bitsCrunch Network

A Decentralized Enriched NFT Data Network

Author: Gopi Kannappan Contributors: Ashok Varadharajan, Saravanan Jaichandaran

October 2023 (v1.2)

Legal Disclaimer: This whitepaper and all the information contained within are provided solely for informational purposes. This document is not a solicitation or offer for buying or selling token or any other financial instruments, and should not be treated as such. Potential token holders should carefully consider the potential risks and consult their legal, financial, tax, and other professional advisors before participating in any token sale or investing in the bitsCrunch network.
The bitsCrunch project, its founders, team members, and any affiliated parties:

- No Guarantees: Do not guarantee any specific outcomes, token value, or future performance related to the bitsCrunch network or its associated token.
- No Liability: Assume no liability or responsibility for any loss or damage that might arise from the reliance on this whitepaper or the use of or reliance on any materials contained within.
- Regulatory Uncertainty: Note that the regulatory status of cryptographic tokens and blockchain technology is uncertain and may change in various jurisdictions. This can consequently affect the rights of token holders, the value of tokens, and the functioning of the bitsCrunch network.
- Incomplete Information: While efforts have been made to ensure accuracy, the content of this whitepaper might not be exhaustive and does not imply elements of a contractual relationship.
- Subject to Change: The details and structures described in this whitepaper are subject to change without notice, based on ongoing developments, regulatory changes, or other reasons.
- Third-Party References: Any references to third-party data, companies, or technologies do not constitute an endorsement or recommendation.

This document does not promise any specific benefits, monetary gains, or outcomes. All potential participants are urged to do their due diligence, understand the specific details and risks associated with the bitsCrunch network and its token, and consult with professionals as needed.

Abstract

Blockchain and cryptocurrency has evolved many fold since the famous bitcoin paper published back in 2008. That paper only talked about the peer-to-peer electronic cash system but it set the stage for many more innovations to follow it. Ethereum's launch in 2013 brought more to blockchain than just crypto currencies, over the course of a few years it set the stage for decentralized finance, decentralized exchanges, paved way for smart contracts technology, NFTs etc.

Today we have 1000s of crypto coins, 100s of blockchain platforms, millions of smart contracts, billions of successful transactions, millions of NFTs, Decentralization of financing, Decentralized exchanges and many more. All this and more to come, thanks to the strong communities behind the blockchain ecosystem.

All this accelerated growth also has meant that we have scammers and looters that want to rig the system to favor them and extract value out of innocent people. These bad actors leverage their knowledge on the blockchain technology to maliciously increase trading volume or price of an NFT, token or a crypto currency and lure the consumers to fomo in to eventually scam them.

While all these malicious practices are public records in blockchain, it is very hard for users to gain clear insights and identify all the patterns. Our goal is to analyze all NFT transactions, use AI/ML to automatically detect malicious activities and make it accessible to everyone. Our initial focus is on the NFT's but we will eventually increase our scope to tokens and crypto currencies.

In this paper we present bitsCrunch, a decentralized enriched NFT data network. We describe the processes on data acquisition, data processing and data delivery in a decentralized and permissionless network deployed on one of the existing EVM based layer 2 solutions. Initially this network will include bitsCrunch developed AI/ML models, metrics, insights etc, as the network matures community developers will be able to contribute to the network with additional models, metrics and other contributions. This will ensure the longevity of the network and also provide a collaborative ecosystem.

This paper will clearly provide an insight into the plans, functional architecture and implementation of the network decentralization including the network security. It will also explain the motivation for decentralization and why this is important for the NFT ecosystem.

Introduction

NFTs, or non-fungible tokens, are unique, non-interchangeable digital assets stored on a blockchain—a decentralized digital ledger. These tokens can represent a wide range of digital items such as images, audio files, videos, and digital art. Each NFT is stored as a one-of-a-kind item on the blockchain, allowing for easy verification of ownership. NFTs have numerous applications and the potential to transform various sectors, including digital art, metaverse, gaming, decentralized finance, blockchain certification, and more. The trading volume of NFTs has seen phenomenal growth, soaring from just a few million dollars in 2020 to over $54 billion in 2022. This remarkable surge shows no signs of abating and is expected to keep rising as blockchain technology permeates various industries.

To illustrate this growth, consider the chart below, which displays the monthly USD volume of NFTs across multiple blockchain. The volume peaked in January before stabilizing in recent months. Furthermore, Q1-2022 was the largest quarter for NFT trading volume, with an astonishing $33 billion in transactions. These figures highlight the immense potential and vast opportunities NFTs offer in the digital realm.

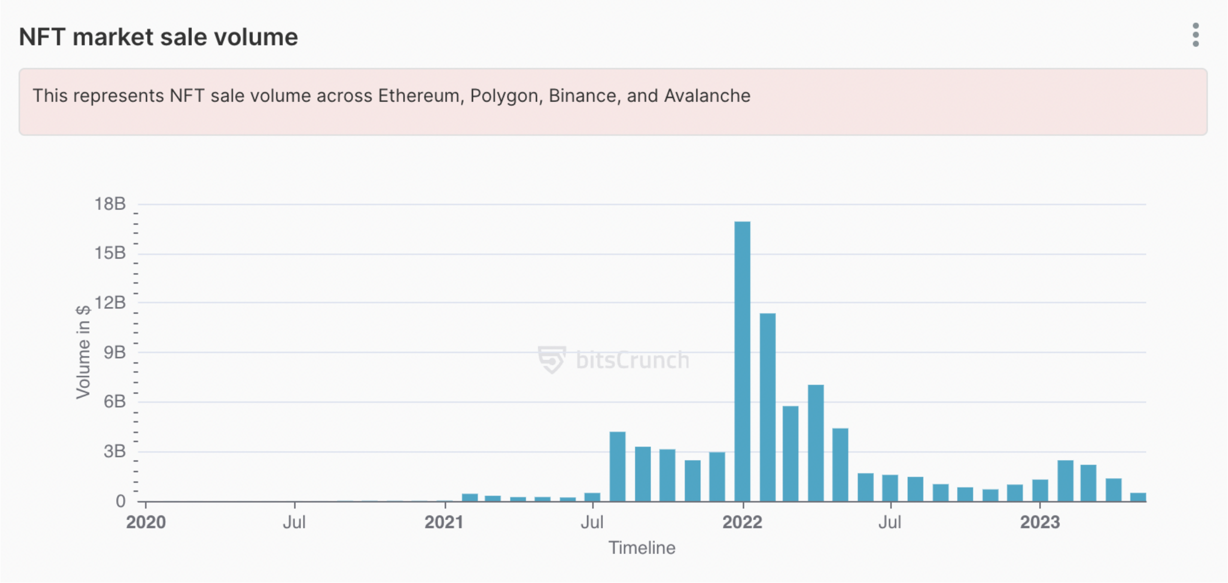


Figure 1: Cross blockchain monthly NFT sale volume chart since the beginning of 2020

As the volume and the hype in NFTs continues to increase, it definitely attracts the attention of some bad actors. These bad actors have engaged in practices like NFT wash trading that harm the market and the NFT collectors. Below you can see the monthly washtrade volume for 2022, we noticed more than $32 Billion in wash trading and about 1 out of 20 secondary market NFT transactions are wash trades.

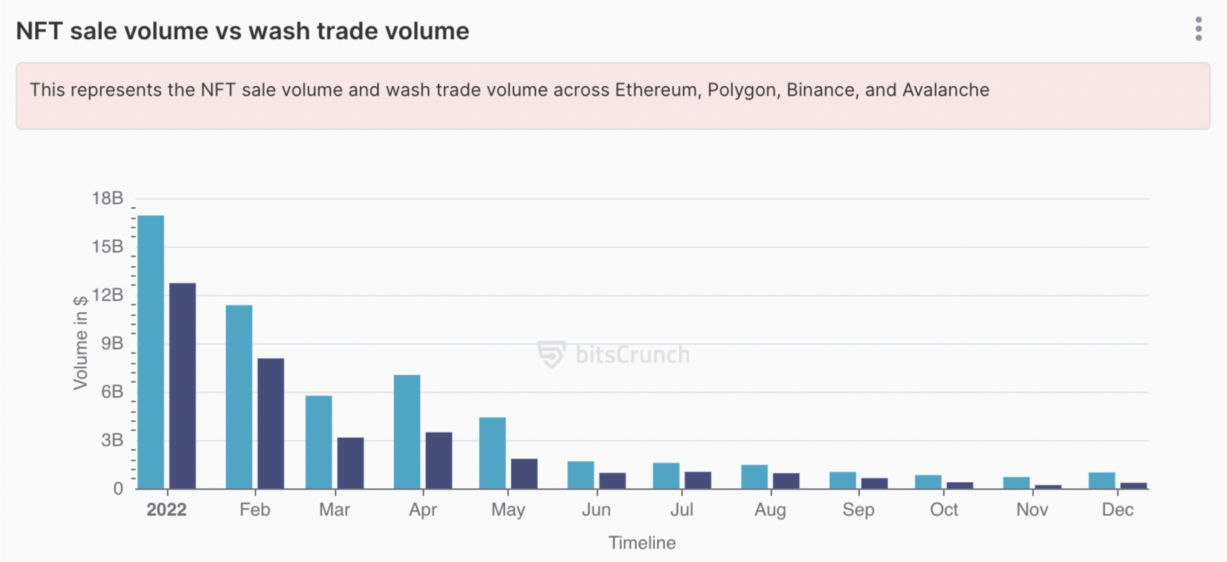


Figure 2: NFT sale volume vs wash trade volume chart since the beginning of 2022

Some of the Key challenges

In recent years, the NFT landscape has witnessed tremendous growth, with 2022 witnessing a 300% growth in NFT sales volume over 2021, so far the total NFT sale volume is at over $80 Billion with 2022 alone accounting for more than $50 billion. However, the surge in NFT popularity has also given rise to NFT fraud. A significant issue with NFT fraud is how easily scammers can create and sell NFTs. Unlike traditional art or collectibles, NFTs are wholly digital, making it more convenient for scammers to create counterfeit NFTs and sell them to unwary buyers.

Another challenge is the absence of regulation in the NFT market. In contrast to the traditional art market, there is no governing body or regulatory framework to guarantee NFT legitimacy and safeguard buyers. This environment allows scammers to operate and sell fake NFTs without the threat of legal repercussions. There have even been instances where NFT marketplaces themselves have engaged in fraudulent activities, such as permitting the listing and sale of counterfeit NFTs or allowing fraudulent sellers to operate on their platforms.

Our research shows that 1 in 10 NFTs minted on the largest NFT marketplace are fraudulent, either as copy mints of popular NFTs or as derivatives. This alarming trend has resulted in a total loss of over $4 million for retail investors in that marketplace alone. Safeguarding retail users and projects from NFT scams is vital, but analyzing NFT sales data is a complex task. The data is intricate and necessitates sophisticated tools for interpretation. Consequently, users must rely on increasingly less reliable statistics, making the due-diligence process cumbersome and often unsatisfactory. Transaction forensics is crucial for analyzing NFT sales data, but it involves running heuristics on vast amounts of user data. To achieve the most precise results, data must be collected from the blockchain's genesis, requiring a comprehensive examination of its entire history.

Merging metadata from off-chain sources like IPFS with on-chain sale/transfer data adds another layer of complexity. This labor-intensive process requires meticulous attention to detail. While raw data is useful, calculated metrics present a more holistic perspective, empowering users to make well-informed decisions. Nevertheless, calculating metrics demands greater CPU runtime and higher costs.

Marketplaces frequently lack dependable statistics about their platform's growth and reach, compelling investors to rely on less trustworthy information and complicating due diligence. This scenario also adversely impacts the community, as wash traders siphon off rewards intended for honest participants. Additionally, NFT pricing and valuation present further challenges. Both creators and collectors struggle to determine an NFT's accurate value, leading to inflated and deflated pricing. Without trustworthy valuations for NFT assets, their potential in the DeFi space remains constrained.

Existing NFT data Providers

Current NFT data providers can be classified into several categories, each facing its own set of challenges and limitations:

1. DeFi protocol-specific data providers: These providers primarily focus on delivering indexed data for DeFi protocols, offering little to no support for NFT-related data. Consequently, users interested in NFT analytics may find these services inadequate for their needs.
2. Centralized solutions: Such data providers suffer from a lack of transparency and limited community collaboration. Centralized control over data aggregation and dissemination can lead to biased information or potential censorship, which undermines the trust and reliability that users seek in the rapidly growing NFT market.
3. On-chain data normalization providers: These services mainly concentrate on normalizing on-chain data but often neglect NFT-specific information. This limitation can result in an incomplete understanding of the NFT landscape, as crucial details about individual NFTs or their associated metadata might be missing.
4. NFT forensics oversight: Many existing NFT data providers pay little to no attention to NFT forensics, an essential aspect of the ecosystem that helps identify fraudulent activities, such as counterfeit NFTs or wash trading. The absence of robust forensic analysis can compromise the security and integrity of the NFT market.
5. No advanced NFT metrics: Current NFT data providers may lack sophisticated metrics and analytics that can provide users with deeper insights into the market dynamics, trends, and valuation. The absence of advanced metrics makes it difficult for users to make well-informed decisions and fully understand the potential of NFT investments.
6. Limited community contribution opportunities: Many existing NFT data providers do not offer opportunities for community members to contribute data, insights, or other relevant information. This lack of community involvement can hinder the growth of a diverse and dynamic NFT ecosystem, which relies on collective intelligence and collaboration.

In summary, the NFT data provider landscape is currently fragmented and faces several challenges, including a lack of focus on NFT-specific data, centralized solutions with limited transparency, inadequate attention to NFT forensics, absence of advanced metrics, and restricted opportunities for community contribution. Addressing these issues is critical for fostering a reliable, secure, and collaborative NFT ecosystem that benefits all participants.

Our Solution

The solution to the challenge of analyzing NFT sales data lies in developing a platform capable of gathering and enriching data for NFTs, ultimately providing more accurate and reliable metrics. This platform will employ advanced computations, AI algorithms, and data from both on-chain and off-chain sources, including IPFS metadata. Decentralization of this platform will allow community developers to contribute additional algorithms for continuous data refinement and unlocking new use cases.

The platform offers reliable statistics on the growth and reach of NFT marketplaces, protecting honest participants from wash traders seeking to steal rewards and value. It also tackles pricing and valuation challenges by delivering precise valuations for NFT assets through ML algorithms, promoting their utility within the DeFi space. The platform streamlines NFT sales data analysis, enhancing accessibility and insights for users. Sophisticated AI models for transaction forensics will be incorporated, requiring meticulous data extraction from the blockchain's genesis and demanding higher memory and processing capacity.

This decentralized platform's capabilities extend beyond NFTs, encompassing use cases such as tracking cryptocurrency prices, monitoring social media sentiment, and predicting market trends. Its strength lies in its adaptability and the ongoing addition of new algorithms to address market demands. As more developers contribute, the platform becomes increasingly robust, versatile, and valuable across various use cases.

A key feature of this platform is its community-driven nature, allowing developers and users alike to influence its direction and suggest new algorithms, features, and use cases. The absence of central authority ensures true decentralization and transparency. The platform will be deployed on an existing EVM-based layer2 solution. As the network expands and accumulates more data, its value across various use cases, such as NFT valuation, fraud detection, market trend prediction, and social media sentiment analysis, will continue to grow. By providing enriched, accurate, and comprehensive data, this decentralized network establishes a new benchmark for data analysis and empowers the community to make informed decisions based on reliable information.

The diagram below illustrates the high-level data flow for extracting, processing, and delivering valuable insights from blockchain data related to NFTs. By leveraging a series of steps, the raw data is transformed into curated and enriched information, providing users with a range of insights such as metrics about NFT collections, estimated NFT prices, or trade alerts.

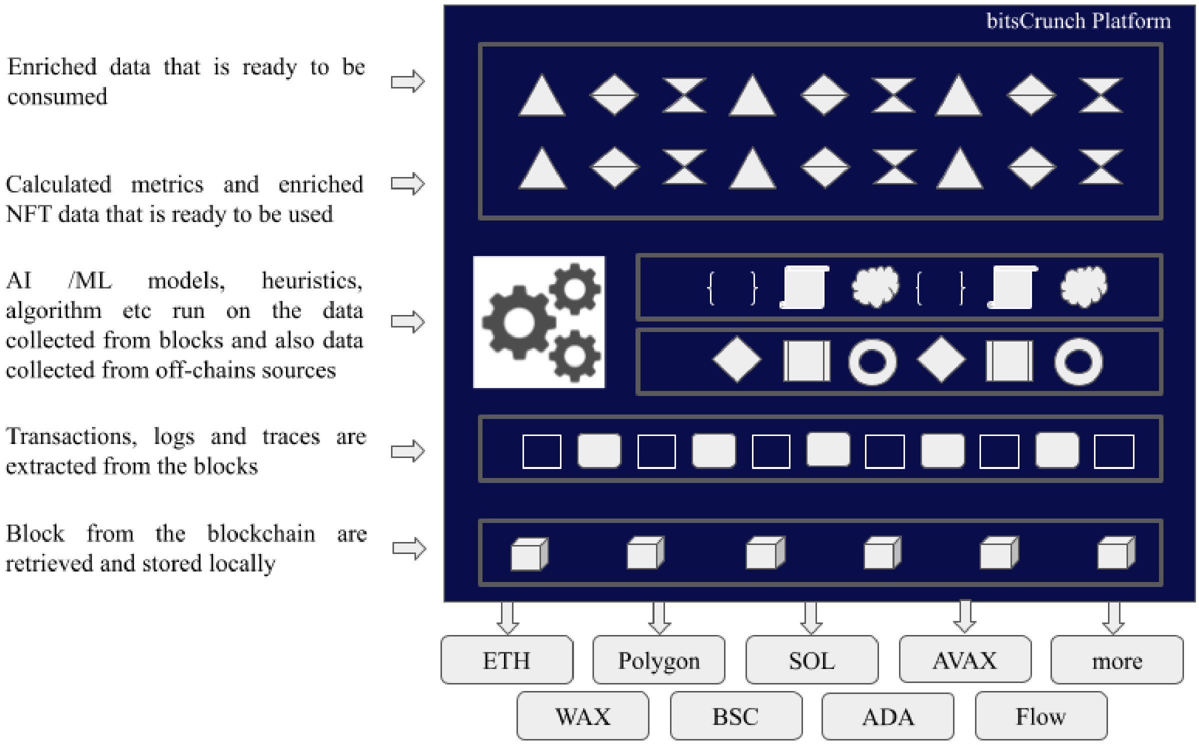

Enriched data that is ready to be consumed
Calculated metrics and enriched NFT data that is ready to be used
AI /ML models, heuristics, algorithm etc run on the data collected from blocks and also data collected from off-chains sources
Transactions, logs and traces are extracted from the blocks
Block from the blockchain are retrieved and stored locally
bitsCrunch Platform
ETH
Polygon
SOL
AVAX
more
WAX
BSC
ADA
Flow

Figure 3: High-level data flow

Here are some of the classification of data that will be available with the network mainnet.

- NFT Analytics and Metadata: Get the most comprehensive NFT analytics and metadata across multiple blockchains.
- NFT Wash Trade Analytics: Get in depth wash trading analysis for NFT collections and tokens across multiple blockchains.
- NFT Price Estimation: Get the most accurate AI based NFT price estimation.
- NFT Portfolio: Get an accurate view of your NFT portfolio.

Use Cases

Accessing accurate and up-to-date data is essential for the success of any project, especially in the world of blockchain and NFTs. The bitsCrunch network offers a reliable and consistent source of data that can be used by a variety of projects in different industries.

Centralized / Decentralized NFT DeFi

The bitsCrunch network offers numerous use cases in the world of DeFi, which is a fast-growing ecosystem of decentralized financial applications built on blockchain technology. One of the primary benefits of the bitsCrunch network is that it provides accurate and reliable NFT data to DeFi projects, which can help users make better investment decisions.

By leveraging the data provided by the bitsCrunch network, DeFi projects can access near real-time information about market trends, trading volumes, and other relevant metrics. This information can be used to create advanced trading strategies, predict market movements, and identify potential investment opportunities.

Moreover, having access to accurate data can also help DeFi projects avoid engaging with malicious contracts and take necessary precautions to protect their users' funds. In addition to DeFi projects, the bitsCrunch network can also benefit centralized and decentralized NFT marketplaces. By providing users with all the necessary information, such as the ownership history, authenticity, and market value of NFTs, buyers and sellers can make informed decisions when trading these unique digital assets.

Overall, the bitsCrunch network's data-driven approach can help bridge the information gap that exists in the world of DeFi and NFTs, enabling users to make more informed decisions and promoting the growth of these innovative ecosystems.

Fraud detection and alerting

NFT fraud detection and alerting is a crucial tool in the digital art world. It is a process of identifying fraudulent activities related to non-fungible tokens (NFTs) and notifying relevant parties about the potential risk. NFT fraud can occur in various ways, such as fake NFTs, scams, and phishing attacks. It can also involve misleading or incomplete information in the metadata associated with the NFT.

bitsCrunch network will provide inbuilt fraud detection and alerting. Projects can consume this data and set up alerts, notifications and react accordingly. Projects can also put in place preventive measures to help reduce the risk of NFT fraud. These can include educating users about NFT fraud, implementing strict verification processes, and increasing transparency in NFT marketplaces.

Compliance and AML

Projects, users, financial institutions, and regulatory bodies can all benefit from the wealth of data available on the bitsCrunch network to ensure a secure and compliant NFT ecosystem. This data can be utilized to generate comprehensive Anti-Money Laundering (AML) and compliance reports that help maintain transparency and adherence to regulatory requirements.

Banks and other financial institutions can analyze this data to verify the legitimacy of NFT transactions and wallet activities, ensuring that they have not been involved in any financial fraud or illicit activities. Additionally, government agencies can leverage this data to oversee market compliance, ensuring that participants adhere to established rules and regulations. This level of oversight is crucial for maintaining a fair and transparent NFT market, fostering trust and confidence among market participants.

NFT Analytics Platform

One of the most significant challenges faced by NFT analytics is staying abreast of the rapidly evolving blockchain landscape and the increasing complexity of transactions due to continuous innovation. As the blockchain and NFT industries are still in their nascent stages, this challenge is expected to grow more pronounced over time. To effectively address these hurdles, analytics projects can capitalize on the data available through the bitsCrunch networks.

The bitsCrunch network is continuously enriched through community contributions, ensuring that it remains up-to-date and reflective of the latest developments in the blockchain and NFT space. By leveraging this ever-evolving data source, NFT analytics projects can focus their efforts on delivering valuable insights to their customers while staying current with the fast-paced changes in the industry.

Utilizing the bitsCrunch network's data enables analytics projects to maintain a competitive edge and adapt to the dynamic nature of the blockchain and NFT markets. This approach not only empowers these projects to provide accurate, timely, and relevant insights to their customers but also fosters a collaborative ecosystem that thrives on shared knowledge and continuous learning.

NFT Lending Protocol

NFT Lending Protocols face challenges in staying updated with the ever-changing NFT landscape and accurately evaluating NFTs for loan collateralization. With the rapid growth of the NFT market and the diverse range of assets, it becomes increasingly difficult for the protocols to maintain an up-to-date and comprehensive understanding of NFT values, trends, and potential risks.

To overcome these challenges protocols can leverage the data from the bitsCrunch network. By tapping into this rich data source, the protocol will be able to access real-time, accurate, and comprehensive information about NFTs, their underlying asset value, and market trends

And more

Artists and creators in the NFT space can also benefit from the data provided by the bitsCrunch network. By accessing accurate pricing information and market trends, they can make informed decisions on the value of their creations and optimize their marketing strategies.

Another use case is in the gaming industry. With the growth of blockchain-based gaming and NFTs, game developers can leverage the data from the bitsCrunch network to analyze the market trends, accurately price their assets, and improve user experience. They can get user specific stats and also understand how users engage with other gaming projects.

Finally, investors in the NFT market can use the data from the bitsCrunch network to perform due diligence and make informed investment decisions. By accessing accurate transaction data and metrics, they can identify potential risks and opportunities, and maximize their returns on investment.

Overall, the bitsCrunch network can provide consistent and quality data to a variety of projects in different industries, enabling them to execute their ideas effectively and efficiently.

Decentralized Network

Decentralization via blockchain technology is a revolutionary concept that has transformed the way we think about data storage, transfer, and management. Essentially, blockchain is a distributed ledger system that enables multiple parties to share and store data in a secure and tamper-proof manner without the need for intermediaries. The importance of blockchain lies in its ability to provide a transparent and trustless system that is resistant to fraud, corruption, and hacking. By decentralizing data management, blockchain can eliminate the need for centralized control and reduce the risk of data breaches and cyberattacks.

The complexity involved in building a blockchain network is significant, requiring a deep understanding of cryptography, distributed systems, and programming languages. Developers must design the system to ensure that the data is replicated across multiple nodes, and the consensus protocol is followed to maintain the integrity of the network. Additionally, the system must be scalable, secure, and fault-tolerant, with proper governance structures to ensure that the network operates efficiently and effectively.

This part of the complexity has already been solved by the existing layer 1 and layer 2 solutions, so we are not going to try to reinvent the wheel by creating a new blockchain. Instead, we will leverage one of the existing proven EVM based layer 2 chains. Our decentralized network will be more focused on data management and data manipulation using AI/ML models, heuristics, and other tools. The result will be highly enriched data that is easy to understand and ready to use.

The journey to create a decentralized bitsCrunch network involves several stages, including planning, design, development, testing, and deployment. The development process involves building and testing the network, creating smart contracts, and deploying them on the network. In this section, you will find detailed information about the components involved in our decentralized network, including a high-level decentralization roadmap in the section titled "*Development Strategy*".

Layers of decentralization

This layered architecture focuses on the decentralization and on the data flow and data management, not on the application architecture. Each layer represents the lifecycle of the data from how it's getting acquired to the final layer exposing the data for consumption. In the following sections we will go into the details about each section.

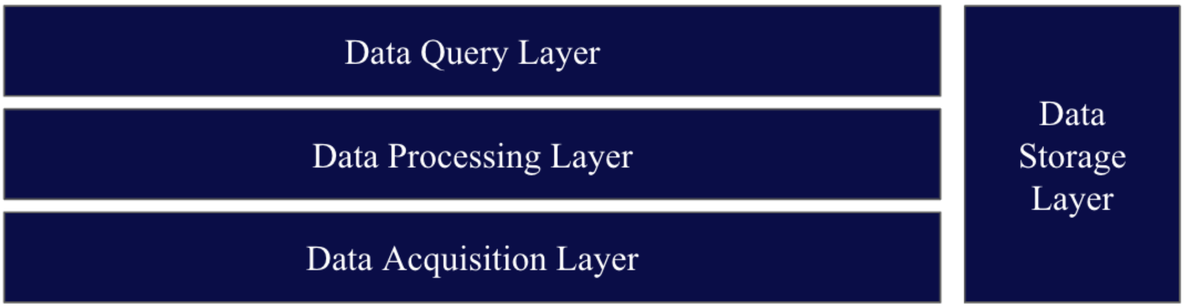


Figure 4: Functional layer of the decentralization network

Data Query Layer

The data query layer is a key component of the network that enables users to access the information they need from the network. This layer provides a way for consumers to securely and efficiently query the network for data that has been enriched by other participants in the network.

This Layer is designed to allow participants to transact and interact without the need for a central authority or intermediary. This means that users should have the freedom to access the network and use its features without any restrictions or requirements. A permissionless system ensures that anyone can join and use the network without needing to seek approval from anyone. It is also made frictionless and easy to use and interact with. This includes a seamless onboarding process, easy navigation, and simple transaction processing. Users should be able to use the network without encountering unnecessary barriers or complications.

High scalability and throughput are essential for ensuring that the network can handle a large volume of queries without slowing down or becoming overwhelmed. A high-throughput system ensures that data can be processed quickly and efficiently, allowing users to get the information they need in a timely manner. State-of-the-art security measures are in place ensuring that the network is safe and secure for users.

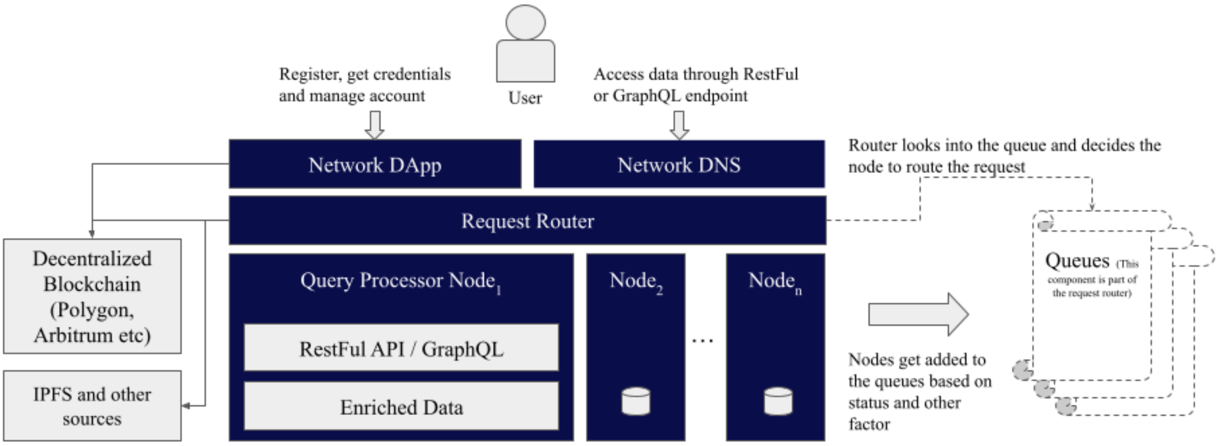

Register, get credentials and manage account
User
Access data through RestFul or GraphQL endpoint
Network DApp
Network DNS
Router looks into the queue and decides the node to route the request
Request Router
Decentralized Blockchain (Polygon, Arbitrum etc)
IPFS and other sources
Query Processor Node$_1$
RestFul API / GraphQL
Enriched Data
Node$_2$
...
Node$_n$
Nodes get added to the queues based on status and other factor
Queues (This component is part of the request router)

Figure 5: Query processing flow

The distributed network architecture enables each node to have access to the full enriched dataset, allowing them to operate autonomously and handle all queries independently. This approach not only ensures high availability and fault tolerance but also promotes scalability and parallelism by distributing the workload across multiple nodes. Furthermore, the use of advanced algorithms and data structures enhances the efficiency and reliability of the network's query processing and data synchronization. As a result, the distributed network can handle a large volume of queries and adapt to changing demands without compromising performance or data integrity.

Network DApp

Users will have the ability to connect their crypto wallet, such as Metamask, to the Dapp network. Once connected, users can register to create secure credentials that will grant them access to the API. After registration, users will receive a secure downloadable access key that will be protected through encryption using the user's wallet.

To manage user accounts and hold user-deposited funds, a billing smart contract will be implemented. Periodically, a portion of the user's funds will be deducted based on query usage from the billing contract to the network treasury. Users will have the ability to view logs of their usage and raise a dispute in the event of a conflict.

This DApp serves as a platform for operators and delegators to interact with the network. Operators have the ability to create an operator account by connecting their crypto wallet and depositing a minimum amount of network utility tokens. This ensures their participation in the network, and as part of the onboarding process, they will receive an access key that is similar to the network users' access key. This key is crucial in securely configuring the node to the network.

Moreover, this DApp provides a comprehensive suite of operator analytics, enabling operators to monitor their network performance and evaluate their contributions. These analytics are available at both an aggregate and individual operator level, offering the ability to drill down into specific metrics and identify areas for improvement. By leveraging these insights, operators can optimize their performance and increase their earning potential within the network.

Delegators have the option to browse through a comprehensive list of operators, and they have the ability to evaluate their earning and service records before making a selection. This enables them to choose the operator that is best suited to their needs. After selecting an operator, delegators can stake the network utility token and become eligible to receive a portion of the earnings generated by the operator.

To attract delegators, operators share their fee earnings and network rewards. This staking process is essential for securing the network. While delegators have the flexibility to withdraw their stake at any time, they may receive only partial or no rewards if they do so before the network settlement event. This event occurs once every epoch, which is typically 30 days or on a fixed day of the month.

This DApp will serve as the primary interface for users and operators to interact with the network's smart contracts. All of the key interactions that the DApp facilitates will be encoded directly into the network's contracts. This approach ensures that the interface is not tethered to any central entity through a hosted UI. By relying on the network's contracts to execute key interactions, the DApp can function autonomously and without any centralized control. This allows for greater transparency and decentralization within the network. Users and operators can trust that their interactions are being executed directly on the network, rather than being funneled through a third-party intermediary.

Network DNS

The domain name serves as the foundation for accessing various query endpoints and the Network DApp. By utilizing this domain name, consumers can easily access the necessary APIs and documentation once they have obtained the proper credentials. These credentials allow them to navigate through the specifications to locate the specific endpoints they need for interaction or integration.

As the Network DApp continues to grow and expand, the domain name will evolve into a decentralized DNS system. With a decentralized DNS, consumers will be able to interact with the Network DApp in a more efficient and secure manner, as it eliminates the need for a central authority to manage and govern the domain name.

Overall, the domain name serves as a critical component in facilitating interaction and integration with the Network DApp. As the system continues to evolve and expand, the domain name will become an integral part of a decentralized DNS system, providing greater autonomy and security for all users.

Request Router

This component is highly scalable, lightweight and boasts an impressive ability to handle more than 100,000 requests per second. Every query to the network is processed by the request router. As security is of paramount importance, this component takes on the responsibility of verifying the requester's credentials before allowing the request to pass through to the node. Only if the credentials are found to be valid will the request be allowed to proceed.

After verifying the credentials, the router consults the routing queue, which helps identify the next node in the sequence to which the request should be forwarded. Further information on this process can be found in the "Routing algorithm" section. As each request is received and processed, the system meticulously records the relevant details, including the requestor's identity, the node number, and the receipt of the request, all of which are stored in the logs.

Routing algorithm

All nodes that have registered with the network are recognized by the request router. The router is responsible for conducting periodic ping tests to each node in order to ascertain their status and maintain a comprehensive record of it. Along with the uptime record, the router also maintains the performance statistics of each node. The router is also responsible for managing multiple queues, it uses these queues to select the node to route the incoming queries. This enables all nodes in the network to have an equal opportunity to participate in the query processing.

Queue Name	Description
General	All live nodes in the network will be placed in this queue.
Best Performer	Nodes with the best performance. Performance parameters like Throughput, Availability etc
Most Accurate	Nodes with the least errors
Staking cap	Nodes that reach the staking cap will be listed in this queue.
Potentially more queues	

Table 1: Request routing queues

Nodes that are included in all queues will have the advantage of receiving more queries to the server than other nodes only in one or few queues. Below is a simulation of how the router works under a 4 queue example

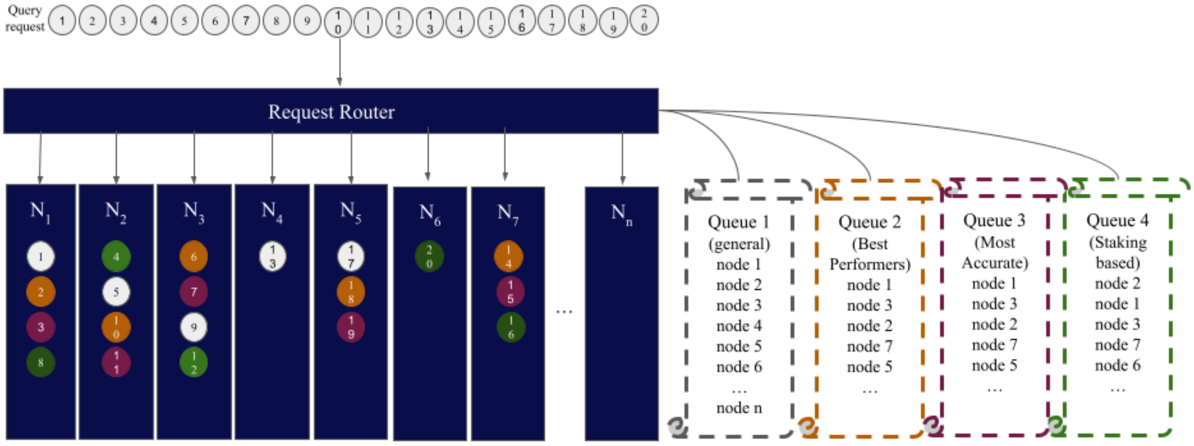

Query request
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20
Request Router
N1
1 2 3 8
N2
4 5 10 11
N3
6 7 9 12
N4
13
N5
17 18 19
N6
20
N7
14 15 16
...
Nn
Queue 1 (general) node 1 node 2 node 3 node 4 node 5 node 6 ... node n
Queue 2 (Best Performers) node 1 node 3 node 2 node 7 node 5 ...
Queue 3 (Most Accurate) node 1 node 3 node 2 node 7 node 5 ...
Queue 4 (Staking based) node 2 node 1 node 3 node 7 node 6 ...

Figure 6: Example of a queuing with single router

Query Processor Node

This is one of the three types of nodes that a network operator can perform and has the specific role of serving user queries. The node operates by receiving user queries based on the queue system, the request router forwards the query to it. Furthermore, a record of each user query is maintained in a decentralized storage system, which is periodically aggregated, and the hash of the file is recorded in the blockchain. This file serves as an essential part of the process, particularly during disputes or validation procedures.

Data Processing Layer

The middle layer of a network plays a critical role in the process of data enrichment and preparation for user consumption. This layer takes the block data produced by the layer below and applies various complex algorithms and processes to it. The purpose of these steps is to enrich the data, meaning to extract more useful information from it and transform it into a more meaningful representation for the user.

In particular, this middle layer is responsible for executing all of the AI/ML model and metric calculation logic. This includes running various machine learning algorithms, performing statistical analyses, and applying other computational techniques to extract insights from the data. The goal of these calculations is to create a more accurate and robust representation of the data, which can then be used by the user to make more informed decisions. Overall, the middle layer is a central component of the network, and its ability to process and enrich data is critical to the success of the network as a whole.

This layer is responsible for integrating and managing AI/ML models and related algorithms plays a crucial role in the system, necessitating stringent security measures. To ensure the highest level of protection, we employ advanced encryption techniques, such as elliptic curve cryptography, to secure access keys and restrict system entry. Additionally, participants are required to lock the network's utility tokens as a safeguard.

In the event of any misconduct or malicious activity, a set of predefined slashing rules will be enforced, providing a robust mechanism for penalizing bad actors and maintaining overall system integrity. This combination of encryption, token locking, and slashing rules establishes a strong security foundation, protecting the layer dedicated to AI/ML models and algorithms from potential threats.

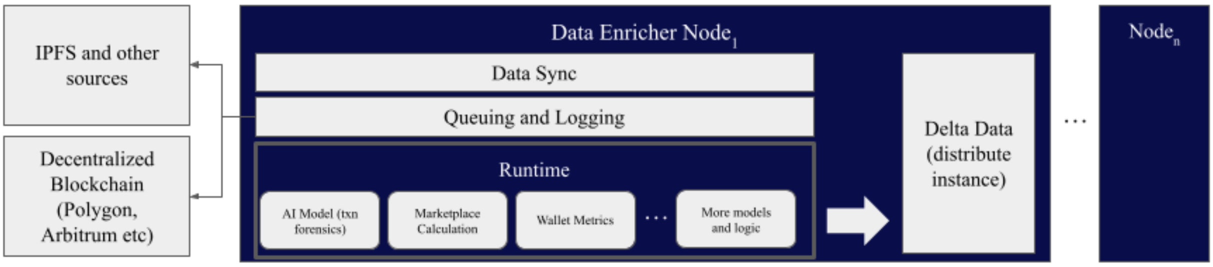


Figure 7: Data processor components

Data Sync Service

This critical component plays a crucial role in ensuring that the data processing layer and data query layer are seamlessly connected. It not only synchronizes data between the two layers but also ensures that the latest information is available to all the query processors registered with the network. This synchronization mechanism is essential to maintain the accuracy and reliability of the data.

Moreover, this component's ability to keep the query processors up-to-date with the latest data helps to enhance the performance and efficiency of the entire system. This ensures that the network is operating at peak performance and can handle large volumes of data efficiently.

Queuing and Logging

Queuing refers to the process of managing and controlling the flow of work items or tasks in a network. Queuing is essential in many applications and systems where multiple tasks need to be executed, and the order of execution is important. Queuing systems typically use a first-in-first-out (FIFO) approach, where the first task that arrives is the first one to be executed, which is what is used in the network. The component contains a peer-to-peer and responsible for queuing the Data Enricher nodes in the network is also responsible for periodically conducting a ping test to check the health of each node. Multiple queues are formed using parameters such as uptime, performance, capacity allocation, and staking ratio. These parameters are based on the data stored in the decentralized storage and are calculated on a daily basis to update the queuing process.

Logging refers to the process of recording events or data into a log file or database for later analysis or troubleshooting. Logging is critical for monitoring and diagnosing the behavior of the network. Logging allows the network participants to understand what is happening inside the system, track down errors, identify performance issues and use this for reward computation or to apply penalties to the operator. Effective logging requires careful consideration of what data to log, how to log it efficiently, and how to analyze the logs to gain insights into the network’s behavior. Additionally, this component is used to log the work done by each node to decentralized storage. The raw file and aggregated data file’s hash are periodically updated to the blockchain. This allows the participants to review the logs when conflicts arise.

Runtime

The runtime component of the network is the central hub where all the machine learning algorithms and computational techniques are executed. This component plays a critical role in the success of the AI system, as it directly affects the performance, accuracy, and scalability of the system. Machine learning algorithms, which are the backbone of any AI system, require significant computational resources to execute efficiently. These algorithms typically involve large amounts of data and complex mathematical calculations that can be computationally intensive. Therefore, the runtime component must be capable of scaling up and down as needed to meet the computational demands of the algorithms.

In addition to machine learning algorithms, the runtime component also performs statistical analyses and applies heuristics to the data. Statistical analyses help to identify patterns and trends in the data, while heuristics are rules or guidelines that are used to guide the decision-making process. These techniques are essential for extracting meaningful insights from the data and making accurate decisions and predictions.

The runtime component may also incorporate other computational techniques such as natural language processing (NLP), computer vision, and reinforcement learning. NLP enables the AI system to understand and interpret human language, while computer vision allows the system to interpret visual data such as images and videos. Reinforcement learning is a type of machine learning that enables the system to learn by interacting with its environment and receiving rewards or punishments based on its actions.

Data Acquisition Layer

This is a logical layer in the network that plays a crucial role in maintaining the integrity of the network. This layer is responsible for retrieving block data from various blockchain and storing it in the node's distributed database. To ensure efficiency and accuracy, the queuing component is used to make assertive decisions on which source to pick data from. This allows the node to retrieve and store block data quickly and accurately.

To support different blockchain types, many chain adopters will be available in the network. These adopters will enable the node to connect and adapt to various blockchain types, making it possible to retrieve and store data from different blockchain networks. Each block that is retrieved and stored in the database will earn rewards for the node operators. These rewards will be in the form of a network utility token and a share of the revenue earned by the network.

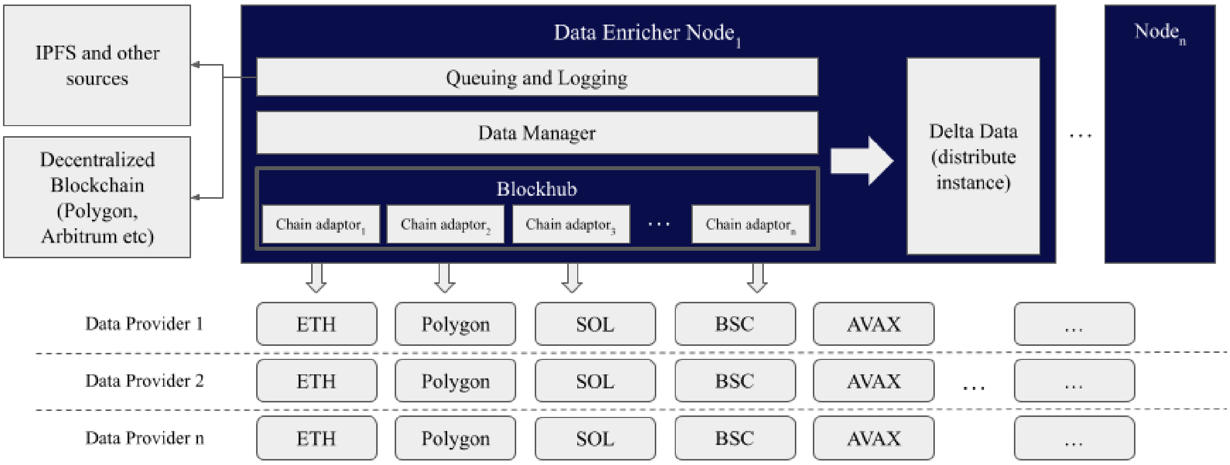


Figure 8: Data acquisition flow

Queuing component is used to queue the nodes and the sources, as mentioned above this factors in many things from availability, performance, capacity allocation, and staking ratio.

Blockhub

This component is for facilitating the retrieval of data from different blockchain nodes via their RPC (Remote Procedure Call) endpoint or other means. One of the key aspects of this component is the chain-specific adaptor that is designed specifically to work with a particular blockchain network. Each blockchain network has its own unique way of managing and storing transactions, and these adaptors are essential for ensuring that transactions are properly retrieved and recorded.

In addition to the chain-specific adapter, this component also includes a mechanism for registering blockchain source endpoints. Once the endpoints are registered, they are shared across all nodes on the network. This helps to ensure that all nodes have access to the same information, which is crucial for maintaining consistency across the network.

This component uses a queue to ensure that the correct provider is used for the next block retrieval. The queue keeps track of which provider should be used next, based on a variety of factors such as network latency and other performance metrics. The record of the provider used is logged in a decentralized storage and the hash value of the log file and the aggregated data files are recorded periodically in the blockchain. This is done to ensure that participants can review the logs if conflicts arise on payouts. By recording this information in the blockchain, it becomes a permanent part of the network's history, and cannot be altered or deleted.

Data Manager

This component is responsible for several critical data processing functions in the network. Let's look at each of these functions in more detail:

1. Parsing Block Data: This component parses the block data retrieved by the blockhub and extracts transactions, logs, traces, and other information. This involves analyzing the raw block data to identify and extract relevant information, which can then be used for various purposes such as machine learning, business intelligence, or decision-making.
2. Retrieving Off-Chain Data: In addition to extracting data from blocks, this component can also retrieve off-chain data from IPFS or other storage when needed. This means that the system can access and use data that is not stored on the blockchain, allowing for more comprehensive data gathering.
3. Onboarding Community Data: Network operators and communities can onboard data like social media handles or other information that are off-chain but on the web. This community data can then be integrated into the network and used for analysis, adding additional insights and perspectives.

This becomes the base data for AI/ML models, heuristics, and metrics calculation. This means that the accuracy and quality of the data are critical for ensuring the effectiveness of these actions. Community developers can contribute to additional data cleansing or data transformation logic via this component. This means that the network can continually improve and evolve based on the contributions of its community members. Overall, the data preprocessing and preparation functions performed by this component are essential for enabling accurate data analysis, effective decision-making, and the development of sophisticated AI/ML models in a network.

Data Storage Layer

This pivotal component intersects and overlaps with the three previously mentioned layers, seamlessly integrating their functions. It is the layer for storing all data coming from the data acquisition and data processing layers. The data acquisition and data processing layers interact with the data storage layer to perform CRUD operations. As its name implies, the data query layer focuses predominantly on executing read operations. In order to guarantee decentralization, a distributed database system will be utilized within this essential cross-layer component.

Benefits of Decentralization

Facilitate enhanced transparency in data aggregation and dissemination processes

Eliminate information bias and censorship for unbiased data access

Implement a trustless and permissionless framework to access the data

Encourage extensive community collaboration to support continuous growth and innovation

Figure 9: Benefits of decentralizing the bitsCrunch network

Network Development Strategy

Development of the network will be a multiphase multi year endeavor. This section only provides a high level overview on the network development, for more detailed feature level roadmap refer to the bitsCrunch Litepaper and or to the bitsCrunch network website.

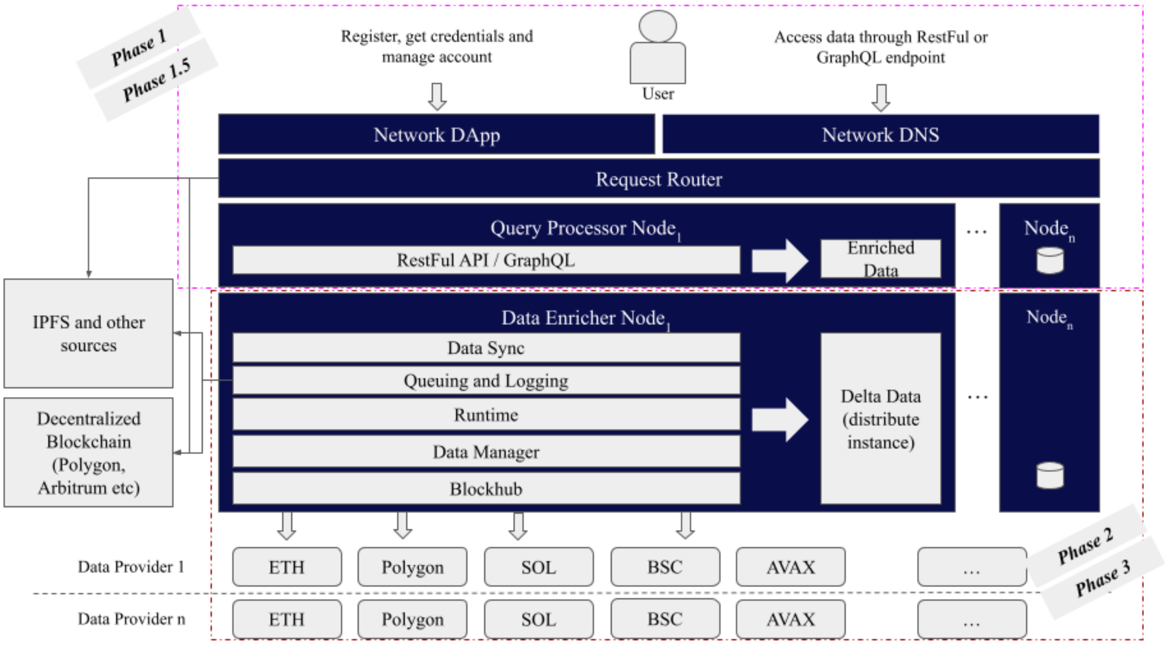
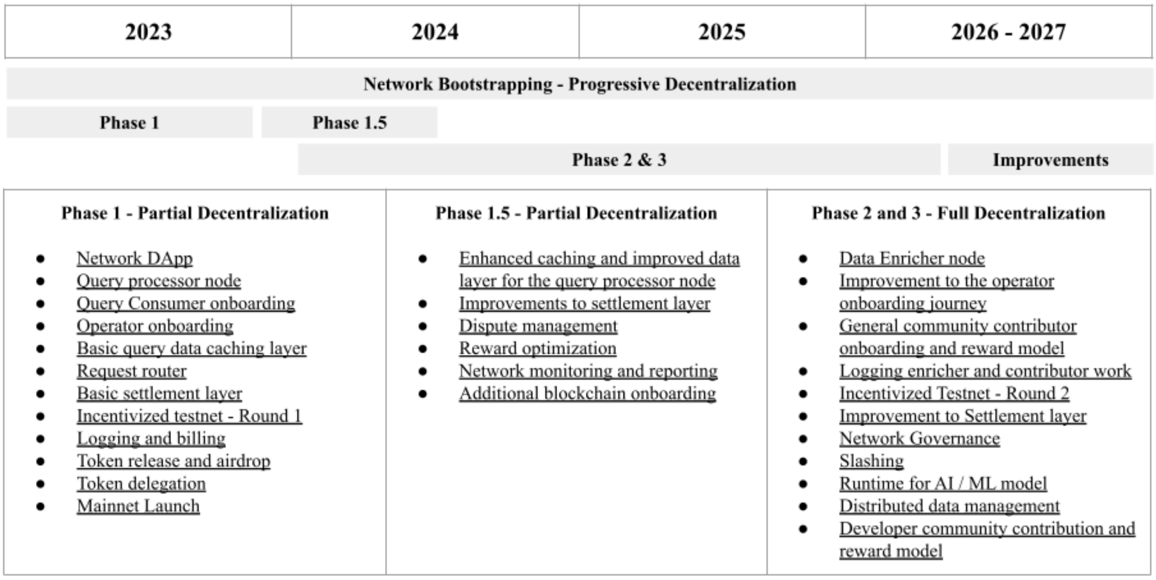


Figure 10: Functional overview with development phase mapping



2023	2024	2025	2026 - 2027

Network Bootstrapping - Progressive Decentralization

Phase 1

Phase 1.5

Phase 2 & 3

Improvements

Phase 1 - Partial Decentralization	Phase 1.5 - Partial Decentralization	Phase 2 and 3 - Full Decentralization
• Network DApp • Query processor node • Query Consumer onboarding • Operator onboarding • Basic query data caching layer • Request router • Basic settlement layer • Incentivized testnet - Round 1 • Logging and billing • Token release and airdrop • Token delegation • Mainnet Launch	• Enhanced caching and improved data layer for the query processor node • Improvements to settlement layer • Dispute management • Reward optimization • Network monitoring and reporting • Additional blockchain onboarding	• Data Enricher node • Improvement to the operator onboarding journey • General community contributor onboarding and reward model • Logging enricher and contributor work • Incentivized Testnet - Round 2 • Improvement to Settlement layer • Network Governance • Slashing • Runtime for AI / ML model • Distributed data management • Developer community contribution and reward model

Figure 11: High-level timeline and network roadmap

The development of the network is currently divided into three phases. The first phase, which involves the creation of the Data Query layer and Query Processor node, is scheduled to be completed by Q2-2023 for the testnet, and the mainnet is expected to be achieved around Q3-2023. During this initial phase, the query processor node will utilize a common shared database. In Phase 1.5, which is a subsequent step to Phase 1, each node in the network will be equipped with its own database, resulting in a decentralized network with no central point of failure. This is an important feature of the network as it increases the security and resilience of the overall system.

The second and third phases of development will focus on the creation of the Data Enricher and Data Harvester layers respectively. More details about these phases will be made available as the project progresses. Overall, the development of the network is expected to take three years. Once completed, the network will provide a secure and decentralized platform for querying and processing data, enabling a wide range of applications and use cases.

Security

The bitsCrunch Network's smart contract security is designed to ensure safe, secure, and trustworthy interactions between all parties involved. Here's a brief overview:

- Contract Auditing: All smart contracts used in the Network undergo thorough auditing by independent third-party security firms. These audits aim to find and fix any potential vulnerabilities or bugs in the contract code.
- Secure Development Practices: The development of the smart contracts follows secure coding practices. This includes thorough testing of functionality, edge cases, and potential attack vectors, before deployment on the mainnet.

- Staking and Slashing Mechanisms: To protect the network from malicious activities, the bitsCrunch Network implements a staking and slashing mechanism. Node operators must stake a certain amount of network utility tokens, which are subject to slashing (reduction) if the operator misbehaves or fails to fulfill their obligations. This creates a financial disincentive for dishonest behavior.
- Access Control: Smart contracts implement various levels of access control, which restrict who can execute certain functions within the contract. This helps to prevent unauthorized actions on the network.
- Data Privacy: While the blockchain inherently makes certain transaction data public, the bitsCrunch Network ensures that sensitive data remains private through the use of secure data handling techniques.
- Asset Security: Users employ their personal, non-custodial wallets to deposit assets, such as stablecoins or BCUT tokens, into the network contract. These assets are held in a non-custodial manner, granting exclusive access and management privileges to their respective users.

Token Economics

Token economies for the bitsCrunch utility token refers to the design and management of the BCUT token. In this case, the token's value is derived from its utility rather than its speculative or investment value. The goal is to create a sustainable and effective ecosystem that incentivizes the use and adoption of the token for its intended purpose. This includes determining the distribution and circulation of the token, setting the supply and demand dynamics, and designing governance mechanisms that align the incentives of users and other stakeholders with the success of the network. Key considerations for token economics are the utility token functionality, user adoption, network effects, and token governance. Successful token economics helps to drive adoption and usage of the network, creating a positive feedback loop that further enhances the value of the token.

Total token supply will be 1 billion, the detailed breakdown of the allocation to different token sale rounds and to other areas can be found in the picture below. Token will become inflationary from year 6 to keep incentivizing the network participants.

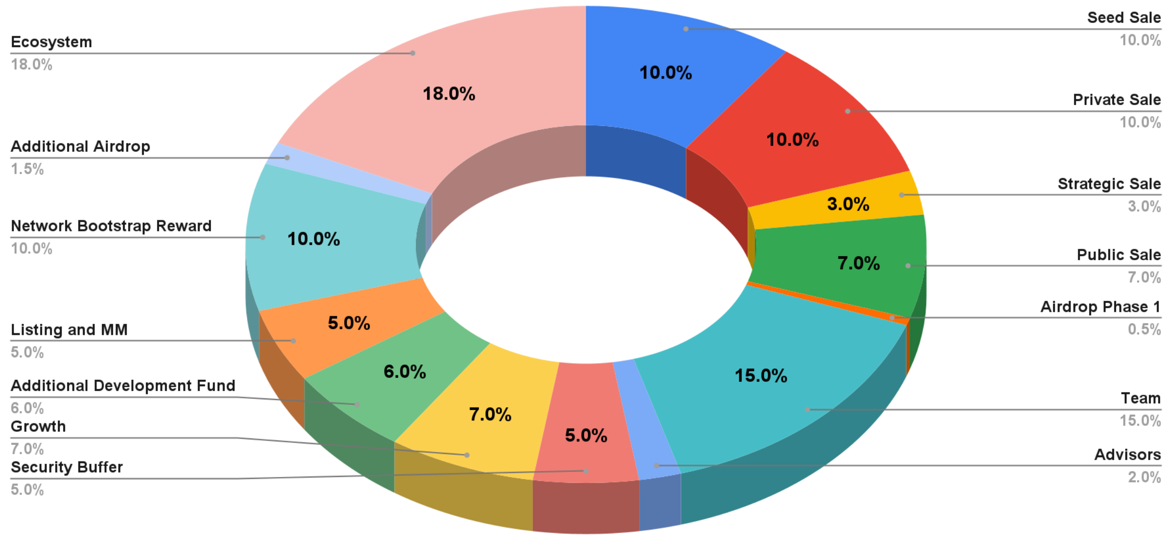


Figure 12: Token distribution chart

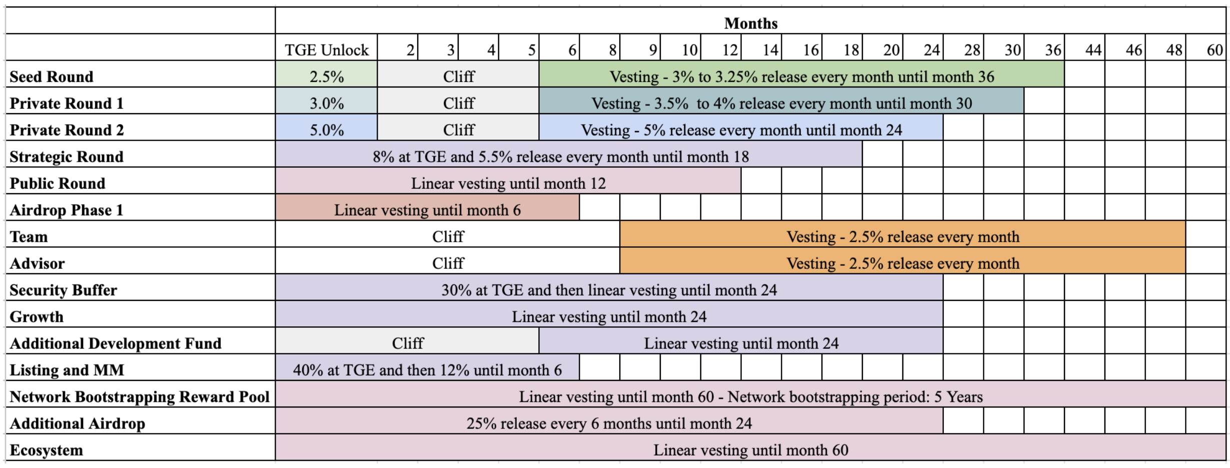
Here is a table explaining the distribution of the tokens as shown above

Total Supply	**1,000,000,000**	**Comments**
Seed Round Token Sale	100,000,000	Initial seed sale that took place in mid 2021
Private Token Sale	100,000,000	This sale was completed by the beginning of 2022
Strategic Token Sale	30,000,000	Extended strategic sale due to demand
Public Token Sale	70,000,000	Planned
Team Allocation	150,000,000	Tokens reserved for the team members of the project
Advisor Allocation	20,000,000	Tokens reserved for the advisors of the project
Airdrop 1	5,000,000	Tokens reserved to reward the phase 1 of the testnet
Security Buffer	50,000,000	Tokens reserved to reward bug discoveries or to cover the loss in case of a security incident
Growth	70,000,000	This allocation would go towards marketing, partnerships, community building and user acquisition
Additional Development Fund	60,000,000	These tokens are set aside to finance future platform development, hire additional team members, and make technical enhancements
Listing and MM	50,000,000	Tokens reserved for CEX listing, DEX listing, and for Market Making

Ecosystem	180,000,000	Tokens allocated towards fostering and growing the bitsCrunch network ecosystem through grants, rewards and marketing initiatives
Additional Airdrop Pool	15,000,000	Tokens reserved for future testnet phases
Network Bootstrapping Reward Pool	100,000,000	Token allocated to reward operators and delegators etc during the network bootstrapping

Table 2: Token supply classification

Token vesting is strategically designed to ensure that there is a controlled release of tokens over a specified period of time, which prevents a sudden influx of tokens into the market. This approach is beneficial in balancing the demand and supply of tokens, as it ensures that there is a steady flow of tokens over a prolonged period, rather than a large release in a short time frame. By doing so, token vesting promotes stability in the market and encourages a gradual increase in demand for the tokens as adoption grows.



	Months																					
	TGE Unlock	2	3	4	5	6	8	9	10	12	14	16	18	20	24	28	30	36	44	46	48	60
Seed Round	2.5%	Cliff				Vesting - 3% to 3.25% release every month until month 36																
Private Round 1	3.0%	Cliff				Vesting - 3.5% to 4% release every month until month 30																
Private Round 2	5.0%	Cliff				Vesting - 5% release every month until month 24																
Strategic Round	8% at TGE and 5.5% release every month until month 18																					
Public Round	Linear vesting until month 12																					
Airdrop Phase 1	Linear vesting until month 6																					
Team	Cliff							Vesting - 2.5% release every month														
Advisor	Cliff							Vesting - 2.5% release every month														
Security Buffer	30% at TGE and then linear vesting until month 24																					
Growth	Linear vesting until month 24																					
Additional Development Fund	Cliff					Linear vesting until month 24																
Listing and MM	40% at TGE and then 12% until month 6																					
Network Bootstrapping Reward Pool	Linear vesting until month 60 - Network bootstrapping period: 5 Years																					
Additional Airdrop	25% release every 6 months until month 24																					
Ecosystem	Linear vesting until month 60																					

Figure 13: Token vesting and release schedule

Percentages mentioned above are all specific to the allocation within that category and not the percentage of the overall supply.

Below is a graph showing token circulation over the course of time. All tokens will be unlocked fully by 49 months from TGE.

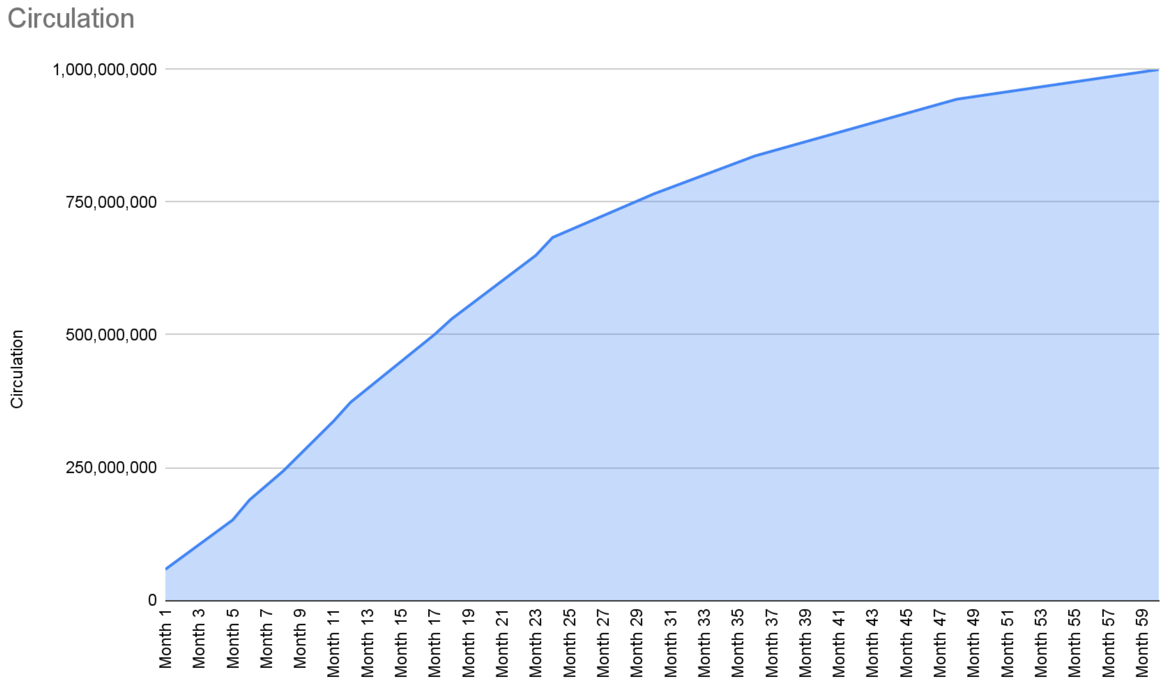


Figure 14: Token circulation

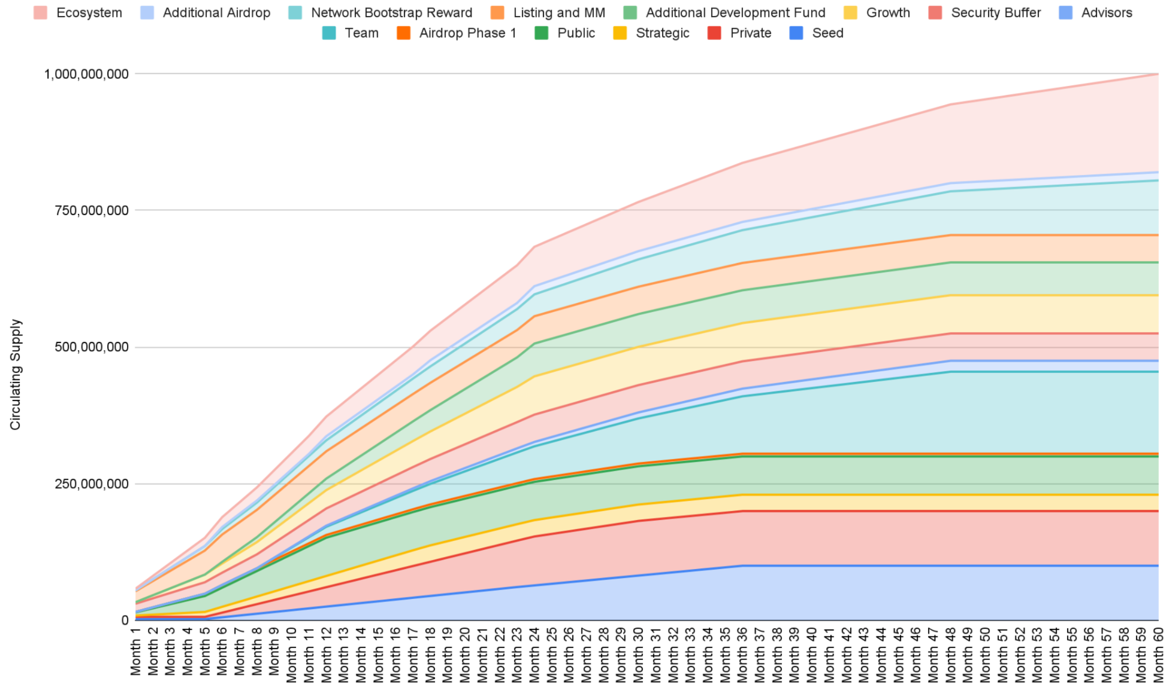
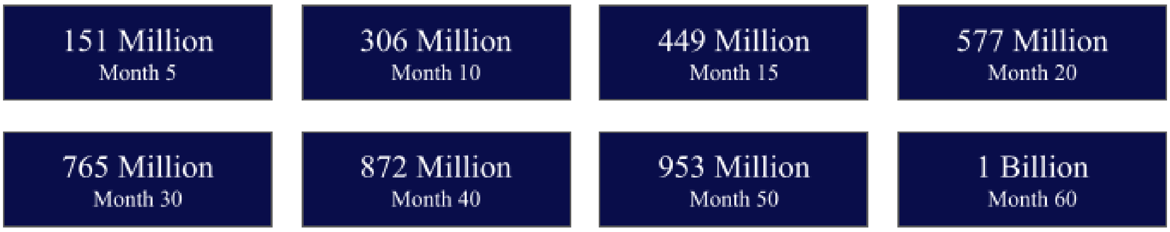


Figure 15: Token emission by category

Even though all 1 billion tokens unlock by month 60 it is highly unlikely that all tokens end up in the market.



151 Million Month 5	306 Million Month 10	449 Million Month 15	577 Million Month 20
765 Million Month 30	872 Million Month 40	953 Million Month 50	1 Billion Month 60

Figure 16: Token emission milestones

Disclaimer

The tokenomics described herein reflect current intentions and are subject to change at the discretion of the project team. Token holdings involve a high degree of risk, including the potential loss of all amounts invested. Past performance, if any, is not indicative of future results, and there is no guarantee that any future version of the token will achieve comparable results or that the token will yield any return on investment.

Token Utility

Purpose

The bitsCrunch utility token (BCUT) is a digital token native to the network, providing access to enriched NFT data within the bitsCrunch ecosystem. Its primary function is to facilitate smooth operations within the network, and it is intended solely for use as a utility token. The secure functioning of the bitsCrunch ecosystem relies on a combination of cryptographic techniques and economic incentives to drive adoption and ensure network security. Following are some of the key functions and purpose of the token

- **Incentive Alignment**: The digital asset acts as a motivational tool, fostering collaboration and commitment among Operators, Delegators, Indicators, and Contributors.
- **Governance**: The digital asset enable decentralized governance, where token holders can vote on proposals and changes to the network's protocol
- **Network Security**: Through mechanisms like staking, our digital asset can add layers of security, making malicious activities costly and thereby protecting the network's integrity.
- **Independence**: Having a digital asset ensures the network's autonomy and reduces reliance on external entities or tokens. It aligns the token's value and functionality closely with our network's objectives and performance.
- **Economic Design**: The digital asset allows us to tailor the economic model to the unique needs and values of our network, controlling aspects like issuance, distribution, inflation, or deflation.

- **Discounting**: Data consumers can stake the token to get a discount on the query pricing.

Bootstrapping the Network

All of the initial network rewards are provided from the staking allocation of the tokenomics, which can be referred to in the token economics section for more information. This allocation is also utilized to reward node operators, LP mining, among other things. The staking allocation will be utilized to cover network rewards for the bootstrapping duration, after which rewards will be primarily based on the revenue generated by the network and the rates will be determined by the network smart contract.

The following chart illustrates the planned token emission for bootstrapping the network over a period of up to 5 years. This emission schedule has been designed to ensure a steady and sustainable release of tokens into circulation, with the ultimate goal of supporting the growth and development of the network over the long term.

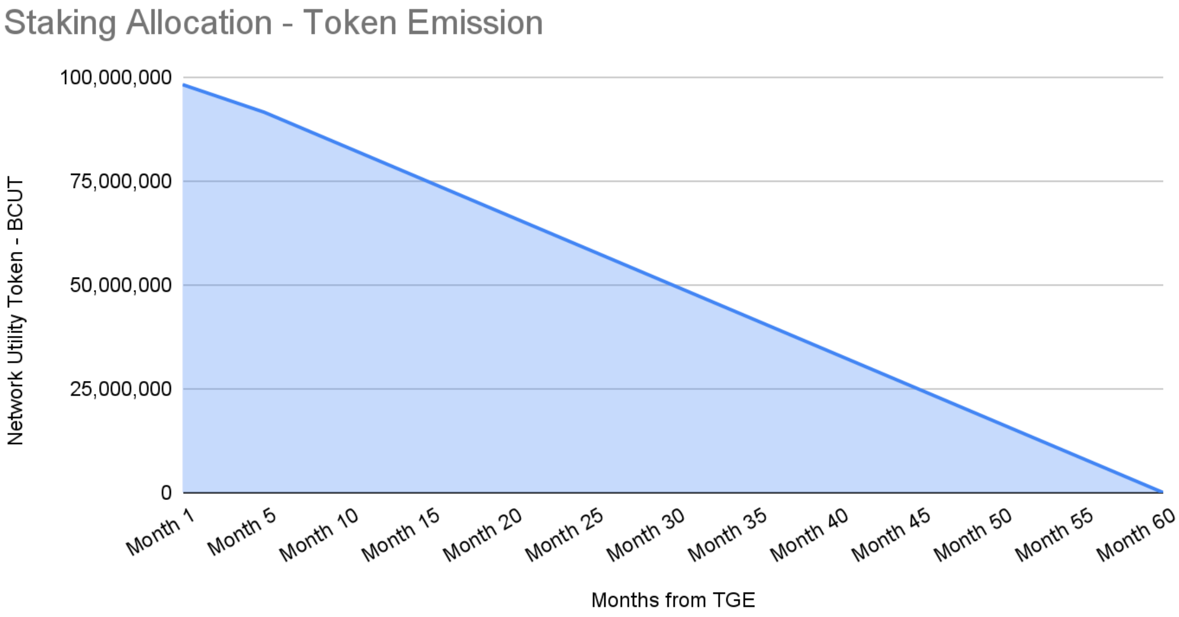


Figure 17: Staking allocation emission assuming the bootstrapping of network is for 5 years

Network Consensus

The bitsCrunch network leverages a Delegated Proof-of-Stake (dPoS) consensus mechanism. Within this system, delegators stake their digital assets with chosen operators, who are then tasked with various responsibilities within the network. The operators are rewarded based on the work they perform, aligning their interests with the overall integrity and functionality of the network.

Network Roles

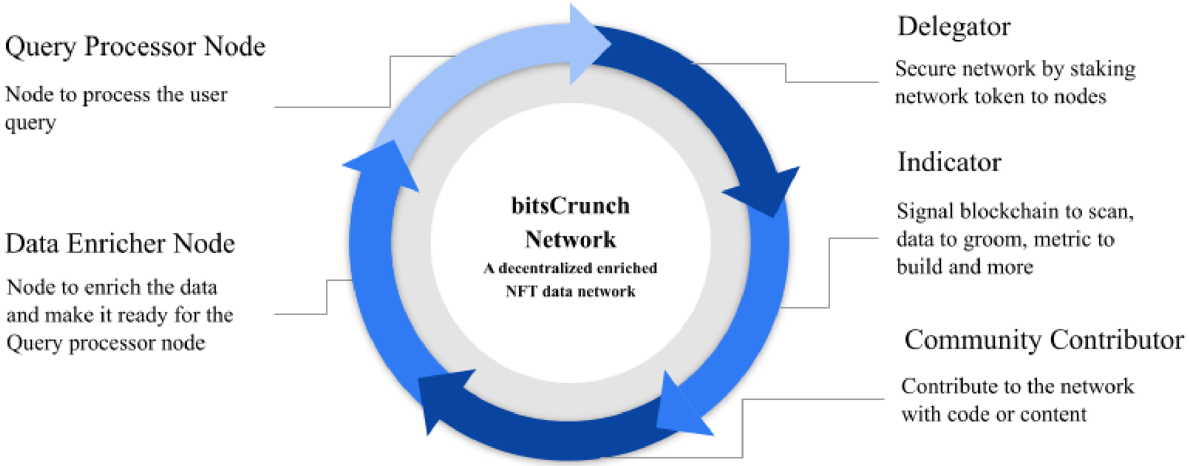

Query Processor Node
Node to process the user query
Data Enricher Node
Node to enrich the data and make it ready for the Query processor node
bitsCrunch Network
A decentralized enriched NFT data network
Delegator
Secure network by staking network token to nodes
Indicator
Signal blockchain to scan, data to groom, metric to build and more
Community Contributor
Contribute to the network with code or content

Figure 18: Different roles envisioned for the operation and self-sustainability of the network

The diagram above presents an overview of the various roles envisioned within the network. Each role is detailed and elaborated upon in the subsequent sections, providing a comprehensive understanding of their functions and responsibilities within the network ecosystem.

Role	**Token Utility**
Node Operator	Stake the token to participate in the network and earn fee and rewards.
Delegator	Delegate stake the tokens to secure the network and influence sufficiently decentralized
Indicator	Stake token to become an indicator of the network to help shape the content direction.
Community Contributor	Contribute to the network with code and content to earn tokens as rewards.
User/Customer/Consumer	Stake token to get discount on the query fee

Table 3: Network Roles and Token utility

Node Operator Roles

In order to ensure smooth operations of a blockchain network, there are typically one or more roles that enable its functioning. These roles are well-defined and allow operators to choose the one that best suits their appetite and experience. Similarly, the bitsCrunch network will also offer multiple roles for operators to choose from. Operators may choose to run a full node with all roles or a partial node that satisfies only one role. It is important to note that bitsCrunch is not a blockchain but rather a decentralized data network that leverages decentralized blockchain technology to maintain proof of use and contribution.

Network operators play a critical role in the success of bitsCrunch's decentralization effort. Each role in the network will share the fee earned by the network and will also be rewarded with network tokens. In the following sections, we will provide more details on the various roles that operators can choose from in the bitsCrunch network.

Query Processor Node

This node in the network is responsible for making enriched data available to consumers through a Restful API. Consumers interact solely with this node, which ensures secure access to data through a cryptographic and secure model. The node comprises components of the decentralization layer, including data query and data storage. This role within the network carries weightage, as described below, which means that node operators with this role will receive fees and rewards based on this weightage. The distribution is calculated using the Cobb-Douglas Production function, refer to "*Network Reward Model*" for more details.

Role	Weightage
Query Processor Node	30% to 50%

Table 4: Query processor node weightage

The Query Processor node is designed to be less complex than the Data Enricher node, which makes it an attractive role for more node operators to participate in. However, despite its relative simplicity, the Query Processor node will still need to be robust and resilient in order to handle high demand and ensure consistent performance.

As a critical component of the network, the Query Processor node plays a critical role in processing queries and facilitating the transfer of data across the network. This requires a high level of reliability and performance, especially as the network grows and more demands are placed on the system.

Therefore, the Query Processor node must be designed with scalability and resiliency in mind, using proven techniques such as load balancing, redundancy, and fault tolerance to ensure that it can handle even the most demanding workloads. By doing so, the network can maintain a high level of performance and reliability, while also attracting more node operators to participate in this important role.

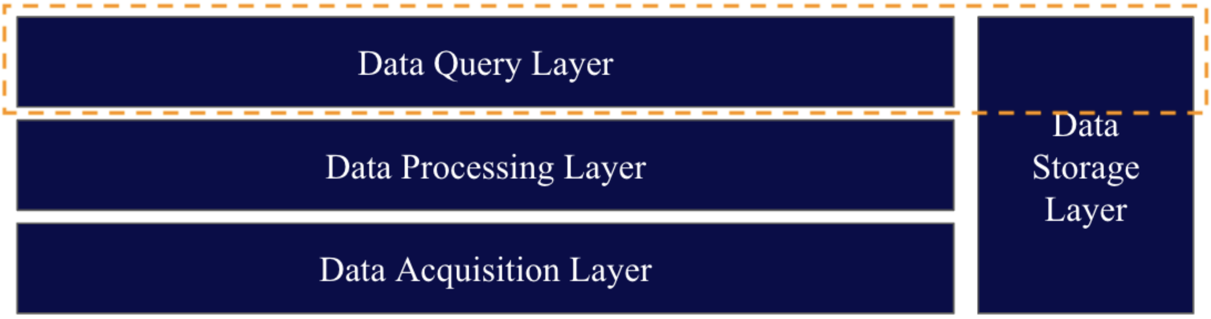


Figure 19: Functional components of query processor node

Data Enricher Node

This node is responsible for providing the necessary runtime for all the algorithms including AI / ML models and also to collect the block data from the blockchain RPC endpoints. It will be possible to distribute these tasks into smaller chunks and execute among all the participants of the network. This node comprises components of the decentralization layer, including data processor, data acquisition and parts of data storage. This role within the network carries weightage, as described below, which means that node operators with this role will receive fees and rewards based on this weightage. The distribution is calculated using the Cobb-Douglas Production function, refer to "*Network Reward Model*" for more details.

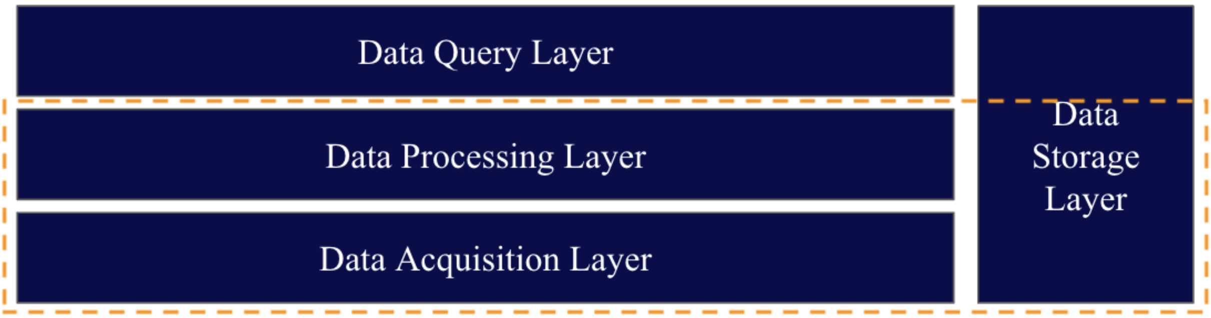


Figure 20: Functional components of data enricher node

Role	Weightage
Data Enricher Node	40% to 70%

Table 5: Data Enricher node weightage

This node will interact with RPC endpoints to get data from different blockchain supported by the network. Between these two nodes 100% of the query fee and the network rewards are shared based on the weightage defined within the roles.

Delegators

Not everyone can be a node operator due to the technical expertise and capital requirements needed to operate and maintain a node. However, token owners who still want to participate in securing the network can become node delegators.

Node operators incentivize delegators to delegate their tokens to their node by offering a share of the fee revenue and rewards earnings earned by the node. The rewards for delegators are influenced by the node's performance and effort, and tend to have low to no influence as more tokens are staked in the node.

To maximize their returns, delegators carefully consider a variety of factors when selecting a node operator. They typically look for operators with a strong work load, favorable sharing rates, and an optimal staking ratio, which allows them to earn the most rewards from their staked tokens. By carefully choosing a node operator, delegators can help secure the network and earn rewards while avoiding the complexity and cost of operating their own node.

Indicators

Essential for the sustained expansion of the decentralized model, the data enrichment process must continuously evolve and adapt. Signaling mechanisms play a vital role in informing network participants about which blockchains to index, what data needs grooming, and which metrics to construct, among other tasks.

Network users can leverage their role as indicators to influence the selection of blockchains or metrics they wish to consume, ensuring the network remains responsive to their needs. Indicators are rewarded with a share of the query fees, creating an incentive for active participation in the network's growth and development.

To ensure indicators prioritize tasks appropriately and make well-considered decisions, staking rewards are unlocked only after the signaled task has been executed. This mechanism encourages careful signaling and fosters a sense of responsibility among indicators, contributing to the overall health and efficiency of the decentralized network.

By promoting active engagement and providing tangible incentives for indicators, the network fosters a collaborative environment that drives the continuous growth and improvement of its data enrichment activities. This dynamic ecosystem empowers users to contribute their expertise and influence the network's direction, ultimately enhancing its utility and value for all participants.

Community Contributor

Developers and projects have the opportunity to make meaningful contributions to the network by introducing innovative AI/ML models and supplementary metrics that can further enhance the network’s capabilities. Additionally, they can provide cutting-edge fraud detection algorithms and logic, which can be used by the users of the project.

Even non-developer contributors can play an important role in the network's success by contributing off-chain data such as social media handles and other relevant information. To encourage and reward such contributions, the network offers incentives in the form of its native utility token. These tokens can be earned by developers and non-developers alike, fostering a collaborative and dynamic ecosystem where all members are motivated to contribute their skills and knowledge. By actively engaging a diverse range of participants, the network can continuously evolve and adapt to the ever-changing landscape in blockchain.

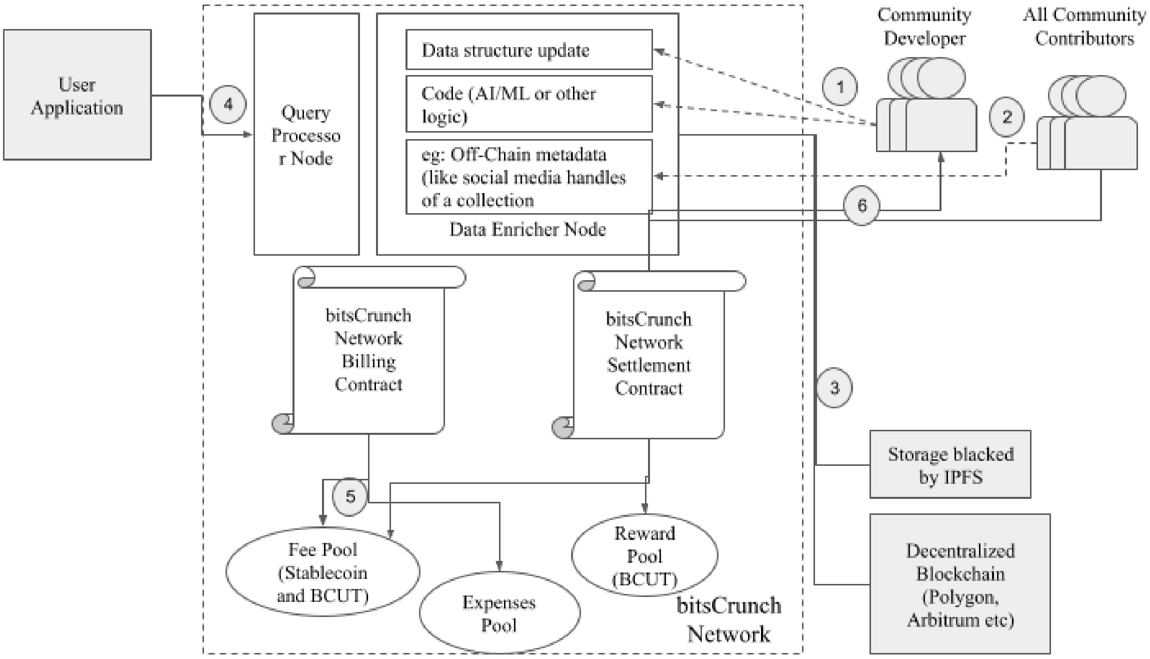

User Application
4
Query Processo r Node
Data structure update
Code (AI/ML or other logic)
eg: Off-Chain metadata (like social media handles of a collection
Data Enricher Node
Community Developer
All Community Contributors
1
2
6
3
bitsCrunch Network Billing Contract
bitsCrunch Network Settlement Contract
5
Fee Pool (Stablecoin and BCUT)
Expenses Pool
Reward Pool (BCUT)
bitsCrunch Network
Storage blacked by IPFS
Decentralized Blockchain (Polygon, Arbitrum etc)

Figure 21: Community contribution

1) Community developers contribute AI/ML models for analytics and forensics or other algorithms to the network.
2) All community members can contribute with Off-chain metadata like eg: social media handle for collections.
3) These contributions are logged securely in a decentralized storage and the same is also recorded in a decentralized blockchain.
4) User application access data via the query processor node.
5) Network billing contract will draw down from the user deposit based on the query usage.
6) A portion of the fee and contributor rewards are distributed to the community contributors based on the contribution.

Community developers will get additional funding from the ecosystem fund if they continue to make reliable contributions.

Network User

Network users are consumers of data from the network, which can be obtained through a permissionless model. All users can connect a crypto wallet to create an account and obtain the necessary credentials to query the network. To obtain credentials, users must lock up stablecoin tokens in the billing smart contract. This contract deducts tokens based on usage and swaps them to BCUT, which is sent to the query fee pool. Stablecoins are used as the payment token to maintain a stable price for services, allowing users to plan and budget account top-ups.

When users log in for the first time to the network interface, they will receive a default billing account. This default billing account includes a predefined test API key with a capped quote to help users test and integrate network services into their applications. Users can manage multiple application integrations or potentially resell services to other users outside the network by having multiple billing accounts.

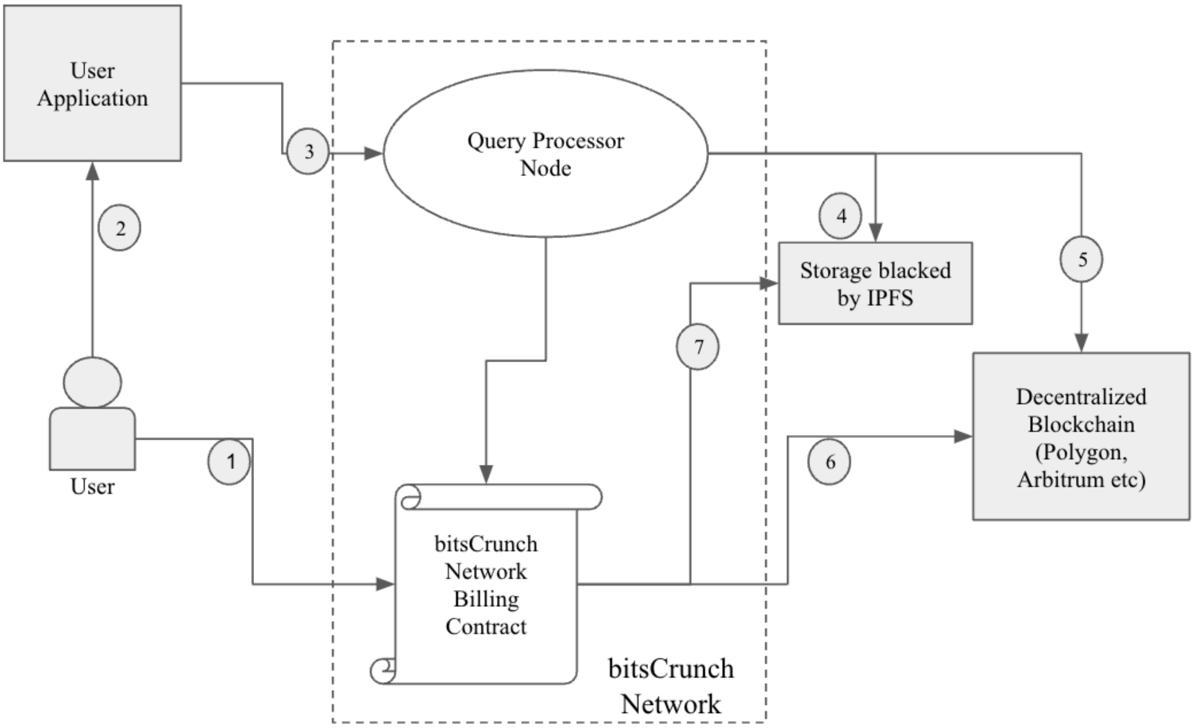


Figure 22: Network user and interactions

1) Users create a billing account and deposit stablecoin into the billing smart contract. They can optionally add BCUT to receive a discount on the query fee.
2) Users obtain credentials and apply them to the application integration settings.
3) The application uses the credentials to query the network.
4) The network responds to the query and records the activity to IPFS-backed storage.
5) Data from the IPFS storage is periodically aggregated, and the resulting file's hash is recorded in the blockchain along with the raw data file's hash. This helps prevent any manipulation of the data.
6) The network's billing contract looks up the blockchain for the latest aggregated file details.

7) The billing contract then uses this information to retrieve the data from IPFS and, based on the aggregated data, deducts from the money deposited by the user based on usage. This step may be manual during the initial phase of the project.

User Fund Management

To avail of our network services, users will be obliged to deposit or stake a stablecoin, such as USDC. This not only fuels the utilization of our services but also forms the basis of our secured payment system.

Throughout the billing cycle, these staked funds will be frozen and non-withdrawable. This provision is to ensure the availability of funds for the consumed services. It's important to note that a halt in services must be initiated by the user before the withdrawal of any outstanding tokens can occur, and this can only happen post the settlement of the final bill.

We maintain a rigid protocol for the security of these funds. There is no manual mechanism or backdoor that allows the withdrawal of funds from the contract. These funds can only be used for service payment, which is automatically handled by the contract, or withdrawn by the customer following the termination of services. This system is designed to ensure the security and integrity of transactions, providing customers with peace of mind.

Query Payment

As noted previously, user deposits serve as the payment medium for the services used, governed by an automated process executed by the smart contract at pre-determined intervals (1H, 6H, 10H - these durations will be configurable).

In an effort to maintain complete transparency and traceability, all records of service consumption are securely archived in IPFS storage, a decentralized system renowned for its data integrity and durability. Subsequently, the hash of these logs is updated and inscribed on the public blockchain (Polygon), creating an indelible record that is both accessible and auditable.

Such a design not only ensures full visibility of transactions for our customers but also equips them with the necessary data to raise and validate any potential disputes. The mechanism aims to instill trust and confidence, fostering a strong customer-service provider relationship based on transparency and fairness.

Network Settlement

The network settlement contract ensures that all operators and delegators in the network are duly compensated for their work. This is made up of one or more smart contracts that leverage the work log files stored in the decentralized storage. The network settlement process is entirely conducted using the utility token BCUT, ensuring seamless and secure transactions.

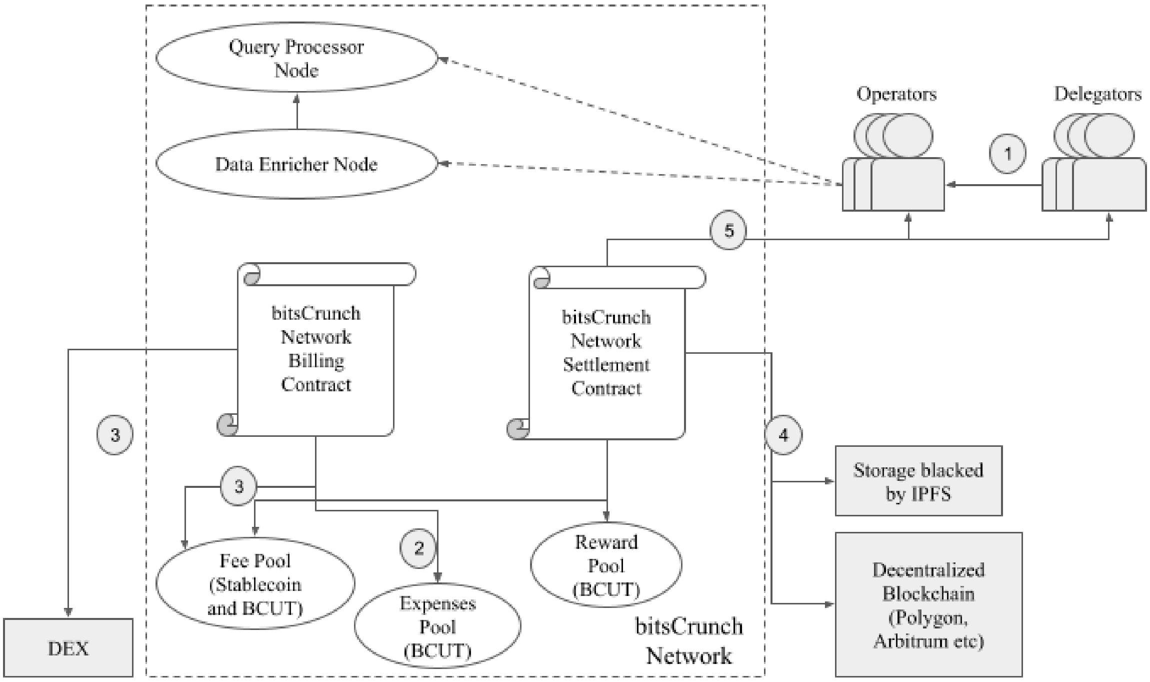

Query Processor Node
Data Enricher Node
Operators
Delegators
1
5
bitsCrunch Network Billing Contract
bitsCrunch Network Settlement Contract
3
4
Storage blacked by IPFS
3
2
Fee Pool (Stablecoin and BCUT)
Expenses Pool (BCUT)
Reward Pool (BCUT)
Decentralized Blockchain (Polygon, Arbitrum etc)
DEX
bitsCrunch Network

Figure 23: Network settlement flow

1) Delegators will stake BCUT token on operator(s) to secure the network and to earn a share of the query fee and rewards.
2) Network billing contract will draw down from the user deposit based on the query usage, a portion of it is kept in an expenses pool for paying blockchain gas fee and IPFS storage costs.
3) A portion of the drawdown is periodically swapped to BCUT and kept in the fee pool. The remaining portion is kept as stablecoin.
4) Network settlement contract will use node effort calculated using the aggregated data in the decentralized storage and the staking ratio. Most of the calculation will be externalized to not complicate the contract code and also keep the cost low.
5) Node operators will be able to claim BCUT from the settlement contract as per the reward and fee allocation calculated in step 3. Delegators will also be able to claim the tokens as per the fee and reward share setup by the operators.

Network Reward Model

Query fees are collected by the billing smart contract and converted to BCUT before being deposited into the query fee pool. Operators receive their share of the tokens from this pool on a monthly basis, with the distribution determined by the Cobb-Douglas Production function. Rewards are calculated and shared daily.

Let’s apply this function for fee sharing and rewards sharing among the network operators and delegators. Node staking is used in the request routing and for reward calculation.

Fee share

All fees generated from processing queries are converted to BCUT (the native token of the network) and collected in a common pool. On the settlement day, which occurs on a fixed day each month, a Cobb-Douglas algorithm is used to determine the distribution of BCUT rewards among node operators and delegators based on their contributions to the network. Both operators and delegators are eligible to claim their respective share of the reward from the pool. Staking ratio is not used in fee share calculation but instead is used as a factor for query queuing.

Query Processor node

$$nodeFeeShare_{qp}(i) = totalFeeEarnings * nodeEffort_{qp}(i) * nodeWeightage$$

Where

- $nodeFeeShare_{qp}(i)$ is the fee share that is allocated to a particular query processor node
- *totalFeeEarnings* is the total fee earned by the network over the settlement cycle (a fixed day of the month)
- $nodeEffort_{qp}(i)$ is the contribution of a node towards query processing. $nodeEffort_{qp}$ *= (# of successful queries processed by a node / total successful queries processed by all nodes)*
- *nodeWeghtage* is derived from the roles played by the node, refer to Network Operator Roles section for more details

Data Enricher node

$$nodeFeeShare_{de}(i) = totalFeeEarnings * nodeEffort_{de}(i) * nodeWeightage$$

Where

- $nodeFeeShare_{de}(i)$ is the fee share that is allocated to a particular data enricher node
- $nodeEffort_{de}(i)$ is the effort contributed by the node. *nodeEffort = (# of bCU by the node / total bCU by all nodes) + (# of blocks retrieved using the node / total blocks retrieved by all nodes)*. bCU is a bitsCrunch compute unit calculated as a combination of the infrastructure and other components contributed by the node. Since not all blockchain have the same block size and hence this will also be factored in towards the node effort.

Rewards share

As previously stated in this chapter, a portion of the BCUT tokens is allocated for bootstrapping the network and rewarding its operators. At the close of each fixed epoch sets, reward shares are computed and made available for distribution to both operators and delegators. Both delegators and operators are eligible to claim their respective share of the rewards.

Query Processor node

$$nodeRewardShare_{qp}(i) = totalRewards * nodeEffort_{qp}(i) * nodeWeightage$$

Where

- $nodeRewardShare_{qp}(i)$ is the rewards share that will be allocated to a particular node
- *totalRewards* is the total rewards allocated for the epoch.
- $nodeEffort_{qp}(i)$ is the contribution of a particular node towards query processing. $nodeEffort_{qp}(i)$ *= (# of successful queries processed by a node / total successful queries processed by all nodes)*
- $nodeWeightage_{qp}$ is derived from the roles played by the node, refer to Network Operator Roles section for more details

Data Enricher node

$$nodeRewardShare_{de}(i) = totalRewards * nodeEffort_{de}(i) * nodeWeightage$$

Where

- $nodeRewardShare_{de}(i)$ is the rewards share that is allocated to a particular data enricher node
- $nodeEffort_{de}(i)$ is the effort contributed by the node. *nodeEffort = (# of bCU by the node / total bCU by all nodes) + (# of blocks retrieved using the node / total blocks retrieved by all nodes)*. bCU is a bitsCrunch compute unit calculated as a combination of the infrastructure and other components contributed by the node. Since not all blockchain have the same block size and hence this will also be factored in towards the node effort.

Disputes

In order to maintain fairness and transparency within the network, all node operators have the right to raise disputes if they believe there are discrepancies or issues with fee and rewards payouts. Disputes are handled through an open and transparent process that involves network operators and community support, with the goal of resolving disputes within a fixed duration.

This process includes a detailed review of the dispute, with input from all relevant parties, and a thorough investigation to identify the cause of the issue. Once the issue is identified, a resolution is proposed and voted on by the network community.

By allowing node operators to raise disputes and providing a transparent and collaborative process for resolving them, the network promotes a sense of trust and fairness that is essential for long-term success.

Governance

Once the network has achieved sufficient decentralization, network governance will be transitioned to the bitsCrunch network DAO. This decentralized autonomous organization will facilitate a transparent and democratic decision-making process, allowing stakeholders to collectively govern and manage the network without the need for centralized control.

The DAO will be responsible for managing various aspects of the network, including protocol upgrades, fee structures, and incentive mechanisms. By leveraging the collective expertise and insights of stakeholders, the DAO will ensure that the network is governed in a fair and transparent manner that aligns with the values of the community.

Using the DAO will allow stakeholders to have a direct say in the rules and regulations that govern the network, ensuring that decisions are made through a consensus-driven process. This will promote greater accountability and community-driven innovation, fostering a greater sense of ownership and participation among stakeholders.

Governance Design Principles

Here is how core design principles apply to governance:

1. Usability: Governance processes should be clear and understandable. Mechanisms for active participation and for voting (where available) should be simple and straightforward. Governance should be effective and efficient so it arrives at decisions quickly and implements them efficiently. The community of stakeholders should have sufficient voice that they support the legitimacy of decisions and do not exit or fork the platform.
2. Scalability: Governance should scale as the scope and complexity of the platform itself grows, as the diversity of its stakeholders increases and as the breadth of participation expands.
3. Simplicity: The most robust processes tend to be the simplest so good governance should avoid overengineering processes and acknowledge that often human-to-human communication is the simplest approach.
4. Sustainable Decentralization: Governance should allow participation from the full breadth of stakeholders in the platform but be resilient against capture by any one of these over time.

It is important that governance design balances between efficiency and resiliency. Decisions must be made and implemented efficiently if a technical platform is to continue to evolve sufficiently to provide the best value for its stakeholders but that platform must ensure that it can not be captured over time by a particular group of stakeholders.

Technical Governance Process

In DAO (Decentralized Autonomous Organization) governance, proposals typically go through several stages or statuses.

- **Draft**: The proposal is in its initial phase, where it is being created, drafted, and refined. This stage allows for early discussions and feedback but does not yet involve any formal decision-making.
- **Submission**: The proposal is officially submitted to the DAO for consideration. This might require meeting certain criteria or gaining preliminary support from members.
- **Review**: The proposal is under review by the community or specific working groups. This stage might include discussions, debates, clarifications, and requests for more information.
- **Voting**: The proposal is put to a vote. Depending on the DAO's rules, this might include different types of voting such as simple majority, supermajority, or consensus. Voting could involve various stakeholders, such as token holders or a governing council.
- **Approved**: The proposal has passed the voting process and has been officially accepted by the DAO. Next steps, such as implementation or allocation of resources, will follow.
- **Rejected**: The proposal has been voted down and will not proceed. Depending on the DAO's rules, it might be possible to revise and resubmit a rejected proposal.
- **On Hold**: The proposal has been temporarily paused, possibly due to issues that need to be resolved, a lack of consensus, or other strategic reasons.
- **Implemented**: The proposal has been successfully implemented, and the changes or actions it proposed are now in effect.
- **Archived**: The proposal, whether approved, rejected, or withdrawn, is archived for record-keeping and future reference.
- **Withdrawn**: The proposer or supporters of the proposal decide to withdraw it before it reaches a vote. This can occur for various reasons, such as a lack of support or the identification of unforeseen issues.
- **Escalation**: In case of disputes or conflicts, the proposal may enter an escalation phase, where mediation, arbitration, or other conflict resolution processes are invoked.
- **Expired**: If a proposal doesn’t meet certain conditions within a predefined timeframe (e.g., not enough votes), it may expire and be removed from consideration.

Governing Council

The bitsCrunch protocol governing council is composed of a diverse group of individuals, organizations, or entities, united with the common purpose of overseeing and guiding the decentralized network. This council's responsibilities encompass the careful management, development, and sustained maintenance of the protocol, ensuring that all decisions align with the community's best interests and contribute to the future growth of the network.

During the initial phases of development and until sufficient decentralization is achieved, the bitsCrunch Foundation may appoint members to this governing council. These appointed members will work closely with the core development team, providing essential oversight, strategic direction, and support.

The rationale behind this approach is twofold. First, it allows the project to maintain a strong, unified direction during its critical early stages. Second, it sets the stage for a gradual transition toward a more decentralized model of governance, reflective of the broader community's values and desires. This transitional model ensures that the core team remains focused on delivering the committed roadmap and vision, while also paving the way for increased community engagement and decentralized decision-making in the future.

Slashing

Slashing is a mechanism in which a node operator's stake is penalized for violating certain rules or engaging in malicious behavior that harms the network. Examples of actions that may result in a slashing penalty include serving inaccurate data, double logging work, censorship, or other forms of malicious behavior.

The purpose of slashing is to discourage node operators from engaging in harmful behavior and to ensure that they have a vested interest in maintaining the security and integrity of the blockchain. While slashing penalizes the node operator, it does not affect delegators. However, delegators can expect reduced earnings as the node is downgraded from the queues.

It is important to note that community contributors of the network may also be subject to slashing penalties for providing inaccurate or harmful content. This ensures that everyone who participates in the network is held accountable for their actions and that the network is operated in a fair and transparent manner.

Overall, slashing is an essential mechanism for ensuring the security and integrity of the blockchain. It incentivizes node operators to behave in a trustworthy and honest manner and promotes a decentralized and resilient network that is less vulnerable to malicious attacks.

Operator Expectations

- Always run the latest version of the node
- Meet the minimum hardware and software specification requirements
- Meet staking requirements
- High availability and reliable infrastructure
- Participate in regular feedback sessions with the team and community
- Participate in network governance