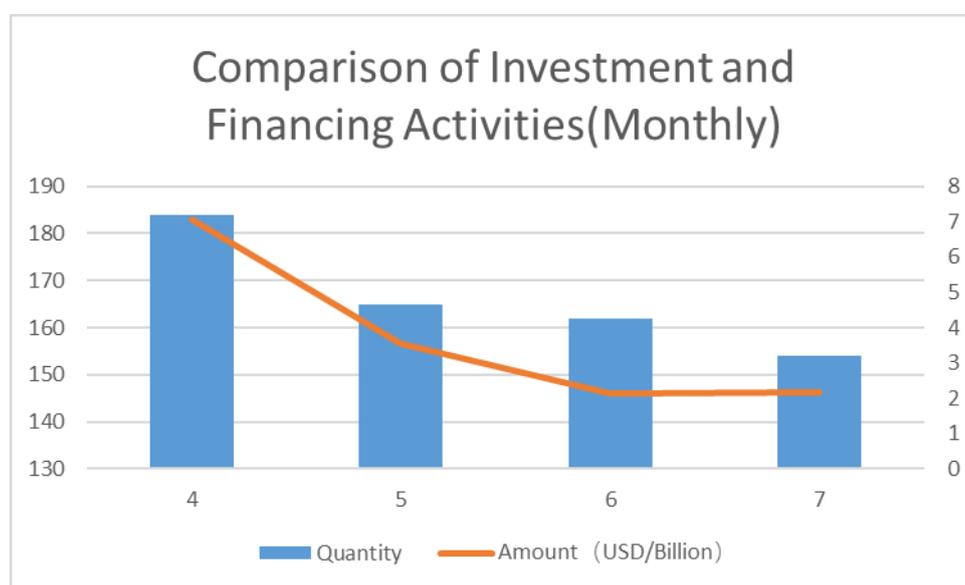

Figure 2: Trend of investment and financing activities in the past 4 months

Here is a review of the areas institutional investors have focused on previously. From the chart below, in Q2, GameFi and NFT were the most favored sectors. 82 funding events were raised for GameFi, GameFi-related infrastructure and technical solutions, hitting the first place and accounting for 16% of the total funding volume. The NFT sector was second in terms of number of fundraising events at 67, and DeFi ranked fourth with 50 financing activities. The infrastructure sector, represented by L1, L2, mining, privacy, identity, etc., became the "long-tail" sector, with around 10 investments each.
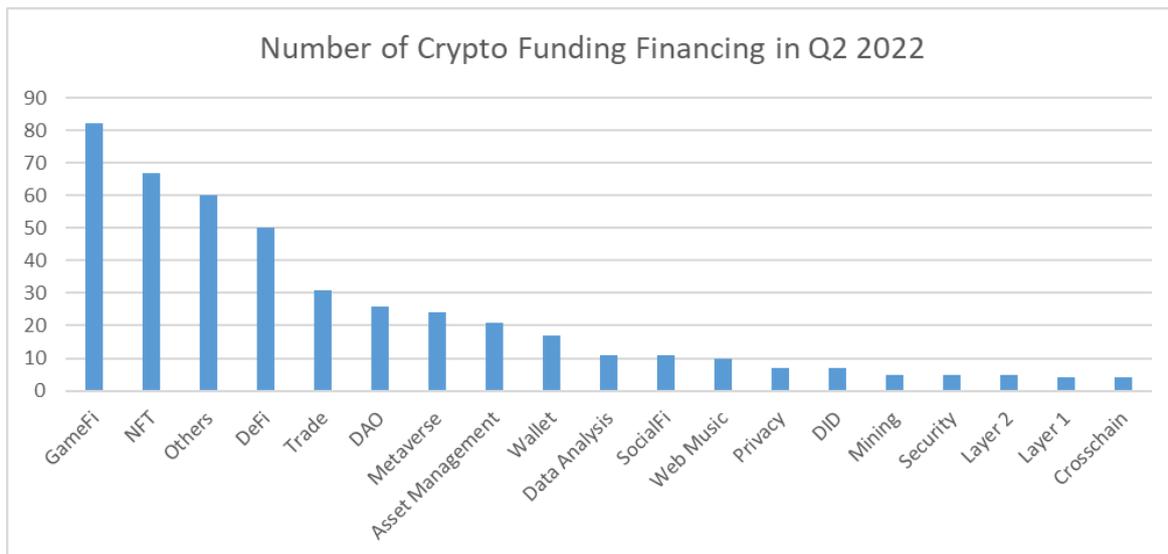
Figure 3: Ranking of the number of fundings by sector in Q2 2022.

Source: Odaily article "2022 Q2 Crypto Market Investment and Financing Report: GameFi Becomes the Keyword for Investment"

As the crypto industry has been continuously changing, the focus of crypto institutional investors has likewise changed even after a mere 2 months.

Huobi Research interviewed more than 20 institutional investors in total, including crypto native top-tier institutions, crypto departments of traditional institutional investors, investment departments of crypto corporate companies (such as exchanges, wallets, asset management, etc.), incubators, and institutional investors about specific segments. We hope to obtain a more comprehensive and realistic perception through a diverse sample of interviews. In these interviews, we mainly had conversations with various institutional investors on their analysis of the current situation and prospects of each track, investment logic and strategies. In doing so, we hope to provide some guidance for readers to better understand the cryptocurrency industry.

2. Ranking of segment potential and investment logics

We have summarized the areas of interest from the institutional investors that participated in the interviews, sorted by the frequency of mentions, in the figure below. Some of the areas in the chart have an inclusive relationship with each other, and we will analyze each area in detail later on in this article.
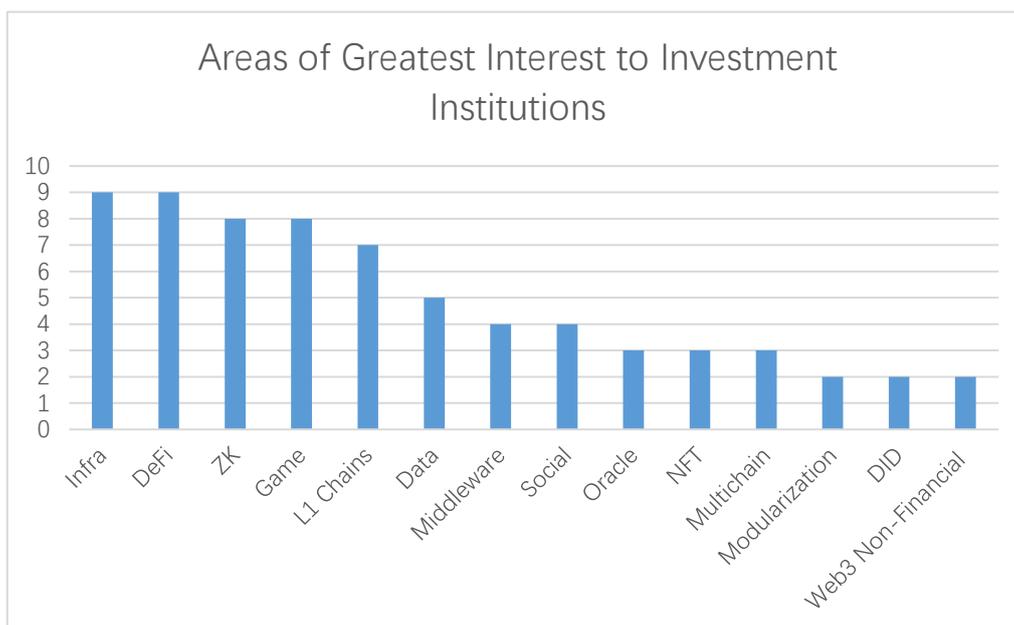

Figure 4: Areas of greatest interest to various institutional investors

    The key areas can be divided into two major categories, infrastructure (Infra) and application. The frequency of mentions on Infra is the highest, and the two main branches are ZK and new L1 chains; areas like middleware, data, oracles, DID also contain infrastructure elements. In terms of applications, DeFi, GameFi, and social ranked in the top 3. Although the DeFi space has stayed quiet for a while, it remains the most promising sector in the eyes of institutions. By contrast, GameFi and social are very controversial: some institutions strongly believe in these sectors, while others are not looking towards these sectors at all. We will dissect each one to elaborate on institutions' underlying investment rationale.

2.1 Infrastructure

The research results show that organizations are significantly more concerned with infrastructure than applications. Some organizations do not explicitly mention the word "Infra", but their focus still falls on areas such as ZK and new L1 chains. In this article, for convenience of discussion, zero-knowledge (ZK) proof, new L1 chains, middleware, DID, data, modularity, etc. are all classified as infrastructure.

Why infrastructure?

There are two main reasons for infrastructure to stand in the spotlight: first, the following of the industry development cycle; second, the new Web3 narrative requires certain preparations.

One cannot go against the industry's development cycle. The word "cycle" here does not refer to the market's bull-bear cycle but the rotation between infrastructure and applications as the main players in the cycle.

IOSG Ventures refers to the "Newton's Cradle" theory to summarize this phenomenon. They believe that emerging technology needs the underlying infrastructure to first reach a certain level of technical competence in order to roll out applications, and only when the infrastructure development reaches a certain level can the performance support early applications' germination (for example, without Ethereum smart contracts, no DeFi applications would be rolled out). While the growth and prosperity of applications require a vast improvement of infrastructure with stronger performance and more complex technical middleware or segmented applications, this would drive further upgrades of infrastructure (e.g., more complex DeFi Layer2 protocols would demand stronger performance to support Rollup development. The current crypto GameFi and SocialFi spheres are also in their early stages, and awaiting the establishment of niche fundamental protocols); this iterative cycle with elastic bounce properties is akin to a Newton's Cradle. According to this law, there will be "fat" protocols and "thin" applications first, which refers to the belief that the protocols will massively capture value first. In investment practice, IOSG has spent five years cultivating the protocol layer and infrastructure investment, investing in platforms such as Cosmos/DoT, Near, Avalabs in Layer1, Starkware and

Arbitrum in Layer2, and a large number of native developer protocols in middleware. As Infra approached stability and maturity, IOSG shifted to a "fat" application investment strategy and began looking for potential in DeFi, gaming and social unicorns (including Metamask,1inch/Project Galaxy, Cyberconnect/Bigtime Studio and Illuvium, etc.).
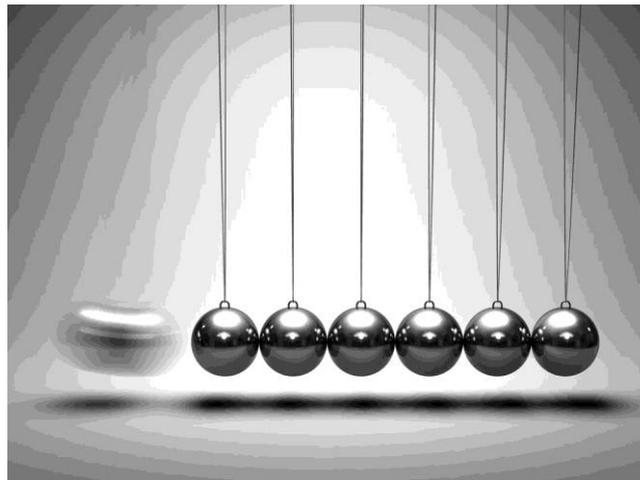

Figure 5: Newton's cradle

Bixin Ventures believes that there are few innovative products emerging from the application layer, and some of the hyped concepts have yet to land, not to mention their eligibility for investment. This time is right to invest in infrastructure and await this segment's prosperity in the next bull market. It is preferable to be investing in infrastructure rather than applications as the former has a higher "winning rate[1]". Matrix Partners has proposed the "80/20 rule" as a practical guide. In a bear market, 80% of the effort will be spent on Infra and 20% on applications, while in a bull market, this ratio would be reversed.

Second, prepare for the new Web3 narrative, which many traditional Internet giants such as Amazon, Google, Meta, ByteDance, Baidu, etc. are actively exploring

---

[1] "Winning rate" and "rate on earnings" are used to measure ROI. "Winning rate" refers to the possibility of receiving positive return, which is how likely to make money. "Rate on earnings" refers to the amount of earnings received in a positive return.

and acting upon. One narrative claims that Web3 is a new generation of Internet ecosystems based on blockchain technology. The user base for this Internet system cannot number in the millions, but billions. Current blockchain infrastructure is far from sufficient to serve such a large number of users, however, and needs to be continuously upgraded and modified.

In terms of how to judge the value of Infra, Cobo Ventures and Foresight Ventures have suggested that infrastructure is a technology-biased field, and the focus needs to be around the diffusion of technology levels, and which solutions are cost-effective, efficient and secure What's more, the vibrancy of the developer ecosystem and recognition of users need to be the end goal so that real value can be created.

The following highlights discussions from organizational views and their value judgments on several key areas within the infrastructure space.

2.1.1 Zero Knowledge Proof

Zero-knowledge proof (ZK) is the area that is receiving the most attention from institutional investors within the infrastructure space. It mainly consists of ZK Rollup and its acceleration network.

ZK's status

Two horizontal comparisons could portray the status of ZK in the eyes of institutions:

First, within the Layer 2 field, ZK has become a synonym for Layer 2, for it is more favored than Optimistic Rollup（OP）. Current Layer 2 mainstream technology is Rollup, which contains two technical divisions: OP Rollup and ZK Rollup. In the course of interviews, almost all the institutions expressed favorable opinions on ZK on Layer 2 rather than OP Rollup, which is comparatively better in data from all aspects. More than one institution is of the opinion that OP should be evaluated on a short to medium-term basis, but is not valuable for the long term. ZK to cryptography's relationship is akin to machine learning's relationship to AI: it occupies the core position, being one of the industry's top narratives.

Second, in the competitive landscape of L1 chains, institutions are more inclined towards ZK than new L1 chains. The reason is that ZK, or Layer2, which it endorses, represents the scaling of Ethereum, which is favored more by institutions currently. JDAC Capital believes that Ethereum will become a settlement protocol in the future, is scalable, and can be expanded to a larger user base, even for traditional Internet users. With high asset attributes and high consensus of network value, settlements on Ethereum will be more trustworthy, and the value of assets will grow in recognition.

Logic behind investment in ZK

The intrinsic value of ZK should be looked into, besides its comparative advantage. Zonff Partners suggests that **ZK is one of the four potential core drivers for the next cycle and holds long-term value. It occupies two core narratives, namely Ethereum scaling and privacy computing.** It is possible that ZK Proof will have the same positioning for cryptography and blockchain as machine learning is for artificial intelligence. Especially in the field of Ethereum scaling, it already has the structure of the upstream and downstream, such as developers, computing equipment providers, node services, application demand, user demand, etc. On the one hand, the track with a stable structure is more suitable for institutional-type funds to layout; on the other hand, the development is expected to be stable, not entirely dependent on macro or a hot event, and it is easier to generate positive feedback in the process of project or entrepreneurial entry.

Firstly, ZK Rollup will play a more significant role in Ethereum scaling, but its capabilities are currently not fully utilized. Besides the improvement in performance, ZK solves the blockchain's problem of losing weight. Because all nodes have to store a large amount of data, it would be difficult for general operators to accommodate, thus aggravating the degree of centralization. ZK Rollup requires a smaller amount of data to be uploaded to the chain, which helps relieve the nodes' storage pressure. The more prosperous the on-chain ecology is, the greater the demand for lightweight, and ZK Rollup will be able to receive more room for development. The raw transaction data still needs to be stored, and this is where the data availability layer in modularized L1 chains comes in handy.

Second, ZK is capable of solving more issues related to privacy protection. Before DeFi and NFT emerged, there was less data on-chain and the importance of privacy was not as pressing — there was nothing to protect, and no effective solutions were in the market. After DeFi emerged, privacy became of the utmost importance. There are no compelling reasons to require everyone to disclose on-chain data, especially for giant investors and institutions, whose on-chain operations might contain significant financial benefits. But current data-analyzing tools amplify the transparency of the blockchain and pose distress for institutions, amplifying the need for privacy protection. Obviously, the need for privacy protection is real and certain. As more data will be on chain, the need for privacy protection grows. However, there are no better ways to protect privacy now. Besides ZK, there are opportunities for homomorphic encryption technologies and multi-party computation (MPC).

Based on the above logic, several organizations believe that ZK Rollup is the best solution in Layer2. Besides, the Ethereum Foundation itself is confident about ZK, and with no commensurately advanced alternative currently, it is necessary to be involved with the bottom layer from the beginning.

ZK's key directions

Zonff Partners, JDAC Capital and HashKey Capital have all explicitly mentioned that they are focusing on ZK accelerated networks and mining. ZK Rollup requires a large amount of computation to generate proofs, and there is a real need for acceleration through hardware. Considering the position of ZK in the overall ecosystem as mentioned above, ZK mining is still a long-term need.

Institutions are more interested in ZK mining's position in the overall industry structure.

ZK's industry chain is relatively similar to Bitcoin mining, with chip manufacturers, miner manufacturers, nodes, and mining pools in the upstream, developers and various applications in the downstream, and with a stable game structure overall. Current upstream technologies involved with ZK mining includes Scroll, zkSync, Starknet, Aztec, Polygon, which are relatively dispersed and inadequate for institutions to invest heavily in, as it is difficult to identify distinct targets with high ROI. Investing in these infrastructures is a gamble. Whereas the

downstream after the summer of DeFi and the spring of the GameFi, no clear application route can be seen in the current time slot, meanwhile, the applications face intensive competition inside the segment. Institutions are also faced with the difficulty in choosing not just the right track, but also the right player within the track, and the odds of succeeding are low. ZK Mining is in the middle of these two, and there is a structural opportunity. When the upstream (each technology route) is very fragmented and the downstream (various applications) is the same, there lies a structural opportunity in the middle that can yield stable returns. This is the logic by which accelerated networks and mining can gain momentum, just like selling mineral water and jeans to gold seekers.

But it would be hard for the ZK hardware industry to reach the same market size as the Bitcoin mining industry. First, it depends on whether ZK underlying protocol is open to decentralized proof for mining, or a centralized approach would do. Secondly, and most importantly, ZK mining is limited by the scale of ZK projects — that is to say, how much volume can be carried on ZK in the future. If there is a breakthrough on funds volume, the ceiling for ZK mining can gain new heights.

The impact of ZK's rise on other tracks

Let's see how ZK's rise interacts with other tracks.

First of all, ZK will strengthen Ethereum's competitiveness. JDAC believes that the level of technical solutions and community strength of Ethereum is invincible compared to other L1 chains and is still difficult to defeat even with EVM. Once ZK is more mature, it will further strengthen the position of Ethereum. Conclusions shall not be drawn at this point, but we can expect that the development of ZK will greatly enhance the competitiveness of Ethereum, and the leading position held by the L1 chain will not change hands so easily. Under last year's favorable market conditions, Ethereum's Layer2 was not adopted on a large scale; while the fees of other new L1 chains were already negligible, Ethereum was still able to lay claim to more than 60% of TVL. If Ethereum catches up with other L1 chains in performance, yet maintains a high degree of decentralization, we have reasons to believe that its leading position will be further cemented.

Second, ZK will expand the demand for the data availability (DA) layer. As mentioned above, although ZK Rollup requires less data to be uploaded, raw data still needs to be stored, and the DA layer is responsible for storing these raw transaction data and ensuring their availability. From this perspective, it can be said that it is an upstream of ZK; the prosperity of ZK will also drive the boom of the DA layer. In our previous article "How the Data Availability Layer Can Shape the Future of Blockchain", we made a simple calculation that if Rollup gains more traction and a "Rollup-centric" situation emerges, along with a reformed, higher, ETH price, the DA layer is expected to reach US$2 billion in annual revenue.

Third, the rise of ZK may not have much impact on data analyzing tools. It appears that ZK Rollup is still focused on scaling. Although projects focused on privacy are out there, they are not mainstream. Privacy is an area that has not received particular attention despite existing for long, unlike how it is regarded in the traditional Internet industry. Protecting privacy incurs costs, and if the cost is not low enough, it will dissuade some small and medium-sized users and reduce the utility of the network. Most users care more about convenience and price, so we think the development of ZK in a short period of time is not enough to affect the survival of data analyzing tools; they could grow together.

Fourth, the development of ZK may give rise to new applications. Small amounts of data uploaded in ZK Rollup endows applications with more complex designs in business logic. There may be some applications that differ from current ones, such as DeFi-type projects with more complex business logic, and the killer application for Layer 2 will probably appear in ZK Rollup. However, it all depends on one prerequisite: the maturity of the generic ZKEVM.

2.1.2 New L1 chains

New L1 chains are also receiving a lot of attention, but are less often mentioned than ZK by institutions, who mostly adopt a strategic big picture perspective, but not specifically for certainty.

The logic of investing in new L1 chains

L1 chain is an everlasting mainstream track in blockchain investment with huge potential. With each new wave of L1 chains comes some degree of development paradigm shift, such as the shift of consensus mechanism from POW to POS, driving the long-term development of the industry. There are significant opportunities here, and if the impossible trilemma is solved, it can even disrupt the current logic and the status of Ethereum. But there will not be many disruptive opportunities: a big paradigm shift is hard to come by since it requires a high level of innovation, whereby the solutions are 10 times better than the current ones. More than one institution has said that no project can reach such a level as. However, the future L1 chain landscape will probably remain a pattern that consists of multiple chains co-existing, and new L1 chains do not necessarily need to occupy a large market share to be considered successful. So long as there is a user base and capital accumulation, there are still opportunities for market cap growth in the bull market, which is why it remains a good choice from an investment perspective.

When evaluating projects, several venture capitalists have suggested that performance should be viewed rationally. First of all, performance per se does not matter; it is the comparison of performances that matters. Each new generation of L1 chains mentions performance improvement, and they are all compared to Ethereum, which is used as a benchmark. But Ethereum itself is also improving performance-wise, and when Layer2 gains more adoption, users may have difficulty discerning the performance gap between L1 chains, or this gap would not be large enough to entice users to switch. Secondly, actual performance is more important than lab performance. The 160,000 TPS claimed by Aptos is merely lab data, and the correlation between transactions needs to be tested in order to better leverage the power of parallel processing; therefore, actual performance remains a question. Solana has meanwhile laid claim to 160,000 TPS, but the network has suffered four massive outages and its performance has been deemed not stable enough.

Highlights of new L1 chains

Although there are no particularly outstanding projects, HashKey and NGC Ventures are excited about two innovations that have emerged from the recent batch

of new L1 chains. The first is the Move programming language used by popular L1 chain projects Aptos and Sui. The second is parallel processing technology. Their value may not be limited to a particular L1 chains themselves, but will have a greater impact on the industry.

A highlight is the Move language, which introduces the idea of resource-oriented programming, abstracting something called a "resource". Users can easily define any type of resource (for example, a common crypto asset is an irreproducible, indestructible resource), and they can define how that resource can be manipulated. This provides the following properties. First, the Move programming language is more secure. It makes the smart contract language more suitable for its asset-oriented scenarios through features, such as separation of resource definition and control authority, static typing, generalization, modular system, and formal validation, securing digital assets from the smart contract level. Second, Move can help developers shift their attention to other areas which deserve more attention, such as writing the right business logic and implementing the right access control policies. Third, smart contracts in the Move language are more composable. This saves block space occupied by contracts and makes it easier to optimize upgrades. Fourth, Move has a lower threshold than Solidity, and there will be an underlying compiler to further lower the development barrier. New L1 chains based on Move can be seen as another round of education for future developers if they don't develop as well as they should. Should they be successful, they will revolutionize programming. From this perspective, the Move's value is greater than the value of L1 chains based on it.

Parallel processing is another highlight, and it could signal the trend for underlying improvements. Currently, transactions on Ethereum are processed serially, and all transactions need to be processed with EVM's single-core CPU. The idea of parallel transactions lies with stopping the use of linear processing but in a parallel way; for example, Aptos uses 16-core CPUs to open multiple threads to process unrelated transactions at the same time to improve TPS. Sharding is actually a typical method of parallel processing, but it is designed to parallelize more at the architectural level. The parallel processing mentioned here refers to the parallelization of processes or threads during program processing, and is situated closer to the underlying system. In the future, parallelization may become the standard for L1 chains, and all L1 chains will have some semblance of this feature. This shift is similar to the adoption of POS

consensus mechanism by all L1 chains after 2018 and 2019, signaling the universal abandonment of POW mechanism.

2.1.3 Middleware

Middleware is second only to ZK and new L1 chains in terms of the attention given to it. Middleware generally refers to software that provides common services and functions for applications: data management, application services, messaging, authentication, and API management are usually handled by middleware. Its role is to connect infrastructure and applications. For ease of discussion, this paper will categorize it under infrastructure.

Since middleware is classified under infrastructure, it will build a critical mass once adopted by some applications, forming an unofficial standard. Therefore, its network effect is very strong, and it is easy to have a winner-takes-all situation. Institutional investors will naturally not overlook such a field. They focus more on decentralized identity, data protocols and wallets.

A decentralized identity (DID) is an Internet address that users can own and control, which is deemed as an infrastructure for many Web3 applications. Users in an existing blockchain network already own certain assets, but their identities in virtual life have not yet been established. Just as how assets in a decentralized world can flow across the margins of applications, users themselves should be able to do the same, which requires an identity that belongs to the user and denotes the user's identity. With an identity, social applications, other Web3 non-financial applications and some of DeFi's new variants can be carried out. For example, when users use social applications, they can authenticate themselves by using an existing account on DeFi protocol, their past experience in the governance of a DAO, or as a previous player of some game, to find more like-minded friends. However, institutional investors are also concerned about whether the protocol can generate sustainable revenue, which has not yet been realized since most DID protocols produce revenues through staking and liquidity mining, which is unhealthy. In the long run, it seems that if a certain user base is available, it can be profitable through service charges. There will be a long building cycle in between and the project team will have to take a long-term perspective.

When it comes to data protocols, accurate privacy definition and quick response are the most important characteristics institutional investors seek. Everest Ventures Groups (EV) has said they have hardly seen any protocol that did a good job of clearly defining which types of data should be privately owned or be available to the public. For example, in general, identity information should be confidential, yet for some specific data, should they be owned by the protocol and made available for others to retrieve and review? A delicate balance must be in place, and data protocols that address this issue are likely to be the winners. Another direction is fast and high frequency response, which responds to the demand of many hedge funds for fast data response to react. Protocols like Dune and Graph have distinguished themselves in the segment, but they also need to be more time-sensitive.

For middleware like wallets, expanding the audience base is the key issue. Most external users have not used crypto wallets, and wallets are a barrier for them to enter the crypto world. StepN is a good example by integrating the Web3 wallet into the product itself, guiding outsiders to create a wallet at the time of account registration, giving them a seamless initial wallet experience. This is also a new idea for the wallet itself, which enables a seamless acquisition of incremental users by deeply integrating with consumer-oriented Dapps.

2.2 DeFi

DeFi, as a pioneer in the application layer, naturally prompted considerable discussion. However, other than the AMM algorithm, DeFi does not have more mechanical innovations, and the nesting type of innovation does not create too much impact in the market. Therefore, as with L1 chains, institutions tend to keep an eye on DeFi, but maintain a wait-and-see attitude overall.

The logic of investing in DeFi

Blockchain has been closely linked to finance since its inception, and with the introduction of smart contracts, DeFi is gradually demonstrating strong financial innovation dynamics and attracting large amounts of capital. At the same time, DeFi, with its own combinable and no-barriers-to-entry attributes, provides the perfect place platform to address the common pain points of traditional finance such as higher entry

barriers, centralized risk and high capital volumes. It enables parties to trade openly and transparently on the blockchain without the risk of private misappropriation of assets, serving as a platform where anyone can correspond based on on-chain liquidity and positions. Smart contracts provide automated rules for how specific financial instruments and protocols should act, executed and managed by code that does not favor any particular investor. The advantages of DeFi are particularly evident after major incidents involving CeFi institutions.

Development Path

Since the emergence of AMM, the DeFi market has become more mature, with a variety of tracks and ecological projects; some large and comprehensive infrastructure has formed a clear head effect, such as DEX, lending, etc. Institutions such as Nothing Research and Matrix have made some basic judgments about the future trend of DeFi as a whole:

1. For existing DeFi protocols, how to successfully survive the current bear market must become top priority. With a retrospective look at the rise of DeFi, subsidies from projects were critical methods in stimulating ecological expansion, relying on a strong narrative to receive market dividends. But this is by no means the way for long-term survival. In a bear market, **projects that have stable cash flow and slowly move away from subsidies are likely to encounter another crisis in the future**. On the other hand, many protocols are user-friendly, but the tokens fail to generate direct value by adopting the protocol. This has resulted in weak token prices, which in turn affected the further development of the protocols. Existing protocols that can improve tokenomics are expected to achieve secondary growth.

2. For new start-up DeFi protocols, all current DeFi tracks are relatively saturated and it is difficult to find new continents for development until disruptive innovations emerge in the general environment. Therefore, **institutions are focusing on DeFi protocols with relatively mature businesses in traditional areas, but with fewer competitors on-chain**, mostly in the derivatives segment. Some derivatives protocols performed quite well based on the model, but the market is not yet knowledgeable enough. In

addition to guiding users to learn by themselves in an up-trending market, they need to acquire incremental users using their operational capabilities.

2.3 Social

The social track has always been a hot topic worthy of attention, but opinions and judgments vary greatly among organizations.

The logic of investing in social

On one hand, organizations can basically reach a consensus on the meaning of the existence of social; that is, social is a basic human need, but also necessary as the interconnection and exchange of value that occurs in the production as well as other social activities. Social on Web3 represents the future trend, with unlimited opportunities. Cobo Ventures believes that **on social platforms in the Web 3.0 era, people will have absolute control over their social data. SocialFi product is a product that underlies Web 3.0 infrastructure and converges the needs of people for decentralized social and financial services. It can break platform monopolies, eliminate single points of risk, and create a new business model and product category in the wave of a global digitized economy.**

On the other hand, opinions vary on mid-to-short-term expectations. Huobi Incubator believes that the **existing SocialFi projects are still in the early stages of development, which have not formed a sustainable paradigm or a clear model for the future. Moreover, if SocialFi solely relies on tokenomics and packaging for a transformation of Web2 social, it cannot compete effectively with traditional giant social operators. In other words, it needs to tap more into Web3 native user characteristics and user needs.** From these perspectives, the conditions for SocialFi to trigger the next wave of bull market are not met.

Development Path

After several interviews, we summarized the development path of the social track, and the following directions could be utilized to empower social by blockchain and tokenomics:

First, blockchain + social improves the drawbacks of Web2 social.

The core idea of some social projects is that they want to break the monopoly of traditional social giants and play a different role according to the peculiar characteristics of blockchain, mainly in the following aspects:

1. Data autonomy. On traditional social platforms, users are only participants or users of data; blockchain enables on-chain data processing that allow users to take control of their data.

2. Data sharing. There are data isolations in the Web2 world that result in data not being interoperable between platforms.

3. Data privacy. Unlike traditional Web2 in which users passively bear the risk of privacy breaches, information on a blockchain is publicly accessible, but users can also protect the privacy of their on-chain address and other data using encryption technology to control the degree of disclosure.

In terms of economics, it is rational for blockchain social projects to reward users by releasing platform tokens. After the introduction of the token economy, the beneficiary relationship between users and the platform will change accordingly, and the bond with the platform will be stronger. The more contributions users make to the platform, the more tokens they can receive, and the higher the value of each token. Meanwhile, to provide more economic incentives, some "X2Earn" or content creation mining models have also brought new ideas to social, leading to a short-lived SocialFi boom.

The token economy can provide blockchain social projects with some support at the early start, but how to stimulate the inherent needs of users for continuous content creation cannot be solved merely by simple tokenomics.

What remain bigger problems are:

1. Small user base. Given that the Web3 social user base is already relatively small, using tokens alone to achieve Web2 traffic conversion is not ideal.

2. Counter-effect of tokenomics. Tokens represent binding benefit that changes with time. Rewards paid out in cash are timely in nature, but the value of the token continues to change over time: when the value of the token falls, the incentives

users received also shrink, exacerbating the deterioration of the project's fundamentals.

3. The portrait of on-chain users is blurred. Since most SocialFi projects focus more on "Fi", i.e., the financial attributes of the project attract a large number of opportunists who will leave once there are no more material gains. This results in the platform becoming less popular and serving fewer on-chain social users, so that real demand cannot be captured.

4. Inadequate infrastructure. The current underlying infrastructure cannot support the complex, data-intensive nature of SocialFi applications.

Second, the exploration of Web3 social continues.

The focus of each project gradually shifted and began to focus more on the Web3 users themselves, refining the underlying Web3 identity based on their respective messaging and relationship building.

- Web3 Identity

The prerequisite for a stable and long journey is concrete infrastructure, and more projects are exploring the creation of Web3 identities to carve out a user base with real social needs. The creation of an identity diagram consists of two aspects.

1. Data parsing. Traditional social products need to build user habits from scratch; however, on-chain data of Web3 is a public resource and anyone can access existing data (e.g., transaction data, NFTs that recognize identity or personal taste) to carve out user profiles and establish identifiable identities.

2. Identity aggregation. Data parsing has no threshold, and any project can develop products based on identity data. However, the source power for sustainable development comes from more accurate and dimensional user portrait by aggregated data, if users are allowed to gather information from multiple chains, multiple addresses and even under chains.

- Messaging

There are two types of messaging.

1. Broad/non-specified messaging which relies primarily on social media to attract public attention and communication by posting content (text, graphics, video).

2. Specified messaging where messages are sent with a specified address or class of addresses. The main scenarios are: NFT OTC transactions, hacker bargaining, and project airdrops.

- Relationship building

When individuals build connections, they establish social relationships which can be strong, weak or temporary in nature. Web2 applications connect users through platforms, and it is difficult to extract monetary benefits from weak connections; while Web3 introduces tokens which strengthen the economic motivation behind social behavior, and weak connections could achieve stronger bonds through transactions.

In general, after the early exploration and SocialFi frenzy, social has slowly figured out a sustainable development path. In the future, with the continuous development of social data, network relationship and other infrastructure, the real demand of social can be slowly tapped, and Web3 social is just around the corner.

2.4 GameFi

From a demand perspective, GameFi and social are highly similar: both are commonly used applications in daily life; the difference is that the wave of GameFi led by Axie in 2021 proved that GameFi can walk out of its own Alpha, while also reaping enough premium on secondary by virtue of tokens for gold-farming and money-making, etc. However, good times do not last, as the head project gradually cools and pessimistic voices against GameFi become louder, putting GameFi in the center of the storm. From this research, GameFi is also full of controversies.

The logic of investing in GameFi

In the discussion of why games should be on chain, most organizations can reach a consensus. This is discussed in detail by Animoca Brands and Huobi Ventures, and we summarize it as follows.

1. Blockchain+game enables the restitution of player ownership, which can let the game better establish decentralized mechanisms for mutual trust as well as asset transferability, endowing the game with more sustainability.

2. Games are easy to derive various trading scenarios from. Gold-farming and free market in traditional online and PC games have existed for a long time with mature regulation mechanism and design logic, regardless of whether it is traded over the counter or floor traded; the demand of prop liquidation and game currency liquidation also exist in the game. Only the secondary market for trading is not too common in traditional games, mainly because the publisher prohibits such activities, and the user experience cannot be deemed good. Blockchain technology has changed this, and it will benefit both game companies and users. While companies now mainly accumulate revenue from selling skins, the secondary market for games also has a huge space where game companies can collect transaction taxes for continuous income. With more freedom, more creations and gameplay will become available. The loyalty of players will be enhanced in step with as the perceived value, hence they will be more willing to pay for it.

3. The multiple purposes of unique in-game assets (trading, speculation, collecting) have a relatively high degree of complementarity with NFTs. Some in-game props are unique, and differ from each other in rarity and function. Therefore, it is natural for game props to be converted to NFTs.

4. Games can be a traffic portal for L1 and a testing ground for L2. GameFi is regarded as the most active sector with the most transactions that is by far the closest to practical applications. In 2021, the role of GameFi to L1 chains started to attract attention, even though the TPS of Ethereum did not meet the requirements of even simple calculations in game scenarios, leading some high-performance L1 chains to seek new opportunities. For L2 at present, there is a lack of cash cows that demand fast trade and a high level of activity, which could be a perfect fit for games; the two may be able to integrate in the future.

From the perspectives above, games are extremely valuable as a long-term investment. However, the existing GameFi development model has also drawn

questions, of which the biggest is sustainability. Most of the current GameFi applications are one-time existence, with the initial burst of Play to Earn models attracting a large influx of funds within a short time. Driven by FOMO, GameFi enjoyed steady growth in its early phase. But in the long run, the economic structure of most GameFi is unhealthy, and can even be described as a Ponzi scheme. When the novelty of the game slowly dissipates, GameFi often loses its appeal and ability to acquire incremental users. The imbalance of the economic structure in turn drives those who previously received the dividends to slowly pull out of the system, triggering a decline in the economic value of game assets, accelerating the decline of GameFi. When the game dies, so do the assets based on it, regardless of whether they are on the blockchain or on a centralized server.

There are 2 ways to crack this puzzle. The first is to add more fun to the game, and keep it so. The second is to develop a more sustainable economy inside the game **so that players have a relatively stable game relationship based on positions of winning/ losing or different roles in the game. Growth is not the panacea to cure everything that the survival of the game depends solely on, if new players are entering and paying previous bills.** At least one of these two approaches must be in effect that a game-based asset could be backed in the long term, only so consensus on value and trading logic could become possible.

Development Path of GameFi

In terms of Maslow's hierarchy of needs, physiological needs and security needs must be met before higher levels of needs such as social relationships, respect, and self-actualization, etc. From this point of view, gaming belongs to higher level needs; it is still an infant in the blockchain world. Specifically, Ethereum is merely 10 years old, and applications started to prosper beginning with the DeFi Summer in 2020, followed by GameFi represented by Axie a year later. The thriving bull market made the development of GameFi somewhat ahead of its time; the primary market needed a new narrative, and the secondary market needed a new way to play. The market sentiment pulled back the rapid rise of GameFi. With a slowdown in the market, we can revisit the game track and see there are shortcomings. But speaking of long-term value, gaming is still seen as a killer application built on infrastructure, and there are still many opportunities it offers.

1. Uncovering opportunities from the game teams

First, let's look at the traditional major players in Web2 gaming. It is often said that traditional Web2 companies are seeking transformation and actively embracing Web3, including gaming. Generally speaking, game producers with many years of experience and resources in game development have established their own system in game distribution, online operation, revenue streaming, advertising and other channels. It is not a problem for them to develop and operate multiple games at the same time. Therefore, such game producers typically enter GameFi with a series of games instead of only one, achieving user conversion from the existing user base, and injecting more incremental users into the ecosystem. Although the user increment brought by such conversion is the most effective, the development and operation process is relatively slow, and it requires long-term input from game producers.

Next, we look at the crypto native game producers. Relatively speaking, there will also be some teams from the native crypto industry that choose to develop blockchain games. However, there is a considerable degree of threshold for game development. Even if the team can bring in talents from Web2 game developers, it is difficult for them to replicate the past success in gameplay in the absence of the original operation and channels. As a result, some game teams started to change their mindset, seeking exits from the token economic model. A sound economic model must support a strong element of confrontation so that players are always against someone else, rather than just enjoying freebies from producers. Foresight Ventures suggested that for GameFi, the economic model is 1 while the gameplay is 0. Native manufacturers cannot compete with traditional games in gameplay; a good economic model is the first priority.

2. Opportunities from the game model

Whether it is the P2E model represented by Axie or the extension of GameFi represented by StepN's X2E model, all can be regarded as pan-DeFi products. This is because the main innovation of such projects is focused on tokenomics, not gameplay. The P2E and X2E models are essentially just liquidity mining with a few more steps, in other words, a new type of token distribution mechanism, which does not promise an absolute advantage. In future, the value of GameFi must be based on the playability of the game and more crypto native model innovation. SevenX claims that

three types of games will see the biggest growth potential: first, simple games, which can acquire many players with a low threshold; second, games with a highly competitive element that retains players; third, games with a stronger economic model that ensures the profitability of some players that an internal recycle could be formed.

In general, from the investment point of view, primary investment in GameFi is riskier. In the traditional Web2 gaming industry, producers will conduct tremendous market research and testing before any actual development takes place. This is costly in terms of human resource, materials and capital, which the crypto industry cannot afford, especially in terms of time. Because this industry is so cyclical, the opportunity is often linked to the overall market condition. If GameFi has to take into account the playability of games, it must recruit a powerful and professional team, which will naturally extend the development cycle. Therefore, the paradox implies increased risk of investment and leverage.

On the flip side, institutional investors within the crypto market typically seek relatively fast liquidation, which puts pressure on GameFi teams for the sake of short-term value. Therefore, GameFi teams that claim continuous development for 1-2 years do not have a good standing in the crypto industry.

Besides that, looking at the game itself, any game has a lifespan. The genre of a game is determined from the very beginning, and the difficulty of updating is relatively high, but investing in GameFi is more of a one-shot deal. Therefore, until the game solves the above-mentioned problems, institutions are too cautious to step forward and invest in games, and tend to do more research rather than take action.

3. Future opportunities

After reading the analysis from such many fields, we can't help thinking what kind of projects will shine in the next bull market, and in which field they will appear. What kind of strategies should be adopted in order not to miss these opportunities? We make some rational predictions in the following section, which does not constitute investment advice.

Infrastructure prognosis and strategy

By a cyclical pattern of segment rotation, the next protagonist in the crypto market is likely to be (and it actually is now) infrastructure.

ZK mining is a good opportunity both in terms of "winning rate" or "rate on earning". Analogous to Bitcoin mining, ZK mining will not see a high degree of concentration, which ensures a relatively stable return. There is plenty of room for imagination, despite the current uncertainty of the technology development path (GPU/FGPA/ASIC). This is because the residual values of the first two are relatively high, which enables high risk tolerance. StarkNet and zkSync are the relative duopoly on the ZK Rollup platform, but the competitive industry landscape is not yet fully defined, which could hold huge opportunities. From a technical strength and financing viewpoint, the two head projects are still in a favorable position. However, StarkWare is at a high valuation, which may incur risks.

The new L1 chains sit in a cluster, which is low in the "winning rate" but high in the "rate on earnings". As they are still at an early stage of development and the market remains in a downturn, it is too early for a boom. Investors will have sufficient time to study the innovative features and dive into the community to witness the development first-hand. Much of the value for L1 chain comes from its ecosystem: when there are a few quality projects or even featured projects on a certain L1 chain, the "winning rate" will be greater by betting on it.

Middleware is similar to new L1 chains, where the "winning rate" is low but the "rate on earnings" is high. The integration of upstream and downstream should receive more attention. For middleware, leading projects will be more sustainable and require which needs continuous attention. Before the competitive pattern of the industry takes shape, investments can be allocated in an indexed way, and it is not advisable to bet on a particular project alone.

Application prognosis and strategy

DeFi still has huge growth opportunities in the next bull market; it is also an area with a low "winning rate" a but high "rate on earnings". DeFi will enter a temporary hibernation period due to the current downturn in the market. Some blue-chip projects

have the potential to ride out the bulls and bears, and their second growth curve will require innovations on the mechanism or business expansion on top of improvements in L1 chain performance. Innovations of DeFi are likely to happen on Layer2 or in the derivatives market of new L1 chains. In the derivatives market, the volume of perpetual contracts is still much lower than that of CEX, and there is still room for development here. As the market continues to pick up and move higher, the demand and narrative for unsecured/under-collateralized lending and algorithmic stablecoins will exist in long term, and they may enjoy potential growth. However, after the collapse of UST and 3AC, evolutions must be made in these two areas. DeFi has huge growth potential and a high degree of concentration in the industry, but leading projects should always be the focus.

The "rate on earnings" for social is surprisingly high, but the "winning rate" is very low. On-chain identity and L1 chain performance improvement must be developed as the foundation, and more application scenarios must be in place. This means social may be a late starter. It is difficult to have breakthroughs by simply replicating the existing model, and it is not competitive enough compared to the traditional social giants. Blockchain-based social is not useless, and there may be opportunities in the following aspects. First, native needs need to be met on chain, such as delivery of accurate information and community development. Second, tokenomics could be adopted to solve actual social needs, such as the trust problem in social.

The "rate on earnings" of GameFi is high, with a higher "winning rate" than social, and it is a market segment that can accommodate many small-to-medium sized projects. As more big players enter the game, more incremental users could be seen, contributing to the overall growth of the segment. As a result, GameFi is likely to see skyrocketing growth. Fun is not necessarily the most important attribute of blockchain games, and the P2E narrative will definitely return. Games with stronger economic models may be more successful, especially in the growth phase of the market. To have a relatively long-term lifecycle, an economic model with a stable game structure is essential.

We extend our gratitude to the 20 institutional investors for their cooperation with the research team, in sharing their thoughts and ideas for this article. The following is a list of participating institutions (in alphabetical order, those that requested for anonymity are not listed).

About Huobi Research Institute

Huobi Blockchain Application Research Institute (referred to as "Huobi Research Institute") was established in April 2016. Since March 2018, it has been committed to comprehensively expanding the research and exploration of various fields of blockchain. As the research object, the research goal is to accelerate the research and development of blockchain technology, promote the application of the blockchain industry, and promote the ecological optimization of the blockchain industry. The main research content includes industry trends, technology paths, application innovations in the blockchain field, Model exploration, etc. Based on the principles of public welfare, rigor and innovation, Huobi Research Institute will carry out extensive and in-depth cooperation with governments, enterprises, universities and other institutions through various forms to build a research platform covering the complete industrial chain of the blockchain. Industry professionals provide a solid theoretical basis and trend judgments to promote the healthy and sustainable development of the entire blockchain industry.

contact us:

Website: http://research.huobi.com

Email: research@huobi.com

Twitter   https://twitter.com/Huobi_Research

Telegram: https://t.me/HuobiResearchOfficial

Medium：   https://medium.com/huobi-research

Disclaimer

1. The author of this report and his organization do not have any relationship that affects the objectivity, independence, and fairness of the report with other third parties involved in this report.

2. The information and data cited in this report are from compliance channels. The sources of the information and data are considered reliable by the author, and necessary verifications have been made for their authenticity, accuracy and completeness, but the author makes no guarantee for their authenticity, accuracy or completeness.

3. The content of the report is for reference only, and the facts and opinions in the report do not constitute business, investment and other related recommendations. The author does not assume any responsibility for the losses caused by the use of the contents of this report, unless clearly stipulated by laws and regulations. Readers should not only make business and investment decisions based on this report, nor should they lose their ability to make independent judgments based on this report.

4. The information, opinions and inferences contained in this report only reflect the judgments of the researchers on the date of finalizing this report. In the future, based on industry changes and data and information updates, there is the possibility of updates of opinions and judgments.

5. The copyright of this report is only owned by Huobi Blockchain Research Institute. If you need to quote the content of this report, please indicate the source. If you need a large amount of references, please inform in advance (see "About Huobi Blockchain Research Institute" for contact information) and use it within the allowed scope. Under no circumstances shall this report be quoted, deleted or modified contrary to the original intent.