









NIGHTPAPER

A litepaper introducing **Midnight**

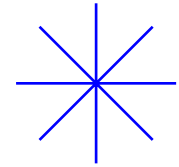
Legal Disclaimer

The Nightpaper outlines current plans regarding the Midnight Network, which could change at its discretion. The information contained herein is for informational purposes only and should not be relied upon for investment decisions.

Table of Contents

	Executive Summary The Midnight Network Use Cases	3
	Token Utility	8
	Architecture Lightweight Design Powerful, Flexible & Interoperable Compact Language	10
	Ecosystem Developers Block Producers App Operators	12
	Roadmap	13
	Further information	14

Executive Summary



Developers are facing decision fatigue regarding the best ways to manage the volumes of data transiting through their applications and databases. Customers demand more control and ownership over their data and intellectual property, while businesses who look to both protect and monetize data face increasing liability from leaks and breaches that risk exposing their sensitive data and IP. This creates a vast web of complexities that leave consumers vulnerable, innovators without a path to entry, and a handful of institutions with disproportionate control and profit power facing ballooning costs and dissatisfied customers.

These challenges lead businesses to explore blockchain technologies, which incorporate a distributed ledger architecture and decentralized applications (“apps”) as a framework to store and process data. Such capabilities address the mix of ownership and utilization, delivering significant security, integrity, and scalability. However, foundational business needs around data protection, service uptime assurance, and cost control went unmet. This has resulted in businesses relegating the adoption of blockchain technology to a select few niche use cases.

The Midnight network (“Midnight”) exists to remove the barriers preventing organizations and service providers from leveraging blockchain technology while offering programmable data protection with selective disclosure. This will enable the creation of new application designs, business models, and revenue streams without requiring developers to amass large amounts of unrelated user data or risk exposure of their customers' or businesses' data to retain its utility. **The Midnight network resolves the business challenge of choosing between data protection, ownership, and utilization.**

— Introduction

The Midnight Network

Midnight is a new generation of blockchain technology. It enables apps that protect user, commercial, and transaction metadata. Its zero-knowledge (“ZK”) proofs offer utility without compromising data protection or ownership.

In addition to providing a transformative approach to data governance, Midnight empowers organizations to monetize their business intelligence without revealing the underlying data. Midnight further improves existing blockchain technologies by addressing key pain points of developers, operators, and ecosystem participants. To help it launch quickly and establish enterprise-grade operations, Midnight formed a strategic relationship with Cardano, a well-established, secure, and mature network, as its launch partner.

For app developers:

1. Learnable

Midnight’s TypeScript smart contracts framework alleviates the need to learn and maintain code that requires niche programming language skills. As of H1/2024, TypeScript is the 2nd most popular programming language.

2. Versatile

Midnight’s ledger supports shielded and unshielded data primitives, enabling developers to exercise selective disclosure. It also offers programmable data protection for advanced use cases, such as helping meet business policies and/or regulatory requirements.

3. Composable

Midnight is a Layer 1 privacy-preserving blockchain that uses TypeScript APIs for easy integration with existing systems. Its ZK architecture (based on BLS12-381 curves) can produce BLS-type (Barreto-Lynn-Scott) proofs and integrates with other chains through its Partner-Chains infrastructure, particularly with Cardano.

4. Scalable

Midnight’s ZK architecture uses Kachina-based research technology, which allows for specific (rather than generalistic) types of ZK circuits. Multiple apps may run simultaneously on the same chain with lower transaction contention, leading to a much larger scale and efficiency when operating in a commercial environment.

For app operators:

1. Protected

Unlike other public blockchains, which expose every element, Midnight can protect data and metadata, enabling businesses to protect their customers without compromising sensitive data security or disclosing activity.

2. Stable

Midnight offers predictable transaction pricing by utilizing a stable resource (separate from Midnight's native token) to operate the chain. Businesses can budget the expected costs of using Midnight as infrastructure for their apps and potentially use FIAT (in addition to using tokens) as payment.

3. Compliant

Midnight's architecture and features strive to empower app operators to comply with evolving regulatory requirements and business policies. Apps can enact selective and/or programmatic disclosure to unveil appropriate data sets to meet business policies and regulatory requirements as applicable to the type of activity, content, and jurisdiction in which they operate.

For Ecosystem participants:

1. Network Security

As a launch partner, Cardano Stake Pool Operators (SPOs) help secure Midnight's block production. This enables Midnight to provide a secure, decentralized framework, establishing an enterprise-grade infrastructure.

2. Data Security

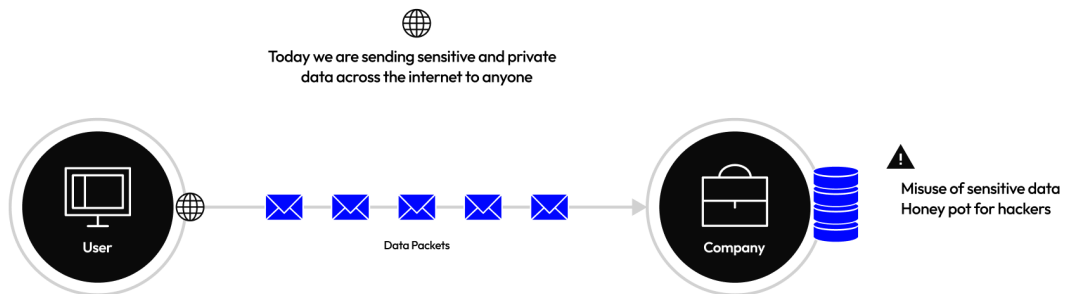
Midnight's architecture stores private data locally on the user's machine. This decentralizes sensitive data across many nodes, making data breaches harder and less frequent than centralized data stores (such as databases).

3. Interoperable

The Midnight roadmap includes support for modular app architectures, allowing developers to benefit from Midnight's data protection to create hybrid apps that continue to leverage their native chains' key capabilities and transaction settlement.

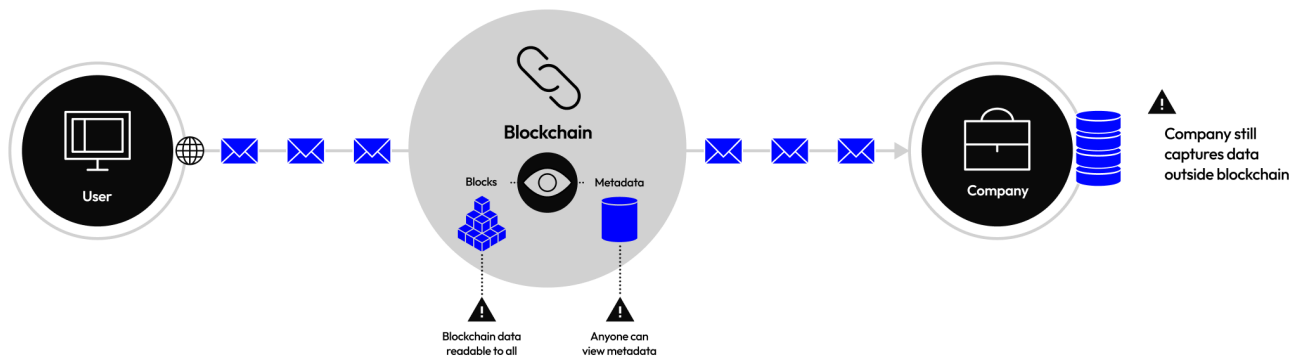
Regular Apps

Today we are sending sensitive and private data across the internet to anyone



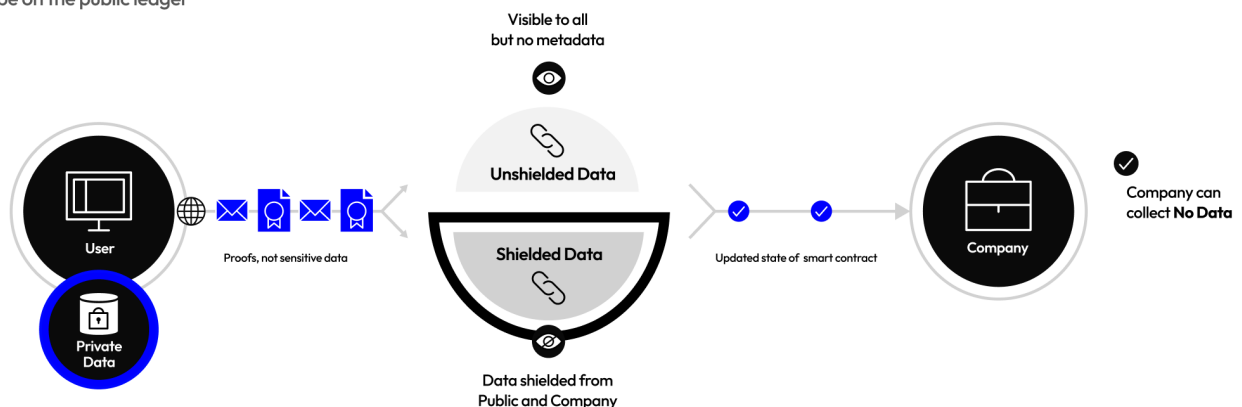
Public Chain DApps

With DApps, you're often still sending sensitive data, and also adding public metadata that people can correlate to find out more about your activities



Midnight DApps

Midnight shields your data, using proofs, with no metadata created on-chain, unless you choose it to be on the public ledger



— Introduction

Use Cases

Midnight is ideal for any use case requiring data and/or metadata protection. Its distributed ledger architecture increases data security and enables self-custody. Its ZK capabilities enable scenarios where attestation about the underlying data is required without revealing the actual information to the querying party. These features are essential to enable innovation in use cases such as:

→ **Digital Identity**

Midnight can enable secure and selective attestation of digital identity (ID) documents and credentials, such as a digital driver's license for age verification, education certificates for employment qualification, or credit history for a loan, without exposing irrelevant sensitive information (e.g., exact birthday, home address, income, etc.). This makes digital IDs more usable and could elevate DEXs (decentralized exchanges) compliance via secure KYC capabilities.

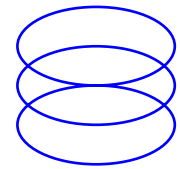
→ **Asset Tokenization**

Midnight protection of data and metadata can help facilitate the tokenization of on-chain and off-chain assets (e.g., Real World Assets (RWA)). Asset ownership certification can live on-chain without compromising the owner's identity, the asset's details, or asset-related activity. This can enable the migration of real-world assets such as real estate, artwork, raw materials, and music licensing into digital forms, opening up possibilities for new economic models.

→ **Balloting**

Midnight can help create fraud-resistant preference reporting systems (e.g. surveying, polling, voting) for member-based organizations, which can prove eligibility and participation status without disclosing personal information or recording individual choice.

Token Utility



Like other blockchain ecosystems, Midnight's token primarily secures its network, helps ensure uptime, and allows the network to be self-sustaining. Most blockchains require a fee, commonly called *gas* or *fuel*, to process and/or prioritize transactions. This tokenized energy is often reallocated to the network's operators as rewards. This *fuel* is usually an unshielded token, which exposes transaction details and users' identities. Blockchains that elect to use shielded *fuel* (to protect metadata) struggle to have such tokens listed due to regulatory concerns. This reduces block rewards liquidity, which deters ecosystem participation and lessens network security.

Midnight innovates by using two (2) tokenized assets working together:

→ **NIGHT**

an unshielded token for governance, consensus participation, and block production rewards.

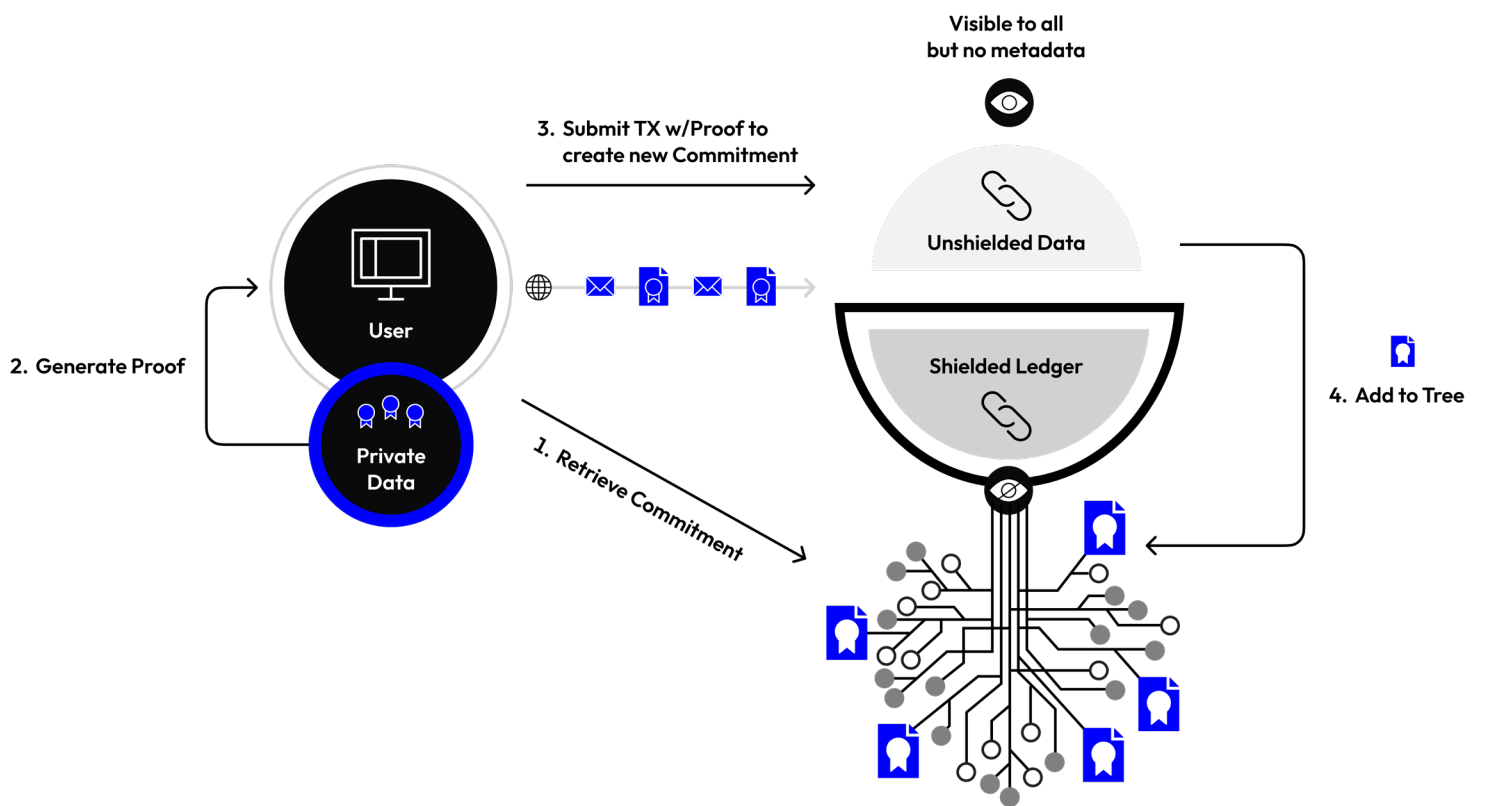
→ **DUST**

a capacity access shielded resource that operates the chain activity (the *fuel*).

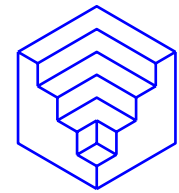
The unshielded token, NIGHT, has a fixed supply and deflationary policy. As an unshielded token, NIGHT is easily accessible and helps ensure network security by operating as the reward token for its block producers. NIGHT will initially exist as a Cardano native asset (CNA), benefiting from Cardano's trusted infrastructure and ecosystem activity. NIGHT will also offer extended functions such as network governance.

Midnight's transaction energy, DUST, is a capacity access shielded resource used to facilitate transactions on the network and ensure that transaction metadata is protected to prevent correlation. DUST behaves like energy in the physical world as it decays over time (i.e., it has value but cannot store value). However, it is continually replenished as a pool of NIGHT generates energy to maintain a proportional supply. DUST cannot be transferred, thus addressing regulatory concerns that are commonplace with shielded tokens or assets. The intent of this design is to maintain the predictability of fees for those transacting on the network.

A future paper, to be released after this paper, will discuss the relationship between NIGHT, DUST, and the Midnight network in more detail.



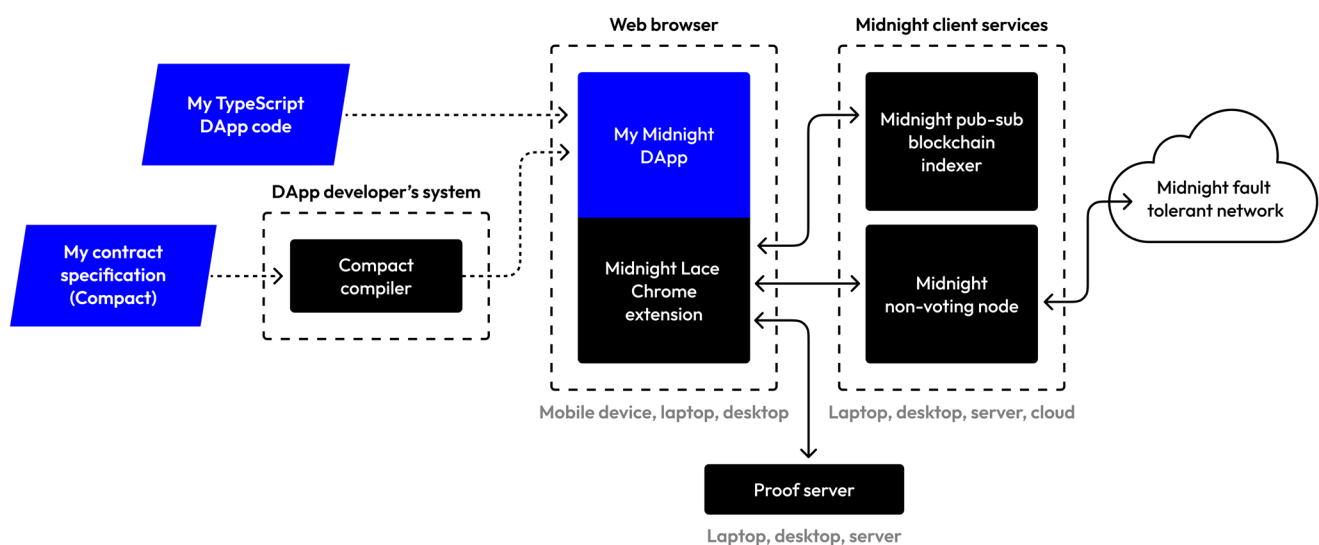
Architecture



Lightweight Design

To ensure the Midnight network is easily accessible to a large cohort of developers and enable easy prototyping, Midnight uses TypeScript (a widely known programming language) API definitions for smart contract integration and a Typescript-based domain-specific language (“Compact”) to describe contracts.

Midnight’s unique architecture uses the Compact programming language to segregate the application layer from the data layer, abstracting the app’s smart contract code from computationally intensive cryptographic operations. This allows the network to maintain security, transparency, and data protection without requiring developers to understand the intricacies of (ZK) technology. Compact gives the developer the tools to preserve privacy and include libraries for a web-based user interface.



Powerful, Flexible & Interoperable

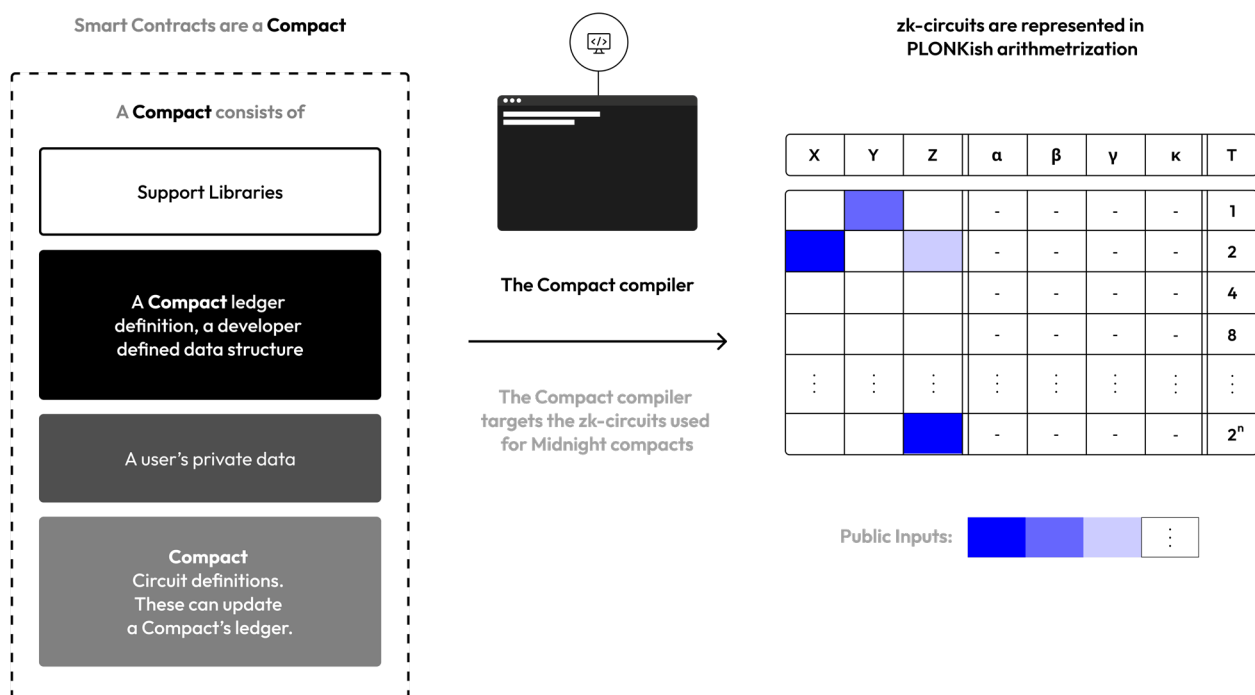
Midnight's ZK technology (based on zkSNARKs using the Halo2 framework) enables succinct proofs that support efficient verification, attestations, and trustless transfers. Midnight leverages the well-established Halo2 framework with BLS12-381 curves to support recursion and cross-chain integration with non-ZK blockchains (such as Cardano and Ethereum.) The platform is designed to support privacy-preserving smart contracts with recursive proof capabilities, and broader multi-chain interoperability through hybrid applications.

Compact Language

The Compact language supports developers who require data protecting and general-purpose smart contract functionality without sacrificing decentralization characteristics¹. Its unique properties empower a large class of distributed computations that benefit from data protection guarantees without additional trust assumptions. It provides an environment capable of leveraging tools for computationally hard or storage-intensive operations outside the zero-knowledge proof, enabling simple integration with the web.

Compact allows smart contracts to bridge public and private data. Data owners (with access to private data) can use Compact smart contracts to interact with both the on-chain public state and the off-chain (e.g., local machines or server) private state. Other parties can use Compact smart contracts to interact only with the public state in a permissible way. Using zero-knowledge SNARK² proofs, a Compact smart contract can attest to the private data correctness maintained by the user. This allows all users of the Midnight blockchain to transact and keep sensitive data secret.

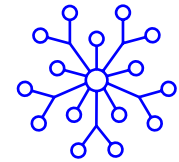
The Compact compiler generates cryptographic materials and circuit descriptions needed for zero-knowledge proofs, which enforce the terms of a smart contract while shielding private data. The architecture makes various deployment options available to shield private information.



¹ <https://www.research.ed.ac.uk/en/publications/kachina-foundations-of-private-smart-contracts>

² <https://z.cash/learn/what-are-zk-snarks>

Ecosystem



Successful ecosystems provide benefits and incentives to a wide spectrum of participants. Midnight builds upon and expands on concepts introduced and battle-tested by existing blockchain ecosystems to be interoperable, where applications, settlement layers, roll-ups, bridges, and other functionality are interconnected.

Developers

Midnight's technology stack is designed to attract and retain a broad base of developers who will build applications or services that leverage data protection capabilities. Midnight aims to:

1. Minimize developers' learning curve by adopting TypeScript programming language structure and APIs as the development framework.
2. Simplify building and deploying applications and services by providing tooling, development environments, and support frameworks.
3. Streamline integration with other products and blockchains by supporting industry-accepted integration interfaces and tools.

Midnight's Documentation³ offers tutorials and building blocks to expedite development, removing the requirement to understand zero-knowledge to leverage its capabilities.

Block Producers

Midnight's consensus mechanisms and block production are designed to appeal to a diverse pool of blockchain network validators or block producers to ensure the network is secure and decentralized. Midnight aims to:

1. Simplify block production incentives by offering NIGHT tokens as rewards.
2. Offer easy on-ramp to become a block producer. Cardano Stakepool Operators (SPOs) will form the initial producers via a simple software package update.
3. Interoperate with other chains. Midnight's roadmap includes a novel multi-resource consensus, enabling validators from different blockchain networks to produce blocks on Midnight.

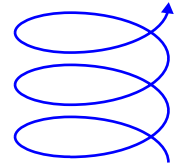
App Operators

App Operators benefit from tools and primitives that help them monitor operations and apply business policies, such as meeting regulatory requirements. Midnight aims to:

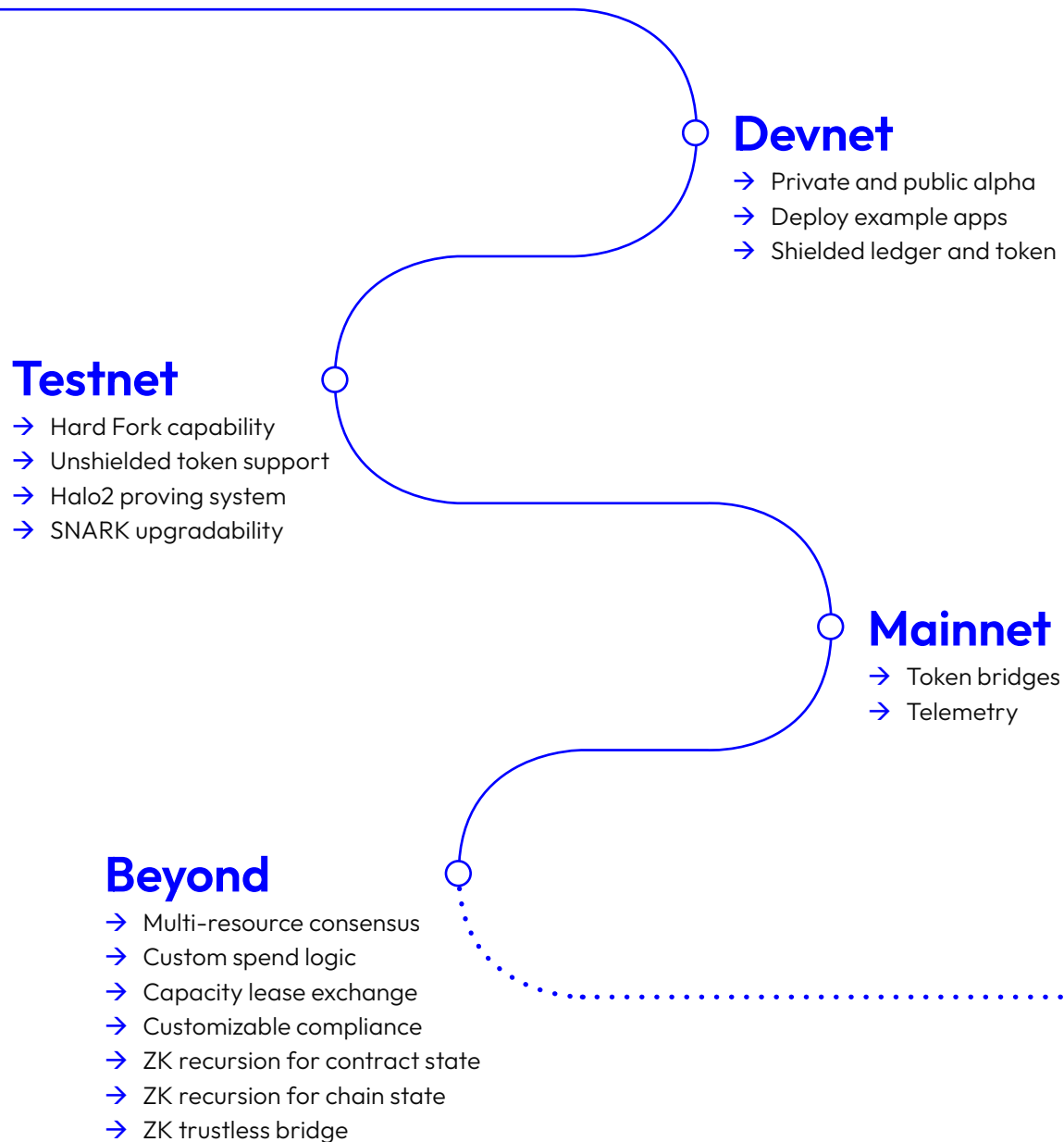
1. Integrate with forensic and blockchain intelligence offerings. This enables seamless integration into existing compliance frameworks for app operators and market players who already utilize such tools.
2. Offer programmable data protection, enabling audit of certain activities without exposing the underlying data to third parties.
3. Provide tooling (e.g. block explorer, performance measurement tools, monitoring tools, and more) to streamline app operations.

³ Midnight Documentation is available at <https://docs.midnight.network>

Roadmap



Midnight technology will be released via a staged approach:





**Learn more about Midnight,
access the codebase, and engage
with the community via:**

 midnight.network

 docs.midnight.network

 [@MidnightNtwrk](https://twitter.com/MidnightNtwrk)

 discord.com/invite/midnightnetwork