

Agoric Token and Crypto Economy White Paper

Version 1.1
August 2022

CRYP2NOVA

https://agoric.com

Dean Tribble, CEO
tribble@agoric.com

Archived copy · cryp2nova.com

1.0 Introduction

The Agoric crypto economy is *the* smart contract platform that can quickly bring millions of developers to the DeFi frontier. Agoric's Hardened JavaScript makes blockchain programming safe and accessible to the 10+ million JavaScript developers. Hardened JavaScript provides a safe, stable environment that developers need in order to build, deploy, and operate sophisticated Dapps, NFTs, and DeFi markets.

The Agoric public blockchain, part of the interchain ecosystem, is designed to mitigate novel risks posed by decentralized financial systems built upon Proof of Stake (PoS) consensus. Moreover, the Agoric programming model, supported by our native market infrastructure, will enable the formation of a cryptoeconomic standard library with the same exponential composability that led to the explosive growth of the Node.js, React.js, and other JavaScript ecosystems.

The design of the Agoric public blockchain benefits from over 30 years (Miller & Drexler, 1988) of deep expertise and experience in building distributed electronic markets, financial services, and providing smart contract risk management to deliver a wide-ranging foundation for financial applications.

1.1 The Agoric solution

The Agoric crypto economy integrates innovative technology with a proven consensus protocol to provide a solid foundation for DeFi.

The Agoric chain is fast and predictable

- **Fast**: Uses the high-performance Tendermint consensus protocol with fast finality, quickly guaranteeing that chain transactions will not be reversed or changed.
- **Predictable**: Improved gas economics removes incentives to game gas prices, letting users better express trade-offs between price and urgency.

The Agoric developer experience is familiar, secure, and composable

- **Familiar**: Program in JavaScript, the most widely-used programming language. Agoric has added enhanced security, determinism, and asynchrony features to JavaScript to meet smart contract development's unique demands.
- **Secure**: Our robust *Object-Capability (OCap)* security model provides multi-layer defense in depth, with better separation and containment of risk—a critical foundation for DeFi markets.

Archived copy · cryp2nova.com

- **Composable**: Our high-level *ERTP (Electronic Rights Transfer Protocol)* token standard enables developers to rapidly build smart contracts from reusable components. The growing library of components uniformly supports diverse types of digital assets and contracts, including fungible tokens, NFTs, and remote assets from other chains.

The Agoric chain *and* economy are built for growth

- **First-Class DeFi**: The built-in *Zoe* contract framework along with the integrated stable token and automated market maker (AMM) empowers DeFi developers to quickly launch robust DeFi protocols.
- **Extensible**: As the blockchain space evolves, both *proof of stake (PoS)* and governance are subject to rapid iteration. By implementing chain governance and staking economics as smart contracts, we can extend them to meet future needs.
- **Interoperable**: We are rapidly evolving into a world with many interacting blockchains. *Dynamic IBC* lets the Agoric chain make use of other chains' assets, collateral, and services.

2.0 The Agoric Tokens

The *Agoric tokens* connect internal transactions in the Agoric ecosystem with global capital markets, computation resource markets, and user demand.

The Agoric chain features two native tokens:

- *IST,* an IBC-enabled stable currency designed to maintain parity to the US dollar (USD). IST provides a local medium of exchange to facilitate transactions, as well as a stable token for the entire IBC ecosystem.
- *BLD,* a staking token supporting economic activity within the Agoric ecosystem. It ensures the chain's security increases in tandem with the network's economic activity.

2.1 Overview

The Agoric chain has three tightly-coupled systems:

- **The Dapp Economy** is where value creation occurs. Market participants transact with each other, have the ability to create digital assets (fungible and non-fungible), build new Defi protocols, and connect DeFi components.

Archived copy · cryp2nova.com

- **Inter Protocol** mints IST, the local stable currency. All protocol fees, including execution (gas) fees, are paid in IST. IST provides users with a medium of exchange, unit of account, and store of value.
- **The Staking Economy** is where BLD holders (the BLDer DAO) stake their tokens with *validators* to ensure the Agoric chain's security and ongoing operation. Each transaction that occurs on the Agoric blockchain must be executed and confirmed by the set of independent validators. Stakers delegate their BLD to validators to incentivize correct execution.

  Staking tokens give validators the right to participate in the network by validating transactions, and participate in chain governance. Stakers earn rewards for securing the network. Misbehaving validators have their stakes slashed.

These systems work together to ensure a vibrant crypto economy, where economic activity secures, stabilizes, and rewards participants in the network.

2.2 Inter Protocol

Inter Protocol is governed by BLD holders (the BLDer DAO), and implemented as a set of smart contracts on the chain. Inter Protocol links activity on-chain to the ongoing operation and security of the chain. The BLDer DAO determines the acceptable collateral types, rules of IST issuance, and other parameters via an economic committee and improvement proposals.

Participants borrow IST by depositing digital collateral in user-controlled vaults and minting IST against that collateral. IST is collateralized by certain digital assets, such as ATOM, ETH, or USDC, as determined by the community through governance subject to risk assessment and legal limitations. IST's value is designed to maintain parity with the US dollar (USD). Movements away from that 1:1 exchange rate can be profitably traded by participants to bring the price back towards one dollar.

Users can borrow and repay IST on demand. Borrowers pay a stability fee denominated in IST, which is used to reward stakers. The more economic activity on the chain, the more demand for IST. This generates additional fees which ensures that network security and economic stability scale with economic activity.

The IST protocol includes an integrated *automated market maker (AMM)*. The AMM lets participants directly trade assets for IST. It also helps maintain parity with the dollar by providing on-chain liquidity and price discovery in IST-collateral pairs.

In addition, the local AMM supports *automated liquidation* of collateral. Automated liquidation happens if the collateral's value falls below the governance-determined collateralization ratio.

Archived copy · cryp2nova.com

2.3 Paying for execution

Market participants pay their fees in IST. Execution on-chain is metered, protecting against spam, and preventing runaway programs that take an unreasonable or unbounded time to finish. This also ensures that code executed on-chain pays for its share of the computational resources used. In addition, participants can bid for scheduling priority.

2.4 BLD, the staking token

The BLD token is used for staking and governance. The BLD holders stake their BLD tokens with validators to earn rewards for helping to secure the chain's operation.

2.5 Stakers

Token holders support the chain's security by *staking* their tokens to specific designated validators. Stakers receive rewards and penalties (including slashing) according to their designated validators' performance. Validators may charge a commission on a delegated stake.

There is an *unbonding* period before stakers are able to withdraw their tokens. At the beginning of each epoch, stakers may redelegate to a new validator or withdraw their stake. However, their stake is still at risk from slashing due to misbehavior by the former validator during their unbonding period. Stakers that wish to unbond must wait for the unbonding period to finish before receiving their tokens subject to slashing.

The BLD Boost contract is an optional component of Inter Protocol that allows stakers of BLD to borrow IST against their future staking rewards, providing liquidity to stakers while maintaining chain security. Stakers may borrow a limited amount of IST by reserving a portion of their staked BLD. Governance-defined parameters determine how much BLD needs to be reserved and the amount of IST that can be borrowed against it.

The BLD remains staked and continues to earn staking rewards, but borrowers must repay the loan plus interest before unbonding their BLD or withdrawing their staking rewards.

2.6 Governance

The community actively participates in the on-going evolution of the Agoric chain by participating in on-chain governance. Governance decisions are determined by BLD holders through token votes.

2.7 Validators

Validators enable safe execution of smart contracts in a stable economy. They are responsible for correctly running the chain software's latest version, staying online to participate in *consensus*, and ensuring their private keys' safety. They should also participate in chain

Archived copy · cryp2nova.com

governance actively. They receive a reward for their participation and risk slashing if they negatively impact the system.

The Agoric chain uses the Tendermint Core engine for consensus. Validators earn rewards for validating and producing blocks. Active validators get block rewards distributed among them based on their relative stake.

The system will penalize any misbehaving validator. Any validators proven to have *equivocated (double-signed)* will see their stake (and the stake delegated to them) slashed by the chain. Equivocating validators are also promptly removed as active validators by chain.

The system also penalizes unavailable validators. They will not receive block rewards for blocks when offline or when they otherwise don't participate in the consensus process. Additionally, the system will temporarily remove validators if they are unavailable for a governance-determined percentage of created blocks within a sliding window.

2.8 Fees and incentives

The Agoric chain tightly couples its consensus layer and smart contract layer, bringing greater flexibility, improved incentives, and better capital efficiency to Proof of Stake.

All protocol-level fees are paid in IST. These include stability fees paid by IST borrowers, protocol fees paid by AMM traders, and execution fees paid by users of smart contracts and Dapps.

Stakers and validators are rewarded initially through new issuance of BLD. As economic activity on the chain matures, staking rewards will increasingly come from the protocol-level fees paid in IST. Protocol fees generated by economic activity on the chain are deposited into a reward pool that are distributed to stakers.

CRYP2NOVA

3.0 The Agoric Technology Stack

The Agoric technology stack integrates proven *Byzantine Fault Tolerance* (BFT) consensus with a distributed, secure, virtual machine architecture that supports our advanced smart-contract framework and robust crypto economy. It provides a secure foundation for the new forms of voluntary cooperation made possible by blockchains.

The Zoe Smart Contract Framework

- **ERTP**: Agoric's Electronic Rights Transfer Protocol provides a standard way to create and exchange fungible and nonfungible digital assets, making it easy to create complex digital assets that are immediately tradable and composable. ERTP enables higher order

Archived copy · cryp2nova.com

composition of smart contacts, enabling reuse of market institutions. With ERTP, developers can easily represent digital assets and cryptoeconomic abstractions in a standard way, speeding up development and mitigating security hazards.

- **Zoe**: Zoe is our framework for writing smart contracts using JavaScript. Developers can focus on their applications' economic logic, letting Zoe handle the escrowing of user assets. It enforces offer safety and payout-liveness guarantees, so users either get what they wanted from a transaction or get back what they offered. This significantly reduces the risk to contract parties.

- **System-defined contracts:** The blockchain itself leverages Zoe's power and flexibility to implement governance, staking, staking derivatives, and other cryptoeconomic primitives. User-defined smart contracts can reuse these contract components, which can be made available to other developers.

The Agoric VM

- **Secure JavaScript runtime**: The Agoric VM provides a secure, distributed JavaScript runtime which enforces OCap for safe composition and code reuse. Currently, DeFi Dapps mainly consist of web2 front-ends built in JavaScript connected to web3 smart contract backends built in Solidity, with no consistent connection framework. Agoric brings the dominant web2 programming language, JavaScript, to blockchain. Front-end developers get a safe and familiar language to work in. Back-end smart contract developers get to code in a secure, deterministic, and asynchronous language. We've made JavaScript safe for blockchains, which leverages its millions of experienced programmers, mature tooling ecosystem, and many reusable libraries and packages for DeFi development.

- **Object-Capability (OCap) security**: The key to making JavaScript safe for blockchains is our OCap security architecture (Miller, 2006). OCap is a battle-tested security model used in secure operating systems (Heiser & Elphistone, 2016). *Hardened Javascript*, developed by Agoric, is a standards-track JavaScript subset that enforces object capability security. OCaps provide fine-grained permissions that support the partitioning and managing of risk. The Ocap approach takes encapsulation seriously, recognizing that encapsulation plays the same role as property rights. Encapsulation of objects ensures that the object's state cannot be tampered or interfered with by others. Message passing between objects ensures that communication rights are similarly controlled and transferable only by mutual consent. The Agoric distributed programming model extends the OCap security architecture across systems, providing a

Archived copy · cryp2nova.com

consistent model for front-end developers and enabling secure, asynchronous programming between chains.

- **Exponential composability**: In large part, JavaScript's popularity was driven by the power of composition. The Node.js 2010 launch with *npm*, *the node package manager* created a culture of reuse. As of June 2021, more than 800,000 reusable npm packages were downloaded over a billion times a day. Ninety-seven percent of modern web application code is from reusable packages; only 3% is newly written code. While dependence on other people's code greatly increases productivity, it introduces security risks. OCap uniquely enables safe composability bringing npm-style reusability to the blockchain.

Best-in-class blockchain technology

- **Cosmos/Tendermint**: The Agoric VM is architected independently of the underlying consensus protocol, so the Agoric chain can run on the best available consensus engine. The Agoric chain will initially launch as part of the Cosmos ecosystem, as a sovereign blockchain built on the Tendermint consensus engine. Tendermint is a proven Byzantine Fault Tolerance (BFT) consensus engine providing fast throughput and finality.

- **Dynamic IBC:** The Inter-Blockchain Communication protocol (IBC), co-developed by Agoric, lets the Agoric programming model operate across chains. IBC gives Agoric chain users access to the protocols, liquidity, and assets based in the Cosmos ecosystem and beyond (current projects are underway to connect to Polkadot via IBC and to peg assets from Zcash, Ethereum, and Bitcoin). IBC provides a bridge to bring external financial assets onto the Agoric chain for participating in DeFi protocols, collateralizing loans, staking, and participating in trade and related transactions. It also makes Agoric assets and smart contracts available to other chains.

The Agoric chain supports the creation and exchange of a wide range of digital assets while providing ease of programming, safety guarantees, composition, and interoperability between chains. As a result, it makes an ideal platform for a wide variety of DeFi use cases from automated market-makers (AMMs) to sophisticated derivatives markets.

Archived copy · cryp2nova.com

Acknowledgments

Many thanks to Jason Potts, Joseph Clark, Sinclair Davidson, and Chris Berg—our economic advisors from RMIT University—and Zaki Manian for their ongoing contributions and insight. We also thank the experts from our extended community who joined us for our token jams, Dan Robinson, James Prestwich, Sunny Aggarwal, and Ethan Buchman. Finally, thanks to our extended team and investors, especially Zooko Wilcox, Miko Matsumura, Jacob Phillips, and Ben Perszyk, and the team at McDermott. Your contributions help make the world of DeFi more exciting and less dangerous.

Archived copy · cryp2nova.com

LEGAL DISCLAIMER

NOT AN OFFER TO PURCHASE OR SELL SECURITIES. This document is for informational purposes and is not an offer to sell or a solicitation of an offer to buy any securities in Agoric Systems, LLC, or any other securities and may not be relied upon in connection with the purchase or sale of any security. Interests in Agoric Systems, LLC, if offered, will only be available to parties who are "accredited investors" (as defined in Rule 501 promulgated pursuant to the securities act of 1933, as amended) and who are interested in investing in Agoric Systems, LLC on their own behalf. Any offering or solicitation will be made only to qualified prospective investors. Any offering of other securities will be made in compliance with all applicable laws.

Prospective purchasers should not construe the contents of the document as investment, legal, tax or other advice. Each investor should conduct its own due diligence and consult its own advisors as to the system described herein , including all legal, tax and related matters.

This document includes statements that are, or may be deemed, ''forward-looking statements." In some cases, these forward-looking statements can be identified by the use of forward-looking terminology, including the terms "believes," "estimates," "anticipates," "expects," "plans," "intends," "may," "could," "might," "will," "should," "approximately," "potential" or, in each case, their negative or other variations thereon or comparable terminology, although not all forward-looking statements contain these words. These forward-looking statements are based on assumptions and assessments made by management in light of their experience and their perception of historical trends, current conditions, expected future developments, and other factors they believe to be appropriate. Because such statements deal with future events and are based on current expectations, they are subject to various risks and uncertainties and actual results, performance or achievements could differ materially from those described in or implied by the statements in this document. Important factors that could cause actual results, developments, and business decisions to differ materially from those anticipated in these forward-looking statements include, among other things: the overall global economic environment; the impact of competition and new technologies; general market, political, and economic conditions; projected capital expenditures and liquidity; changes in strategy; government regulations and approvals; litigation and regulatory proceedings. By their nature, forward-looking statements involve risks and uncertainties because they relate to events, competitive dynamics, and regulatory developments and depend on the economic circumstances that may or may not occur in the future or may occur on longer or shorter timelines than anticipated. Although Agoric believes that it has a reasonable basis for each forward-looking statement contained in this document, it cautions you that forward-looking statements are not guarantees of future performance and that actual results of operations, financial condition and liquidity, and the development of the industry in which it operates may differ materially from the forward-looking statements contained in this document. In addition, even if results of operations, financial condition and liquidity, and the development of the industry in which it operates are consistent with the forward-looking statements contained in this document, they may not be predictive of results or developments in future periods. Any forward-looking statements in this document speak only as of the date of such statement, and no obligation is undertaken to update such statements to reflect events or circumstances after the date of this document.

Archived copy · cryp2nova.com