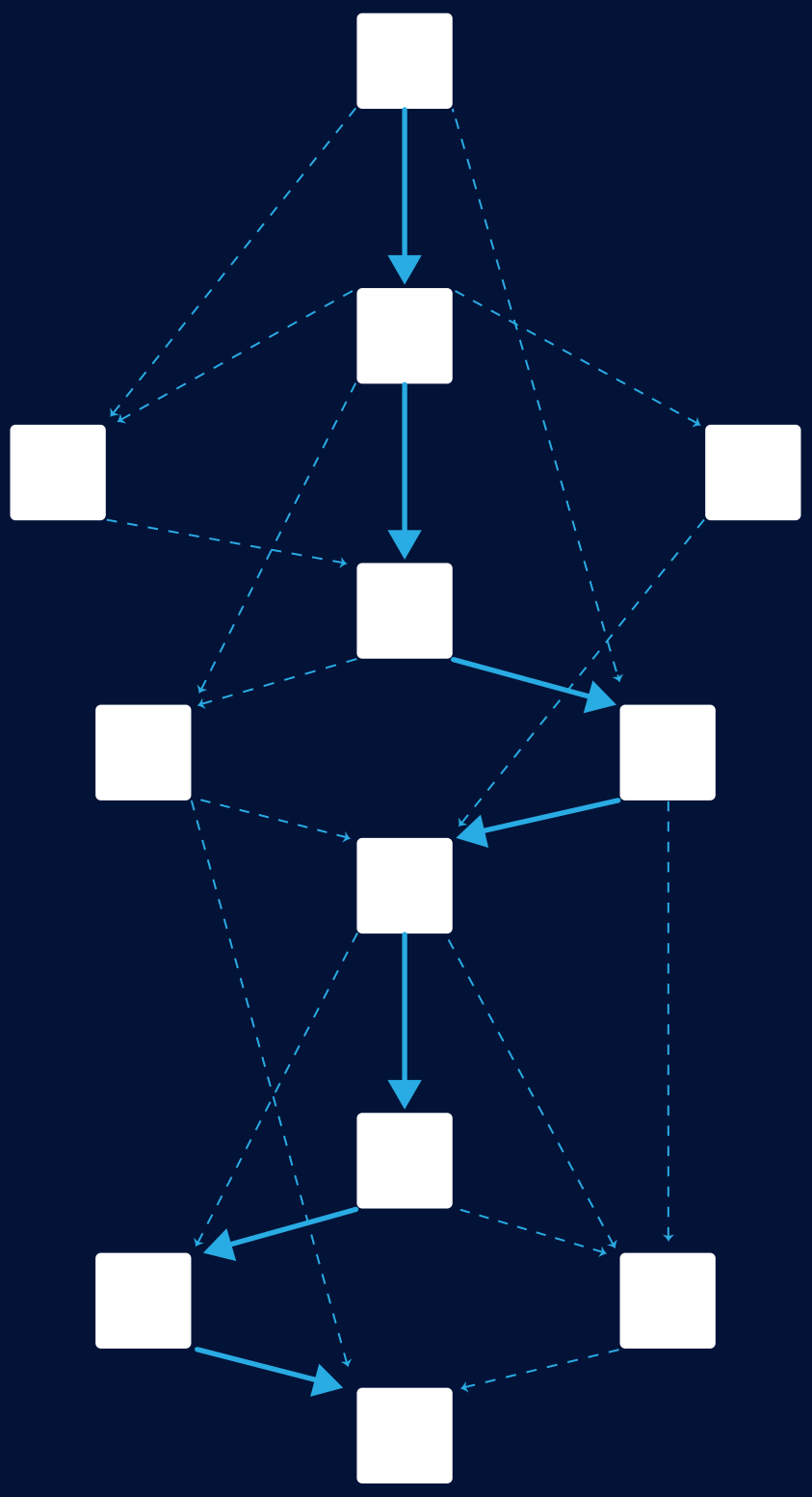
BlockDAG



Litepaper

December 2024

Table of Contents

Overview

BlockDAG: A New Era in Decentralized Blockchain Technology

BlockDAG is an adaptive, next-generation blockchain protocol poised to onboard the next billion users. It does this by merging rapid finality with robust EVM capabilities—all without compromising decentralization. BlockDAG builds on Bitcoin's core principles while introducing improved scalability and pushing the boundaries of what high-performance EVM chains can achieve. The team is dedicated to creating a network that prioritizes community, fairness, and openness while enabling novel applications.

Central to BlockDAG's mission is its seamless integration of an Unspent Transaction Output (UTXO) model and an Ethereum Virtual Machine (EVM), allowing it to operate at scale without friction. This approach reflects the lessons learned from current and prior blockchain limitations and recent innovations. Unlike traditional proof-of-work (PoW) blockchains, BlockDAG leverages the DAG structure, enabling the processing of multiple blocks in parallel and ensuring swift, secure transaction confirmations. This architecture is supported by the open-source GhostDAG protocol, a groundbreaking method that organizes parallel blocks cohesively, enhancing the network's capacity, responsiveness and transaction speed.

BlockDAG was designed according to the project's core thesis: blockchains should facilitate the smooth, frictionless exchange of digital assets in a decentralized manner. The challenge of scaling blockchains while maintaining decentralization is pivotal for the next phase of Web3 adoption. By addressing this, BlockDAG paves the way for trustless and practical real-world use cases across money, payments, decentralized finance, real-world assets, gaming and many others.

A Commitment to Decentralization

BlockDAG upholds decentralization as a non-negotiable value and embodies the belief that fully trustless networks are essential for the ecosystem's growth and credibility. This commitment distinguishes it from legacy and newer blockchain solutions that often trade decentralization for performance and speed. The BlockDAG network aims to do for everyday users what Bitcoin did for value storage and Ethereum for composability: enable simple, fully decentralized digital asset exchange that anyone can use without technical expertise.

BlockDAG's real-world relevance is underpinned by its proactive community-driven development. In contrast to many well-funded Layer 1 (L1) projects that never achieved meaningful adoption previously referred to as "Ethereum killers" or "high-performance" blockchains - the project is far from an isolated academic exercise but thrives on the active engagement of users, builders and miners. BlockDAG avoids the common pitfalls of past-generation L1s that have struggled with being too academic or insider-focused. Instead, it bets on its community and culture, involving its rapidly growing group of enthusiasts early on to drive collective innovation and steady growth.

Still, BlockDAG is standing on the shoulder of giants such as Bitcoin and Ethereum in that it builds on what past blockchains have achieved and aims to solve the key challenge of scalability while keeping decentralization intact. It acknowledges the achievements of Bitcoin and Ethereum and wants to win alongside them, following the open-source ethos and using mining as a core feature of decentralization. This balanced approach helps BlockDAG to support secure transfers and serve as a reliable dApp platform for everyday use.

Vision & Value Proposition

BlockDAG envisions a decentralized superhighway for dApps that bridges technological innovation with cultural relevance. It's not just about transactions or smart contracts; it's about creating a network where technology and communities intersect. BlockDAG fosters a vibrant on-chain culture, turning creativity, financial innovation and culture into tangible, tokenized assets.

The founding team recognizes that blockchain adoption starts with people and their passions as opposed to a purely technological approach. Inspired by consumer-focused design, the roadmap prioritizes intuitive onboarding, effortless app discovery, and a seamless ecosystem experience. It's built to take Web3 mainstream by making interactions user-friendly and engaging. BlockDAG doesn't just connect users to technology; it connects them to communities and lifestyles they care about - such as trading, sports, gaming and meme culture, to name but a few. The result is more than just utility - it's meaningful, human-centered blockchain engagement.

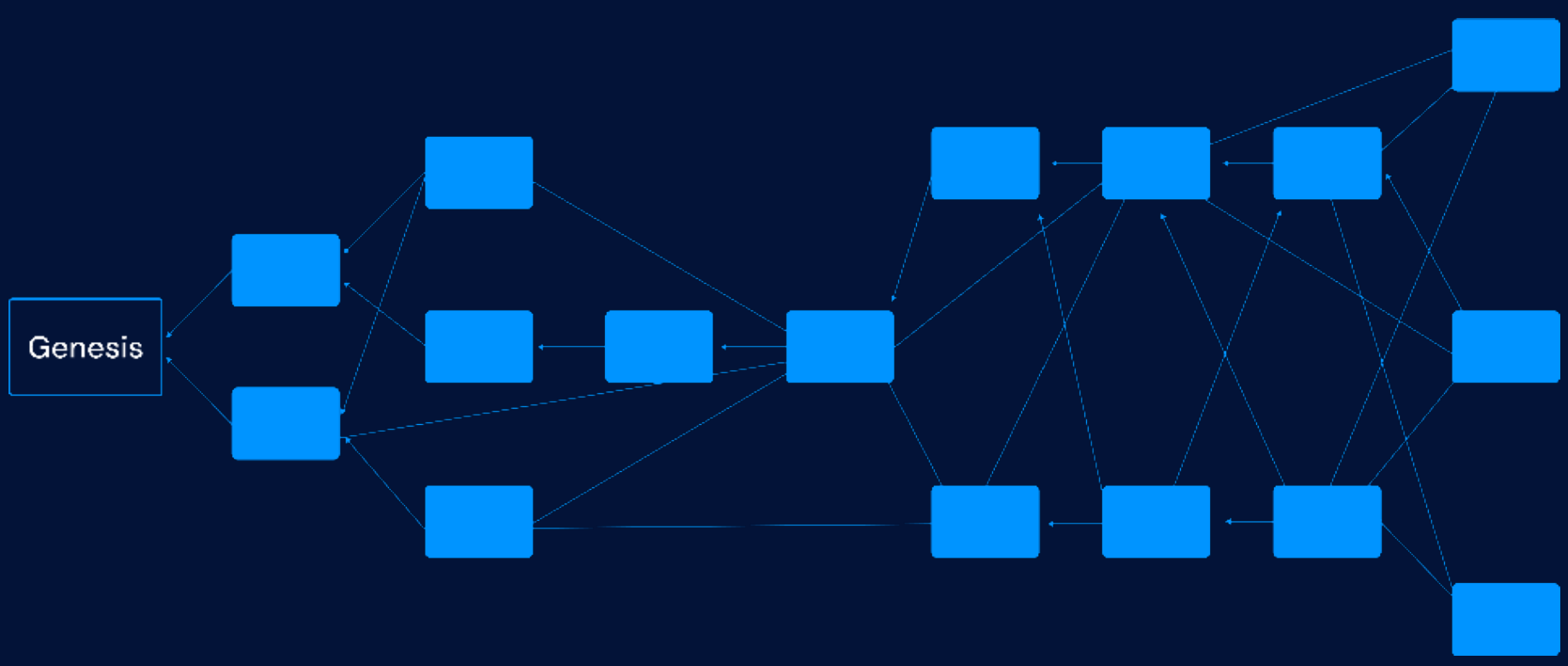
At its core, BlockDAG combines UTXO scalability with EVM programmability to create a powerful and versatile platform. Whether for high-speed payments or new DeFi applications, it delivers interoperability without compromise. Rooted in fairness, BlockDAG avoids exclusive venture capital deals to the detriment of its community and hidden agendas, ensuring a transparent, equitable ecosystem. This is blockchain done right: fast, decentralized, secure, inclusive, and ready to power the next wave of blockchain innovation.

BlockDAG incentivizes and rewards early builders from the start through targeted grants and rewards programs. Developers will also benefit from a juicy fee-sharing model that allows them to earn from 25% of transaction fees generated by their protocols. Fee-sharing rewards successful applications for their on-chain activity, directly linking dApp performance to financial incentives. Developers creating applications benefit directly from their usage growth on the network.

An Introduction to BlockDAG

DAG

BlockDAG uses a Directed Acyclic Graph (DAG) structure combined with a Proof-of-Work (PoW) consensus mechanism. The DAG ensures that blocks created in parallel are not orphaned. Instead, they are still included and ordered within the consensus, allowing high block rates and minimizing confirmation times. Unlike traditional blockchains, BlockDAG organizes blocks in parallel chains, allowing greater scalability and more efficient use of resources. This design improves transaction speed and scalability while avoiding orphaned blocks. BlockDAG's use of the UTXO model makes tracking ownership and validating transactions more efficient, especially in high-volume systems. As one of the first blockDAG-based networks, BlockDAG allows for high throughput, extremely fast confirmations, and next-generation scalability - all while staying decentralized.



EVM Identical

BlockDAG's execution layer is EVM-compatible, enabling seamless deployment of EVM-based smart contracts and integration with existing decentralized applications (dApps). This compatibility supports a comprehensive suite of Ethereum development tools like Truffle, Remix, MetaMask, and Hardhat, among other things, and ensures interoperability with ERC standards such as ERC-20 and ERC-721 tokens. By leveraging composability—the ability for different smart contracts and dApps to interact and build on each other - BlockDAG boosts innovation and rapid development within its ecosystem. This approach allows developers to migrate EVM dApps with minimal changes, benefiting from cross-chain compatibility and secure, deterministic execution while maintaining state persistence and leveraging its robust gas mechanism for resource management.

WASM Compatibility

BlockDAG has recently introduced WebAssembly (WASM) compatibility, allowing developers to build dApps and smart contracts using languages they already know. Unlike traditional blockchain platforms like Ethereum, which limit developers to specific languages like Solidity, BlockDAG supports multiple languages, including Rust, C, and C++. This means developers can get started faster and build more efficiently without learning something new. WASM compatibility will be added at launch or shortly thereafter.

WASM compatibility doesn't just speed up development—it transforms how blockchains work. By running code at near-native speeds, it delivers the performance needed for demanding applications like DeFi, gaming, and NFTs. Its cross-chain functionality fosters interoperability, enabling dApps to seamlessly connect across platforms, while its sandboxing feature enhances security by isolating smart contracts. With WASM, BlockDAG enables developers to create faster, more secure, and interoperable applications, addressing key challenges in blockchain development like performance bottlenecks and cross-platform compatibility.

The Problem

The evolution of blockchain technology has been inherently constrained by what is often called the blockchain trilemma, a concept describing the tradeoff between security, scalability, and decentralization. Historically, the blockchain trilemma forced developers to prioritize certain properties at the expense of at least one other property. In practice, this challenge has made it difficult for blockchains to achieve a balanced, efficient network without sacrificing one of these key aspects.

First, security is crucial to protect the network from malicious actors and ensure that transactions and data are safe from tampering or double-spending, preserving trust among users. Second, transaction speed and throughput are important for scaling, as they enable the network to handle a growing number of users and transactions efficiently. This prevents congestion and allows the blockchain to support broader adoption. Finally, decentralization is crucial because it ensures that no single entity or group has control over the network. This promotes trust, censorship resistance, and maintains the core values of permissionless and open systems.

In traditional blockchain and cryptocurrency networks such as Bitcoin, decentralized networks must limit their block creation rate to manage "orphans" which are blocks created off-chain while a latent block is being propagated across the network. High orphan rates can severely undermine the efficacy of a Proof-of-Work (PoW) network by reducing its defenses against potential attacks from malicious actors joining the open network. This necessity throttles throughput and leaves classic blockchains, such as Bitcoin, with a scalability bottleneck.

General-purpose Layer 1 (L1) blockchains were created to solve these problems. However, many of them have not met expectations when it comes to resolving the scalability trilemma. L1s have often struggled with various issues beyond scalability, including complexity, security vulnerabilities, downtime, poor user experience, and unsustainable tokenomics. The quest for increased throughput has led some blockchains to adopt models that accelerate performance but at a significant cost. While some next-generation L1s have claimed breakthroughs in performance and scalability, they often achieved this by sacrificing decentralization - a core principle that gives blockchain technology its value. The centralization of Proof-of-Stake (PoS) validator sets, driven by reliance on specialized hardware, has skewed many of high-performance blockchains toward industrialized, resource-heavy operators, effectively crowding out smaller participants and validators. This entry barrier erodes the key values that make blockchains unique, such as decentralization, censorship resistance, credible neutrality, permissionlessness, and trustlessness.

Even the Ethereum community, known for upholding these core values, has acknowledged the significant challenge of scaling without major trade-offs. Ethereum's roadmap has hit many roadblocks, including sidechains and sharding. As a temporary fix, it evolved to scale the network through Layer 2 (L2) solutions, focusing on a rollup-centric approach to enhance its Layer 1, albeit with mixed results so far. Although this direction promises better scalability, it comes with its own challenges, particularly around centralization. Most current rollups continue to rely on centralized sequencers which raises concerns about maintaining true decentralization.

How BlockDAG Addresses the Problem

BlockDAG presents an innovative resolution to the blockchain trilemma by achieving a new way to balance security, scalability, and decentralization. The core advantage of BlockDAG lies in its unique utilization of a Directed Acyclic Graph (DAG) structure rather than the traditional linear blockchain. This approach allows transactions to be processed in parallel, enhancing throughput and confirming multiple blocks simultaneously without conflict. Unlike traditional blockchains where every node must sequentially process every transaction, BlockDAG's partial ordering method enables unrelated transactions to be verified simultaneously which significantly boosts performance.

The application of the Phantom GhostDAG protocol underpins BlockDAG's ledger, ensuring that the network can maintain order and security across parallel block generation. By incorporating this system, BlockDAG ensures that blocks are quickly produced and confirmed, with multiple blocks being visible to the network within seconds and achieving full transaction finality in 1-2 seconds on average. This rapid processing power scales transaction throughput to levels that outpace Ethereum and Bitcoin, achieving scalability without compromising decentralization. In contrast to centralized solutions that require powerful hardware or create reliance on a few validators, BlockDAG remains accessible for regular users to run nodes or mining nodes, promoting true decentralization.

Security, a crucial pillar of the trilemma, is upheld through BlockDAG's proof-of-work (PoW) algorithm. The system benefits from its Keccak-256 algorithm for consensus and security, which incorporates the lessons learned from years of DAG research and PoW implementation. This method maintains the robust, battle-tested security of traditional PoW blockchains while adapting it for a more energy-efficient and high-throughput model. The energy optimization ensures that BlockDAG is less resource-intensive, countering the inefficiencies associated with conventional PoW systems.

Another standout feature of BlockDAG is its full Ethereum Virtual Machine (EVM) compatibility, bridging the gap for developers familiar with Ethereum's ecosystem. This compatibility empowers developers to seamlessly port and build decentralized applications (dApps) using Ethereum's established toolsets, such as Solidity. The combination of DAG's parallelized transaction capability with EVM functionality provides a fertile ground for the growth of DeFi and broader blockchain applications.

GhostDAG Tutorial

The GhostDAG protocol underpins BlockDAG's UTXO side, offering an innovative approach to block ordering in a blockchain. Unlike traditional blockchains that enforce a strict order, GhostDAG organizes blocks into a directed acyclic graph (DAG). This structure allows miners to reference multiple previous blocks, enhancing parallelism and reducing latency.
In this system, each block is classified by its position relative to other blocks as either "past," "future," or "anticone." Blocks in an anticone are not connected in a sequential order, posing a risk of double spending when dishonest miners attempt to create conflicting transactions. GhostDAG addresses this by gradually imposing a total order using a tie-breaking algorithm, which ensures that blocks with smaller anticones—typically produced by honest miners—are ordered before those with larger ones.
The protocol defines a k-cluster, where blocks in this set have anticones of size less than or equal to a system parameter, k. Honest miners are more likely to form larger k-clusters, while dishonest miners' blocks, with larger anticones, are placed later in the order or ignored if they conflict with honest blocks.

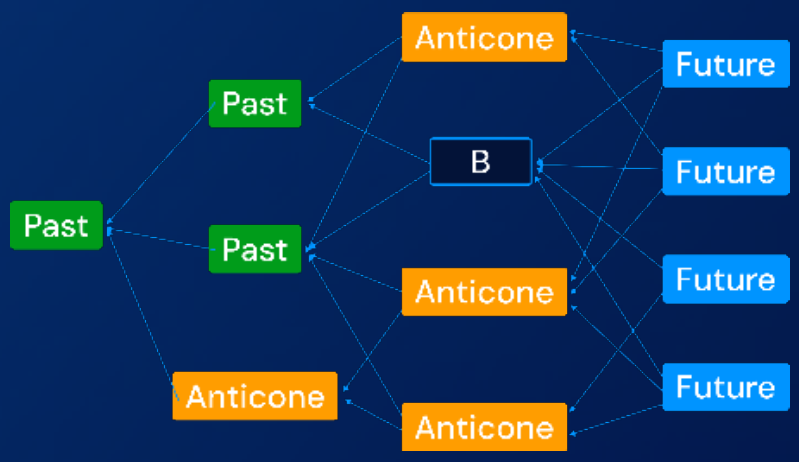


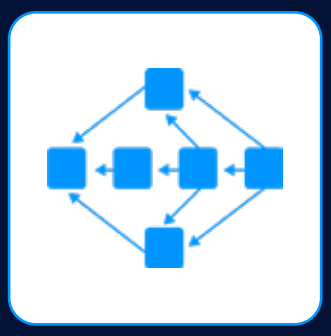
Figure 1: This figure shows how a block B divides the DAG into three parts: future (B) is the set of blocks that reference B, directly or indirectly, past (B) is the set of blocks that B references, directly or indirectly, and anticone (B) is the set of blocks that B does not reference.

While finding the largest k-cluster is computationally hard (NP-hard), GhostDAG efficiently finds a large k-cluster, ensuring a reliable block order. This prevents dishonest transactions from being processed over legitimate ones. For more technical detail, the original GhostDAG white paper offers deeper insights.

This method maintains decentralization and security while addressing blockchain performance issues, making it a robust solution for modern transaction ordering challenges.
Interested readers are encouraged to consult our whitepaper and the original **GhostDAG white paper.**

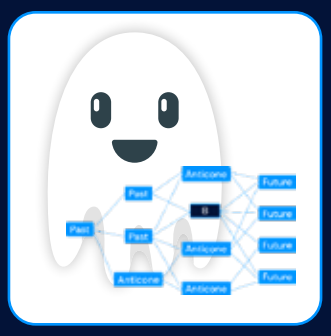
Key Features & Architecture

BlockDAG combines a Directed Acyclic Graph (DAG) with Proof-of-Work (PoW) for secure, scalable block production. This hybrid approach supports parallel block validation and high transaction throughput, while a P2P network ensures efficient block and transaction propagation using TCP and UDP. What makes BlockDAG unique as a DAG-based network is that it also features an EVM bridge, enabling seamless transfer of its native currency, BDAG, between the UTXO and EVM domains with a 1:1 exchange rate.



DAG Structure

The heart of BlockDAG, enabling parallel block production and high transaction throughput while maintaining security and scalability.



GhostDAG Protocol

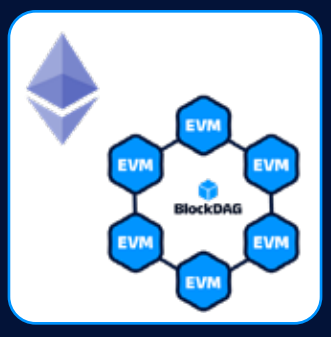
Ensures a universal transaction order in the DAG while enabling concurrent block production, delivering scalability and finality with robust resistance to attacks.

Consensus Layer

The backbone of BlockDAG's security, combining PoW with a DAG to achieve robust and scalable asynchronous consensus.

High transaction speed

BlockDAG is capable of more than 2,000 transactions per second (TPS) at launch. It targets 10,000+ TPS within the next 12 months after launch. The protocol's scalability enables both high-speed payments and smart contract functionality on a single platform.



EVM and WASM Compatibility

Fully supports Ethereum-based smart contracts, enabling the deployment of existing dApps and tokens with minimal friction while leveraging familiar tools. WASM integration is planned around the time of launch or shortly thereafter.

UTXO-EVM Interoperability

The protocol bridges the UTXO model's scalability and privacy with the EVM-compatible account model. A seamless 1:1 asset bridging system for the native BDAG token ensures smooth transfers between UTXO and EVM domains, preserving security and preventing double-spending across ecosystems.

BDAG - Two Tokens

BDAG is the official token of the BlockDAG ecosystem, serving as its economic backbone. Two forms of the utility token will exist: one on the UTXO side, and one on the EVM side. Designed for transparency and fairness, its issuance avoids hidden allocations or exclusive rounds, ensuring a level playing field for all participants.

Three Main Purposes

- **Native token across UTXO and EVM**
  BDAG is used to pay network fees and serves as the native token for both the UTXO-based and EVM-compatible domains, enabling seamless cross-domain transactions, smart contract execution, and decentralized application functionality.

- **Reward to miners**
  Miners compete to earn block rewards and transaction fees in the form of BDAG tokens. The rewards paid to miners for validating blocks and transactions will be calculated over a 40 year period, based on a linearly reducing payout.

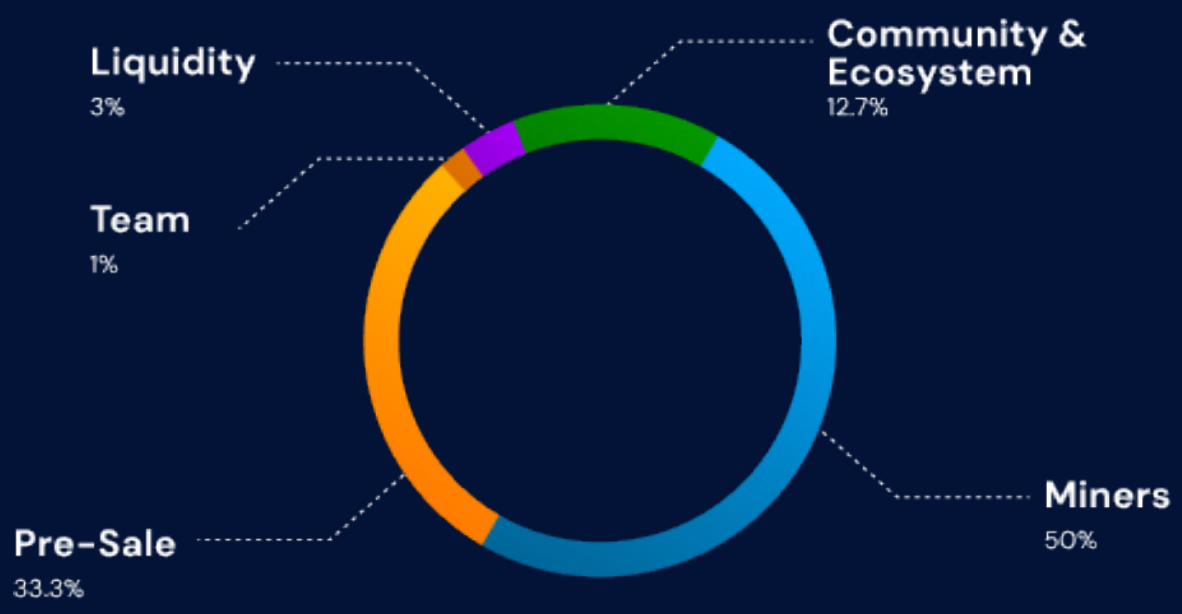
- **Staking**
  In BlockDAG, staking is the process of locking up BDAG tokens in exchange for rewards. Staked tokens cannot be spent, but they yield attractive rewards.

Tokenomics

Supply
The native BDAG token is central to BlockDAG's mission to build a fair and transparent platform. BlockDAG would be nothing without its community. With the introduction of BDAG, we aim to level the playing field and offer fair access to both existing and new members of our growing ecosystem. BDAG has a maximum supply of 150 billion tokens, distributed through mining rewards, community building, and a transparent pre-sale. The allocation prioritizes the community and avoids exclusive VC rounds, thus prioritizing accessibility and fairness.

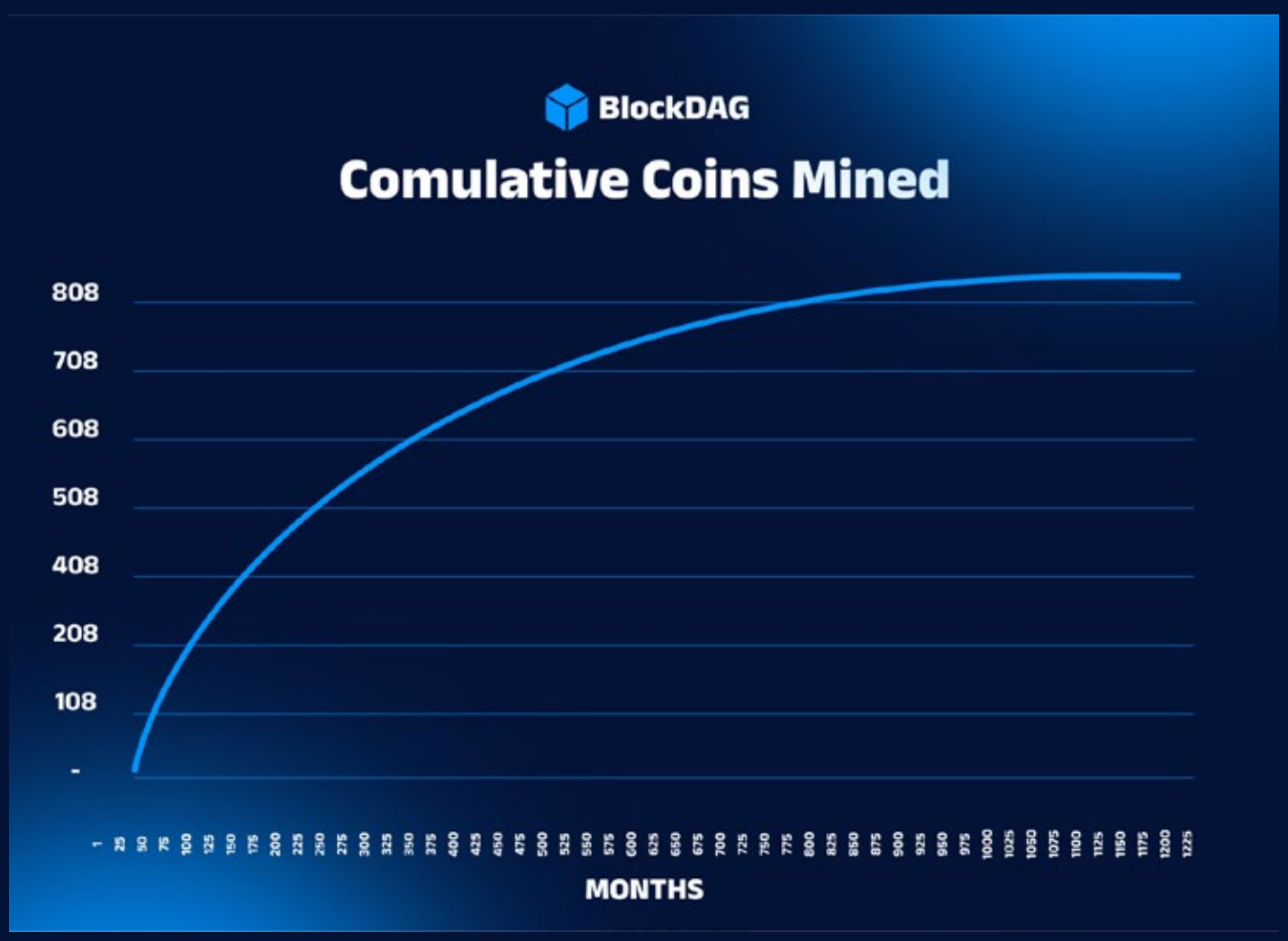
Category	Quanity	Percentage	Minting	Vesting/Lockup Notes
Pre-Sale	33.3%	50bn	At Launch	40% vest at launch & 20% per month thereafter
Team	1.0%	1.5bn	After Lockup	2 years lockup
Miners	50%	75bn	Based on pre-defined continuous geometric reduction per month.	No lockup
Community & Ecosystem	12.7%	19bn	Over time as required to support & grow the ecosystem	Depends on the use case
Liquidity	3.0%	4.5bn	At Launch	n/a

The total outstanding supply of BDAG tokens is split across pre-sale, miners, community & ecosystem, liquidity provision, and the team:



BDAG Emission Schedule

The coin's issuance follows a continuous geometric reduction, with monthly adjustments to avoid sudden supply shocks. This ensures sustainable token economics and incentivizes early network participation from miners.



Development Roadmap

BlockDAG's roadmap outlines key plans for growth and development. Here's what lies ahead:

Phase 1: 2024

Focus on developing the core DAG based blockchain, along with the Explorer, Faucet, and appropriate Smart Contracts.

1. **Q4 2024:** Launch the public Alpha Testnet

Phase 2: 2025

During this phase the development team will focus on the following areas:

2. Further **Improvements** to the core blockchain, including:
   - Optimizations to improve blockchain size, speed, resilience
   - Explorer enhancements including the ability to view and interact with Smart Contracts, ERC20 coins, NFTs, Nodes
   - Explorer Analytics

3. Development of core **DeFi components**, including stablecoins, staking, lending & borrowing, swaps, and cross chain bridging

4. Development of a Launchpad to support new project launches, borrowing the best ideas from existing products such as Pinksale.finance and pump.fun

5. **Q1 2025:** Launch the public Beta Testnet

Beyond 2025

The focus will shift to broader ecosystem expansion, including advanced interoperability, decentralized governance, and the integration of emerging technologies like AI and privacy-enhancing protocols.

Mining & Miners

Mining is at the heart of the BlockDAG ecosystem. Similar to the launch of Bitcoin, mining ensures decentralization and Sybil resistance from day one. Hence, BlockDAG's Proof-of-Work (PoW) consensus and mining ecosystem is a deliberate design choice. Mining creates a tangible link between the network and the physical world by requiring miners to invest in energy and specialized hardware, aligning economic incentives to maintain security and fair distribution. By solving computational puzzles, miners contribute to the network's integrity while deterring attacks, since the cost of malicious behavior is high, in part due to the more energy-intensive nature of PoW.

BlockDAG – akin to Bitcoin and similar ecosystems - mining promotes decentralization by fostering dynamic competition among participants. This avoids consolidation of power. The innovation-driven hardware evolution—moving from CPUs to ASICs—has improved efficiency and strengthened network security. In addition, PoW-based mining encourages the use of renewable energy and stranded resources, making it an environmentally adaptive solution. This mechanism not only anchors the network's value in real-world inputs but also inspires technological advancements that extend beyond blockchain, such as energy efficiency and hardware optimization.

BlockDAG's mining rewards system is designed to distribute 75 billion BDAG tokens - 50% of total supply - to miners, with rewards decreasing geometrically on a month-by-month basis. Miners can choose from specialized hardware devices or use the X1 Miner Mobile App. The X1 app enables mobile mining, incentivizes user referrals, and includes a leaderboard for competitive engagement.

Ecosystem Development

The success of a blockchain can normally be measured by the size and strength of its community and ecosystem. To this end BlockDAG is developing various programs and initiatives to grow and encourage builders and technology partners to join our ecosystem.

BlockDAG's $30M Grants Program

Over the next three years BlockDAG is investing in bold ideas that create better dApps and tools for the ecosystem. From infrastructure to DeFi and stablecoins, BlockDAG will be funding transformative projects with grants ranging from $5,000 to $100,000. Payments will be made in USDT, USDC, and other stablecoins compliant with MiCA regulations, alongside BDAG tokens, empowering developers to build, grow, and succeed. Early stage and even retrospective projects will be welcome, ensuring no great ideas go unnoticed. Applications will open early in 2025 and will be evaluated on innovation, feasibility, and impact.

Hackathons

Launching in 2025 these virtual, high-energy events are perfect for venture-ready EVM teams. Teams get to pitch their ideas to top investors, showcasing their innovation and skills, and compete for cash prizes.
Successful projects will be invited to launch on the BlockDAG network, and may even qualify for fast tracking through the grants program.

Team

Antony Turner
CEO / Founder

Jeremy Harkness
Chief Technology Officer

Dr. Prof. Youssef Khaoulaj
Chief Security Officer

Steven Clarke
Senior Advisor

Dr. Maurice Herlihy
Blockchain Advisor

Website & Social Media

BlockDAG

https://blockdag.network

Medium

X (Twitter)

Facebook

Discord

Telegram

YouTube

Instagram

Legal Disclaimer

1. Disclaimers and Limitations of Liability
To the fullest extent permissible by the applicable law, the issuer of the BDAG Token and any of their subsidiaries, affiliates, and licensors, and their respective employees, agents and contractors make no express warranties and hereby disclaim all implied warranties (including, without limitation, regarding any crypto tokens, smart contract, etc.), including the implied warranties of merchantability, fitness for a particular purpose, non-infringement, correctness, accuracy, or reliability. Nor does the issuer of the BDAG Token provide any warranties over any third-party services such as wallets, or marketplaces which you may use to access the BDAG Token. You accept the inherent security risks of providing information and dealing online over the internet.

The issuer of the BDAG Token will not be responsible or liable to You for any losses You incur as the result of your use of any blockchain network or any digital and/or electronic wallet, including but not limited to any losses, damages or claims arising from: user error, such as forgotten passwords or incorrect smart contracts or other transactions; server failure or data loss; corrupted wallet files; or unauthorised access or activities by third parties, including but not limited to the use of viruses, phishing, bruteforcing or other means of attack. Crypto tokens are intangible digital assets that exist only by virtue of the ownership record maintained on the Blockchain. All smart contracts are conducted and occur on the decentralised within the blockchain, which is early stage and/or experimental technology. The issuer of the BDAG Token makes no guarantees or promises with respect to smart contracts. The issuer of the BDAG Token is not responsible for losses due to blockchains or any features of or related to them or any electronic and/or digital wallet.
The issuer of the BDAG Token and their subsidiaries, affiliates, and licensors, and their respective employees, agents and contractors, will not be liable to You or to any third party for any indirect, incidental, special, consequential, or exemplary damages which you may incur, howsoever caused and under any theory of liability, including, without limitation, any loss of profits (whether incurred directly or indirectly), loss of goodwill or business reputation, loss of data, cost of procurement of substitute goods or services, or any other intangible loss, even if they have been advised of the possibility of such damages.

You agree that the issuer of the BDAG Token's total, aggregate liability to you for any and all claims arising out of or relating to the BDAG Token, is limited to the amounts You actually paid the issuer of the BDAG Token in the twelve (12) month period preceding the date the claim arose. The issuer of the BDAG Token sold the purchased BDAG Token in reliance upon the warranty disclaimers and limitations of liability set forth herein, which reflect a reasonable and fair allocation of risk and form an essential basis of the bargain. Some jurisdictions do not allow the exclusion or limitation of incidental or consequential damages, and some jurisdictions also limit disclaimers or limitations of liability for personal injury from consumer products, so the above limitations may not apply to personal injury claims.

2. Governing Law and Jurisdiction
Any action related will be governed and interpreted by the Laws of the Seychelles, and shall, in the case of any legal action, be subject to the exclusive jurisdiction of the Seychelles, and You waive any objection to this jurisdiction and venue.

3. Arbitration
You and the issuer of the BDAG Token agree that any and all disputes arising out of or in connection with the BDAG Token will be resolved exclusively by means of individual arbitration. You and the issuer of the BDAG Token agree that such disputes will be settled in accordance with the Centre for Effective Dispute Resolution ("CEDR") Model Mediation Procedures, and a mediator shall be nominated by the CEDR. You and the issuer of the BDAG Token are waiving your rights to normal recourse to the Courts of Law.

4. No Class Action
You and the issuer of the BDAG Token agree that any claims brought against each other will be brought in their own individual capacity, and not as a member of a class of claimants in any legal action.