



HASHKEY
Capital

ASIA CRYPTO INSIGHTS

OCT 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

Section I	Blockchain and Crypto Deals	— 4
Section II	Blockchain Community and Market Update	— 7
Section III	Listing Companies and Token	— 13
Section IV	China Blockchain Headlines	— 14
Section V	Feature Piece: Bitcoin Scaling Solution Overview	— 16

Blockchain and Crypto Deals

Membrane Labs

Membrane Labs, an enterprise-grade digital asset management and settlement platform, raised \$20 million in a Series A funding round with participation from Brevan Howard, Point72 Ventures, Jane Street, Jump, Two Sigma Ventures, Electric Capital, Framework Ventures, and GSR.

Commentary by HashKey Capital:

Membrane Labs provides modular, enterprise-grade software for managing, trading, and lending digital assets. Membrane offers cross-custodial settlements, lifecycle position servicing, and improved capital efficiency to serve the needs of financial institutions and individuals with a secure, streamlined approach to digital asset management. With their flagship product, Membrane, users can effortlessly engage in management and settlement of OTC spot, derivatives, lending, and collateral management.

The digital asset space has been blighted by friction from poor UI/UX, which has led to the loss of millions of dollars in cryptocurrency. Addressing this friction with institutional-grade infrastructure is vital for bringing new capital into the space, and a cap table decorated with institutional, traditional finance investors is a very good sign for the future of our industry.

Parsec

Parsec, a DeFi and NFT analytics platform, raised \$4 million in a seed funding round led by Galaxy Digital, with participation from Uniswap Labs, Robot Ventures, and CMT Digital.

Commentary by HashKey Capital:

Parsec offers modular dashboards with real-time data feeds, custom charts and graphs, and technical analysis tools for assessing digital assets. With over 100 different interchangeable components, Parsec provides unique insights and expansive functionality to digital asset traders for both fungible and non-fungible tokens.

All transactions and positions in DeFi are public and can be viewed openly on block explorers, but transmuting this raw data into actionable insights so far has been a complex task. For years now, Parsec has been on the cutting edge of resolving this problem, informing traders on key metrics to power trading decisions. We're watching closely as Parsec continues to lead the way in creating transparent and accessible DeFi ecosystem across multiple chains and ecosystems.

Blackbird

Blackbird, a restaurant discovery and loyalty rewards app in the Base ecosystem, has raised \$24 million in Series A funding in a round led by a16z crypto, with participation from American Express Ventures, QED investors, Union Square Ventures, Variant Capital, Shine Capital, and Rustic Canyon.

Commentary by HashKey Capital:

Blackbird allows users to discover restaurants and accumulate rewards, perks, and their native \$FLY token whenever they dine at spots within the network. Users can also read reviews, make reservations, and earn cashback rewards, which can be redeemed for future meals. Customers tap their phones on near field communication (NFC) readers -- the devices that allow smartphones to connect to payment readers -- and mint a membership NFT to prove their attendance at restaurants within the Blackbird network.

Blackbird represents a shift in consumer crypto apps, as the blockchain infrastructure is abstracted away from the user as much as possible. This is an incredibly important change that is fast becoming the norm among consumer Web3 apps, as they strive to become more user-friendly and therefore more approachable for non-crypto natives. As investors, we're very excited to see Blackbird and similar consumer apps driving mass adoption for blockchain-based products in mainstream markets.

Section II

Blockchain Community and Market Update

- **About the BTC ETF**

On September 6, 2023, Ark Invest and 21 Shares submitted an application to the U.S. Securities and Exchange Commission (SEC) for a proposed ETF called ARK 21 SHARES ETHEREUM ETF. This is the first Ethereum spot ETF application submitted in the United States, although not the first worldwide. Canada had already approved the trading of Ethereum spot ETF for Canadian investors in 2021.

Bitwise also submitted an amended prospectus for an equal-weight Bitcoin and Ethereum futures ETF, which might be launched alongside VanEck's ETF. Asset management giant Invesco submitted an application to the U.S. SEC for an Ethereum spot ETF named "Invesco Galaxy Ethereum ETF," with Galaxy Digital Funds LLC serving as the ETF's executive agent to facilitate its Ethereum sales. At the same time, Grayscale has partnered with NYSE Arca to apply for the conversion of Grayscale Ethereum Trust into an Ethereum spot ETF. Kelly ETFs, in collaboration with HashKey, has also applied for an Ethereum strategy ETF with the code EX.

SEC has once again delayed its decision on approving the first Bitcoin spot ETF. This marks the third delay for the Ark Investment Management and 21Shares ETF initially submitted in April this year. The SEC is now expected to make a final decision by January 10th of next year.

On October 16, 2023, due to the SEC's failure to appeal the Grayscale ruling, the discount of Grayscale Bitcoin Trust (GBTC) to its net asset value (NAV) fell below 16% for the first time since December 2021, closing at 15.9% last Friday (Oct. 20th, 2023). With the deadline passed, regulatory authorities are reassessing Grayscale's application to convert its GBTC product into a spot Bitcoin ETF, although the SEC may find other reasons to deny it. SEC Chairman Gary Gensler declined to comment on the matter when asked during a press conference last Friday.

Commentary:

Among all ETF investors, financial advisors account for approximately 70-75% of the share, while institutional investors and retail investors account for 10% and 15%, respectively. Financial advisors in the United States manage around \$30 trillion in assets. This represents a massive market, and ETFs provide them with a familiar and convenient investment tool. If ETFs are successfully launched, it would bring significant incremental capital to the crypto market. The SEC's handling of GBTC may indicate that various types of ETFs could be approved in the near future.

- **Cointelegraph reported a mix-up regarding a Bitcoin spot ETF**

On October 16, 2023, Cointelegraph reported a mix-up regarding a Bitcoin spot ETF. The report initially stated that the U.S. Securities and Exchange Commission (SEC) had approved BlackRock's iShares Bitcoin spot ETF, but it was later met with skepticism from Bloomberg analyst James Seyffart and others. Shortly after, Fox Business reporter Eleanor Terrett tweeted, "BlackRock just confirmed to me that this is false news. Their Bitcoin spot ETF application is still under review."

Meanwhile, the Bitcoin price briefly surged over \$30,000, experiencing a short-term increase of over 10%. However, after the news of the Bitcoin spot ETF approval was debunked, the price of BTC dropped back below \$28,000. Within one hour, the cryptocurrency market saw over \$100 million worth of liquidations across various contracts. Cointelegraph subsequently deleted the tweet stating, "SEC approves Bitcoin spot ETF" and issued an apology, mentioning an ongoing internal investigation. The investigation revealed that the false Bitcoin spot ETF news originated from an unverified screenshot posted by a user on platform X, claiming it was from Bloomberg Terminal. Cointelegraph failed to verify the source before erroneously publishing the information on platform X.

This highlights the occurrence of misinformation in news reporting and the impact of false information on the market. It emphasizes the importance of investors' ensuring they obtain reliable and accurate information, especially when it comes to financial markets and investment products.

Commentary:

False news in the crypto industry impacting the market is not an isolated incident, but each occurrence results in a majority of investors falling victim and bearing unnecessary losses. This serves as evidence of the immaturity of news sources in the crypto market while also highlighting the manipulative nature of the secondary market. The path to maturity and improvement in the crypto market is still long and challenging. Investors should exercise caution and carefully verify the authority and authenticity of news sources before making investment decisions in the current stage.

- **Celestia Airdrop Plan**

On the evening of September 26, 2023, modular blockchain project Celestia announced an airdrop with a snapshot time set for January 1, 2023. A total of 60 million Celestia tokens (TIA) were distributed, benefiting 7,579 developers and 576,653 on-chain active addresses. The airdrop excluded Celestia Labs team members and advisors from participation. Eligible users were required to claim their tokens before October 17, 2023, 20:00 UTC.

This airdrop specifically excluded identified whale clusters and also excluded blacklisted addresses from previous airdrops, such as HOP protocol and Optimism. It also excluded addresses associated with on-chain vulnerabilities and other compliance standards. Compared to previous airdrops, Celestia designed the rules to prioritize fairness and genuine contributions. The airdrop aimed to incentivize genuine blockchain technology and project developers, as well as addresses with higher on-chain activity, rather than solely focusing on addresses within the Celestia network as the community had anticipated. Of the total allocation, 26.8% was designated for research and ecosystem development. This included tokens allocated to the Celestia Foundation and core development team for research, development, and ecosystem plans. It encompassed protocol maintenance and development and plans targeting rollup developers, infrastructure, and node operators.

Commentary:

Celestia's airdrop approach targets genuine developers and ecosystem contributors, as well as on-chain active addresses to the best of their ability. By selecting an earlier snapshot date, they were able to filter out a significant number of studio-created addresses that engaged in artificial transaction volume at the beginning of the year. This strategy incentivizes developers' technical contributions and leverages the promotional benefits of addresses with higher on-chain activity, thus achieving two objectives at once.

- **The introduction of KYC and fees by Uniswap sparks controversy**

On October 16, 2023, the introduction of a new hook called the "KYC hook" in the open-source directory of Uniswap V4 sparked controversy within the crypto community. This hook allows users to undergo KYC checks before accessing the trading pool. This move potentially opens up the possibility of DeFi protocols being whitelisted by regulatory authorities and enforce regulations.

On October 17, Uniswap announced the implementation of a 0.15% exchange fee on certain tokens in its web application and wallets, including ETH, USDC, WETH, USDT, DAI, and more. These fees are only applicable when trading these tokens through the Uniswap Labs interface on the mainnet and Layer 2 networks, aiming to sustain Uniswap's operations. The announcement clarified that fees are only charged for exchange transactions involving both the selling and buying of tokens, while exchanges between stablecoins and wrapped ETH (WETH) are exempt from these fees.

Commentary:

The current criticism of Uniswap's introduction of the KYC hook primarily stems from a minority of builders, while the majority of concerns come from players worried about fund security and market liquidity. From the perspective of DeFi's essence, decentralized exchanges (DEXs) should not involve centralized audits. However, under regulatory pressure, the introduction of KYC by DEXs may be seen as a necessary step. It is possible that in the future, DeFi and CeFi (centralized finance) will gradually merge as they adapt to market regulations, which may become unavoidable.

- **BigTime kicks off preseason and launches on multiple exchanges**

On October 11, 2023, the highly anticipated AAA-level blockchain game, Big Time, began its three-month preseason. Existing players who had obtained the pass were eligible to participate, and new users could also experience the game by using invitation codes. The BIGTIME token was listed on various trading platforms, including OKX and Coinbase. Within 24 hours, the price of the BIGTIME token surged from \$0.01 to surpass \$0.15.

Big Time was established in April 2021 as a PC-based multiplayer action role-playing game. Its gameplay is similar to that of World of Warcraft and Diablo, combining fast-paced action combat, NFT collection and customization, and time-traveling adventures. Big Time was also one of the early blockchain games to embrace the concept of AAA gaming. The game is deployed on the Ethereum blockchain and utilizes a dual-layer architecture of "on-chain assets, off-chain gameplay" to ensure a smooth user experience. Unlike common dual-token models in blockchain games, Big Time only has one token called \$BIGTIME, with a total supply of 5 billion tokens, all of which are generated through gameplay. In addition, "skins" NFTs are another major core asset in the game. Rare NFTs can showcase status and uniqueness, allowing players to access restricted areas or exclusive dungeons.

Commentary:

Overall, Big Time exhibits good gameplay and maintains a satisfactory level of game quality. Additionally, the game has lowered the entry barrier, and the public market based on Vault technology has reduced the complexity and costs associated with on-chain asset transactions. The generation of \$BIGTIME tokens through gameplay, coupled with their multiple consumption values within the game, contributes to the establishment of a sustainable economic cycle system. However, as the supply of \$BIGTIME tokens increases, there may be increased selling pressure in the market, and it remains to be seen whether the internal economic system can operate in a healthy manner. Big Time, in a sense, brings GameFi back into the spotlight, emphasizing the importance of gameplay and game quality in blockchain games, which may be a significant trend in the future.

- **The FTX case goes to trial for hearing**

On October 3, 2023, the trial of the case involving FTX founder SBF commenced. Caroline Ellison, former girlfriend of Sam Bankman-Fried (SBF) and former CEO of Alameda Research, testified on the third day of the criminal fraud trial, stating that Alameda Research borrowed approximately \$10 billion from FTX and loaned around \$5 billion to FTX executives and affiliated entities. She expressed significant concerns about the repayment of the loan from Alameda in June 2022 and mentioned that she prepared seven different spreadsheets showing Alameda's balance sheets under the guidance of SBF. These spreadsheets included the loans provided to FTX executives and the amounts borrowed from FTX.

Caroline Ellison further stated that the Federal Bureau of Investigation (FBI) had previously seized computers belonging to her mother and her new boyfriend, who also worked at Alameda and FTX. In December of last year, Caroline Ellison had multiple meetings with the government, during which discussions regarding the criminal charges took place, and she acknowledged the charges.

As assets are gradually liquidated and recovered, the value of FTX user assets in off-exchange trading has significantly rebounded, rising from around 10% at the beginning of the year to 30-40%.

Commentary:

The trial proceedings of the FTX case indicate that the FTX collapse event is nearing its conclusion. It has been nearly 10 months since SBF's arrest in the Bahamas, and the current developments do not seem favorable for SBF. The testimonies of his former girlfriend and employees suggest that the misappropriation of customer assets by SBF has become a factual matter. Investors should continue to monitor the situation, especially those who have investments in tokens related to FTX concepts.

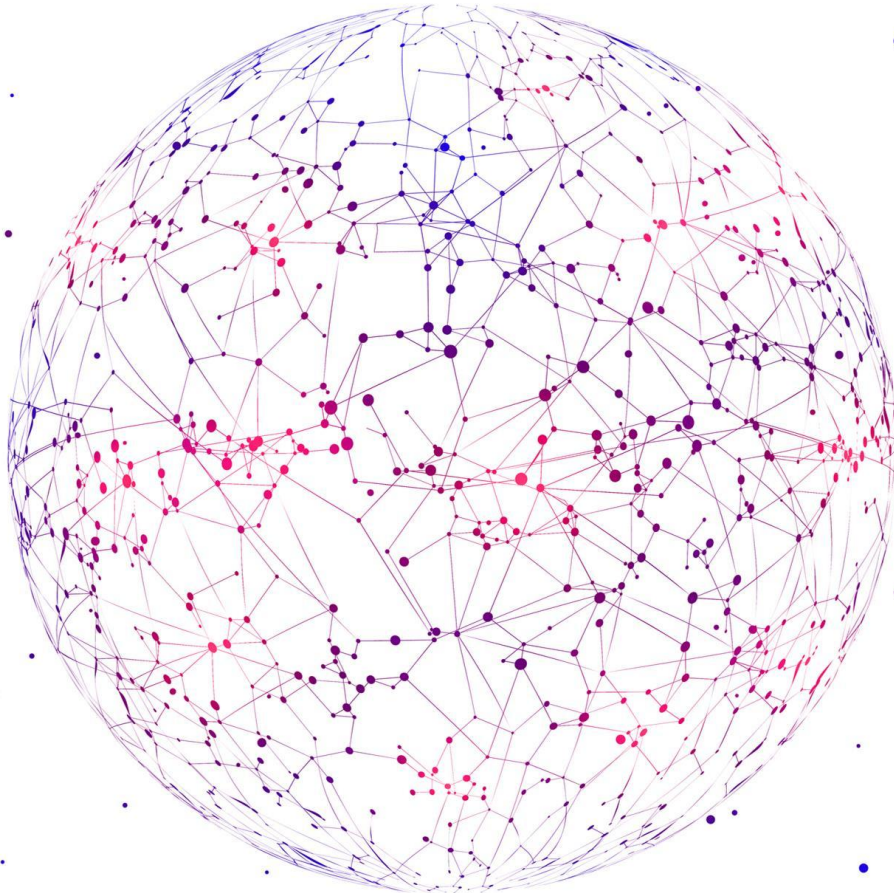
- **The renewed Israeli-Palestinian conflict has once again sparked a geopolitical crisis, affecting certain crypto projects**

The recent escalation of the Israeli-Palestinian conflict has resulted in thousands of casualties, and certain crypto projects have been affected by this conflict as well. Alon Muroch, the founder of the decentralized staking platform SSV Network, announced on X on October 11, 2023, that he has been conscripted into military service. Apart from SSV, other projects such as Secret Network in the L1 sector, StarkWare in the L2 sector, Bancor in the DeFi sector, NFTrade in the NFT sector, Fireblocks in the wallet sector, and more have also been impacted.

Following the escalation of the Israeli-Palestinian conflict, the Israeli police collaborated with Binance to freeze cryptocurrency accounts associated with the Palestinian militant group Hamas. Any funds seized from these accounts will flow into the Israeli treasury. In response to this, Binance co-founder He Yi stated that Hamas is designated as a terrorist organization by the United Nations, and any international organization receiving an inquiry to freeze assets must comply. No trading platform has the ability to refuse such a law enforcement request.

Commentary:

Despite being seen as decentralized tools, cryptocurrencies and blockchain technology are still subject to the influence of national policies and international political events in the real world. This poses important challenges for the future development of blockchain and cryptocurrencies. Finding ways to minimize the potential negative impact of political and social turmoil on the blockchain industry will be an important topic within the industry.



- **Bitcoin mining company Cathedra Bitcoin has filed a prospectus for an initial public offering (IPO) in Canada.**

Source: <https://www.businesswire.com/news/home/20230907628807/en/Cathedra-Bitcoin-Files-Final-Base-Shelf-Prospectus>

Northern Data Group's subsidiary has signed a \$150 million mining equipment purchase contract with MicroBT, a Bitcoin mining company

Source: <https://ir.northerndata.de/news/corporate-news/peak-mining-a-northern-data-group-company-signs-usd-150-million-contract-for-next-generation-liquid-cooled-mining-hardware-from-microbt/>

Bitcoin mining company Mawson produced 88 BTC in the month of August

Source: <https://www.globenewswire.com/news-release/2023/09/22/2747975/0/en/Mawson-Infrastructure-Group-Inc-Announces-Monthly-Operational-Update-for-August-2023.html>

Section IV

China Blockchain Headlines

Managing Partner of EY Hong Kong and Macau, has stated that the central government is committed to developing new industries such as blockchain in addition to other emerging sectors

EY Hong Kong and Macau's Managing Partner, Shirley Leung, stated that the central government is committed to developing new industries such as AI, blockchain, and clean energy and exploring new regional investors like those from the Middle East. She also emphasized that the business still sees prospects in the Greater Bay Area, and therefore, the financial industry, especially banking, still has opportunities.

Xi Jinping: New technologies such as blockchain have greatly changed the global allocation of factors and resources, industrial development patterns, and people's way of life

On September 5th, it was reported that Chinese President Xi Jinping sent a letter of congratulations to the 2023 China International Intelligent Industry Expo. In the letter, he pointed out that new technologies such as the internet, big data, cloud computing, artificial intelligence, and blockchain are undergoing profound evolution. The digitalization, intelligence, and green transformation of industries are accelerating, and the intelligent industry and digital economy are flourishing. This transformation is greatly changing the global allocation of factors and resources, industrial development patterns, and people's way of life. China attaches great importance to the development of the digital economy and continuously promotes the deep integration of digital technologies and the real economy. China is actively advancing digital industrialization and industrial digitalization and accelerating the construction of a strong cyber nation and a digital China.

Ximalaya has been elected as an executive director unit of the Zhongguancun Blockchain Industry Alliance

The Zhongguancun Blockchain Industry Alliance held its 2nd 2nd Member Congress at the Beijing National Convention Center. During the conference, the alliance's board of directors and supervisors were also convened, bringing together experts and industry professionals from member organizations, as well as various sectors including government, industry, academia, research, and application, to discuss the development trends and practices in the blockchain industry.

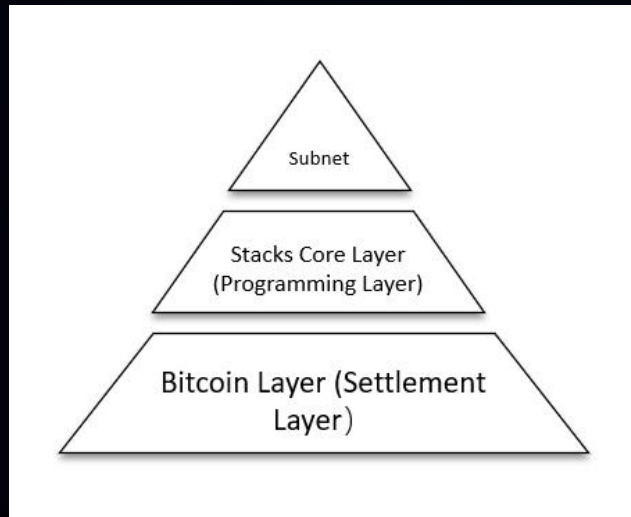
YU Xiaohui, the President of the China Academy of Information and Communications Technology (CAICT) and Chairman of the alliance, and JIN Jian, the Director of the Industrial Internet and IoT Research Institute of CAICT and Secretary-General of the alliance, delivered keynote speeches at the conference, providing valuable guidance for the healthy development of the industry.

Fu Haibo, Senior Vice President of Ximalaya, attended the conference and participated in the signing ceremony of the Digital Landmark Ecological Union Cooperative Partnerships. During the event, Ximalaya was elected as an executive director unit of the Zhongguancun Blockchain Industry Alliance.

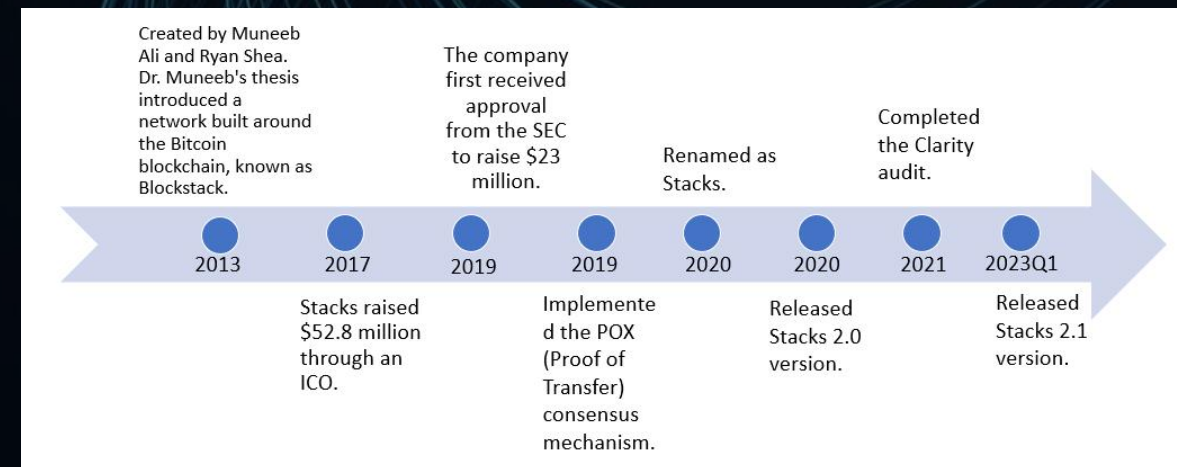
Bitcoin Scaling Solution Overview

2.2 Stacks

Stacks is a foundational open-source smart contract platform based on Bitcoin. It allows developers to build decentralized applications (DApps) or issue tokens. Stacks follows a layered architecture where Bitcoin serves as the underlying settlement layer, confirming transactions and data on the Stacks platform. The middle layer consists of the Stacks core, which can be seen as the programming layer for Bitcoin. Developers use the Clarity language to write smart contracts. The top layer is the Stacks' subnetwork, which provides higher throughput and scalability. In the following sections, we will delve into the workings of Stacks and its communication with Bitcoin.



Stacks, formerly known as Blockstack, was initially proposed in 2013. It conducted an Initial Coin Offering (ICO) in 2017 and rebranded as Stacks in 2020. In 2021, Stacks launched its 2.0 version, establishing itself as one of the longer-standing Bitcoin Layer 2 projects. The following are significant milestones in its development:



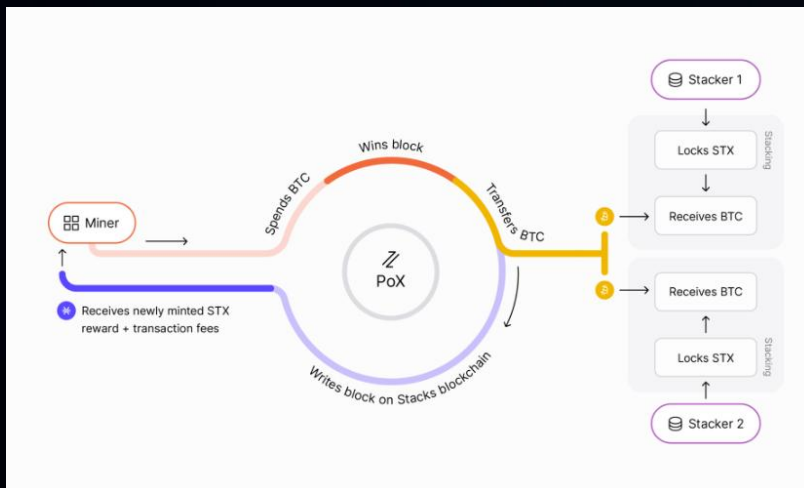
*Source: Compiled by HashKey Capital

2.2.1 Technical Principle

Stacks utilizes a consensus mechanism called PoX (Proof of Transfer), which involves two roles in the network: Miners and Stackers. Similar to Bitcoin or Ethereum, Miners compete by contributing resources to add new blocks, and those who successfully add blocks receive rewards. The specific process is as follows: unlike Bitcoin, in Stacks, miners do not initially need to invest expensive upfront costs such as hardware and electricity. They only need to send Bitcoin to a specific address. The protocol then combines the amount of Bitcoin sent by the Miner and a verifiable random function (VRF). The more Bitcoin a miner contributes, the higher their probability of winning. Once selected, Miners can add new blocks to the Stacks network and earn STX rewards. Stakers lock their own STX tokens within the network. As a reward for stacking, miners send Bitcoin to the Stakers. This mechanism completes the cycle of proof-of-transfer. Miners participate in the competition by sending Bitcoin and receiving STX rewards when they successfully add blocks, while Stakers participate in the process by locking their STX tokens and receiving Bitcoin rewards from Miners.

As shown in the chart below, the miners who participated in over 7,000 matches have spent a significantly higher amount of BTC, won more blocks, and received greater rewards compared to other miners who spent less.

How does Stacks anchor to Bitcoin? Each Stacks block has a hash value that is formed by combining the hash value of the previous Stacks block with the hash value of the previous Bitcoin block. As mentioned in the Ordinals section earlier, Bitcoin's OP_RETURN opcode allows transactions to store up to 40 bytes of data, similar to a memo. The hash value of each Stacks block is stored within this opcode.



*Source: stacks docs

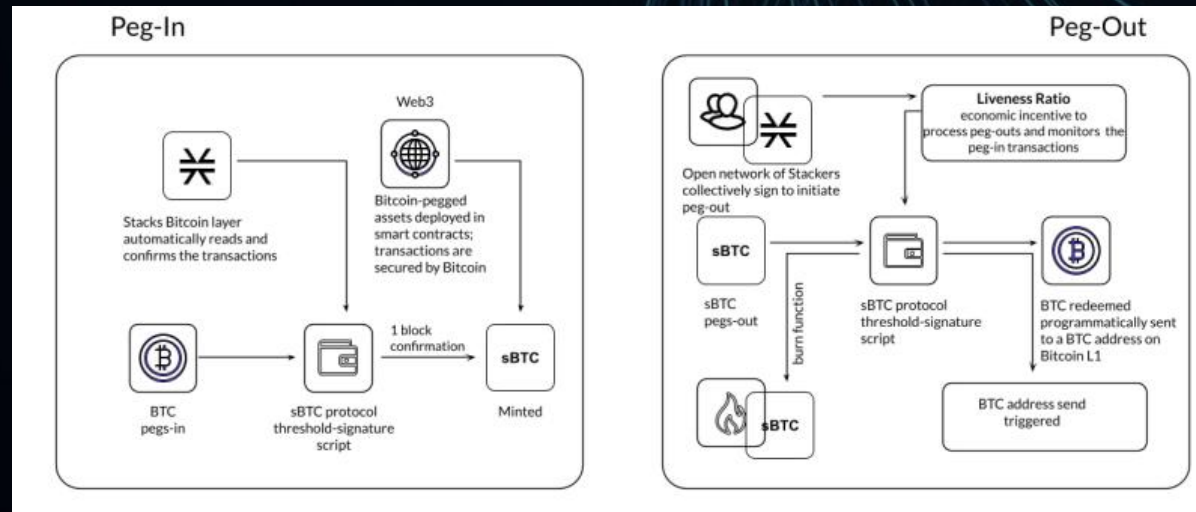
Address.	Total Spent (sats)	Total Participation	Total Block Won	Total Reward (STX)
bc1q3l89...dkszael4	3200000	18	0	0
bc1qqdq6...m5ggafcr	71490800	7501	540	583000
bc1qw27e...hvmp9a2	149400000	332	127	140000
SP06HBN5...XC5NWJ3P	15000000	50	8	24664
SP0B0EYF...ZZAWEKZE	92704000	212	0	0
SP1000R3...JBE8SKWP	3557543700	7278	1241	1337000

*Source: Onstacks

2.2.1 Technical Principle sBTC

The Nakamoto upgrade is a significant upgrade to the Stacks network, planned for release in Q4 2023. It involves several key features, including the introduction of subnets, sBTC, and a new smart contract language called Clarity. One of the focuses of this upgrade is to enable the use of BTC assets within the Stacks network. In this context, let's primarily discuss sBTC and Clarity.

sBTC, similar to solutions like wBTC, renBTC, etc., provides an anchoring solution for BTC within the Stacks network. The general idea behind such asset solutions can be summarized as follows: locking BTC on the BTC chain, minting 1:1 BTC assets on another chain, redeeming and destroying assets on the secondary chain, and releasing BTC on the BTC chain. However, the degree of decentralization in locking and releasing BTC varies. The widely used approach, such as wBTC, involves centralized custody and operation of the BTC assets by a custodial service provider. On the other hand, sBTC's locking and unlocking mechanism is not reliant on a centralized entity. Users send BTC to a threshold signature wallet controlled by stackers, who are the individuals locking STX tokens. In order for the minting or burning of sBTC to take effect, it requires collective agreement from 70% of the stackers. This decentralized approach helps mitigate centralization risks.



2.2.1 Technical Principle

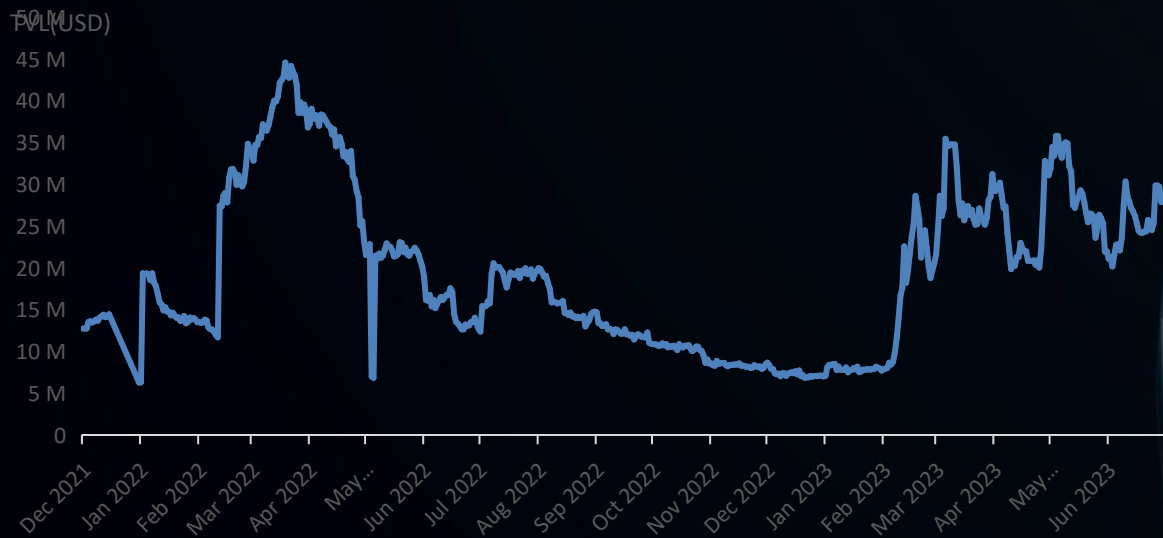
Smart Contract Language Clarity

Developing a new programming language requires a significant investment of resources and time. In the Stacks ecosystem, a self-contained smart contract language called Clarity has been introduced. It has been optimized specifically for smart contracts and blockchain technology. Taking into account discussions with Marvin Janssen, the Development Director at Hiro, and the Technical Lead at the Stacks Foundation, the following two advantages of Clarity can be summarized:

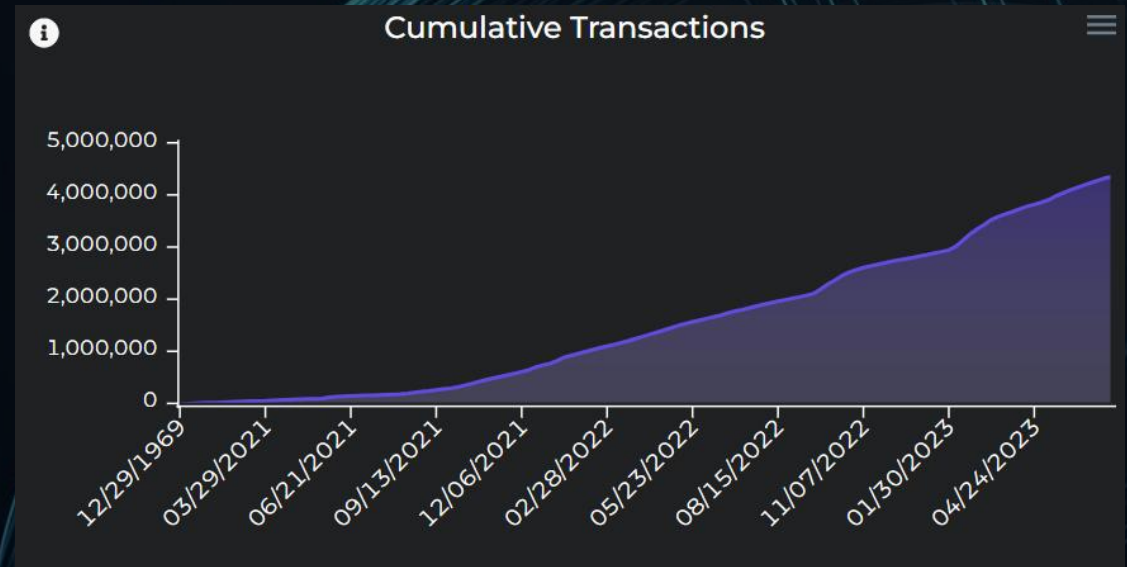
- **Clear and Predictable Logic:** For example, languages like Solidity, which are Turing complete, lack predictability in terms of code execution paths. The logic cannot be pre-determined, making the code vulnerable to attacks. Clarity, on the other hand, supports type safety and function purity, making it easier for developers to understand the behavior and intent of smart contracts. This enables easier verification of contract correctness and security. Clarity also provides tools and techniques such as simulators and formal verification to assist developers in better validating and testing contracts.
- **Enhanced Security:** Clarity incorporates design restrictions to reduce the complexity of smart contracts and improve security. For instance, Clarity prohibits recursion and unrestricted loops, which helps prevent common programming errors and attack vectors such as infinite loops and stack overflow attacks. Instead of traditional loops, Clarity offers higher-order functions like map, filter, and fold to iterate and process data structures. This simplifies contract development, improves readability, and reduces potential security risks.

2.2.2 Ecosystem

According to Defillama , driven by the Ordinals protocol, Stacks' Total Value Locked (TVL) has surged from around \$7 million at the beginning of the year to nearly \$30 million currently. Based on Stacks on Chain data, the cumulative transaction volume on the Stacks network has exceeded 4.3 million transactions. The number of non-zero addresses is close to 500,000, and the deployed contract count is over 66,000. Particularly, in February 2023, there was a significant increase in network transaction volume and the number of transactions in the mempool awaiting processing.



Source: Defillama, Compiled by HashKey Capital








Source: stacksonchain

2.2.2 Ecosystem

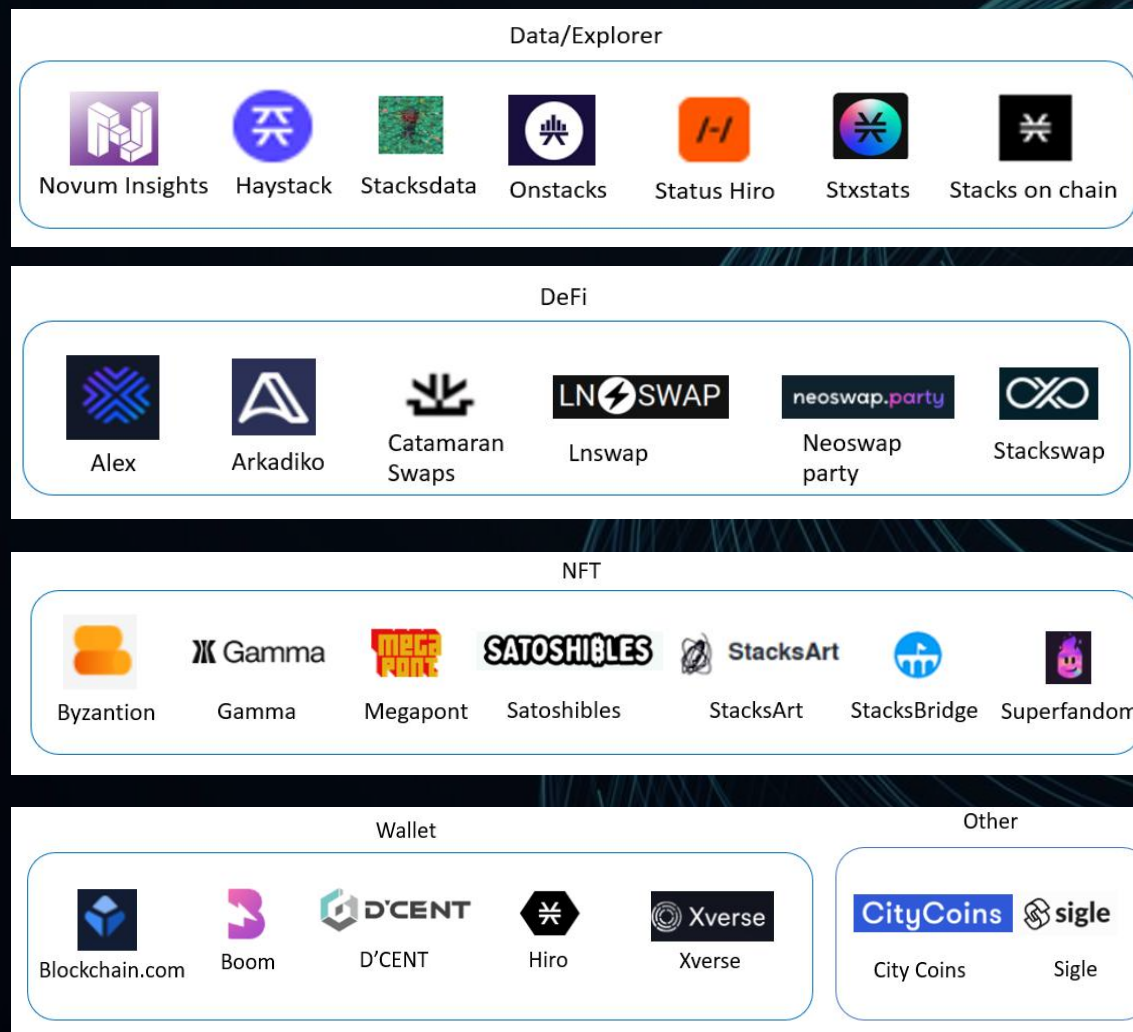
The following image summarizes the main projects within the Stacks ecosystem, including DeFi, NFT, and wallets. The projects with the highest Total Value Locked (TVL) are primarily DeFi projects. Alex is the project with the highest TVL within the ecosystem, accounting for over 90% of the Stacks ecosystem. Its TVL has grown from \$5 million at the beginning of 2023 to \$22 million, representing a growth of over 4 times. Alex offers various features, including a decentralized exchange (Dex), lending, launchpad, and perpetual contracts. The second-ranking project in terms of TVL is Arkadiko, similar to MakerDAO, which requires users to provide collateral to mint the stablecoin USDA.

CityCoin is a project that utilizes the Proof-of-Transfer (PoX) mechanism mentioned earlier to pledge STX tokens and raise funds for city treasuries. Both Miami and New York have joined this project. Additionally, the Bitcoin Name System (BNS) project has been deployed on Stacks, with the number of registered BNS domains approaching 300,000.

		TVL			
Name	Category	TVL	1d Change	7d Change	1m Change
1  ALEX 1 chain	Dexes	\$22.05m	+3.47%	-6.01%	+8.46%
2  Arkadiko 1 chain	CDP	\$5.95m	+2.55%	+315%	+361%
3  CityCoins 1 chain	Yield	🔍 \$272,513	+2.58%	-5.54%	+22.05%
4  StackSwap 1 chain	Dexes	\$226,144	+3.13%		
5  UWU Protocol 1 chain	CDP	\$2,992	+2.58%	+29.34%	+85.12%

Source: Defillama

2.2.2 Ecosystem



Source: Compiled by HashKey Capital

2.2.3 Limitations

We believe that Stacks has the following two risks and limitations:

- **Potential Lack of Miner Incentives:** The Proof-of-Transfer (PoX) mechanism requires miners to burn existing BTC to compete for the right to add blocks and earn STX rewards. The mining rewards for STX are similar to BTC, halving every 4 years. In the first 4 years, each block rewards 1000 STX; in the following 4 years, it rewards 500 STX per block; and then, in the subsequent 4 years, it rewards 250 STX per block. Finally, it stabilizes at 125 STX per block. However, if the number of miners increases in the future and STX rewards decrease, the value of the burned BTC may exceed the value of STX rewards, leading to reduced profitability for miners and insufficient incentive to participate. Unless the number of participating miners is limited or the value of STX is increased to stabilize the STX/BTC exchange rate, this issue may persist.
- **Relatively Limited Development Tools and Ecosystem:** Currently, Stacks' development tools and ecosystem are relatively small. The Clarity smart contract language supports only a limited range of functionalities, primarily focusing on basic features. Developers may not be able to utilize certain advanced functionalities and libraries to develop more complex smart contracts.

However, as mentioned earlier, the simplicity and security of Clarity are its strengths. The Stacks team is continuously improving and expanding the functionality of Clarity to meet the growing demands of applications.

2.3 Rootstock (RSK)

Rootstock is a Bitcoin sidechain that offers a significant advantage in its compatibility with the Ethereum Virtual Machine (EVM). This compatibility allows smart contracts to be written in the Solidity programming language, making it more conducive to integration with the Ethereum ecosystem. Rootstock utilizes a merged mining model, which means it doesn't require additional resources beyond Bitcoin's existing mining infrastructure. Both Rootstock and its infrastructure, RIF (Rootstock Infrastructure Framework), are developed by IOV Labs.

The goal of RIF is to provide developers with a range of tools and services to facilitate easier construction and deployment of dApps (decentralized applications). These components and features include a decentralized domain name system, storage solutions, payment protocols, and toolsets. IOV Labs introduced a \$2.5 million funding program in May of this year to support the adoption of Rootstock.

2.3.1 Technical Principle

Merged Mining

Rootstock also uses the SHA-256 algorithm and employs merged mining to record new blocks. Apart from RSK, there are other projects that utilize merged mining, such as Namecoin. The principle behind merged mining is to reuse PoW by leveraging the computational power of the Bitcoin network to secure RSK. Miners can mine RSK while mining Bitcoin. Miners embed the hash of RSK blocks as a tag within Bitcoin blocks, allowing the secondary RSK blockchain to locate this tag. The RSK tag can be placed anywhere in a transaction, such as the coinbase field or within the OP_RETURN of any output. If a Bitcoin block meeting the RSK mining difficulty is found during the Bitcoin mining process, the block header and block are sent to the RSK network, thereby adding a new block. In this process, the mining difficulty of RSK is lower than that of Bitcoin (RSK has an average difficulty of 70 bits, while Bitcoin has a difficulty of 74 bits). As a result, the sidechain generates new blocks at a faster pace than Bitcoin. According to stats from RSK, on average, a new block is produced every 30 seconds (the whitepaper originally stated 10 seconds).

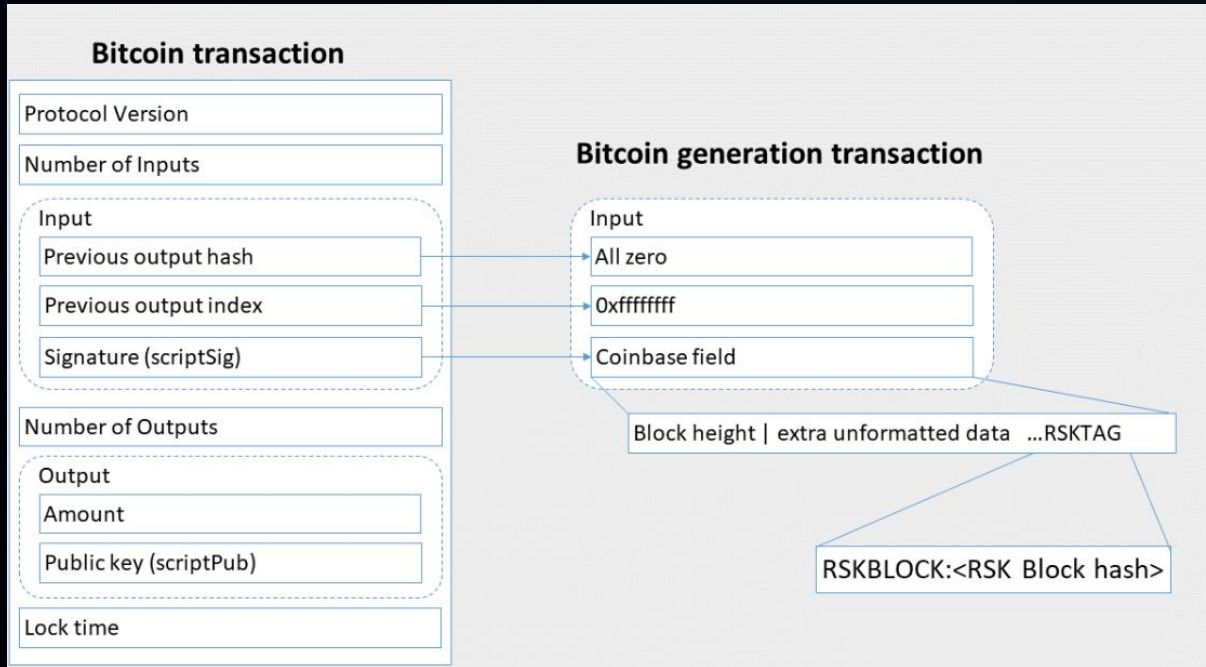
Most of the computational power supporting RSK comes from Bitcoin, with a small portion also coming from BCH. Sergio Demian Lerner, the Chief Scientist of RSK, claims that 40% to 51% of Bitcoin miners are engaged in merged mining with RSK.

Solution	Block Interval	The average number of random number iterations performed to find a solution	Assumptions
Bitcoin	10min	2^{74}	100% Bitcoin hash rate
RSK	30s	2^{69}	50% merged mining
Shared block in mining pools	3.3s on average for each client	2^{52}	20% hash rate, 4000 client Ckpool software

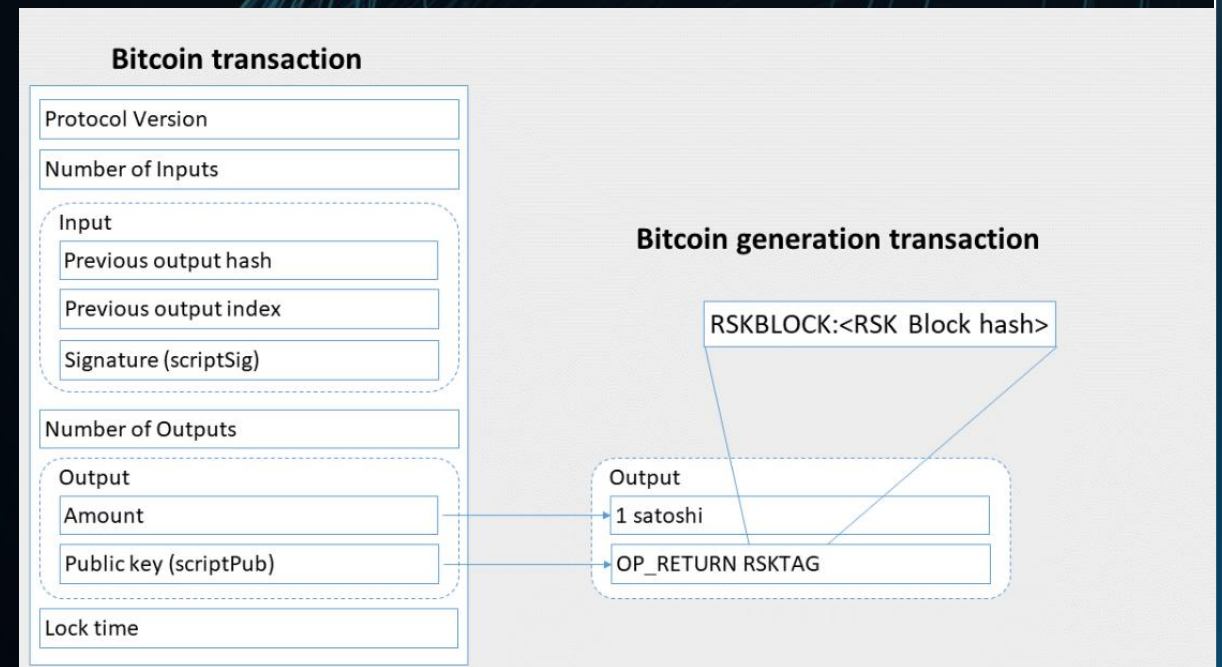
Source: <https://blog.rootstock.io/zh-hans/noticia/rsk>

2.3.1 Technical Principle

The RSK tag stored in the Coinbase field



The RSK tag stored in the output's OP_RETURN field



2.3.1 Technical Principle

Rbtc

The assets on RSK pegged to BTC are called RBTC, which is also used for transaction fees on the RSK network. In the pegging-in process, users send BTC to a multi-signature address controlled by the RSK federation on the Bitcoin blockchain. The BTC is locked and a transfer proof is generated, which is then sent to a special smart contract called the bridge contract on the RSK chain. Upon receiving the proof, the bridge contract issues an equivalent amount of RBTC to the user. On the other hand, in the pegging-out process, users need to send RBTC to a specific bridging address on the RSK blockchain. The RSK federation verifies the redemption transaction for RBTC and signs the corresponding Bitcoin transaction for payment. The redemption request requires signatures from a majority (51% or more) of the federation members to be valid.

Currently, according to the official RSK website, there are nine members in the RSK federation:

BLOCKVENTURE

COINFIRM

COLLIDER

CONSTATA

MYCOINTAINER

PNETWORK

IOVLABS

SOVRYN








XAPO

Source: <https://rootstock.io/powpeg/>

2.3.2 Ecosystem

According to DeFiLlama data as of July 14, 2023, the Total Value Locked (TVL) on Rootstock is approximately \$98 million, with the ecosystem primarily composed of DeFi protocols. The leading protocol is the lending protocol MoneyOnChain, accounting for over 40% of the total TVL. The second-ranking protocol is the Bitcoin trading and lending platform Sovryn, contributing to over 20% of the ecosystem's TVL. MoneyOnChain allows users to collateralize RBTC to mint the stablecoin DOC, which can be used for lending, trading, and includes leveraged products. Sovryn supports the trading and lending of Bitcoin assets, including leverage.

This year, Sovryn introduced DLLR, a stablecoin backed by BTC collateral. Users holding DLLR can also convert it to Bitcoin equivalent to the value of USD at any time.

Name	Category	TVL ↕	1d Change ↕	7d Change ↕	1m Change ↕
1  MoneyOnChain 1 chain	Lending	\$50.16m	+7.14%	+3.77%	+23.54%
2  Sovryn 1 chain		\$26.75m	+3.21%	+3.10%	+21.90%
3  Sovryn Dex 1 chain	Dexes	\$19.69m	+1.81%	+2.92%	+11.72%
4  BabelFish 1 chain	Yield	⊙ \$3.53m	-0.34%	-1.01%	-8.09%
5  Tropykus RSK 1 chain	Lending	\$1.59m	+3.53%	+3.80%	+22.69%
6  RskSwap 1 chain	Dexes	\$59,079	+7.05%	+2.10%	+7.95%
7  Blindex 1 chain	Algo-Stables	\$18,295	+7.44%	+7.28%	+20.48%

Source: Defillama

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

hashkey.capital

ir@hashkey.com