
HASHKEY
Capital
ASIA CRYPTO INSIGHTS
NOV 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

HASHKEY Capital

Table of Contents

Blockchain and Crypto Deals

HASHKEY Capital

0xScope

The core of 0xScope is a set of algorithms based on a knowledge graph, utilizing entity induction to aggregate all addresses controlled by the same entity. The project has been iterating since March, building databases and models. As the algorithm continues to run, the accuracy and identification have been improving. The key advantage of the 2C product lies in its granular capture of user behavior and extensive user profiling. It enables ordinary users to clearly understand their own transaction behavior as well as the transaction behavior of other users. Additionally, it incorporates social engagement, fostering data-driven content through community discussions.

In terms of the 2B aspect, the project focuses on three types of user profiles:

- **Providing KYT (Know Your Transaction) services for clients such as exchanges that require financial risk control. This service utilizes data analysis to determine if transfers originate from malicious sources (black money).**
- **Offering protocol user profiling services for project parties, with nearly 700 projects already identified. This allows clear visibility into a project's actual user count, distinguishes wash trading, and measures user overlap with competitors, among other features.**
- **Providing pre and post-investment tools for venture capitalists (VCs), enabling monitoring of team addresses for any improper income and observing portfolio addresses to track fund usage.**

Commentary by HashKey Capital:

The project has received attention since the early seed round and the team has shown strong drive, completing the product development on schedule, with a good understanding of the overall market. They have explored multiple directions in terms of the business model and demonstrated self-motivation in discovering new functionalities.

HASHKEY Capital

Carv

The main product of Carv is a credential platform for game players in web2 and web3. Web2 data comes from traditional game accounts such as Epic, Xbox, and Steam (users need to give the platform access to establish a game account API connection), and there are also social media sign-on like Twitter and Discord. In terms of Web3, it combines the on-chain data of user wallet addresses and establishes user IDs (in the form of SBT) within the platform based on achievements and social activities. The Carv platform currently integrates with 150+ games, including leading games like Delysium, Bigtime, Step, Axie, and Otherside, etc.; It cooperates with 20+ public chains such as BNB Chain, Polygon, Immutable X, and Oasys, etc. As of April 2023, the platform has 600,000+ registered users and 120,000 monthly active users.

Commentary by HashKey Capital:

CARV's advantage lies in being supportive of new projects, and it has been effective in promoting new user activities. There are high-quality games on the platform, and users have a strong willingness to pay, and the large ecosystem is willing to cooperate.

HASHKEY Capital

Web3Port

Web3Port is a web3 accelerator that mainly holds demo days, and bootcamps, and provides FA services, among other services. The project has been implemented at a very fast speed, successfully transformed from the initial Icport, and its main network has been fully opened in less than a year, with a high degree of recognition in the Binance ecosystem. The revenue model includes:

1. **Sponsorship fees: sponsorship fees collected for various activities;**
2. **Service fees: fees for providing integrated market marketing and other services for Startups;**
3. **Product membership fees: Member Fees, where members pay to enjoy the use of various tools provided by the platform;**
4. **Startups Token Share: Provide acceleration and launchpad, for Startups and get project token allocations;**
5. **Platform advertising fees: The platform relies on a strong Connect Network to provide project parties/service providers with paid advertising and recommendation-related service fees;**
6. **In the future, there may also be Defi fee sharing: service fees related to collaboration with partners, including Farming, Staking, lending, income aggregators, and other handling fee sharing.**

Commentary by HashKey Capital:

The team has a very strong execution capability. Whether it is accelerator business or product development, the rhythm is very fast. The response speed to demand is also very fast, and the efficiency of recommending projects is very high.

Section II

Blockchain Community and Market Update

- **FTX Founder SBF Trial Concludes, Jury Unanimously Finds Him Guilty of Fraud, Facing a Maximum Sentence of 115 Years**

On November 2, 2023, the jury's deliberations concluded, and the judge read out the guilty verdict, which included charges of wire fraud, conspiring to commit wire fraud against FTX customers, wire fraud, and conspiracy to commit wire fraud against Alameda lenders, conspiracy to commit securities fraud against FTX investors, commodity fraud against FTX customers, and conspiracy to launder money. According to the US Department of Justice, each charge carries a maximum sentence of 5 to 20 years.

If all the charges are upheld, SBF could face a maximum sentence of 115 years. The prosecution has described this as "one of the biggest financial fraud cases in US history".

Judge Lewis Kaplan has tentatively set the sentencing date for March 28, 2024. Given that SBF's defense attorney opposed many of Kaplan's rulings before and during the trial, it is expected that an appeal will be filed. In addition, SBF faces five additional criminal charges in another trial currently scheduled for March 2024, including defrauding customers in derivatives trading, securities fraud against FTX investors, and three counts of conspiracy. Therefore, the final verdict and sentencing of SBF will take at least another half year to be known.

Commentary:

From SBF's performance in court, his defense was filled with phrases like "I don't remember," and he tried to attribute many of the crimes to others. Judge Lewis Kaplan scolded him more than once and reminded him to answer the questions posed. SBF's attempt to give vague answers did not succeed, and the prosecution also brought out media reports, videos, SBF's tweets, etc., as evidence to corroborate the charges. The jury members also made a reasonable verdict, which marks an important step in the trial of the SBF case.

HASHKEY Capital

• Bitcoin Ecosystem Explodes Again

• Bitcoin Ecosystem Explodes Again

The Bitcoin (BTC) ecosystem made tremendous progress in 2023, with the emergence of several native protocols such as Ordinals, Atomicals, PIPE, among others. In October, as the market warmed up, the BTC ecosystem witnessed another explosion. There was also the Lightning Network version of BRC20 and the EVM chain migration version of BRC20, causing Bitcoin inscription excitement in the community.

On January 21, 2023, Bitcoin developer Casey Rodarmor launched the Ordinals protocol, opening up a new gameplay for the Bitcoin ecosystem. On October 24, the Ordinals protocol underwent a major update, releasing version v0.10.0, adding multiple features such as bulk engraving, metadata, and inscription numbering endpoints. On November 7, Binance listed $ORDI, pushing $ORDI up significantly, with a single-day increase of nearly 100%. $SATS, deployed on March 9, 2023, saw a nearly tenfold increase in a month, successively landing on Bitget, Kucoin, Gate, and other exchanges, with a market value close to $300 million.

In November, BRC20 tokens Trick and Treat, issued by the Lightning Network protocol Nostr, kept soaring, with a market value exceeding $20 million. BRC20 issued on various EVM public chains, like POLS, caused congestion on the Polygon network and consumed more than 100 million MATIC gas.

Commentary:

Since 2023, the BTC ecosystem has seen astonishing development, with a multitude of native protocols emerging, bringing not only more gameplay and applications to BTC, but also huge profits for BTC miners. Looking at the leading tokens in the BTC ecosystem protocol, the market value of $ORDI has reached $400 million, while $ATOM and $PIPE have a market value of around $30 million. Since they only have meme attributes, whether there will be subsequent community operations and consensus is key to their long-term development. Investors should be cautious when investing in the FOMO inscription market.

HASHKEY Capital

• HashKey Launches Hong Kong's First Licensed Virtual Asset Exchange App and Platform Token HSK

On November 1, 2023, the licensed virtual asset exchange HashKey Exchange announced that it had received approval from the Hong Kong Securities and Futures Commission (SFC) to enable full trading functionality on its mobile app. Dr. Xiao Feng, Chairman and CEO of HashKey Group, and Livio Weng, COO of HashKey Group, jointly unveiled the HashKey Exchange APP, announcing the official launch of Hong Kong's first licensed virtual asset exchange app. At the same time, HashKey Exchange chose HSK as the platform token, revealing new application scenarios and user participation plans for HSK.

Livio Weng, Chief Operating Officer of HashKey Group, said, "Over the past year since the Hong Kong government issued the 'Policy Statement on the Development of Virtual Assets in Hong Kong', HashKey has witnessed the implementation of key policies such as VASP. After multiple rounds of careful checks by regulatory authorities, we have finally obtained the SFC's approval to launch the HashKey Exchange mobile app. We are committed to providing a safe, compliant, and professional trading platform for investors. Meanwhile, we will add more support for the HSK token, including fee discounts, special activities, and more."

HSK token has a total circulation of 10 billion. The initial circulation is 500 million, all of which will be allocated to users through airdrops, community building, and platform activities. The remaining 95% of the tokens are locked for two to four years, and will be released gradually in line with the expansion of the platform.

Commentary:

The launch of HashKey's licensed virtual asset exchange app is a milestone in Hong Kong's financial technology industry. It demonstrates the effectiveness of the SFC's regulatory framework and the region's willingness to embrace digital currencies. Moreover, the introduction of HSK token represents a common practice among exchanges to incentivize user participation and loyalty. However, investors should pay attention to the lock-up period and release schedule of HSK tokens to avoid potential market manipulations.

HASHKEY Capital

- **USDC Stablecoin is Fully Backed, says Auditing Firm Grant Thornton**

According to a report published by Grant Thornton on November 16, 2023, the USDC stablecoin is fully backed by U.S. dollars. The accounting firm stated that as of October 31, 2023, Centre, the consortium behind the USDC stablecoin, held $28.6 billion in assets, which exactly matched the number of USDC in circulation.

This audit was conducted in response to longstanding concerns among cryptocurrency investors about the transparency and trustworthiness of stablecoins. Many investors have been skeptical about whether stablecoin issuers actually hold enough reserves to back up the tokens they issue.

Commentary:

The audit result should put to rest some of the concerns about the credibility of USDC. However, it is important to remember that an audit is only a snapshot in time and cannot guarantee future actions or conditions. Therefore, ongoing transparency and regular audits are necessary to maintain the trust of investors and regulators. It's also worth noting that the audit of USDC is part of a larger trend of increasing scrutiny and regulation of stablecoins, which could have significant implications for the broader cryptocurrency market.

HASHKEY Capital

• First NFT Art Museum Opens in Seoul

The world's first physical NFT Art Museum has opened its doors in Seoul, South Korea. The museum, which opened on November 15, 2023, displays both physical and virtual artworks, with a specific focus on NFT (Non-Fungible Token) art.

The museum features several galleries with large screens and virtual reality (VR) equipment to showcase digital NFT art. It also has a physical gallery space for traditional art. The museum aims to bridge the gap between the physical and digital art world and educate the public about NFTs and the potential they hold for artists and collectors.

Commentary:

The opening of the NFT Art Museum is a significant milestone for the NFT and art world. With the rapid growth of NFTs, it's exciting to see physical spaces dedicated to showcasing and educating about this new form of digital art. However, the sustainability of such a museum will largely depend on the continued interest and growth in the NFT market. As with any investment in art or digital assets, potential collectors should do their due diligence and be cautious of price volatility and potential scams.

HASHKEY Capital

- **U.S. October CPI Cools Down More Than Expected**

According to data released by the U.S. Bureau of Labor Statistics on November 14, the U.S. October CPI increased by 3.2% year-over-year, lower than the market expectation of 3.3%, with the previous month's data at 3.7%. The month-on-month growth rate slowed down from the previous month's 0.4% to 0.0%, also below the expected 0.1%. The core CPI, which excludes food and energy costs and is more closely watched by the Federal Reserve, slowed slightly from the previous month's 4.1% to 4.0%, falling to its lowest since September 2021. After the CPI data was released, the US dollar index fell 50 points, and non-US currencies collectively rose; the three major US stock index futures rose short-term, all up over 1%. Bitcoin also rose over 1% in the short term to nearly 37,000 US dollars, then slightly fell back to around 36,300.

According to Fedwatch data, the probability of the Federal Reserve keeping interest rates unchanged in the 5.25%-5.50% range in December is 85.7%, and the probability of raising interest rates by 25 basis points to the 5.50%-5.75% range is 14.3%. The probability of keeping interest rates unchanged until January next year is 73.3%, the cumulative probability of raising interest rates by 25 basis points is 24.6%, and the cumulative probability of raising interest rates by 50 basis points is 2.1%.

Commentary:

The U.S. CPI data is an important reference for whether to continue raising interest rates within the year. The market currently expects that there is a high probability that the Federal Reserve will not raise interest rates in December, and bets on the Federal Reserve lowering interest rates early next year. The period before the rate-cutting cycle is the best opportunity for investment. Investors should closely watch the Federal Reserve's decision and the macro environment to ensure they grasp the key investment timing.

HASHKEY Capital

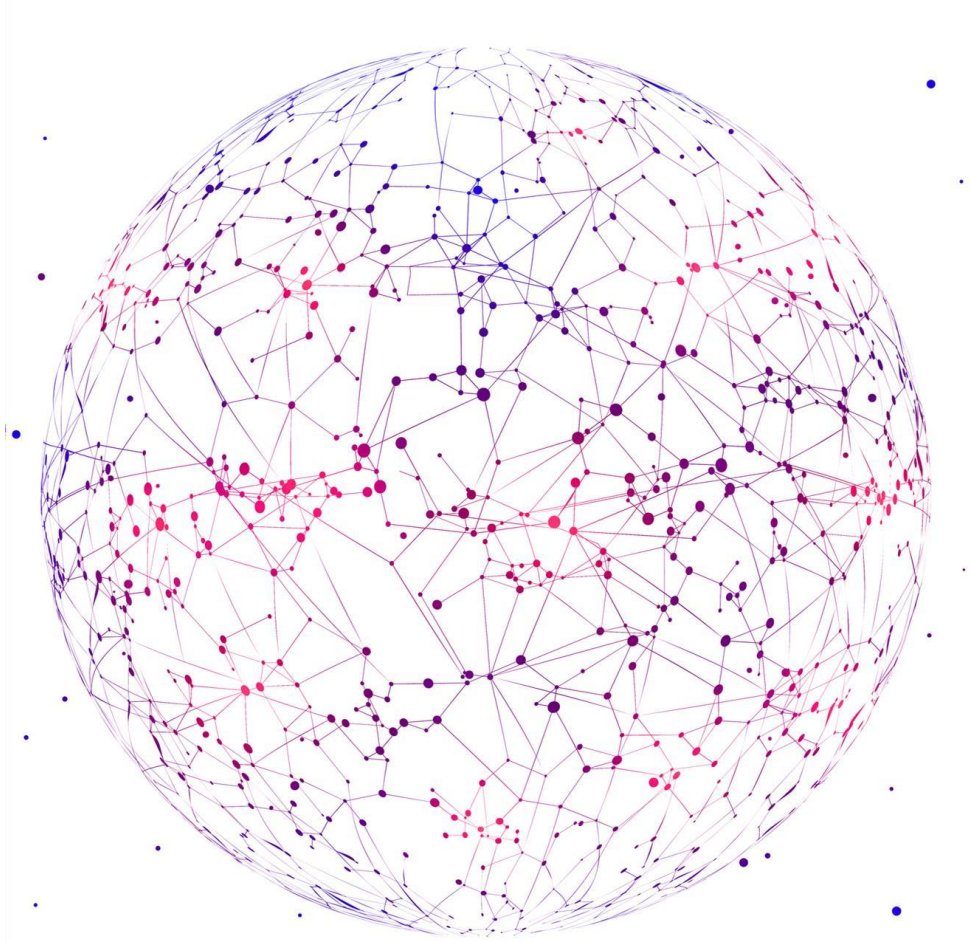
- **ETF Related News**

On November 16, 2023, the SEC announced that it would delay its response to the Bitcoin ETF applications of Hashdex and Franklin Templeton, meaning that the SEC's next vote on Bitcoin ETF will be before the ARK Bitcoin ETF Final Deadline on January 10, 2024. According to previous statements by the SEC, it hopes not to give too much of a first-mover advantage to any one ETF, and it is possible that in January 2024, ETFs applied for by companies like BlackRock, Bitwise, and ARK will be approved simultaneously. At the same time, BlackRock has formally submitted an application for an ETH spot ETF, and the market expects that if the BTC ETF can be smoothly approved, then the ETH ETF will also be approved subsequently. This month, as the ETF expectations approach and various positives continue to be released, the BTC price has seen a substantial increase, although affected by the delayed response, the BTC price has experienced a small decline, but the overall market's FOMO sentiment has not decreased, and the market's strength starts spreading to other tokens.

Commentary:

Investors' expectations for the approval of ETFs are extremely high, and the market expects the probability of passing ETFs in January next year to be over 90%. With the gradual abundance of the money market, there may be a bull market lasting 2-3 months. As ETFs continue to price in, investors should be cautious about market fluctuations before and after the official approval of the ETF.

Listed Companies & Token



- **TIA (Celesita) Listing**

In October 2023, Celestia airdropped a total of 6% to early EVM public chain users, Atom ecosystem users, and BTC/ETH/Cosmos developers. On November 1, TIA officially went live on exchanges like Binance, Coinbase, Kraken, Bithumb, etc, with a trading price around $2.5. Subsequently, as the market warmed up and TIA's circulation was relatively low, the price rose sharply, and by November 17, it had risen to a new high of $6.5.

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

Source: https://twitter.com/proactive_UK/status/1718893514396766555

Section IV

China Blockchain Headlines

Taiwan's Administration for Digital Industries to Focus on Key Technological Developments such as Generative AI and Blockchain Technology

Under the strong global push for digital transformation, Taiwan has also established the " Administration for Digital Industries " as the specialized body for digital economic development. The administration handles the policy planning for digital-related industries, the drafting of laws and regulations, and the promotion of digital technology applications. It assists various industries in meeting the challenges and opportunities of the digital economy era, strengthening the digital resilience of industries. With RISE - "R (Resilience), I (Integration), S (Security), E (Empowerment)" as the main axis of business promotion, the bureau will also focus on "A (Generative AI), C (Blockchain Technology), E (Net Zero Transformation), S (Software Strategy)" and other key technological development issues in the future. It aims to build a good digital development environment, select demonstration fields and service scenarios, integrate the power of industries and communities, drive continuous innovation in the industrial economy, promote the development of Taiwan's digital economy, and accelerate the digital transformation of various industries.

Fuzhou Publicizes Blockchain Industry Development Special Fund Reward Companies: Planned Support Amount is 429.384 Million Yuan

According to the "Notice of the Fuzhou City Big Data Development Management Committee on Organizing the 2022 Fuzhou City Blockchain Industry Development Special Fund Application Work", the Fuzhou City Big Data Committee organized the "Digital Fuzhou" experts to review the 2022 Fuzhou City Blockchain Industry Development Special Fund application enterprises (institutions). The expert review and the city's Big Data Committee's research decided that Fujian Fuchain Technology Co., Ltd. and other ten enterprises (institutions) meet the policy conditions and are publicized, and are proposed to receive special fund rewards. The planned support amount is 4.29384 million yuan.

Haikou Releases Blockchain Industry Development White Paper, Multiple Application Scenarios Implemented

The Hainan Free Trade Port "Digital Economy Lecture Hall" blockchain special seminar and the Haikou City Blockchain Development White Paper release conference were held. The conference disclosed that the White Paper summarizes and analyzes the overall development status, conditions, and effects of blockchain development in Haikou City, as well as the problems and challenges faced. It also refers to the blockchain development experience of other regions to propose development ideas and application prospects. At the beginning of 2022, Haikou City was approved as a national comprehensive pilot area for innovative blockchain applications, and the development of blockchain in Haikou City entered a substantial acceleration stage. Fuxing City Internet Information Industry Park, as a provincial key industrial park, is also the main carrier park for promoting the development of the blockchain industry in our city, with a total of 52 registered blockchain companies. The initial formation of the blockchain industry in Haikou City has been achieved, and multiple "blockchain+" application scenarios have landed.

HASHKEY Capital

Bitcoin Scaling Solution Overview

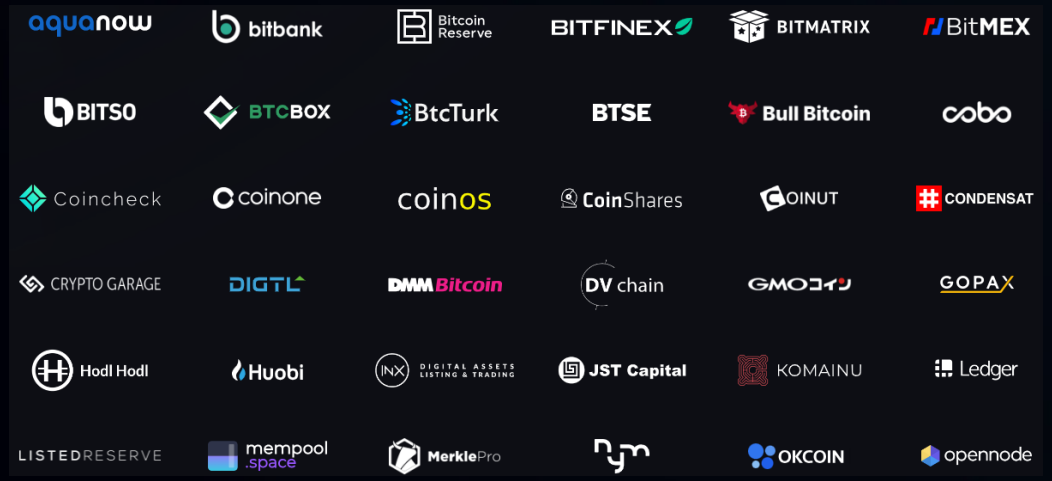
2.4 Liquid Network

Liquid Network is a Bitcoin sidechain launched by Blockstream in September 2018. It specifically caters to institutional-level users, serving as a settlement network for exchanges, brokers, market makers, and other institutions. It enables faster and more confidential Bitcoin transactions among these entities. Notable participants on the Liquid Network include OKCoin, BitMEX, Bitfinex exchange, Dgroup OTC desk, XBTO, and Altonomy market makers, among others. Due to its nature, Liquid Network operates more like a federated blockchain, and Blockstream charges them monthly maintenance fees. In addition to its transfer functionality, Liquid also supports the creation of smart contracts and the issuance of assets. Within the ecosystem, there are DeFi protocols like Hodl Hold and Sideswap.

HASHKEY Capital

2.4.1 Signing to record blocks

Blocks on the Liquid blockchain are not generated through mining hash competition but rather through signing, governed by a consortium of cryptocurrency institutions. According to the Liquid official website, there are currently 60 members in the consortium. The Byzantine Fault Tolerant Circular Multisignature mechanism is employed, where block-signing members take turns proposing alternative blocks. Once a proposed block is published, if it receives signatures from 2/3 of the signers, the block is recorded on the ledger. This rotating process continues repetitively. Due to the reliance on block signing and the limited participation of "miners," block generation on Liquid is relatively fast, with a predictable rate. Approximately one block is generated every minute.



Source: https://liquid.net/

2.4.2 Privacy Transactions

Confidential Transactions (CT), a privacy technology invented by Blockstream, helps protect transaction privacy on the Liquid Network. CT technology allows for the hiding of transaction amounts, ensuring that the transaction amounts are not publicly disclosed. Only the transaction participants have access to important metadata such as transaction amounts and recipient addresses. CT technology utilizes the Pedersen Commitment algorithm to conceal transaction amounts. The Pedersen Commitment algorithm is based on the discrete logarithm problem and converts the transaction amount into a random number. It then combines this number with a publicly available parameter and performs a SHA-256 calculation. This process effectively hides the transaction amount while still allowing the validity and correctness of the transaction to be proven. Participants have the option to selectively disclose transaction information. By default, the protocol broadcasts transactions in a non-transparent manner, but users can manually configure settings to publicly disclose metadata if desired.

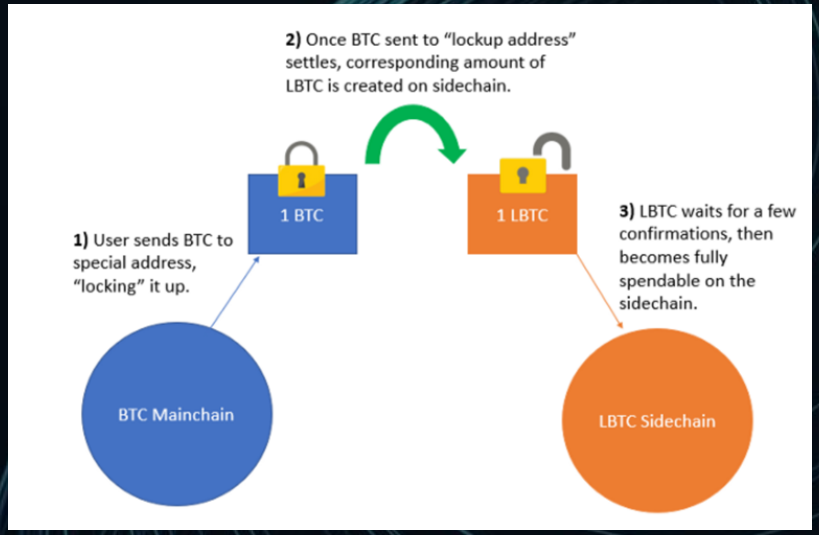
2.4.3 Asset Issuance

Issuing assets on the Liquid Network requires becoming a member of the Liquid Federation and meeting a series of conditions and reviews. Various types of assets can be issued on the Liquid Network, including tokens, NFTs, stablecoins, securities, ETFs, and more. Issuing assets involves using specific tools such as the Issued Asset Management (IAM) control panel and the Liquid Core wallet. Issuers need to set parameters for the assets, such as the asset name, symbol, total supply, asset description, and more. Asset issuance on the Liquid Network requires providing collateral, usually in the form of Bitcoin, to ensure stability and redeemability of the assets. According to the Chief Strategy Officer of Blockstream, issuing assets on Liquid Network offers several benefits compared to other platforms. For example, Liquid Network is exclusively used for financial transactions and settlements, without adding excessive redundant data to the blockchain, thereby avoiding congestion.

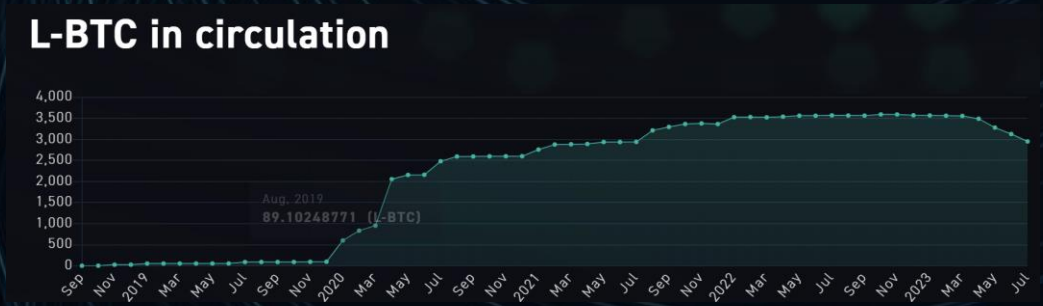
HASHKEY Capital

2.4.4 LBTC

The native token in the Liquid sidechain is LBTC, which is pegged 1:1 with BTC. Currently, the supply of LBTC remains stable at around 3,000 BTC. The pegging process requires users to send BTC to a P2SH address and "freeze" it. After 102 confirmations in the Bitcoin blockchain (to prevent reorganizations), users can obtain the corresponding LBTC on the sidechain. The unpegging process involves users transferring LBTC to a destruction address within Liquid and waiting for 2 block confirmations (instead of the 100 required for pegging). Afterward, the functionary members sign an 11/15 multisignature transaction on the Bitcoin blockchain to return the BTC to the original owner and destroy the LBTC. From the user's perspective, exchanges and other members of the Liquid Network hold LBTC balances to facilitate BTC exchanges with users. Exchanges can directly transfer LBTC between each other. For example, if exchange A and exchange B are both members of the Liquid Network and a user wants to transfer BTC from exchange A to exchange B, exchange A only needs to transfer the corresponding LBTC to exchange B, deducting the user's BTC balance. Upon receiving LBTC, exchange B can then credit the user's BTC to their account on exchange B. Therefore, users do not need to be involved in the LBTC conversion process. They only experience fast and timely BTC transfers.



Source: https://blog.goodaudience.com/overview-7b9ea0b0d5af



Source: https://liquid.net/

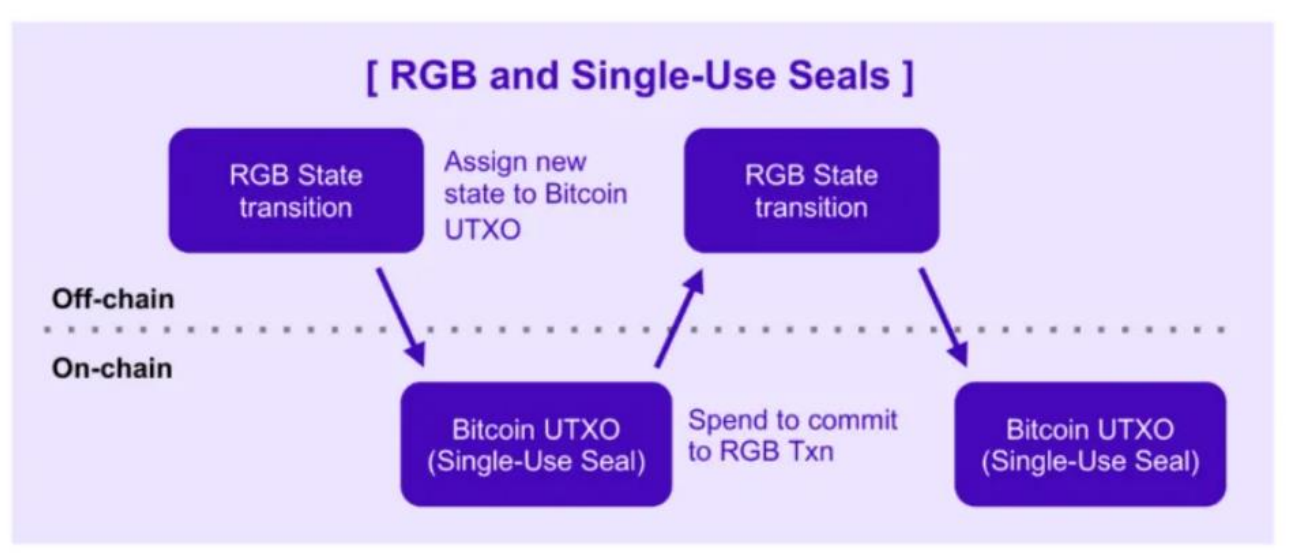
2.5 RGB

The name RGB originates from the three primary colors. The protocol's initial direction was to create colored coins. The development of the RGB protocol began in 2018 and was proposed by Bitcoin developers Giacomo Zucco and Peter Todd, among others. The core idea of the protocol is to leverage Bitcoin's decentralized nature while providing higher-level programming capabilities. The RGB protocol modularizes different functionalities of smart contracts, including issuance, data, and state. This modular design allows different parts of smart contracts to be independently processed and executed off-chain, with the Bitcoin mainnet serving as the ultimate state confirmer. Its off-chain logic is similar to the Lightning Network and is compatible with it. Applications supported by the RGB protocol include Iris Wallet, My Citadel, Bitmask, and others. These applications utilize the functionalities of the RGB protocol to create and manage colored coins, enabling more complex transactions and contract logic.

In summary, the RGB protocol utilizes the underlying technology and decentralized nature of Bitcoin to provide higher-level programming capabilities for smart contracts while maintaining the security and reliability of the Bitcoin mainnet.

2.5.1 Technical Principle

The technical principle of RGB can be summarized as the binding of off-chain asset states with the UTXOs (Unspent Transaction Outputs) of the Bitcoin mainnet, as shown in the diagram below. When transferring tokens, the off-chain payer needs to provide the recipient with information about the asset flow sequence. On-chain, the corresponding UTXOs need to be spent. When spending the UTXO, the Bitcoin transaction must include a data commitment, which is the RGB payment information. The payment information includes inputs, quantities, asset IDs, etc. The RGB payment information is hashed, and the resulting hash value is added to the OP_RETURN output of the Bitcoin transaction, binding the transaction information with the Bitcoin transaction.



Source: ViaBTC Capital, https://medium.com/@ViaBTC_Capital/viabtc-capital-insight%E4%B8%A8a-brief-analysis-of-rgb-a-scalable-confidential-smart-contract-protocol-b449f7dbb323

Single-Use Seals

As mentioned in the diagram, Single-Use Seals are one of the technical details implemented in RGB. In the RGB protocol, Single-Use Seals refer to an encryption signature technique used to ensure the immutability of asset ownership. Each asset state is associated with a unique Single-Use Seal.
The mechanism of Single-Use Seals can be described as follows:

- **Initial State: When an asset is created, an initial Single-Use Seal is generated, which is associated with the initial state of the asset.**
- **Asset Transfer: When the ownership of an asset is transferred, the old Single-Use Seal is destroyed, indicating that the old asset state is no longer valid. At the same time, a new Single-Use Seal is created to represent the new asset state.**
- **Seal Verification: Other participants can verify the Single-Use Seal in the asset to confirm ownership and state. If the Single-Use Seal of the asset does not match the current valid seal, it indicates tampering or inconsistency in ownership.**

The destruction and generation of UTXOs correspond to the changes in Single-Use Seals. By destroying the old UTXO and generating new UTXOs, the consistency and traceability of asset transfers are ensured, preventing tampering with asset ownership. This mechanism of Single-Use Seals and UTXOs helps maintain the integrity and security of asset ownership within the RGB protocol.

Client-side validation

In the RGB protocol, transactions are created and verified in client applications rather than directly executed on the blockchain. This differs from traditional blockchain protocols where transactions are broadcasted to the blockchain network for validation and recording. In the RGB protocol, transactions are represented using commitments and proofs. As mentioned earlier, commitments are encrypted values that conceal specific assets and amounts, while proofs are additional information used to verify the correctness and legitimacy of transactions. These commitment and proof data are stored in client applications and verified to ensure the validity of transactions.

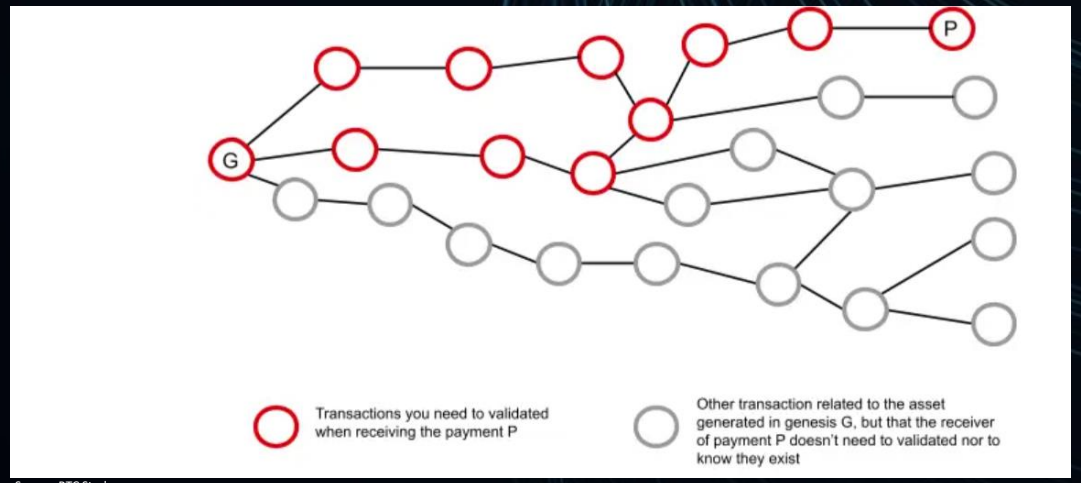
Specifically, transaction verification in the RGB protocol typically involves the following steps:

-**Commitment Verification:** Client applications validate the commitments used in the transaction to ensure their validity. This includes verifying the signatures of the commitments, consistency between commitments and asset states, and other relevant checks.

-Proof Verification: Client applications use proof data to verify the correctness of the transaction. These proofs can include ownership proofs for assets, transfer condition proofs, and more. The client verifies these proofs to ensure that the transaction complies with the rules and requirements of the RGB protocol.

-Data Storage: The relevant data of the transaction, such as commitments and proofs, are stored in the client application for future verification and querying. This data is not directly stored on the blockchain but can be stored in the client application's local storage or other appropriate data storage mechanisms.

By completing transaction verification and data storage on the client side, the RGB protocol provides increased privacy, scalability, and flexibility. Furthermore, to confirm that the sender truly owns the assets being sent and to ensure the integrity and validity of the transaction, it is not enough to only verify the current payment information. It is necessary to trace the transaction history of the asset, as shown in the diagram below. However, it is sufficient to verify only the asset transfer path related to the current transaction.



Source: BTC Study

By completing transaction verification and data storage on the client side, the RGB protocol can provide higher privacy (without the need for network-wide broadcasting), scalability, and flexibility.

Output Blinding

Output Blinding is an important privacy protection mechanism in the RGB protocol. With output blinding, the party initiating a payment request can send tokens to a hash value without revealing the actual UTXO (Unspent Transaction Output) receiving the tokens. The recipient of the tokens selects a target UTXO and generates a random blinding secret value. The recipient then concatenates the target UTXO and the blinding secret value, calculates their hash value, and sends the generated hash value to the payer as the receiving address for the tokens. This provides a higher level of privacy protection for the transaction. However, when the tokens are spent, the blinding secret value needs to be disclosed to the recipient to verify the transaction history. Therefore, when using the RGB protocol, users need to balance the trade-off between privacy and traceability.

3. Conclusion

Bitcoin will experience its next halving event in March 2024, reducing the block reward from the current 6.25 BTC to 3.125 BTC per block. Miner income is primarily composed of block rewards and transaction fees, and the halving event will directly impact miner revenue. However, if miners can receive sufficient rewards from transaction fees, they will still choose to actively maintain the security of the Bitcoin network.

Although Bitcoin has experienced a decrease from its previous all-time high, the emergence of the Ordinals protocol has injected new vitality into the BTC ecosystem. Ordinals can bring a 6.1% increase in income for miners. While opinions within the Ordinals community may differ, "Bitcoin purists" believe that Bitcoin should adhere as much as possible to its transactional properties as electronic cash and should not add more redundant data. Another part of the community is excited about the additional possibilities and space that Ordinals brings to Bitcoin. There is no unified consensus on what Bitcoin should be used for, and no single person or entiry can define the purpose of Bitcoin.

In conclusion, the emergence of Ordinals has prompted the community to reconsider the development space of the Bitcoin ecosystem. The locked value of Bitcoin scaling solutions is only around $400 million, while the market capitalization of Bitcoin is close to $600 billion. Compared to Ethereum, Bitcoin's scaling solutions are still in the early stages of development, although many of the projects have been established for a while. We believe that the Bitcoin community needs to continue exploring and researching diverse scalability and application solutions to provide users with a better experience. This will allow Bitcoin to unleash more possibilities beyond being just a store of value. Let us look forward to the renaissance of the Bitcoin ecosystem together.

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