HASHKEY Capital

ASIA CRYPTO INSIGHTS

SEPT 2023

HashKey Capital

HashKey Capital is an institutional asset manager that invests exclusively in blockchain technology and digital assets. As one of the most experienced blockchain investors based in Asia, the HashKey Capital team has deep knowledge of the blockchain ecosystem in the region and has built a network connecting entrepreneurs, investors, developers, community participants and regulators.

HashKey Capital is affiliated with HashKey Group, a digital asset management and financial services institution in Asia.

Authors

Jupiter Zheng
Research Director
jupiter.zheng@hashkey.com

Henrique Centieiro
Senior Research Manager
henri.centieiro@hashkey.com

Scarlett Xiao
Senior Research Analyst
scarlett.xiao@hashkey.com

Table of Contents

FCF - Fan Controlled Football

Fan Controlled Football is a fan engagement platform for sports events. The project originates from a 7-man rugby league with eight teams, with players being former NFL professionals and college and high school players. Audiences can vote on offensive and defensive strategies during the game through the FCF app, and players will make offensive or defensive choices based on the voting results. If the vote leads to a successful offense or defense, users who voted correctly can earn reward points.

In the previous business model, the company operated all the games and bore all the costs. The company has, in the meantime, transitioned to FaaS (Fan Engagement as a Service). The product is still a mobile app, and future partnered events will interact with users through the controlled app. The app has an avatar system and provides a social scene for users to live stream games and vote in the app. In addition, the app will issue mini-games of the same sports based on future games. The scores accumulated by users through mini-games before the official game will determine their voting power during the game.

Commentary by HashKey Capital:

Compared to the last financing node, the project team has changed its business model, transitioning from a heavy-operational content producer to a light-operational tech provider, significantly reducing operational costs and personnel expenses. The current business model can also easily cooperate with different sports events. The team has been operating sports leagues since 2017, accumulating sufficient sports event resources and operational experience over five years, and the fan engagement product also has two years of experience.

Blockfence

Blockfence is a security database and security plugin based on the knowledge graph. The project provides security services around a three-layer architecture, combining knowledge graph databases, third-party platform services, and AI. At the smart contract level, the team captures bytecode to generate 200 feature vectors; on the web page side, it captures at the JavaScript level to generate a library of similar feature vectors, including metadata creation time, and the number of other web pages linked by the page rank algorithm. Because there is interaction between smart contracts and some web pages, the corresponding feature vector libraries have a mapping relationship. The Israeli team has extensive experience in predicting phishing websites and has deployed many bots to predict/discover phishing websites. These bots can bypass the protection layer and solve the code obfuscation problem to extract the code and block data.

Commentary by HashKey Capital:

The team has a traditional security background, and the founder applies traditional experience to smart contracts, showing a high familiarity with the security business. The team has several years of working together and has created a security database based on the knowledge graph.

ChainML

ChainML is an AI agent creation platform based on a decentralized computing power network. Its underlying architecture is a decentralized computing power network, where all participants in the network protocol are P2P nodes. There are several types of participants in the network protocol, including API clients, smart contract clients, service implementations, and data providers, which are located outside the protocol. The protocol forms a dynamic committee among validator nodes, which execute a Byzantine Fault Tolerance (BFT) consensus protocol based on HotStuff. This consensus mechanism is used to execute data proofs to verify the validity of the data read by services in the protocol. It is also used to perform inference proofs to prove the validity of the computations used to compute service outputs. It is also used to execute learning proofs to verify the effectiveness of model training and confirm the validity of zero-knowledge proofs of service outputs.

Commentary by HashKey Capital:

The team comes from traditional companies like Google, Teradata, Vector Institute, Quantcast, etc., with an average of more than 10 years of relevant work experience, showing a high degree of familiarity with data, AI, and other businesses. Its infrastructure is well integrated with space and time, which can create agents that better meet the needs of the blockchain. Compared to other AI computing power network platforms, it paid earlier attention to the AI agents building platform. This platform has a well-developed architecture, and the team has already developed 20 skills, a DeFi agent, and Houston of space and time.

Section II

Blockchain Community and Market Update

Token2049 Held in Singapore

Token2049 was held at Marina Bay Sand in Singapore from September 13-14, with a total of over ten thousand participants and more than 200 project booths. Ethereum founder Vitalik Buterin, BitMEX founder Arthur Hayes, Gemini CEO Tyler Winklevoss, Circle CEO Jeremy Allaire, and several other well-known figures both inside and outside the industry participated in the summit.

In addition to the main venue event, the F1 Singapore Grand Prix happened to be held over the weekend, with many events combined with the car race. From September 11 to September 17, more than 200 sub-venue events were held in Singapore. The hotspots in this conference focused on compliance regulation, payment, RWA, layer2, social and other fields.

Commentary:

Token2049 landed in Singapore for the second year, and this year there was a significant increase in the event's popularity. More information exchanges and activities were not at the main venue, and sub-venue activities held by participating projects and VCs provided more opportunities for exchanges. For project parties, it is more about seeking financing through this opportunity. Although the event was very lively, the financing market remains cool.

HASHKEY Capital

The 9th Wanxiang Blockchain Summit Held in Shanghai

From September 15-20, the 9th Shanghai International Blockchain Summit was officially held. The summit continued the model of previous years, with the hackathon and developer conference held in the first three days and the main venue conference held on 19-20. Given the mainland China's restrictions on the token economy, the main topics of this conference included technical topics such as Web3.0, industrial blockchain, metaverse, AI, etc., and gave more explanations on business models and technology development.

Commentary:

Since Token2049 was held last week, and mainland China's crypto business has moved to Hong Kong, and China's related policies also chose to pilot in Hong Kong. This Shanghai summit had fewer participants than in previous years. The HKweb3 held in Hong Kong in April also took away some traffic. The summit in Shanghai was more of a gathering of developers, as well as a blockchain reform for the real economy and government.

HASHKEY Capital

Friend.tech Explodes in Social Network, Tipcoin Fan Economy Rises Again

The test version of Friend.tech was launched on August 10, with more than 30,000 transactions and a trading volume of 4,400 ETH in the first 24 hours. With the continuous spread of the community and the boost from various KOLs, the overall active users are showing a rapid upward trend. The potential airdrop of Tipcoin bound to Twitter and used by Friend.tech has also been hotly pursued by the market, and everyone wants to get a share in the new web3 social application. Friend.tech's innovative model allows KOLs to issue their own fan tokens, and also gives KOLs the ability to monetize certain traffic.

Commentary:

On September 19, the governance token Tip of Friend.tech was launched, and it started to gradually decline after a brief boom. This reminds everyone of several Web3 social Apps that were hot in the past two years, such as Clubhouse, MonacoPlanet, and Bitclout (Deso). The token airdrop model easily allows the community to spontaneously promote and rapidly expand, but more users do not have the motivation to continue using it after the airdrop, Web3 social apps still need to innovate from the product itself. Friend.tech is currently in a hot period, and whether it can have the motivation for continuous growth after the heat passes needs to be observed in the future.

PEPE Team Disputes, Multisig Address Assets are Sold Off

The newly risen Memecoin PEPE experienced rapid growth and expansion in the middle of this year, and its market value once chased DOGE and SHIB. However, the subsequent development of PEPE is far less than the latter two. On August 26, a large transaction suddenly appeared in the PEPE team's multisig address, transferring assets from the multisig address to multiple wallets, and some assets entered exchanges such as Binance and OKX for sale. Subsequently, news broke out that there was a dispute within the team, which involved the issue of uneven distribution of benefits. This caused panic among investors and the coin price continued to plunge by more than 50%. This also caused a problem with PEPE's consensus, and the price drop may be difficult to recover.

Commentary:

The development of Memecoins is often part of crypto communities, and the success rate of future transformation through community governance is low. Caution should be exercised when participating in such trades. Losing community consensus can easily pop the memecoin bubble

HASHKEY Capital

Progress of Bitcoin Spot ETF

According to Bloomberg data, there are currently nine applications for Bitcoin ETFs and two for Ethereum ETFs. The SEC's overall statement has been unclear, and it has currently decided to postpone the decision at the first deadline. The market expects a high probability of making a decision at the third deadline or final deadline on whether to approve some Bitcoin ETFs. The estimated time is around January-March 2024. Although the recent XRP lawsuit has been won, the SEC's attitude towards the cryptocurrency market is still very strict, and market uncertainty remains high.

Commentary:

After the application for ETFs came out in July 2023, the short-lived market heat soon passed, and the US Congress and the SEC have significant differences of opinion regarding crypto. Industry insiders are generally optimistic about the approval of the Bitcoin ETF. Given BlackRock's extremely high application approval rate in the past, the approval of the ETF may just be a matter of time.

September FOMC Meeting Does Not Raise Interest Rates, Fed Remains Conservative, Future Still Uncertain

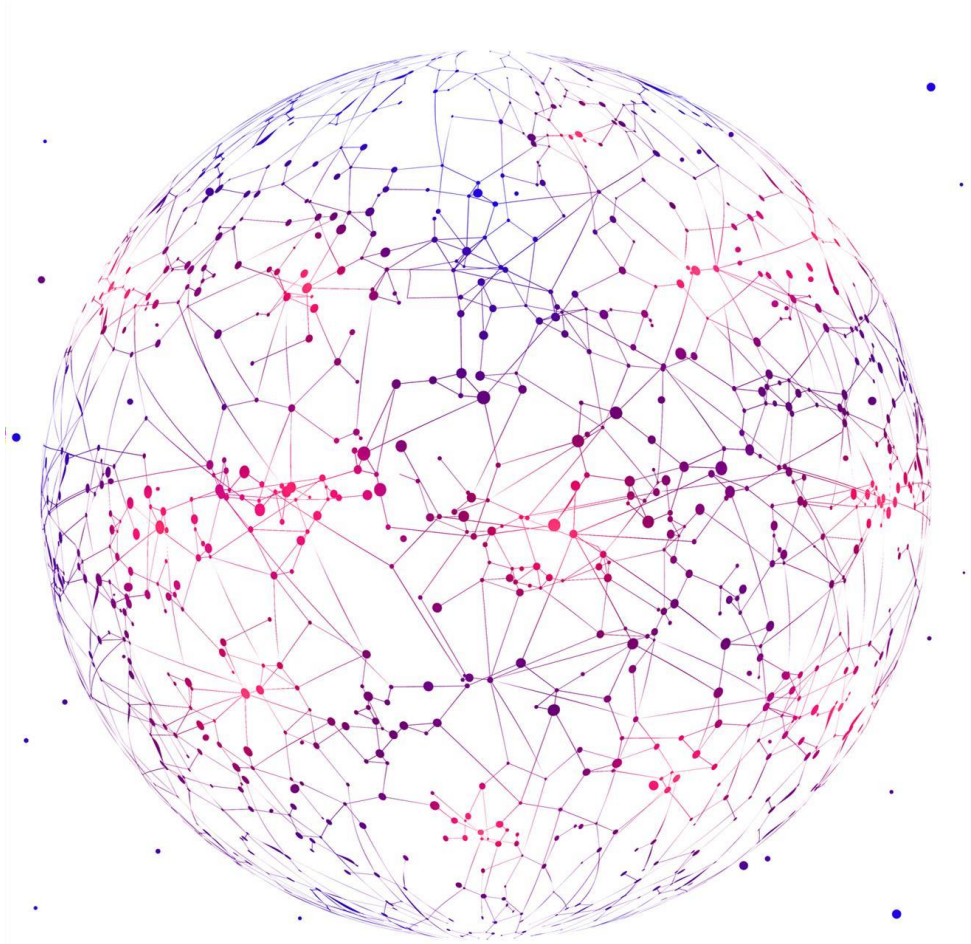
In the early morning of September 20, Hong Kong time, the FOMC meeting was held, and US Federal Reserve Chairman Jerome Powell announced that interest rates would remain unchanged. However, the consensus is that there is still a need for a rate hike this year, and the market expects that the rate cut will be postponed until September 2024. In the previously released September CPI data, the CPI rose by 3.7%, rebounding from the previous two months. Due to rising energy prices, the core CPI rose by 4.3%, reflecting a significant rebound. This also indicates that the Fed's goal of controlling inflation has not yet been achieved.

Commentary:

The Fed's expectations for inflation are becoming clearer, and the market's reaction to the FOMC is getting smaller. Current interest rates are already sufficient to limit inflation, and the short-term inflation rebound is more due to energy impacts. More optimistic expectations might come after the next quarter.

Section III

Listed Companies & Token



Crypto mining company Argo reported a net loss of $18.8 million in the first half of the year and repaid $4 million in debt.

Source: https://cointelegraph.com/news/argo-blockchain-cuts-2022-debt-by-half-down-to-75m

Iris Energy, a mining company, produced 410 BTC in August, with mining revenue of approximately $11.45 million.

Source: https://irisenergy.gcs-web.com/news-releases/news-release-details/iris-energy-announces-monthly-investor-update-august-2023

Cathedra Bitcoin, a Bitcoin mining company, generated a revenue of $2.14 million in Q2 and produced 77.15 BTC.

Source: https://www.businesswire.com/news/home/20230829115319/en/Cathedra-Bitcoin-Announces-Second-Quarter-2023-Financial-Results

Section IV

China Blockchain Headlines

People's Daily: Promoting the Development of the Blockchain Industry through Standardization

The People's Daily published an article stating that the first national standard for the field of blockchain technology has been introduced. Recently, the "Reference Architecture for Blockchain and Distributed Ledger Technology" was officially released, which provides specifications for the functional architecture and core elements of blockchain systems. It serves as a reference guide for the industry to achieve a unified understanding of blockchain concepts, construct and improve blockchain systems, and select blockchain services. This standard is a fundamental and general guideline for guiding the application and development of blockchain technology in China and has already been implemented in hundreds of typical blockchain enterprises.

The establishment of standards is one of the signs of the maturity of an industry. Over the past few years, blockchain technology has rapidly emerged and its applications have expanded in various fields such as finance, energy, supply chain, and judiciary. Previously, China has issued dozens of industry and group standards for the blockchain, but the effectiveness of these standards in practice has not been ideal, and there has been a lack of a "common language" among different blockchain systems. The development of national standards will help achieve secure and trustworthy information interaction among different blockchain systems, promote the construction of an open-source ecosystem, and accelerate the development of a complete blockchain industry chain.

Chengdu Provides Special Subsidies to the Blockchain Industry

According to the Chengdu Municipal Economic and Information Bureau and the New Economy Commission, the "Implementation Rules for the Special Policies for the Construction of National Blockchain Innovation Application Comprehensive Pilot Projects in Chengdu" and the "Implementation Rules for the Special Policies for Promoting the Development of Big Data Industry in Chengdu (Revised)" have been recently released to support the development of related industries. The construction of blockchain technology evaluation agencies will receive a one-time subsidy of up to 2 million yuan, while enterprises that independently invest in the construction of data service platforms will receive a subsidy of up to 3 million yuan.

Section IV

China Blockchain Headlines

Zhejiang: Accelerating the Construction of Future Industries in the Metaverse and Encouraging Major Achievements in Blockchain and Other Fields

Zhejiang held a provincial conference on the high-quality development of the platform economy, with representatives from 100 platform enterprises such as Alibaba and NetEase in attendance. This is the first provincial conference in China focused on the platform economy. During the conference, the "Implementation Opinions on Promoting the High-Quality Development of the Platform Economy" was released, marking the first set of implementation opinions for promoting the high-quality development of the platform economy nationwide. The "Opinions" encourage platform enterprises to achieve significant landmark achievements in areas such as blockchain and promote the construction of computing power infrastructure. Platform enterprises are also encouraged to utilize innovative technologies such as blockchain to create diverse future-oriented application scenarios. Efforts will be accelerated to build new advantages in the future industry of the metaverse, support the construction of comprehensive experimental platforms for the metaverse by diverse entities, strengthen the application of the metaverse in various scenarios, and comprehensively promote the industrialization, scaling, and internationalization of the metaverse industry chain. Platform enterprises are encouraged to participate in the pilot projects for digital currency (Digital RMB).

HASHKEY Capital

Bitcoin Scaling Solutions

As we all know, Bitcoin produces a block approximately every 10 minutes and can process around 7 transactions per second. However, the block space and the number of transactions it can accommodate are limited. Therefore, users need to compete by bidding higher fees to miners in order to have their transactions included in blocks as quickly as possible. Apart from the issue of transaction speed, Bitcoin lacks the ability to execute smart contracts in the traditional sense due to the design of its scripting language. Developers need to use script operations combined with cryptographic techniques for application programming. This poses significant challenges to scalability and ecosystem development.

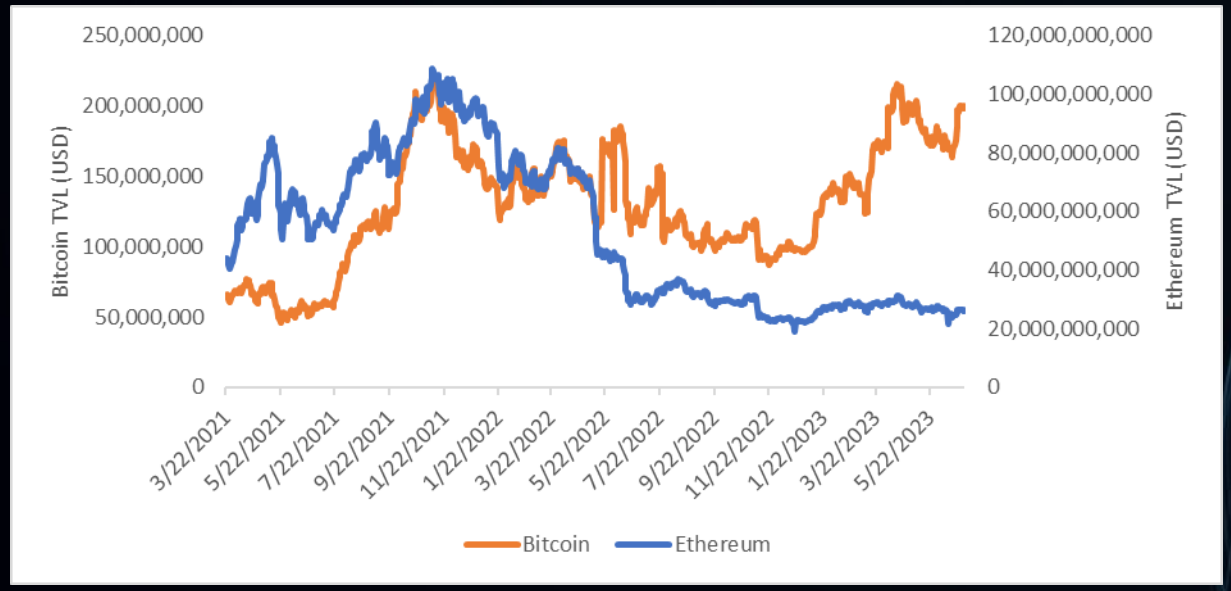
In simple terms, unlike Ethereum, Bitcoin's scripting design is based on a stack, and the scripting language only supports basic operations such as addition and subtraction. It lacks looping structures and cannot directly implement loop operations, making it more streamlined. The original intention of Bitcoin's design was to create a peer-to-peer payment system. Looping structures introduce complex code logic, are prone to errors during execution, and consume a significant amount of computational resources. Therefore, the absence of looping structures in Bitcoin's design helps ensure the security of Bitcoin transactions to a certain extent. Ethereum, on the other hand, supports Turing-complete smart contract development using the Solidity language. Smart contracts in Ethereum can utilize loop statements such as for, while, do-while, if-else, and switch to implement loop operations, making them more versatile and flexible in terms of functionality. However, executing loop operations on the blockchain is subject to certain limitations.

*June 2023

HASHKEY Capital

Bitcoin Scaling Solutions

The following chart shows that the current TVL in Bitcoin is around 200 million USD, while Ethereum's TVL is approximately 20 billion USD. Although BTC's locked amount has been increasing since January 2023, the difference in the monetary value between the two ecosystems is roughly 100-fold. DeFillama calculates the TVL of both ecosystems by aggregating the locked amounts of most protocols within each ecosystem.

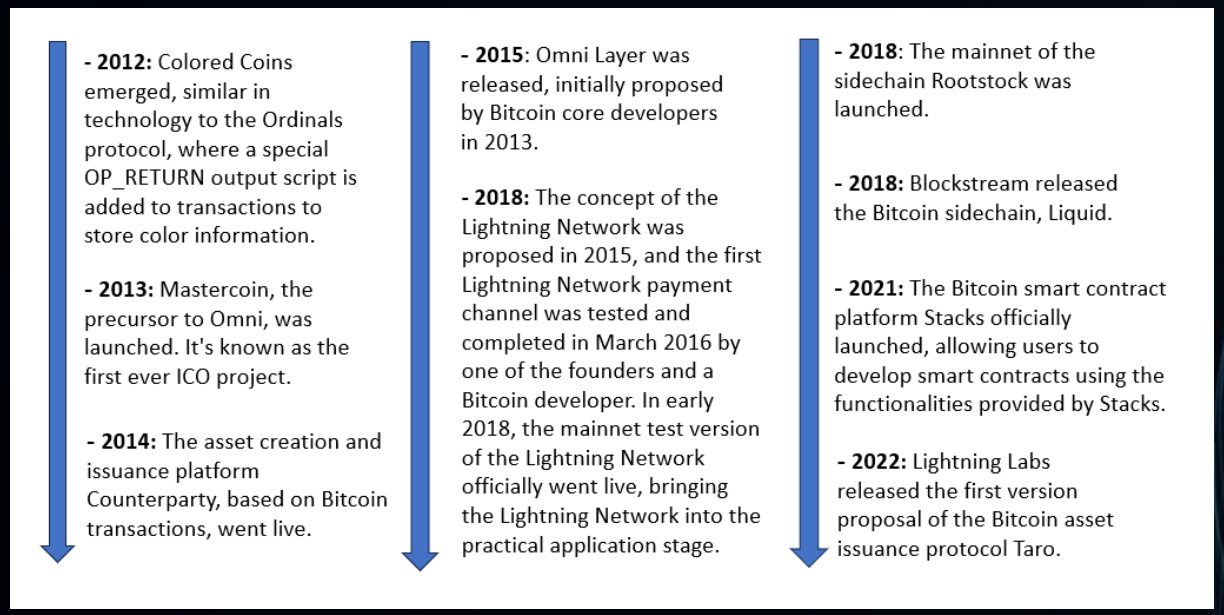


Source：Defillama

HASHKEY Capital

Bitcoin Scaling Solutions

For a significant period of time after Bitcoin's emergence, it was widely regarded as a value storage asset similar to gold. DeFi activities in the Bitcoin ecosystem primarily revolved around wrapped assets like wBTC and RenBTC, which are cross-chain representations of Bitcoin. The development of native applications within the Bitcoin ecosystem has been relatively scarce. Bitcoin, known for its stability and secure blockchain network, has been continuously explored for its potential beyond value storage. Following the launch of the Bitcoin mainnet, several underlying protocol projects have been exploring Bitcoin's scalability. The roadmap below illustrates the major scaling events that have taken place since the launch of the Bitcoin mainnet.



Source：Complied by HashKey Capital

HASHKEY Capital

Bitcoin Scaling Solutions

Regarding Bitcoin's scalability solutions, there are various options available, including Lightning Network, Stacks, Rootstock (RSK), Liquid Network, RGB Protocol, Taproot Assets, Drivechain, Statechains, Rollkit, Omni, and more. Due to space limitations, let's focus on analyzing the following five solutions: Lightning Network, Stacks, Rootstock (RSK), Liquid Network, and RGB. The table below provides a comparison of these five solutions:

	Lightning Network	Stacks	Rootstock（RSK)	Liquid Network	RGB
Establishment year	2015	2018	2015	2018	2018
Team	Joseph Poon and Thaddeus Dryja published a white paper, and Joseph Poon is also one of the co-founders of the Plasma project.	Blockstack PBC	IOV Labs, with one of its co-founders being Lucas Llach, is a company that includes an economist and an early supporter of Bitcoin among its founders.	Blockstream	Giacomo Zucco and Alekos Filini and other Bitcoin developers.
Nature	Payment Channel	Smart Contract Platform	Sidechain	Sidechain	Asset issuance Protocol
Consensus	NA	PoX	PoW Merged Mining	Signing	NA
Independent of Bitcoin miners	NA	Yes	No	Yes	NA
Block Interval	NA	10 minutes currently, but after the Satoshi Nakamoto upgrade, it would be approximately 4-5 seconds.	30s(average)	1min	NA
TVL（$M)	147.22	27.43	94.77	96.37	NA
Anchored assets	NA	SBTC	RBTC	LBTC	NA
Token	NA	STX	RSK	NA	NA

HASHKEY Capital

Bitcoin Scaling Solutions

Regarding Bitcoin's scalability solutions, there are various options available, including Lightning Network, Stacks, Rootstock (RSK), Liquid Network, RGB Protocol, Taproot Assets, Drivechain, Statechains, Rollkit, Omni, and more. Due to space limitations, let's focus on analyzing the following five solutions: Lightning Network, Stacks, Rootstock (RSK), Liquid Network, and RGB. The table below provides a comparison of these five solutions:

	Lightning Network	Stacks	Rootstock（RSK)	Liquid Network	RGB
Introduction	• It is an off-chain payment channel with its own independent network nodes. To communicate with the Bitcoin main chain, specific transactions need to be created on the main chain. • It has low fees, fast transactions, and has a higher capacity, number of channels, and number of nodes compared to several other solutions. The ecosystem is also relatively diverse and well-developed.	• It can be seen as the programming layer of Bitcoin, supporting smart contracts. • It was the first to receive SEC approval for fundraising. • It has introduced its own ecosystem with a smart contract language called Clarity.	• It is compatible with the Ethereum Virtual Machine (EVM), allowing smart contracts to be written in the Solidity language, which facilitates integration with the Ethereum ecosystem.	• It is a settlement network between exchanges, brokers, market makers, and other institutions. • The network is maintained by a consortium of 60 members. • It offers good transaction privacy and has the ability to issue assets.	• It is a decentralized protocol without the concept of a blockchain. It binds with the Bitcoin mainnet through commitments anchored in UTXOs, thereby endorsing the issuance and transfer of assets. • It has strong privacy and is compatible with the Lightning Network, serving as a Layer 2 or Layer 3 solution.
Ecosystem Projects	LND, Breez, bluewallet, muun, strike, Joule, etc.	Alex, Arkadiko, Citycoins, etc.	Sovryn, MoneyOnChain, etc.	Hodl Hold， Sideswap, etc.	DIBA， Iris Wallet, Bitmask, My Citadel， COSMINMART， Bitswap- BiFi, etc.
Key investment and financing events	•In April 2022, Lightning Labs completed a Series B financing round of $70 million, led by Valor Equity Partners. • In May 2022, Lightspark, founded by Meta's Cryptocurrency Head David Marcus, completed a funding round of $173 million, at a valuation close to $1 billion, led by a16z and Paradigm. • In September 2022, Strike announced the completion of a Series B funding round of $80 million.	• In February 2022, Trust Machines, a project in the Stacks ecosystem, completed a financing round of $150 million, with participation from DCG and others. • In March 2022, Mechanism, another project in the Stacks ecosystem, completed a financing round of $8 million.	• In May 2016, the company completed a financing round of $1 million. • In May 2017, the company completed a financing round of $3.5 million.	• In January 2023, Blockstream secured $125 million in funding, bringing the total funds raised to $265 million.	NA

HASHKEY Capital

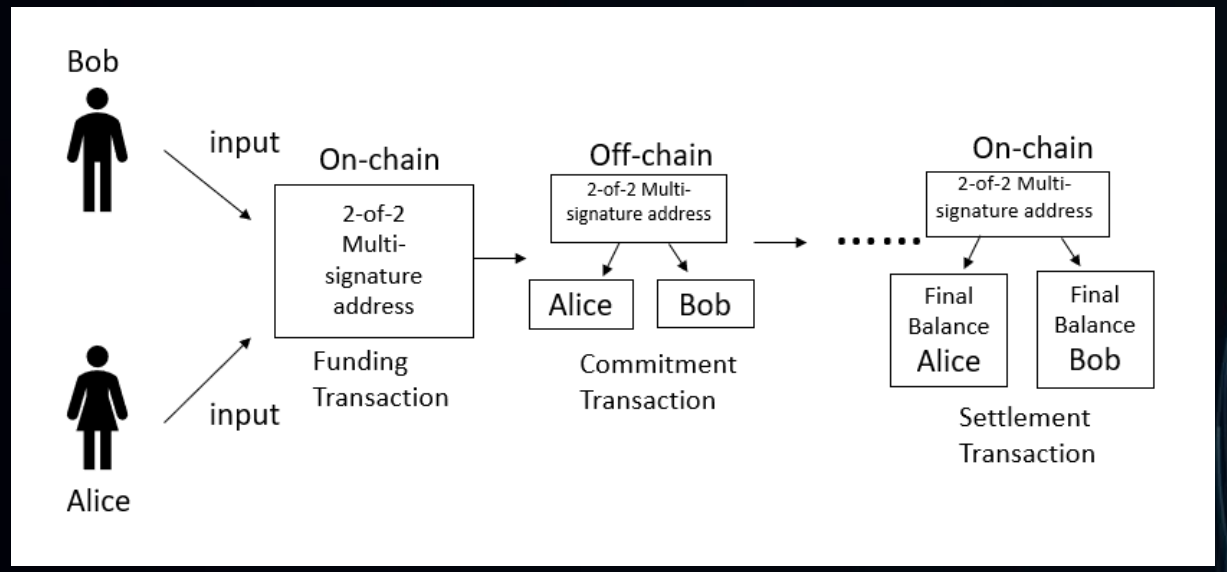
2.1 Lightning Network

The Lightning Network, one of the early Bitcoin scaling solutions, originated in 2015 when Joseph Poon and Thaddeus Dryja published a whitepaper introducing a decentralized payment solution based on Bitcoin. This is considered the inception of the Lightning Network. The Lightning Network is an off-chain payment protocol that operates with its independent network of nodes. Communication between the Lightning Network and the Bitcoin main chain requires the creation of specific transactions on the main chain.

HASHKEY Capital

2.1.1 Technical Principle

Let's briefly review the working principle of the Lightning Network, as shown in the diagram below. The Lightning Network operates by participants creating a multi-signature address (a script hash or P2SH address). Opening a channel requires only one transaction, while closing a channel requires another transaction. All intermediate transactions occur off-chain. The initial funding transaction determines the channel's balance and needs to be broadcasted on-chain. The final settlement transaction (either initiated by both parties or a single party) also needs to be sent to the blockchain. All intermediate transactions, known as commitment transactions, are executed off-chain. The entire channel operates as a trustless channel, with potential fraud mitigated through Hash Time-Locked Contracts (HTLCs) and Asymmetric Revocable Commitments.

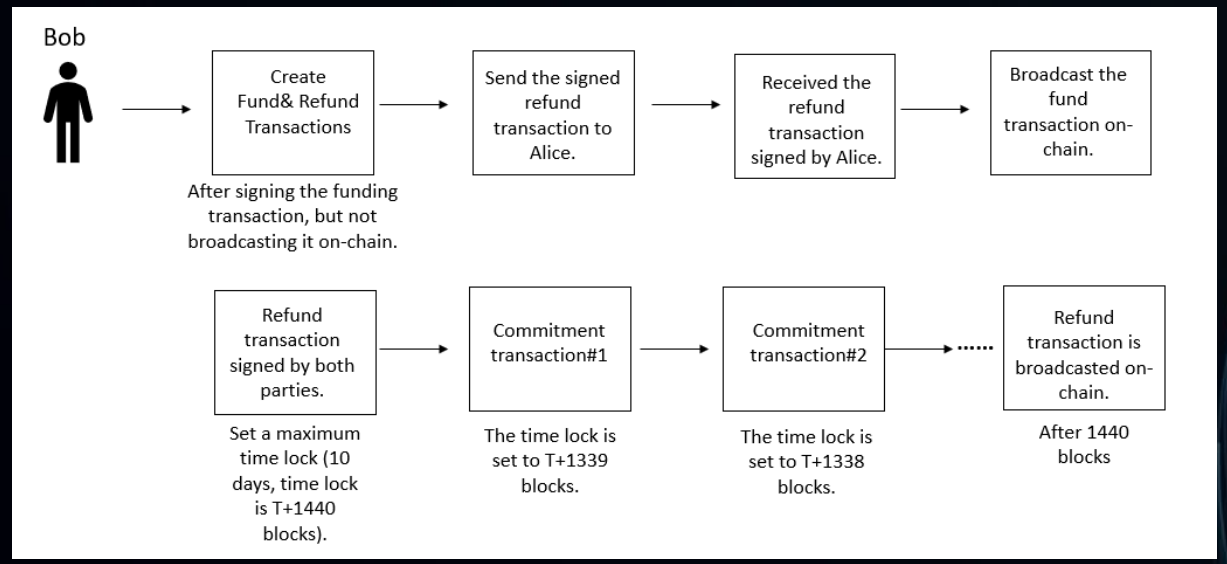


Source：https://medium.com/softblocks/lightning-network-in-depth-part-1-payment-channels-b943607950dd, Compiled by HashKey Capital

HASHKEY Capital

2.1.1 Technical Principle

Hash Time-Locked Contracts (HTLCs): In order to ensure that funds are not permanently locked in a channel and to prevent a sudden disappearance or offline situation of one party, both parties do not immediately share and broadcast the funding transaction when creating it. Instead, they first create a refund transaction as the initial commitment transaction. After receiving the counterparty's signature on the refund transaction, they broadcast the funding transaction to open the channel. The refund transaction has a time lock set, determining the duration of the Lightning Network channel. Each subsequent commitment transaction has a time lock that is earlier than the previous transaction, allowing the latest transaction to be broadcasted to the blockchain. The diagram below illustrates this process.



Source：https://medium.com/softblocks/lightning-network-in-depth-part-1-payment-channels-b943607950dd, Compiled by HashKey Capital

HASHKEY Capital

2.1.1 Technical Principle

In short, time locks serve the following purposes:
(1) Preventing one party from going offline and preventing the other party from retrieving funds from the multi-signature address.
(2) Avoiding malicious use of older commitment transactions.
However, the HTLC mechanism has two weaknesses:
(1) There are limits to the number of transactions and the duration of the channel.
(2) Participants need to constantly monitor the blockchain to ensure the successful on-chain execution of the final commitment transaction.

Asymmetric Revocable Commitments : To address the limitations of time lock-based solutions and mitigate the risk of maliciously broadcasting earlier commitment transactions, an additional measure is implemented known as "Asymmetric Revocable Commitments." In simple terms, both parties create incomplete signatures and utilize a "revocation key" to ensure that maliciously broadcasting previous transactions becomes unprofitable or even results in penalties for the participant. This approach eliminates the need for channel lifespan restrictions and transaction quantity limits imposed by time locks, while effectively preventing malicious behavior. Essentially, it involves constructing a punitive transaction as a deterrent.

HASHKEY Capital

2.1.1 Technical Principle

Routing

In the Lightning Network, when there is no direct payment channel between two nodes, it is necessary to request intermediate nodes to relay the payment. The Lightning Network uses a routing algorithm based on Dijkstra's algorithm. The goal of the routing algorithm is to find the shortest path that allows the payment request to be forwarded through as few intermediate nodes as possible, minimizing fees and delays.

Intermediate routing nodes have the option to accept or reject payment requests and decide whether to forward them to the next node. These routing nodes charge a fee for relaying payments, which is determined by the amount being forwarded. Additionally, they need to have sufficient payment channel balance to relay the payment. When a node receives a payment request, it checks if its payment channel balance is enough to fulfill the payment and cover the associated fees. If the balance is insufficient, the node cannot forward the payment request and returns an error message.

To provide payment forwarding services on the Lightning Network, it is essential to ensure that the payment channel balance is sufficient to accommodate any potential payment requests reaching the node. This requires timely replenishment of payment channels. If a node cannot forward a payment request, it can forward the request to neighboring nodes until it finds a node with enough balance to fulfill the payment request.

Sender A------> Node B ------> Node C ------Recipient D

HASHKEY Capital

2.1.1 Technical Principle

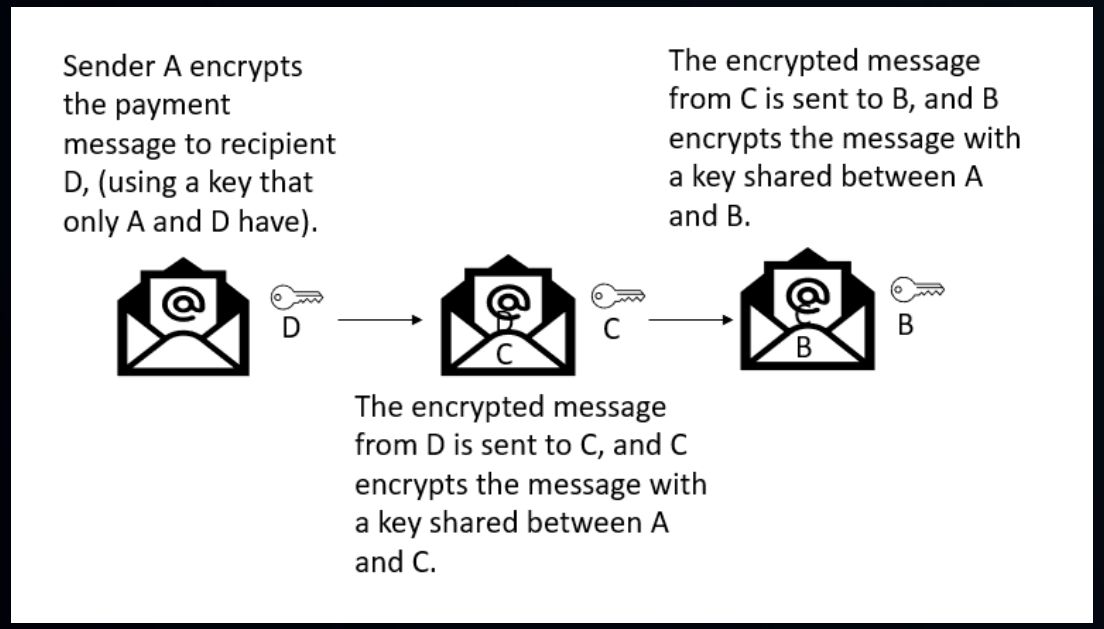
The Lightning Network employs **Onion Routing** to protect payment privacy. Its workings are similar to Onion Routing in the Tor network, where payment information is hidden through multiple layers of encryption and decryption, preventing the identification of senders and recipients. When a payment request is initiated in the Lightning Network, it is forwarded through several nodes. Each node only knows the identity of the previous and next nodes in the route, without knowledge of the entire payment path or the identities of the sender and recipient. Additionally, nodes are unaware of their own position in the route. At each node, the payment request is re-encrypted and forwarded to the next node until it reaches the final destination. The endpoint node decrypts the payment request and completes the transaction.

Onion Routing safeguards payment information from interception or tampering by intermediate nodes, enhancing the security and privacy of payments within the Lightning Network. However, it may introduce some latency and reduce efficiency as each node needs to perform encryption and decryption operations, requiring substantial computational resources, bandwidth, and potentially higher fees.

HASHKEY Capital

2.1.1 Technical Principle

The following diagram provides a simplified representation of the Onion Routing principle. Starting from the endpoint D, each intermediate node can only access a message specifically created for it (e.g., the message received by the first intermediary B is "forward the message to C"), unaware of the message's content or the entire payment path.



Source：Complied by HashKey Capital

Subsequently, the Lightning Network has undergone technological advancements such as the Watchtower mechanism (punishing dishonest nodes), submarine swaps (enhancing Bitcoin's on-chain/off-chain interoperability), and Atomic Multi-Path Payments (solving payment failures caused by flaws in the routing economic model).

HASHKEY Capital

2.1.2 Adoption Status

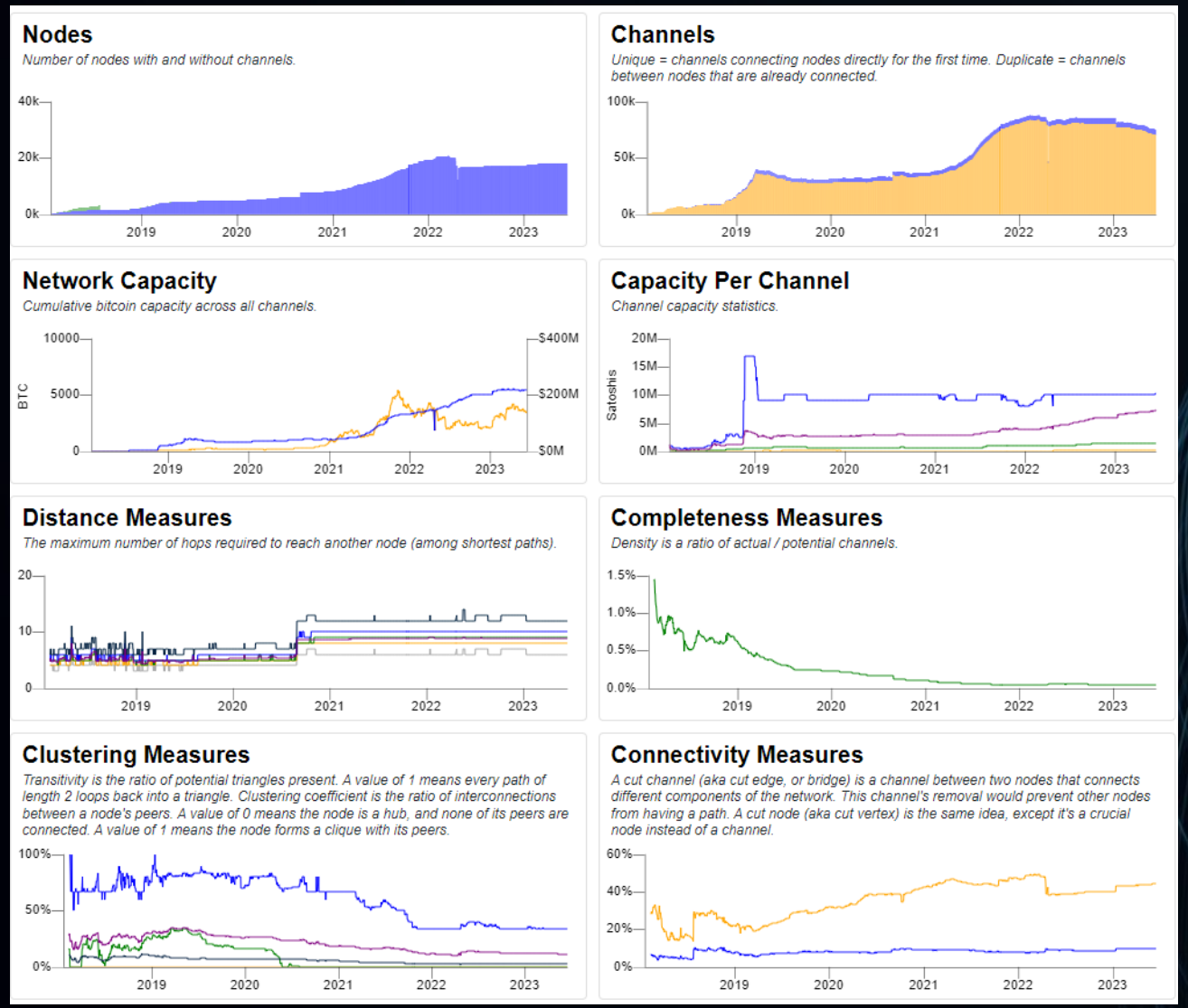
According to Bitcoin Visual data, as of June 29, 2023, the number of Lightning Network nodes has reached 18,048, with 70,295 channels and a capacity of around $140 million. Over the past few years, there has been an overall upward trend in the Lightning Network's adoption, with notable increases in capacity. Particularly, there was a significant growth of 40 times from July 2018 to May 2019 within a ten-month period, as well as a doubling of capacity from January to July 2021.

The initial phase of growth was mainly driven by the launch of the Lightning Network mainnet, while the second phase was influenced by the overall decrease in Bitcoin's on-chain fees and El Salvador's announcement of adopting Bitcoin as legal tender.

In terms of channel funding distribution, the United States accounts for over 60% of the capacity, followed by Germany at 7%, Canada at 3%, and the remaining 30% distributed among other countries and regions. The majority of Lightning Network activity is concentrated in European and American countries.

HASHKEY Capital

2.1.2 Adoption Status

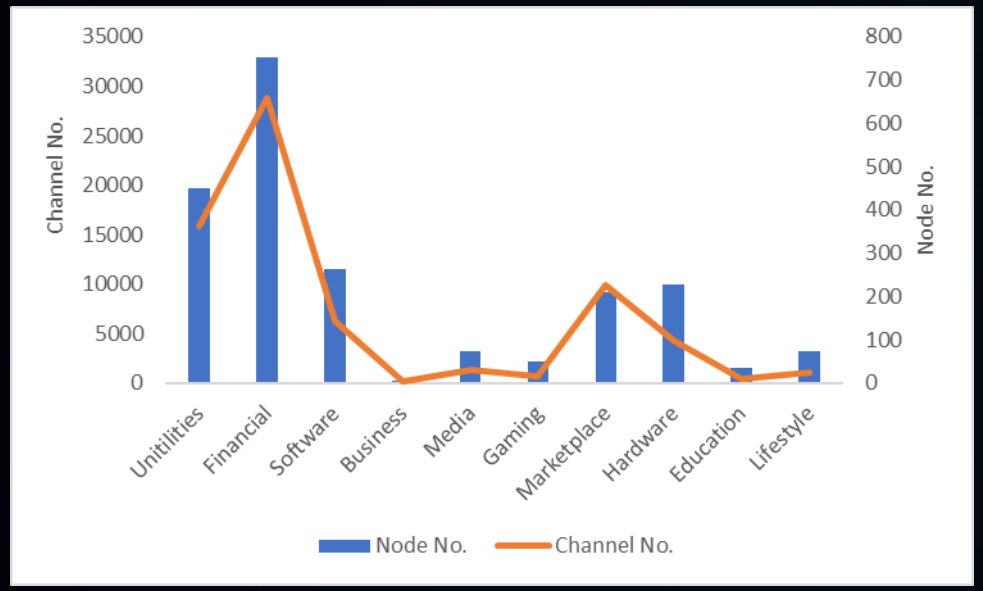


Source：bitcoin visuals

HASHKEY Capital

2.1.3 Ecosystem

Here is a summary of the proportion of application nodes categorized by different sectors. It can be observed that the most significant application direction for nodes and channels is in the financial sector.



Source：1ml.com

As an early Bitcoin scaling solution, the Lightning Network has developed a relatively rich ecosystem, primarily consisting of three major categories of use cases:

- Infrastructure/Node Management Services
- Wallets/Payments
- Gaming/Social/Retail Scenarios

HASHKEY Capital

2.1.3 Ecosystem

Below is an overview of the ecosystem:

Infrastructure/Node Service/Management

Wallet/Payment

Gaming/Retail/Social//Others

Source：Arcane Research, Compiled by HashKey Capital

HASHKEY Capital

2.1.4 Limitations

As mentioned earlier, being an early Bitcoin scaling solution, the Lightning Network has experienced fluctuations in capacity, node count, and channel count, showing an overall upward trend. However, there are still some limitations that exist:

- **Large Node Monopoly and Centralization Risk**: The services provided by Lightning Network nodes are relatively homogeneous, with the main differentiating factor being the number of nodes they are connected to. Additionally, due to the fee structure, opening multiple payment channels incurs costs. Therefore, larger nodes that are connected to more channels have an advantage, as they save on channel opening fees and are more likely to have successful transactions. As a result, smaller nodes have minimal survival space, and their earnings are insufficient to cover the costs of setup, operation, and locked-up funds. The monopoly of large nodes presents a certain degree of centralization risk to the entire network.

- **User Onboarding and Inbound Liquidity Issues**: New users can join the Lightning Network by establishing channels (recharging) with existing nodes in the network, known as single-funded channels. This mechanism prevents attackers from easily creating numerous channels and locking up their funds. However, it also leads to inbound liquidity issues for users. After the channel is established, liquidity exists only on the side of the new user, while their counterpart has not recharged the channel. Consequently, the new user cannot receive funds through this channel and can only make outgoing payments. This creates challenges for users in terms of initial setup and usage. Some current workarounds include using wallets with liquidity service providers (LSPs), such as Breez, to quickly access the network or renting channel liquidity from marketplaces like Amboss Space. Additionally, solutions like dual-funded channels are being designed and implemented.

- **Dependence on Online Node Support**: The Lightning Network relies on the support of online nodes to forward and process payment requests. If a node is offline, it cannot participate in the forwarding and processing of payment requests, impacting the performance, availability, and liquidity of the network. Current workarounds include certain mobile wallets using background monitoring or system notifications to prompt users to switch to an online state. Additionally, asynchronous payments, which are currently being designed and implemented, will allow funds to be temporarily held at intermediate forwarding nodes when the receiving node is offline, and the final transfer can occur once the receiving node comes online.

Disclaimer

The information contained in this document has been compiled by HashKey Group (as defined below) from sources believed to be reliable, but no representation or warranty express or implied is made by HashKey Group, its affiliates or any other person as to its fairness, reasonableness, reliability, accuracy, completeness or correctness. All illustrations, examples or forward-looking information (if any) contained in this document have been provided in good faith for illustrative purposes only as of the date of this document, and are not intended to serve as, and must not be relied upon as, a guarantee, an assurance, a prediction or a definitive statement of fact or probability. Whilst efforts are made to ensure the accuracy and completeness of the information contained in this document at the time of publication, errors or omissions may occur. Past performance is not a guide to future performance, future returns are not guaranteed, and a loss of original capital may occur. HashKey Group reserves the right to correct any errors or omissions, and to change or update information at any time without prior notice.

Each legal jurisdiction has its own laws regulating the types of investments and/or services which may be offered to its residents and/or in its jurisdiction, as well as the process for doing so. As a result, certain investment products or services discussed in this document may not be eligible for sale or offered in some jurisdictions. This document is not an offer to sell or a solicitation of an offer to purchase any investments or services. Unless otherwise specified, HashKey Group does not hold itself out to be licensed to carry on regulated activities in any jurisdiction. Additionally, providing this material is not, and under no circumstances should be construed to act as a regulated business in any jurisdiction by any person or company that is not legally permitted to carry on such regulated business in that jurisdiction.

Nothing in this document constitutes legal, accounting, or tax advice, and you are advised to seek independent legal, tax and accounting advice prior to acting upon anything contained in this document. The contents of this material have not been reviewed by any regulatory authority. Investors are advised to exercise caution in relation to any investments or services in relation to this document. If you are in doubt about any of the contents of this material, you should obtain independent professional advice.

To the full extent permitted by law, neither HashKey Group nor any of its affiliates accepts any liability whatsoever for any direct or consequential loss arising from any use of this document or the information contained herein. No information contained in this document may be reproduced or copied by any means without the prior written consent of HashKey Group.

“HashKey Group” is a brand name to describe any one or more entities of the group companies composed of HashKey Digital Asset Group Limited and its Affiliates.

hashkey.capital | ir@hashkey.com