

REDBELLY

Cryp2Nova

White Paper

Version 1.4.3

Archived copy · cryp2nova.com

Disclaimer

You must read this page (“Disclaimer”) before reading or making any use of this document or any information contained within this document.

This document is issued by Redbelly Network Pty Ltd (ACN 640 415 069) of 304/74 Pitt St, Sydney, NSW, 2000, Australia (“Redbelly”); and is solely for informational purposes. By reading this Disclaimer, you are acknowledging that you have read the terms and conditions of this Disclaimer, and agree to be bound by the terms and conditions of this Disclaimer, including any future modifications of this Disclaimer.

This document is not a draft disclosure document or a pathfinder document for the purposes of section 734(9) of the Corporations Act 2001 (Cth). This document is not a prospectus, product disclosure statement or a disclosure document for the purposes of the Corporations Act 2001 (Cth). This document has not and will not be lodged with the Australian Securities and Investments Commission.

This document does not contain all of the information which would be required to be disclosed in a prospectus. Neither Redbelly nor any of its officers, employees, related bodies corporate, affiliates, agents or advisers guarantees or makes any representations or warranties, express or implied, as to, or takes responsibility for, the accuracy, fairness, reasonableness, correctness or reliability of any information contained in this Document.

Redbelly does not represent or warrant that this document contains all material information about Redbelly or which a prospective investor may require in evaluating a possible investment in Redbelly by acquisition of shares in Redbelly. You must conduct your own independent investigations and enquiries as you deem necessary.

Any timeframes provided by the Redbelly within this document are estimates and are subject to change without notice. This includes, but is not limited to: the future development of the Redbelly product, the token, the listing of the token on the public market, and the applications that may use the Redbelly product.

Before making any investment, investors are advised to take their own independent accounting, taxation, legal and any other advice appropriate to your jurisdiction. No person mentioned in this document will offer or may be construed as offering, advice to any potential investor of Redbelly.

Archived copy · cryp2nova.com

Summary

The Redbelly Network is a revolutionary open finance platform that embeds distributed ledger technology into the heart of financial relationships. This eliminates information asymmetry and dramatically increases efficiency, helping to build a fairer financial system for all.

With a novel leaderless consensus mechanism, democratic byzantine fault tolerant (DBFT) consensus developed with The University of Sydney and CSIRO's Data61, we are able to achieve high performance, and guarantee the impossibility of forking and mitigate double spending with near instant finality.

The Redbelly Network is designed to focus on accountability. Accountability is enforced at a protocol level through a novel mechanism that constructs undeniable proofs of fraud - Polygraph; and at the functional level through an innovative identity layer that ensures all network participants are known. Through standards-based smart contract templates, real world financial relationships are deployed as Ricardian contracts on The Redbelly Network, thereby benefiting from reduced information asymmetry, huge gains in efficiency, low and known transaction costs, as well as the accountability afforded by legal and regulatory enforcement that is required for any real world financial relationship.

This paper details the purpose of the Redbelly Network, describes its infrastructure topology, and gives an overview of supporting infrastructure crucial to its success.

CRYP2NOVA

Archived copy · cryp2nova.com

The Redbelly Network Overview **5**
The Problem 5
A lack of accountability 5
The importance of regulation 6
The Solution 7
The accountable blockchain 7
Known participants 7
Known finality with performance & accountability 7
Known costs 7
Known data 8
Known relationships 8
Known means of exchange 8

The Redbelly Network Topology **9**
Networking 9
The Redbelly Blockchain 10
Blockchain Architecture 10
DBFT 10
Superblock Optimisation 11
Sharded Verification 11
Polygraph and Proof-of-Fraud 11
Scalable Ethereum Virtual Machine (SEVM) 12
Interoperability and Asset Bridges 12
Role Decoupling 12
Validation Reduction 12
Transaction Fees 13
Sharding 13
Core Platform Components 13
ID Connect 13
Identity Registration 14
Identity Verification 14
Identity Recovery 14
Multi-User Accounts 14
Policy Management & Delegation Engine 14
Pay Connect 15
A Note on Stablecoins & CBDCs 15
Ricardian Contracts 15
Products 15
Supporting Components 16
Oracles 16
Open Source Templates 16
RBN dAppstore 16

Tokenomics **17**

Archived copy · cryp2nova.com

Uses of the Coin 17
Allocations 19
Token Release Schedule 20

Ecosystem Governance **21**
Ecosystem Governance Responsibilities 21

References **22**

CRYP2NOVA

Archived copy · cryp2nova.com

The Redbelly Network Overview

The Problem

For decades we have seen growing trends of financialisation and centralisation. Financial relationships have increasingly become organised in centralised, unfair ways that embed information asymmetry. From retail banking to financial advice to interest rate benchmarks, individuals are continually at risk of unfair outcomes when dealing with the financial world. Compounding this issue, these relationships are typically run and managed in ways that are slow and inefficient.

It does not have to be this way. Distributed ledger technology (DLT) allows us to share data, independently agree and verify its legitimacy, and coordinate the execution of business logic using that data between parties at incredibly low cost. This allows us to turn competing parties into cooperating parties, empowering everyone with full and equal knowledge of the relationship, as well as the performance of the rights and obligations defined in that relationship, thereby removing the need to trust that the counterparty will do what they say they will do. By extension, the more we can automate the provision of goods and services, the less we need to rely on the organisation. If the technology to do this is commoditised and shared fairly, this should put downward pressure on prices.

Furthermore, DLT shifts the locus of data sovereignty back to the user where it belongs. With DLT, individuals are empowered with true ownership, agency, and control over their data, what is done with it, and the ability to take it with them from one service provider to another. This in turn gives service providers the means to create hyper-personalised value propositions bespoke to individuals and their historical data sets, rather than forcing individuals to choose the 'least worst option' for their needs.

The range of applications is vast - from illuminating complex financial transactions like mortgage-backed securities, to simplifying property transactions, to issuing and managing central bank digital currencies, DLT has the potential to improve the financial system for everyone.

Yet, despite DLT's clear potential, it has yet to be embedded into many, if any, of our real world financial relationships - even though it has matured for more than a decade. Why is this? We believe that this is largely because blockchains are unable to, on their own, provide the sufficient accountability required for maintaining high value, complex, real world financial relationships.

A lack of accountability

Current blockchain designs limit accountability because they focus on censorship resistance, hindering their applicability to important high value financial relationships that require the enforcement of rights and obligations that cannot all be programmed. With classical blockchains, double spending attacks can occur when one of two branches are discarded from the system. As a result, there is by definition no proper way to detect a double spending attack or identify the participant responsible for the attack. There is simply no accountability.

Real accountability means having known network participants; being flexible enough to be compliant with law and regulation; being able to prove when fraud is attempted or performed;

Archived copy · cryp2nova.com

and having confidence in transaction finality - financial relationships can not rely on probabilistic outcomes.

The importance of regulation

As DeFi and cryptocurrency markets grow, eventually they will have to become regulated in order to protect consumers. When a market is regulated, it provides confidence to that market to help it grow by virtue of the protections that regulation affords. Starting from a basis of accountability will assist in that process. If the blockchain community continues to focus exclusively on unregulated assets, those completely separated from the existing financial system, then the true potential and scope of distributed ledger technology will forever be curtailed and stunted.

The role of regulation and legal systems is to enforce the rights and obligations detailed in real world contracts in order to protect everyone's interests. The regulator protects market participants from abuses of power which are themselves arguably due, in part, to market inefficiencies and information asymmetry. In so doing, however, regulated inefficiencies are introduced in order to ensure protection.

This regulated inefficiency could be drastically reduced by standardising and programming the regulated assets and their associated rights and obligations through the use of smart contracts. However, it is important to note that much of the work of legal contracts is in navigating the grey areas of subjectivity and negotiation. Whilst this approach is undeniably imperfect, it is essential for the appropriate and adequate protection of rights defined in contract.

The goal of DLT, specifically smart contracts, should not be to replace the need for legal infrastructure. Rather we should look to augment lawyers and contracts with technology to automate the performance of *specific* rights and obligations within contracts that are able to be programmed and therefore automated.

With DLT, it is possible to design and build compliance into our agreements by implementing 'rules as code' where we can perform a single audit of the code and agreements and have confidence that they will execute as designed, leaning on appropriate legal recourse where necessary.

In summary, embedding DLT into existing financial relationships will dramatically improve the efficiency and transparency of assets, and the markets in which they are traded. It will also bring the real world benefits of true accountability and enforceability to the digitised assets we choose to put on the blockchain.

Archived copy · cryp2nova.com

The Solution

The Redbelly Network is a revolutionary open finance platform that commoditises and shares DLT infrastructure for transacting with accountability and transparency, making accessible to everyone the automation of economic relationships between known entities, with known means of exchange, informed and held accountable by known data.

We are building a fairer and more efficient financial system that is more transparent and inclusive. We believe that this means empowering everyone with fairer access to financial services and infrastructure. Redbelly is not a blockchain for institutions. We are empowering everyday people with access to institutional tools at incredibly low cost in order to level the playing field by eliminating information asymmetry. In order to build this future, we must start from a place of accountability.

The accountable blockchain

The Redbelly Network has been designed with accountability at its core. Our DBFT consensus algorithm combined with Polygraph, our novel proof-of-fraud protocol, ensures high performance, security, and accountability. Redbelly does not fork, and if a participant attempts to fork the blockchain, Redbelly automatically constructs an undeniable proof-of-fraud.

Known participants

All participants on The Redbelly Network are identified through our network of off-chain digital identity providers. Prospective network participants must prove their identity in order to onboard onto the network and create an account. This allows network participants to use their real world identity as their blockchain identity. Our zkSnark based solution allows users to prove their identity without revealing any personal or sensitive information to the verifier. Additionally, because the authorisation is performed on a per transaction basis, the user has full control to accept or reject any specific authorisation request.

Known finality with performance & accountability

Our novel leaderless DBFT consensus algorithm was jointly developed by The University of Sydney and CSIRO's Data61 through funding from the Australian government's ARC grant program. DBFT allows a high throughput of transactions, with a peak throughput of 660,000 transactions per second under ideal conditions, to be deterministically finalised in a matter of seconds [4], unlike the probabilistic finality of most blockchains based on Nakamoto consensus. It guarantees that no forks can occur and prevents the possibility of the double spend. This is crucial for real time, high value applications which require certainty. The addition of our innovative protocol-level accountability mechanism, Polygraph, allows the network to punish malicious nodes [1].

Known costs

In order to facilitate high value real world financial relationships, transaction costs need to be known beforehand in order to give confidence and certainty to users and businesses. Thus, gas fees paid in the native Redbelly Coin are kept stable against fiat currency (USD) terms, despite possible price volatility of Redbelly Coin. For any given transaction on The Redbelly Network, the transaction costs will depend only on the complexity of the operations that need to be performed, which can easily be calculated ahead of time, and the fixed fee component.

Archived copy · cryp2nova.com

Known data

The Redbelly Network employs a ‘first party’ oracle approach to obtain data directly from the source. We enable traditional Web2.0 API providers to cheaply and easily run their own on-chain infrastructure that connects seamlessly to their API, in an approach inspired by API3’s Airnode [3]. This approach removes the need for third party intermediary oracles or aggregators and greatly accelerates the growth of The Redbelly Network by making the rich datasets and functionality provided by Web2.0 API providers accessible to all use cases on the network.

Known relationships

Redbelly is designed to natively support the deployment of Ricardian contracts where a hash of the full legal agreement is referenced in a smart contract’s code to irrefutably link the real world relationship (legal contract) with the execution of a subset of its rights and obligations (the smart contract). Templates of high value financial relationships will aid in the ease of deployment. Our Ricardian contracts benefit from the automation, efficiency and transparency of smart contracts but also provide real world compliance and enforceability. In addition to the Ricardian contract templates, tools will be built to aid the development of novel relationships and programmed dependencies between existing relationships in a concept we call ‘value webs’.

Known means of exchange

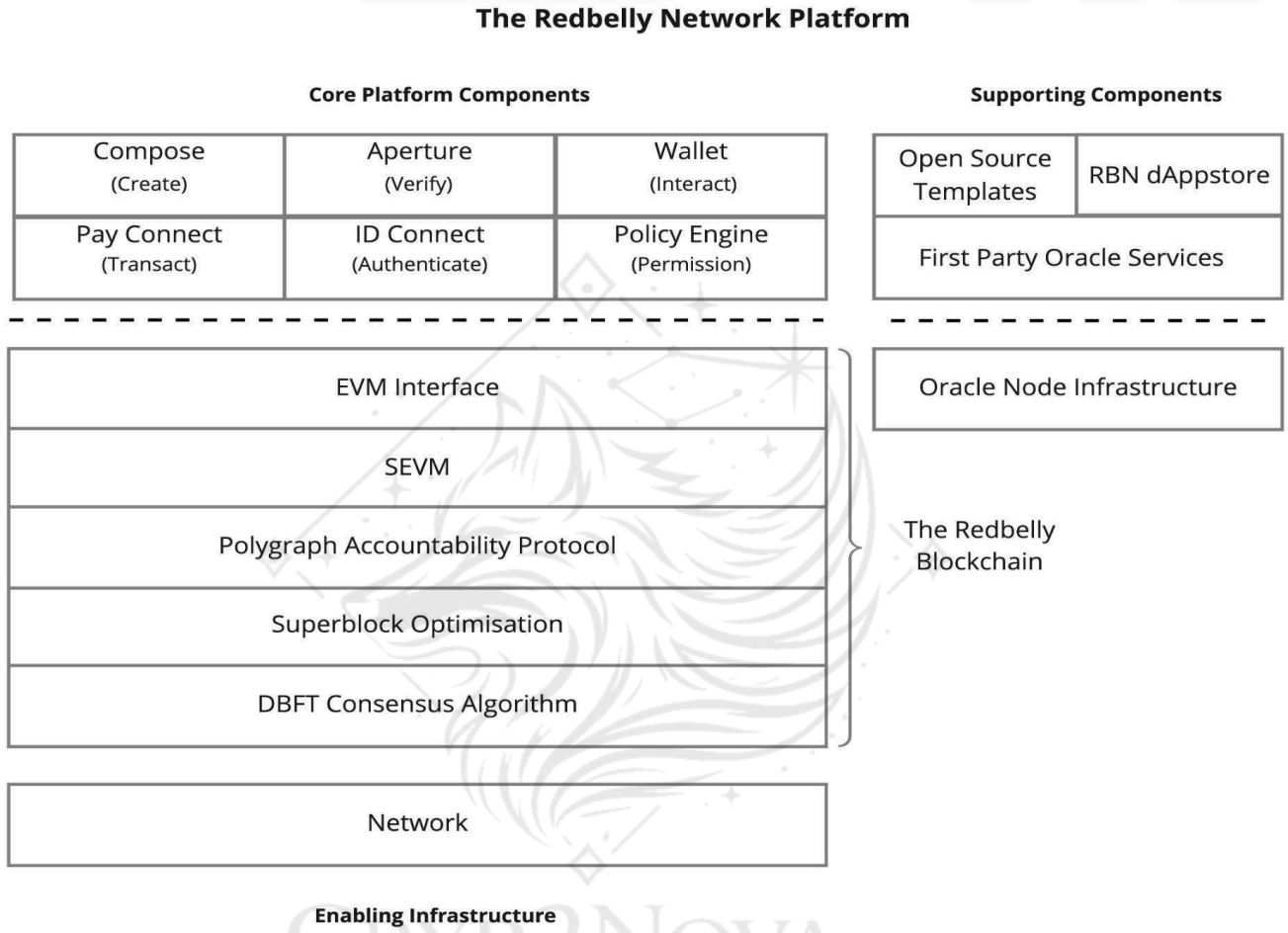
Most high value, real world financial relationships will settle using fiat currencies. Thus, The Redbelly Network will support transaction settlement in fiat currencies through a global payment gateway. This payment gateway will support a marketplace of payments providers such as SWIFT, Visa, Mastercard, and the NPP, amongst others. Whilst in the future we may expect centrally backed digital currencies (CBDCs) to be issued using the Redbelly infrastructure, this is a longer term ambition.

CRYP2NOVA

Archived copy · cryp2nova.com

The Redbelly Network Topology

The Redbelly Network can be segmented into its main components: the enabling infrastructure, the core platform components, and the supporting components. Each of these is described in more detail below.



Networking

The Redbelly Network currently utilises grpc to communicate between nodes. However, we have observed that network conditions become the bottleneck at high levels of throughput. This is primarily due to two reasons:

1. Available end-to-end network bandwidth
2. Network latency

We will seek to minimise bandwidth requirements by further optimising the protocol in the future. Introduction of technologies such as multipoint generic routing encapsulation (mGRE) will allow for secured multicast transmission of block information, rather than multiple peer-to-peer unicast streams. This will reduce the number of network transmission flows by each node to one or two flows, rather than the flow per peer that is currently required.

Archived copy · cryp2nova.com

While network latency is largely constrained by the speed of light through fibre optic transmission circuits, it is anticipated that the reduced overhead from minimising unicast transmission/ re-transmission will reduce latency otherwise introduced by the node's computational processing.

The Redbelly Blockchain

As discussed above, accountability is a property inherently absent from traditional blockchains. By design, these protocols discard one branch in favour of another, which leaves no trace of any double spending attempt. By contrast, the Redbelly blockchain does not fork: it reaches consensus on a block before it is appended to the chain, hence guaranteeing a unique branch.

Blockchain Architecture

The Redbelly Network is a public, permissionless blockchain. Anyone can run either a consensus or a storage (SEVM) node, but they must have created an account on the network and have the minimum resources required to spin up the relevant node. The decoupling of consensus and storage roles allows for better tuning of resource provisioning as well as security and resilience optimisation.

Additionally, once the mainnet is live and scaled up, there will be a minimum of 200 nodes participating at any given time to help mitigate the possibility of centralisation and increase the security and performance of the network. The pool of consensus nodes that are actively participating in consensus will be dynamically reconfigured on a periodic basis to further increase the security and performance of the network.

DBFT

The Redbelly Blockchain builds upon the Democratic Byzantine Fault Tolerance (DBFT) consensus protocol [4] to achieve unprecedented performance. DBFT was jointly developed by the University of Sydney and CSIRO's Data 61 with funding from the Australian government. DBFT is able to achieve a peak throughput of more than 660,000 transactions per second when deployed on 300 nodes. Later performance tests on 1000 nodes at a global scale demonstrated an average transaction latency of 3 seconds [4].

In addition, there are often bugs in blockchain protocols that affect their security [8]. In order to mitigate the risks of errors while designing a complex consensus protocol, we ran the protocol through a process of formal verification [5]. We recently demonstrated through a machine-checked proof that our consensus algorithm is correct. This was done with the use of parameterised model checking: our consensus protocol is proved correct for any set of n participants and any number f of tolerated failures.

Furthermore, most consensus algorithms rely on having a 'correct' leader or coordinator node in order to terminate. However, DBFT can terminate even when any coordinator is faulty, rendering it leaderless. In essence, Redbelly allows processes to complete asynchronous rounds as soon as they receive a particular threshold of messages rather than having to wait for a message from a coordinator that may be delayed. The implication of this is that as the number of network participants grows, the transaction throughput increases.

Archived copy · cryp2nova.com

The result is a decentralised topology particularly well suited to blockchains because each node is equal in the sense that they play the same role in the execution of consensus, making the decision inherently 'democratic'. Additionally, this topology avoids cumbersome bottlenecks through balancing the load for optimised scalability. For more detail on the technical implementation and testing of DBFT, see [5], [6], and [7].

Superblock Optimisation

In classical blockchains, participants solve consensus by having different participants engage in 'fierce' competition: proposing their own block and trying to impose it on the system. If they succeed, then all other participants lose: only their block is the one appended at the next available index of the chain. This is a waste of resources as only *1* participant succeeds and *n-1* fail.

In contrast, Redbelly participants solve consensus by combining distinct sets of transactions into a 'superblock' in a leaderless manner to commit more transactions per consensus instance, enhancing scalability and performance. In this sense, Redbelly consensus is collaborative instead of competitive: blocks proposed by different participants are combined into a 'superblock' that gets appended to the chain.

Sharded Verification

In addition to the superblock optimisation described above, Redbelly also implements sharded verification. Unlike existing blockchains whose nodes typically are required to verify the same transactions, sharded verification allows us to spit the computational load across different verifiers. Each transaction signature is verified by at least $t+1$ and at most $2t+1$ verifiers (where t is the maximum number of faults). Both the superblock optimisation and sharded verification further enhance the scalability of The Redbelly Network. For more information on the implementation of sharded verification, see [7].

Polygraph and Proof-of-Fraud

The Redbelly blockchain enforces accountability even when a prospective attacker controls most of the network. The Redbelly blockchain ensures that *either* consensus is reached *or* malicious participants attacking the system in an attempt to create a disagreement are caught. At runtime, the Polygraph protocol efficiently creates an undeniably proof-of-fraud for misbehaving participants. Polygraph requests dedicated messages to be signed by their sender to allow participants to cross-check these messages in order to detect liars that have sent conflicting information to different participants. As these conflicting messages are signed by their senders, they constitute an undeniable proof-of-fraud. For more detailed information about Polygraph, see [1].

Scalable Ethereum Virtual Machine (SEVM)

The Redbelly Network combines the consensus of the original Redbelly blockchain [7] with an optimised and scalable version of the Ethereum virtual machine (EVM) to enable The Redbelly Network to support smart contracts written in bytecode that is EVM compatible. This scalable Ethereum virtual machine (SEVM) allows The Redbelly Network to support a diverse ecosystem of smart contracts and dApps with the underlying security and efficiency of the Redbelly blockchain. Similarly, privacy preserving technologies built on Ethereum such as Aztec, Nightfall, and Zeth can be implemented on top of Redbelly in the same way. Note that in the future Redbelly will investigate the use of other privacy preserving technologies including encryption,

Archived copy · cryp2nova.com

zero knowledge proofs, multi-party computation, and trusted execution environments to further enhance the privacy capabilities of the network.

Interoperability and Asset Bridges

There is a vast amount of value already deployed in the diverse set of existing blockchain ecosystems. The Redbelly Network will have bridges to other blockchain based assets so that those assets can benefit from the scalability, security, and accountability of The Redbelly Network. This will also add significant value and utility to the growing Rebelly Network by giving use cases deployed on The Redbelly Network access to these valuable assets and protocols.

For example, smart contract bridges can be deployed to facilitate the transfer of value between any two chains with Turing complete smart contracting languages. Alternatively, a higher order protocol can be used if one of the chains does not support smart contracts.

Role Decoupling

The Redbelly Network distinguishes the two main tasks to be executed by its nodes. One task is to run the DBFT consensus algorithm and the other is to validate and execute transactions. Redbelly separates the role of executing each task with consensus nodes responsible for executing DBFT consensus and SEVM nodes responsible for validating and executing transactions. As the consensus nodes and SEVM nodes communicate through gRPC, they can easily be loaded on two distinct physical machines or VMs or kept on the same machine in two separate processes. This gives us great flexibility in dynamically scaling the network.

Validation Reduction

In contrast to Ethereum, the nodes running the SEVM do not have to validate each individual transaction twice. In Ethereum, for example, each transaction is propagated to the whole network, every miner validates the transaction upon reception and once it is included in a block, the transaction is revalidated by every validator before being executed.

To minimise the wasting of resources, the SEVM nodes do not propagate a transaction to other nodes after it is validated. Instead, a node validates a transaction upon receiving it to propose it to the consensus but does not propagate it to all nodes. The node proposes a block with the validated transaction for consensus and the SEVM nodes validates it when consensus is reached about the superblock to be appended. In other words, in Redbelly, each transaction is validated $n+1$ times where n is the number of SEVM nodes in the system (once by the proposer node and once by all SEVM nodes in the system). This is in contrast to Ethereum where each transaction is validated $2n$ times. As n increases towards infinity, Ethereum validates transactions twice as much as Redbelly.

Transaction Fees

As in Ethereum, gas is the unit of work that is performed for each distinct computational operation in the SEVM. The amount of gas required to perform a specific operation is defined according to a predefined fee schedule where each operation has a different, fixed, gas cost.

Redbelly has the distinct advantage of high performance, meaning the network can handle a large number of transactions. So, in order to provide transaction cost certainty to users the gas price will remain fixed. Thus, on Redbelly, the total fees for a given transaction are the fixed gas

Archived copy · cryp2nova.com

cost of the transaction (defined by the number and type of computational operations inside the transaction) multiplied by the fixed gas price plus the fixed transaction fee component, which is paid to the nodes providing the blockchain services. Importantly, gas is priced in units of fiat currency (e.g. USD) but paid in the native coin of the Redbelly blockchain.

Sharding

The primary goal of sharding is to increase the scalability of the network. The Redbelly Network allows participants to open dedicated shards on which shard participants can transact with even greater performance without revealing the details of their transactions to the rest of the network. Each shard can be thought of as its own blockchain backed by the security of the main chain (the beacon chain).

The nodes of each shard process only their transactions, enabling greater throughput across the entirety of the network by reducing congestion and bottlenecks. Not only does opening a shard allow a user, business, or use case to access greater performance, it also adds privacy benefits for shard participants. The details of a shard's transactions are completely hidden from the beacon chain as only the shard initiation deposits are present on the main chain.

The Redbelly Network's sharding functionality will be available as a consumable service, allowing anyone to spin up a shard easily and efficiently. The sharding service will also be highly configurable, giving greater flexibility for a wide range of complex use case needs that will inevitably arise.

Core Platform Components

ID Connect

Redbelly's innovative identity gateway allows users to create a secure off-chain identity that can be verified for on-chain authentication purposes. It consists of three main components; a Redbelly compliant identity app installed on the user's mobile device, an identity smart contract (one per user), and a zkSnark circuit that all interact with each other to confirm the user's identity, without needing to reveal sensitive personal information to the requesting party.

The user has full control over which third parties are authorised to access their information. It is locked behind multiple factors of authentication on their device that can include:

- A secret or a pin (something the user knows)
- An identity token that exists only on the user's device (something the user has), and
- A biometric factor (something the user is)

Identity Registration

Identity registration is performed when the user is creating their Redbelly account on the Redbelly Identity app. The application communicates with a marketplace of digital identity providers, one of which will perform identity checks on the user. Once this is done successfully, a set of zkSnark artefacts are generated including a zkSnark circuit, a verification key, a proving key and the deployment of the identity smart contract. In addition, a secret is generated and stored in the secure enclave of the user's device behind biometric methods of authentication.

Archived copy · cryp2nova.com

Identity Verification

Identity verification is performed on an as needed basis, with the user always in possession of their personal information. When a request for verification is made, the user uses the Redbelly compliant Identity app to authenticate themselves using biometrics. If the authentication is successful, the app then generates the proof for the zkSnark. The app then sends the proof to the identity smart contract, which authenticates the proof and sends the result to the initiating smart contract.

Identity Recovery

The loss of private keys is one of the biggest user experience challenges facing many blockchains. To mitigate this challenge, Redbelly generates a recovery key at user registration specifically for the purpose of account recovery. The recovery key is sharded amongst several delegates chosen by the user. These delegates serve as guardians for the user should they lose access to the device on which they registered their identity. If the user's device is lost, they will perform account recovery through the Redbelly compliant Identity app on a new device. This process requires them to re-register their identity through an identity provider on the digital identity marketplace. The recovery key is then recombined from the delegates and the user's identity smart contract is upgraded.

Multi-User Accounts

Once a user has registered as an individual on the platform, they are able to add additional roles to their identity, including creating a multi-user account to which other registered users can be added. Multi-user accounts are useful for representing legal entities such as companies and trusts where multiple individuals are required to authorise the actions of the entity. This is crucial in order to enable real world financial relationships on The Redbelly Network which in many cases involve these kinds of legal entities represented by multiple individuals.

Policy Management & Delegation Engine

In many cases, a multi-user account may not suffice for representing the complicated nesting of permissions and delegation that is needed to facilitate the effective management of financial relationships. As such, The Redbelly Network has a dynamic and flexible policy creation and management engine through which complex permissioning and delegation rules can be programmed and the relevant users added to specific roles within a policy.

Pay Connect

The Redbelly Network will support settlement in the native Redbelly Coin. However, many use cases will require settlement in fiat currency. Thus, Redbelly has a global payment gateway, Pay Connect, built directly into the protocol as a global payment smart contract that allows anyone to program payment obligations in fiat currency through a smart contract. Any dApp on the network can thus initialise payment flows on off-chain fiat payment rails, assuming that the relevant user authorises the transaction.

The payment gateway leverages fast fiat payment rails, such as the New Payments Platform (NPP), to power smart contract triggered instant transfers of fiat currency between bank accounts. Initially, the payment gateway will support the NPP, with other payment rails such as SWIFT, Visa, and Mastercard to be integrated in the future.

Archived copy · cryp2nova.com

A Note on Stablecoins & CBDCs

The Redbelly Network infrastructure is able to support the creation, use, and bridging of new and existing stablecoins. It is also possible to issue Centrally Backed Digital Currencies (CBDCs) leveraging the performance of DBFT consensus. We expect to focus more development effort on these applications as demand for them increases.

Ricardian Contracts

Given The Redbelly Network's focus on marrying the benefits of DLT with the accountability of legal infrastructure, there needs to be a mechanism that links any deployed instance of a smart contract with a specific legal contract. The Redbelly Network achieves this through native support of Ricardian contracts and a platform based mechanism for creating new instances of standardised Ricardian contract templates.

We define Ricardian contracts as a combination of a smart contract and a written legal contract. The two are linked together by a one way function that generates a hash of the written legal agreement that is included in the smart contract code at deployment. This binds the smart contract, and any actions of that smart contract, directly to the legal agreement. The two should not be thought of as separate, the smart contract code should be considered an augmentation to the legal agreement. In effect, the smart contract is the mechanism by which a subset of the rights and obligations defined by the legal agreement are performed. In this sense, The Redbelly Network provides a non-repudiation and notary service for legal agreements.

Products

To aid in the adoption of The Redbelly Network, we will develop several key products whose primary purpose is to make it as easy as possible to access, use, and benefit from our transformational technology. These products will initially focus on: creating and deploying Ricardian contracts on chain (Compose), independently viewing and verifying contract execution (Aperture), and interacting with deployed contracts (Wallet).

Supporting Components

Oracles

Leveraging our standardised Oracle Node Infrastructure, prospective Web2.0 API providers will be able to cheaply and easily deploy their own on-chain infrastructure that connects directly to their existing API. Once on-chain, the oracle is able to be called by smart contracts deployed on the network to inform the execution of smart contract functions that depend on off-chain data in an approach based on API3's Airnode [3].

The decision of which data source to use as an oracle is made by the relevant parties at the time the legal agreement is entered into. Both parties agree ahead of time that a specific data source will be used to inform the execution of the contract terms. The standardised oracle node infrastructure, once deployed by the oracle service provider, serves to inform those smart contracts with off-chain data as needed.

Archived copy · cryp2nova.com

Open Source Templates

The Redbelly Network aims to create open source Ricardian contract templates of commonly used legal agreements for high value financial relationships. These Ricardian contract templates can be quickly deployed by anyone using the platform. Over time, we hope that these templates will come to be the new standard for a fairer and more efficient version of these financial relationships,

RBN dAppstore

The Redbelly Network dAppstore serves as the single place from which to find an aggregated view of all the dApps that have been built on top of, or ported to The Redbelly Network. It gives users a single portal into the possibilities of participating in the network and also provides users with confidence in the dApps that are listed there.

CRYP2NOVA

Archived copy · cryp2nova.com

Tokenomics

The Redbelly Network is powered by the native Redbelly Coin, which has a fixed supply of 10,000,000,000. The coin is used in core parts of the network to power its cryptoeconomic dynamics. These include transaction fees, staking, sharding, governance, and rewards and incentives. These activities are described in more detail in the table below.

Uses of the Coin

Category	Use	Description
Gas	Gas	The payment of gas fees to execute transactions on the network
Governance	Voting: network upgrades	The facilitation of community input to major upgrades to the network
	Voting: governance decisions	The facilitation of decisions related to foundation responsibilities e.g. allocation changes, top ups
	Voting: network reconfiguration	The facilitation of the core network security function of reconfiguring the set of validator nodes from time to time (both consensus and EVM nodes)
Staking	Consensus staking	The act of locking up native coins in order to participate in consensus on the network. The act of doing so earns the staker a reward
	SEVM staking	The act of locking up native coins in order to participate as a state machine on the network. The act of doing so earns the staker a reward
	Oracle staking	The act of locking up native coins in order to participate as an oracle on the network. The threat of having the stake slashed acts as an incentive to provide timely and quality data. The use of the oracle services provides a revenue stream for the oracle
Sharding	Shard initiation & management	The act of locking up native coins in order to create a shard on the network. Each participant in the shard needs to contribute to this deposit
Incentives & Rewards	Network effect acquisition	Incentives paid to early use cases based on the value they bring to the network (e.g. # users, # transactions, # contracts), paid in native coins from a dedicated incentive allocation
	Node incentives & rewards	Incentives and rewards paid to node hosts because of the essential service they provide to the network, paid in native coins from a dedicated allocation
	Oracle provision	Incentives paid to oracle providers for providing real world data input to the network, paid in native coins from a dedicated allocation
	Product Adoption Incentive	Incentive paid to early users of the product, paid in native coins from a dedicated incentive allocation

In addition, the table below describes how each of the key entities will use the coin to interact with the system through the key activities described above.

Archived copy · cryp2nova.com

User	Interaction	Description
Consensus Node	Staking	• Native coins are deposited 'at stake' as a disincentive for bad behaviour • Native coins are rewarded to stakers as an incentive for providing this critical service
	Gas	Consensus providers receive a portion of gas fees, paid in native coins, as compensation for providing the consensus service
SEVM Node	Staking	• Native coins are deposited 'at stake' as a disincentive for bad behaviour • Native coins are rewarded to stakers as an incentive for providing this critical service
	Gas	SEVM providers receive a portion of gas fees, paid in native coins, as compensation for providing the SEVM service
Oracle Provider	Staking	• Native coins are deposited 'at stake' as a disincentive for bad behaviour ○ Bad behaviour includes bugs that provide wrong data, uptime/downtime thresholds • Native coins are rewarded to stakers as an incentive for providing this critical service
Shard Participant	Shard Initiation	Native coins are locked/deposited by each participant in order to initiate a shard. These coins are locked from being used elsewhere on the network whilst the shard remains active
Governance Member/ Delegate	Governance Voting	Holders of Native coins will be able to vote on governance decisions that require a community vote. If coins are staked then the voting weight compounds
	Gas	Governance Members/Delegates pay gas fees, paid in native coins, as compensation to the actors that facilitate the governance transaction
Use Case	Incentive	Native coins are rewarded to early use cases on the platform from a dedicated incentive allocation as an incentive to bring as much network effect on to the platform as early as possible
	Gas	Users/use cases pay gas fees, paid in native coins, as compensation to the actors that facilitate the transaction
Product User (Use case)	Incentive	Adopters of the Redbelly Network products are rewarded an incentive, paid in Native Coins (or a rebate on the cost of the product) for being an early adopter of the Redbelly Network product suite

Archived copy · cryp2nova.com

Allocations

Furthermore, the allocations at launch for the native Redbelly coin are detailed in the table below. These allocations are subject to governance, which is described in the final section of this paper.

Category	Type	Allocation	Description
Ecosystem Development	Incentives & Rewards • Multi Phase Rewards Program • Node Operator Provision • Oracle Provision • IDP Provision • Staking reward	37% 3.7 billion	Incentives & rewards allocated for behaviours that add social and network value to the Network, as well as entities that host Consensus and/or SEVM nodes, provide oracles and services that verify credentials.
	Ecosystem Grants Program • Protocol R&D • Capital Markets & Innovation • Research and Social Good • Redbelly Community		Funds are allocated for various grant purposes, including technical innovation, research and development, capital market innovation, and activities that promote and maximise community and social good leveraging Redbelly Network technology.
	Network Effect Acquisition & Product Adoption Incentives		Incentives & rewards allocated to entities that bring significant network effect to the Redbelly Network in terms of users, contracts, transaction throughput, interactions, marketing partnerships, etc.
Entity Allocation	Redbelly Network Governance DAO	3% 300 million	Funds allocated to the Redbelly Network Governance DAO to fund and help facilitate its governance activities
	Investors ○ Seed (13%) ○ Private Sale A (7.3%) ○ Private Sale B 6.9%) ○ Private Sale C (0.7%)	28% 2.8 billion	Funds allocated to investors
	Team (10%)	10% 1 billion	Funds allocated to the team to incentivise the continued development of the network
	USYD & CSIRO (2%)	2% 200 million	Funds allocated to the co-developers of core innovations of the network
	Reserve	20% 2 billion	Funds held in reserve, controlled by governance to help fund the long term future development of the Redbelly Network and broader ecosystem

Archived copy · cryp2nova.com

Token Release Schedule

Finally, the token release schedule for the native Redbelly coin is detailed in the table below. The "First Month" column refers to the number of calendar months following the listing on a public market. Tokens will vest weekly, commencing from the "First Month" column described below, on the same calendar day that the public market listing occurred. For example, if the token was first listed on the 15th day of a month, the Private Sale tokens will vest weekly from the 15th day of the calendar month that occurs 2 months after the public listing event. If there is no equivalent calendar day in the "First Month" (for example if the First Month has fewer days than the calendar month that the token was first listed in), it will instead fall on the last day of the First Month.

Vesting will complete on the last respective day of the "Last Month" column detailed below. In the previous example of the Private Sale tokens, all tokens will be vested by the 15th day of the same calendar month 14 months after the public listing event.

Note, these are subject to potential changes before the mainnet release. Note that the Ecosystem Development, and reserve allocations may also be subject to a custom token release schedule, as offered at the time.

				Release Schedule	
Entity	**Allocation at launch (%)**	**Total Allocation**	**# Released at Listing**	**First month**	**Last month**
Redbelly Network Governance DAO	3%	300 million	100 million	1	36
Team	10%	1 billion	0	12[1]	36[1]
USYD/CSIRO	2%	200 million	0	6	36
Seed Investors	13%	1.3 billion	0	6	32
Private Sale A	7.3%	730 million	0	2	14
Private Sale B	6.9%	690 million	0	2	12
Private Sale C	0.7%	70 million	7 million	2	10

1 It is a condition of release that a Team token holder is either actively employed by the Redbelly group of companies, or is engaged by Redbelly to perform services.

Archived copy · cryp2nova.com

Ecosystem Governance

There are several key entities relevant to the governance of The Redbelly Network, these are listed below:

- The Redbelly Network Governance DAO
- Redbelly Network Pty Ltd
- Governance Participants
- Consensus Node Operators
- SEVM Node Operators

The Redbelly Network Governance DAO is a decentralised autonomous organisation that operates independently from Redbelly Network Pty Ltd. The Redbelly Network Governance DAO is a not-for-profit, community organisation focused on protocol governance, token dynamics, ecosystem support and administration, and ecosystem wide economic and policy decision making.

Redbelly Network Pty Ltd is a private company registered in Australia whose sole purpose is to focus on layer-1 development of the Redbelly Protocol and enabling the widespread adoption of Redbelly blockchain technology in the real world. The Foundation and company collaborate from time to time on innovative projects and initiatives to accelerate and maximise the value to the wider Redbelly ecosystem.

Whilst The Redbelly Network is in its bootstrapping phase, governance functions (excluding treasury management) will be performed by Redbelly Network Pty Ltd until such time as The Redbelly Network Governance DAO has been developed and the governance transition plan, as detailed in the roadmap, has been completed.

The main responsibilities of network governance are listed in the table below.

Ecosystem Governance Responsibilities

Responsibility	Description
Network Upgrades	Updates to the core protocol run by nodes
Security	Network reconfiguration, changing the set of validator nodes on a regular basis
Ecosystem Support & Administration	• Community rewards • Community grants
Economic & Policy Decision Making	• Entity reallocations • Treasury Management • Other economic and policy decisions
Facilitate On-Chain Standardisation Processes	Proposal and adoption of new standards and specifications

Archived copy · cryp2nova.com

References

[1] Civit, Gilbert, Gramoli. Polygraph: Accountable Byzantine Agreement. *Proceedings of the 41st IEEE International Conference on Distributed Computing Systems.* July 2021, DC, USA. https://ieeexplore.ieee.org/document/9546489

[2] Fischer Lynch, Paterson, Impossibility of distributed consensus with one faulty process. Journal of the ACM, 32(2), 1985.

[3] API3 whitepaper: https://drive.google.com/file/d/1GzkLKc6DYxImgeDhoKLA4wHGlE0eGGgo/view

[4] Crain, Gramoli, Larrea, Raynal. DBFT, *Proceedings of the 17th IEEE International Symposium on Network Computing and Applications* 2018. http://redbellyrw.cluster021.hosting.ovh.net/pubs/DBFT-preprint.pdf

[5] Bertrand et al. Compositional Verification of Byzantine Consensus. HAL 03158911. https://hal.archives-ouvertes.fr/hal-03158911/document

[6] Ekparinya et al. The Attack of the Clones against Proof-of-Authority. *Proceedings of the Network and Distributed Systems Security Symposium*, Internet Society, Feb 2020

[7] Crain, Natoli, Gramoli. Red Belly: A Secure, Fair and Scalable Open Blockchain. *Proceedings of the 42nd IEEE Symposium on Security and Privacy S&P* 2021. https://drive.google.com/drive/u/0/folders/1_Dz5r8EvJvR_I1xIem9QutK6n_wzz7Iw

[8] Natoli, Gramoli. The Balance Attack or Why Forkable Blockchains Are Ill-Suited for Consortium. *Proceedings of the 47th IEEE/IFIP International Conference on Dependable Systems and Networks*. p.579-590, 2017

CRYP2NOVA

Archived copy · cryp2nova.com



CRYP2NOVA

Archived copy · cryp2nova.com