Creditcoin

A Decentralized Credit Network

Whitepaper
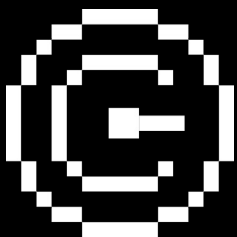
Abstract

Blockchain technology has enabled us to create objective history—decentralized ledgers represent facts that are backed by verifiable[1] computation, not a bet on the trust in central authorities. Bitcoin proved the value of its financial utility as a decentralized transaction ledger by leading to the creation of a total cryptocurrency market capitalization in excess of $1 trillion in mid-2023.[2]

However, a large market cap alone is insufficient to build a self-sustainable financial ecosystem. Building such an ecosystem requires three pillars: savings, payments, and investment. Investment works as a "wormhole" of sorts, connecting "parallel universes" that we call markets.

According to the IMF, global nominal GDP was $96.31 trillion in 2021. However, Aon pegged the total size of the global capital investment market at $137.3 trillion in February 2021.[3] If this relationship stays the same for the cryptocurrency, then the $1 trillion market cap in 2023 means a potential cryptocurrency investment market of $1.425 trillion.

Creditcoin is a decentralized credit network that turns digital wallets into an investment market. The validators and nominators of the market earn Creditcoin by minting blocks: The block reward is shared between validators and their respective nominators. The network achieves robustness by decentralizing credit history, while automatically punishing fundraiser default. Investors can select credit history parameters to accommodate various risk models.

Creditcoin and its network are designed as a simple blockchain that serves a single purpose extremely well: enabling blockchain-based lending transactions. Blockchain by itself is no silver bullet, so we leave the development of related services - such as identification and credit scoring - to others. These higher level platforms will build on top of the Creditcoin foundation. We also recognize that lending transactions facilitate various business activities. Instead of implementing them within Creditcoin, the blockchain achieves versatility through the creativity of its users and the ability to connect with other blockchain networks.

1) "Bitcoin: A Peer-to-Peer Electronic Cash System - Bitcoin.org." https://bitcoin.org/bitcoin.pdf. Accessed 5 Feb. 2019

2) "CoinMarketCap." https://coinmarketcap.com/. Accessed 13 June, 2023.

3) "Global Invested Capital Market - Aon." https://insights-north-america.aon.com/managing-volatility/aon-global-invested-capital-market-article. Accessed 13 June 2023.

This whitepaper:

(1) Introduces the vision of Creditcoin.

(2) Illustrates the Creditcoin ecosystem.

(3) Provides a detailed explanation of the Creditcoin protocol.

(4) Explains how Creditcoin's Proof of Stake implementation functions.

(5) Describes the design philosophy and history of Creditcoin.

I. Introduction

Some of the fundamental services of finance are savings, payments, and investment. Banks hold funds from savers and make them readily available for withdrawal when needed. At the same time, banks invest unused saver funds, turning dormant capital into working capital for society. When done correctly, such activities can optimize the flow of funds and increase the productivity of the economy.

However, this is not always the case. As seen in financial disasters such as the subprime mortgage crisis, banks often take on far too much risk in an effort to achieve high short-term gains. Since savers cannot get clear information on how banks are redistributing their funds, and the goals of bankers often do not necessarily align with those of savers, decisions contrary to the savers' best interests are often made without their knowledge or permission.

In response to the subprime mortgage crisis, Satoshi Nakamoto invented blockchain technology to bring self-determination to economic activities. Before this invention, it was nearly impossible to measure the objectivity of shared information without a central authority. Today, you can perform financial transactions without having to trust any intermediaries.

Although there are advantages and disadvantages to making one's own investment decisions, this can be a possible defense against credit crises. For example, the focus of credit unions on benefits for their members influences the level of risk that the unions are willing to take on. This might explain why credit unions survived the financial crisis in relatively better shape than traditional banks.

The blockchain market seems very successful, with a $502 billion market cap and nearly $10 billion daily transaction volume for Bitcoin alone in June of 2023. However, it is still difficult to use cryptocurrency in the current fiat-centric ecosystem. The long transaction confirmation time, high fees and volatility of cryptocurrency make it hard for people living in the fiat currency ecosystem to adapt cryptocurrency into their lives.

Gluwa and Aella jointly created Creditcoin as an adapter that seamlessly connects the best of the two worlds. It takes the blockchain closer to the original vision of Satoshi Nakamoto: a sound currency for everyone.

II. Creditcoin Ecosystem

Creditcoin is a blockchain-agnostic investment protocol where investors can lend with any cryptocurrency. The Creditcoin network is a general blockchain for investment activities. The network connects investors and fundraisers with matching conditions. The record of activities lasts forever on the blockchain, and the data can be used for future credit evaluation by any interested parties.

An investment in the Creditcoin network starts by matching offers from investors and fundraisers. A fundraiser posts seeking an amount, interest rate, and due period. If there is an investor with matching conditions, the fundraiser and the investor announce the deal to the Creditcoin network. The system verifies the deal's completion by confirming the transfer of the loan.

A collection of investments goes through a process similar to the investment process. If the fundraiser is ready to return the investment with interest, the fundraiser makes a repayment and announces the repayment to the Creditcoin network. In some cases, the investor of a loan may exempt the fundraiser from repayment of a loan.

Each announcement on the Creditcoin network has a transaction fee denominated in the Creditcoin currency. Fees are locked on the network for roughly a year and are then returned to the user.

Overall, Creditcoins are presently functional in that they have been developed in order to allow Creditcoin Users to: (1) lend, borrow, and repay currency on the Creditcoin network; (2) have direct access to other Users for borrowing, lending, and repaying currency; (3) interact on the network and communicate with other Users for borrowing, lending, and repaying currency; (4) verify and validate transactions of borrowing, lending, or repaying currency that are recorded on the Infrastructure; (5) view and possess a decentralized and public credit history of Users which is recorded and expands with each User transaction; and (6) validate and verify transactions and receive Creditcoins for such validating. The Creditcoin Network empowers users with all of these functionalities.

Gluwa must make it clear that holders of Creditcoin have no rights to participate in or govern that common enterprise or to share in the profits or losses of Gluwa and do not represent an equity or other ownership interest in Gluwa or any other legal entity. Creditcoin Tokens are not designed or intended to provide holders with any income, dividends or returns based on the activities of the Company or any third party. Additionally, Creditcoins do not reflect or show the indebtedness of anyone or anything, including but not limited to any person or entity.

The details behind the Creditcoin protocol are explained in the next section.
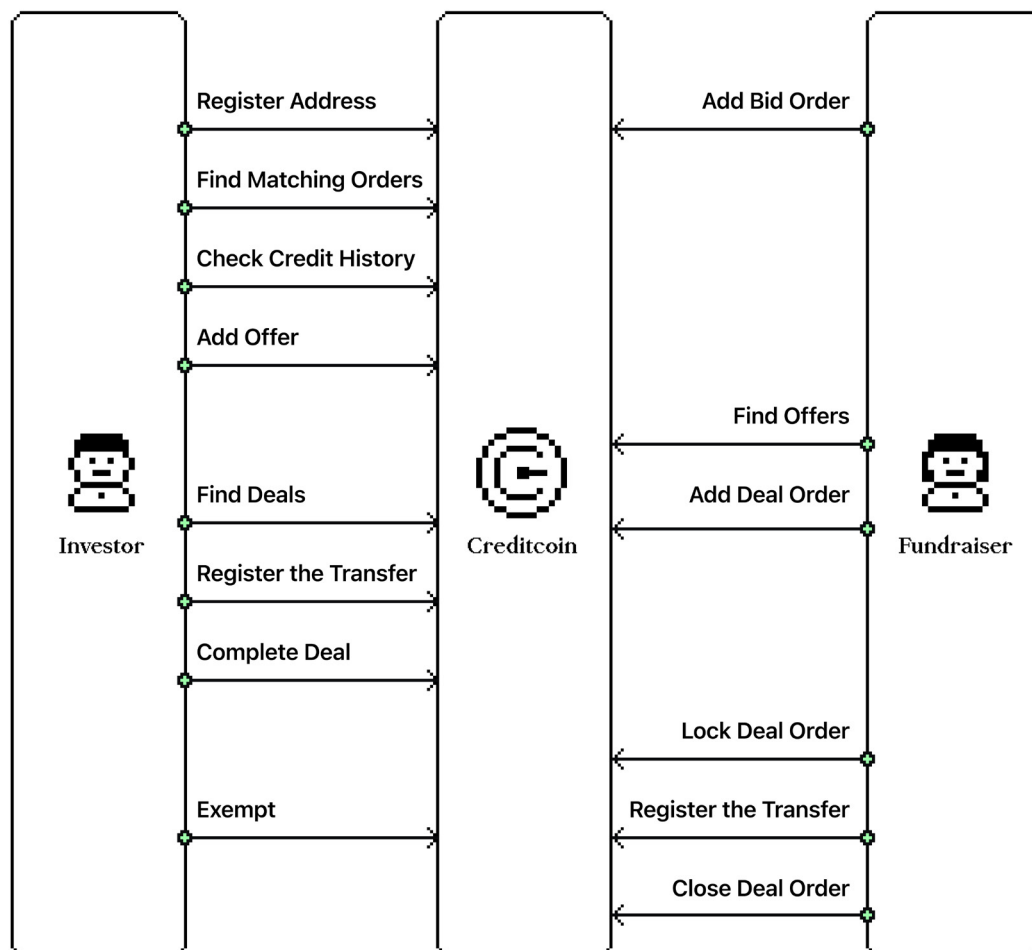
III. Creditcoin

1. Introduction

The Creditcoin blockchain is a network matching investors and fundraisers. A fundraiser posts an offer to the network, pegged with some Creditcoin. The Creditcoin works as a reward to the validators of the network. Investors can use the credit history of a fundraiser on the Creditcoin blockchain to evaluate the risk of potential investment, using a credit-scoring model of their choice. The fundraisers can choose to share more information about themselves in order to receive more favorable terms.

There are several reasons why we need the blockchain of credit investments:

1. Direct link between investors and fundraisers: Removes intermediaries to get better interest rates and enables a variety of investment quantities that were previously infeasible due to cost.

2. Decentralized and public credit history: Allows multiple credit scoring systems and lets investors use the system that fits their market of choice.

3. Creating sustainable cryptocurrency ecosystem: Enables cryptocurrency investment to build a sound financial ecosystem on blockchains. The financial ecosystem is self-sustainable if and only if you can save, pay, and invest.

4. Security: Allow sharing credit history without providing personal information to centralized institutions, which are often the target of hacker attacks.

2. User Flow

Introduction

Purpose

This section covers a step-by-step guide on how a Creditcoin user will use the blockchain through a loan-cycle.

Scope

This section explains how a user would pay Creditcoin to execute a loan deal. From the perspective of an investor, how to create a loan offer, find a fundraiser for the offer, learn the fundraiser's credit history, and make an investment. For a fundraiser, how to search for a loan offer, request for the loan and make a repayment.

Overview

Creating a transaction on a blockchain is essentially making an announcement. To get your message recorded on a new block, you pay a transaction fee to the blockchain. Unlike Bitcoin, which only has a send transaction, the Creditcoin network supports a different type of transaction per each step of a loan cycle. Investors and fundraisers pay fees via Creditcoin to process each stage of their loan.

Fundraiser's Flow

On the Creditcoin network, a fundraiser is an account that borrows funds from another account. A helpful diagram can be found at the beginning of this section.

I. Find a Loan Offer

A Fundraiser will start a loan-cycle by creating a bid order describing the loan condition he wants. The bid order is announced to the Creditcoin network to attract potential investors.

1. Create a Bid Order

A fundraiser can announce the details of his bid order. It includes amount, interest, and maturity. For example, a fundraiser may offer to borrow 100 Bitcoin for a 10% interest per 30 days.

The fundraiser will pay Creditcoin as a transaction fee to the Creditcoin network to create the order.

Note that the offer is in Bitcoin, not in Creditcoin. On the Creditcoin network, you are not lending or borrowing in Creditcoin, but a cryptocurrency on another blockchain. Currently, the Creditcoin network supports Bitcoin, Ethereum, and ERC-20 token loans.

2. Find Investment Offers

If an investor likes the fundraiser's bid order, he can create an offer. The offer information includes a set of one ask order and a matching bid order.

The fundraiser can retrieve a list of offers for free.

3. Create a Deal

If a fundraiser likes an offer he received, he can accept the offer by sending a corresponding deal to the investor. The deal will have the exact loan condition described in the offer.

The fundraiser will pay Creditcoin as a transaction fee to the Creditcoin network to send the deal.

II. Make a Repayment

A fundraiser can repay the full amount to finish the loan-cycle without the involvement of the investor.

1. Lock a Deal

Before making a repayment, the fundraiser has to block another account from making any change to the deal. Else, we have a potential concurrency problem. The fundraiser may be closing the deal at the same time as the ownership of the loan is sold to another account. In this case, there may be two transfers registered against the same deal order. The Creditcoin network prevents the problem by requiring a fundraiser to lock the deal before making a repayment.

The fundraiser will pay Creditcoin as a transaction fee to the Creditcoin network to lock the deal.

2. Transfer the Repayment to the Investor

A deal includes where the investor would like to receive the repayment. Note that the repayment transfer happens on another blockchain (e.g., Bitcoin or Ethereum). The fundraiser may pay a transaction fee on that blockchain, but not on the Creditcoin network.

III. Make a Repayment with an Exemption

Optionally, a fundraiser may negotiate with the investor for an

exemption. 1. Negotiate for an Exemption

In some cases, a fundraiser may not be able to repay the full amount but a part of it. If so, the investor may choose to accept partial repayment since it is better than nothing. The investor and the fundraiser can communicate outside of the Creditcoin network and negotiate for an exemption.

Since the negotiation happens outside of the blockchain, it does not cost any Creditcoin.

2. Send a Partial Repayment

Once the investor agrees to exempt some of the loan amount, the fundraiser will have to repay the rest. Just like the investment transaction, the repayment transaction also happens on another blockchain (e.g., Bitcoin or Ethereum).

The fundraiser may pay a transaction fee on that blockchain, but not on the Creditcoin network.

Note that in case of repayment with an exemption, the fundraiser cannot conclude the deal on his own. The investor needs to approve an exemption by registering the partial repayment transaction ID to the Creditcoin network. Learn more about the process in the Investor's Flow.

Investor's Flow

On the Creditcoin network, an investor is an account that lends funds to another account. A helpful diagram can be found at the beginning of this section.

I. Find an Investment Opportunity

An investor will start a loan-cycle by creating an ask order describing a loan offer. The ask order is announced to the Creditcoin network to attract potential investment deals.

1. Create an Ask Order

An investor can announce the details of his ask order. The detail includes amount, interest, and maturity. For example, an investor may offer to lend 100 Bitcoin for a 10% interest per 30 days.

The investor will pay Creditcoin as a transaction fee to the Creditcoin network to create the order.

Note that the offer is in Bitcoin, not in Creditcoin. On the Creditcoin network, you are not lending or borrowing in Creditcoin, but a cryptocurrency on another blockchain. Currently, the Creditcoin network supports Bitcoin, Ethereum, and ERC-20 token loans.

2. Find Matching Bid Orders

Using the ID string of an ask order, the investor can search for matching bid orders. Fundraisers create bid orders by describing the desired loan conditions. The investor can retrieve a list of matching orders for free.

3. Review a Fundraiser's Credit History

If an investor is interested in any matching bid order, the investor can retrieve a full transaction history of the fundraiser who created the deal. Each bid order includes an identification string of the fundraiser, a sighash. The investor can use the sighash to retrieve the fundraiser's credit history from the blockchain for free.

4. Create Investment Offers

If the investor likes the credit history of the fundraiser, he can create an offer. The offer information includes a set of one add order and a matching bid order.

The investor will pay Creditcoin as a transaction fee to the Creditcoin network to create the offer.

If the fundraiser likes the offer, he will send a deal to the investor.

II. Make an Investment

If an investor likes a deal, he can accept it by registering the investment transaction on the Creditcoin network.

1. Transfer the Investment to the Fundraiser

A deal includes where the fundraiser would like to receive the investment. Note that the investment transfer happens on another blockchain (e.g., Bitcoin or Ethereum). The investor may pay a transaction fee on that blockchain, but not on the Creditcoin network.

2. Complete the Deal

Once the investment transaction is confirmed on the blockchain, the investor can make the investment official by registering the transaction ID to the Creditcoin network.

The investor will pay Creditcoin as a transaction fee to the Creditcoin network to complete the deal.

III. Collect a Repayment

A fundraiser can repay the full amount to finish the loan-cycle without the involvement of the investor. However, an investor may choose to exempt a partial amount of the repayment.

1. Negotiate for an Exemption

In some cases, a fundraiser may not be able to repay the full amount but a part of it. If so, the investor may choose to accept partial repayment since it is better than nothing. The investor and the fundraiser can communicate outside of the Creditcoin network and negotiate for an exemption.

Since the negotiation happens outside of the blockchain, it does not cost any Creditcoin.

2. Accept a Partial Repayment

Once the investor agrees to exempt a loan, the fundraiser will have to repay the rest of the loan. Just like the investment transaction, the repayment transaction also happens on another blockchain (e.g., Bitcoin or Ethereum).

After the repayment transaction is confirmed on the blockchain, the investor can finalize the exemption by registering the repayment transaction ID on the Creditcoin network

The investor will pay Creditcoin as a transaction fee to the Creditcoin network to register the repayment transaction ID.

IV. Transfer a Bond

An investor may choose to transfer the ownership of a loan, bond, to another account. We call the new account a "collector." Once a bond is transferred to a collector, the repayment of the loan will be sent to the collector. This allows investors to liquidate their bonds before the maturity of their loans.

1. Searching for a Collector

An investor can find a collector for the bond outside of the Creditcoin network. The blockchain does not support any communication tool for this purpose.

Since the search and communication happen outside of the Creditcoin network, it does not cost any Creditcoin.

2. Searching for a Repayment Order

A collector will send a repayment order to the investor to purchase a bond. The investor can search for outstanding repayment orders on the Creditcoin network for free.

3. Accepting a Repayment Order

A repayment order will include payment for transferring the bond. If the investor likes the repayment order, the investor can transfer the bond by accepting the payment.

The investor will pay Creditcoin as a transaction fee to the Creditcoin network to accept the repayment order.

Collector's Flow

On the Creditcoin network, a collector is an account that receives the ownership of a loan from another account. A helpful diagram can be found at the beginning of this section.

I. Purchase a Bond

A collector can buy a bond from the investor to transfer the ownership of a loan, bond, to his account. Once a bond is transferred to a collector, the repayment of the loan will be sent to the collector. This allows collectors to acquire bonds closer to maturity.

1. Searching for a Bond

A collector can find an investor outside of the Creditcoin network. The blockchain does not support any communication tool for this purpose.

Since the search is a read-only process, and the communication happens outside of the Creditcoin network, it does not cost any Creditcoin.

2. Create a Repayment Order

A collector will send a repayment order to the investor to purchase a bond. The repayment order includes a payment to the investor for the bond. The payment can be in any cryptocurrency supported by the Creditcoin network (e.g., Bitcoin, Ethereum, or ERC-20).

The collector will pay the Creditcoin transaction fee to the Creditcoin network for creating the repayment order.

3. Searching for an Accepted Repayment Order

The collector can search for accepted repayment orders on the Creditcoin network for free.

4. Close a Repayment Order

After a repayment order gets accepted by the investor, the collector can finalize the purchase of the bond by registering the payment transaction ID. In other words, the collector closes a repayment order. The payment happens on another blockchain, and the collector may have to pay a transaction fee on the blockchain.

Once the repayment order is closed, repayment of the loan goes to the new owner – the collector.

The collector will pay Creditcoin as a transaction fee to the Creditcoin network to close the repayment order.

Conclusion

Creditcoin network has been built to support various investment scenarios and assist in decision making and transitioning of the relevant artifacts through their lifecycle.

3. Software Architecture

Introduction

Purpose

This document provides a comprehensive architectural overview of the system, using several different architectural views to depict various important aspects of the system.

Scope

This Software Architecture Document provides an architectural overview of the Creditcoin system developed by Gluwa, Inc. to provide a decentralized credit network.

Overview

The Creditcoin system is a decentralized credit network for investors and borrowers and to facilitate efficient and safe transactions between parties. A special cryptocurrency named Creditcoin is used as an aid in performing transactions and incentivizing parties to support, develop and expand the network and keep it operational.

Architectural Goals and Constraints

1. To support decentralization, the network is based on blockchain (distributed ledger) technology.

2. To reduce the work required to build a robust and trustworthy foundation for the network, an open source blockchain project was selected based on feature completeness and ease of configuration and modification (Parity Substrate).

3. The network supports the booking of investment and borrowing orders in a credit market order book for which canceled or outdated orders are of little interest.

4. The network supports matchmaking, communication between involved parties, and deal booking. The latter is stored permanently on the ledger and may be used for dispute resolution and credit history verification.

5. The network supports interoperability with other cryptocurrencies through a generic gateway that may be customized for use with a particular cryptocurrency.

6. The network uses a Nominated Proof of Stake consensus algorithm to incentivize validators and prevent network abuse.

7. All performance, bandwidth and storage requirements were taken into consideration to develop the architecture.

Subsystems and Layering

The Creditcoin system is built on top of the Substrate framework, which provides an implementation of a distributed ledger and interoperation between distributed components of the network. The system provides:

1. **An implementation of the Creditcoin transaction family—a group of operations or transaction types allowed on the ledger—which supports all required operations.**

2. **An implementation of a consensus algorithm to support the requirements.**

3. **An implementation of a generic gateway to interconnect with other cryptocurrency networks, such as Bitcoin, Ethereum, etc.**

A family of client applications was developed for testing and use by end users, which includes a command-line client and a staking dashboard to manage nominations and staked tokens.

Processes

Each Creditcoin node runs a validator, Creditcoin runtime, and Creditcoin consensus plugin. Additionally, "authority nodes" are run to allow confirmation of transactions on other cryptocurrency networks.

Client applications send requests to a validator to perform operations on data for a given transaction; the validator then dispatches the request to a relevant processor. The processor submits the transaction to the ledger. Clients read the current state of data that has been made persistent by recording it on the ledger.

Deployment

In the final distributed system, client applications can connect with validators across local or global IP networks. Any validator accepts transactions from one or more clients and clients send transactions to one or more validators.

Implementation Notes

Gluwa will contribute initial validators and infrastructure on Ubuntu virtual machines running in Azure. The Creditcoin runtime is a WASM binary. The primary development language for Creditcoin is Rust. Typescript is used for the staking dashboard and the CLI client.

IV. CTC Tokenomics, Rewards, and Penalties

1. CTC Token Description

Creditcoin's CTC is a proprietary utility token that fuses together a decentralized credit investment economy. It facilitates transactions between lenders and borrowers, and provides for the recording of transactions onto the Creditcoin blockchain, thus creating an immutable record of credit histories for borrowers. As the ecosystem/network grows, lenders will have an increasing array of borrowers with scored credit histories to choose from, and vice versa.
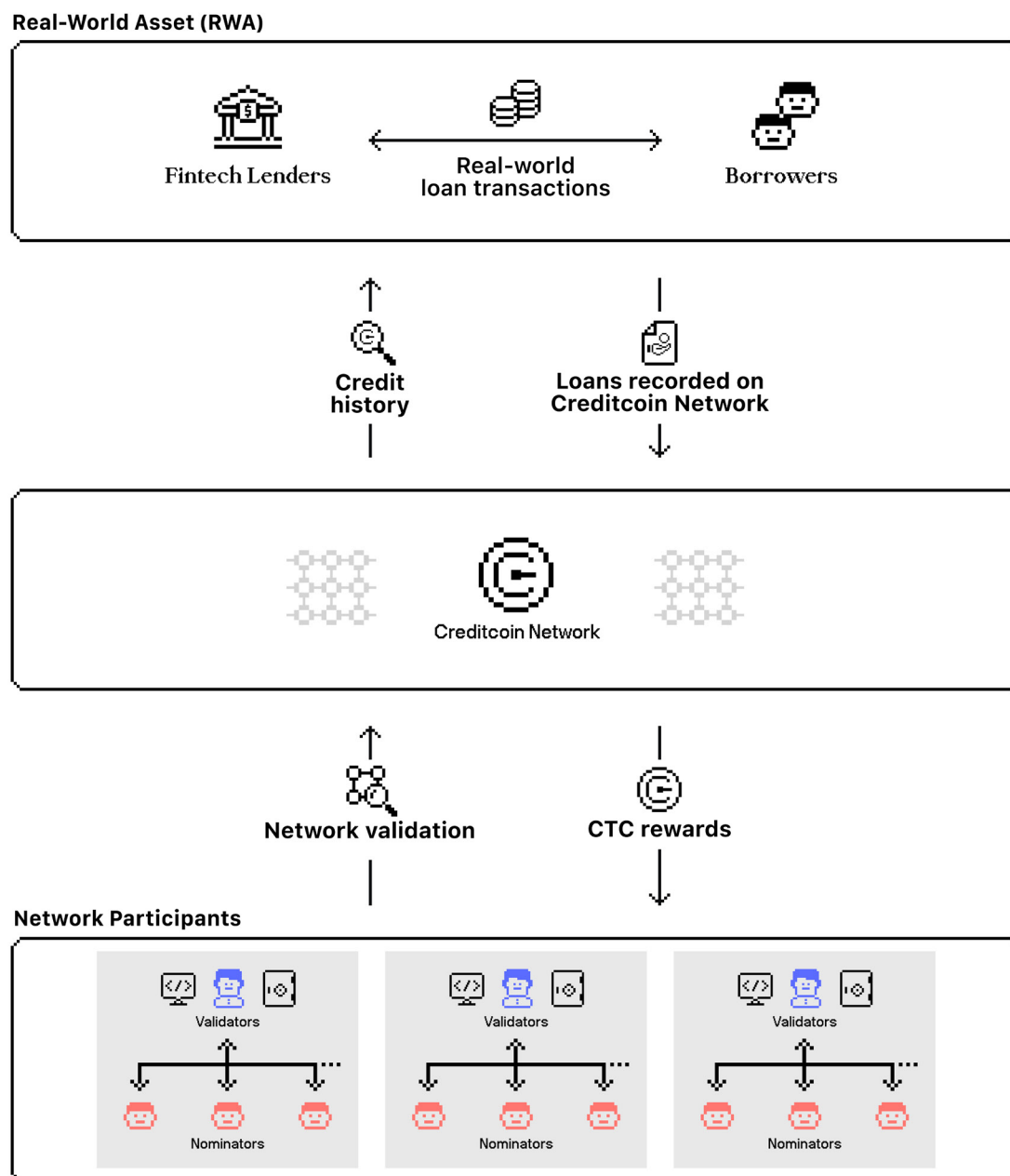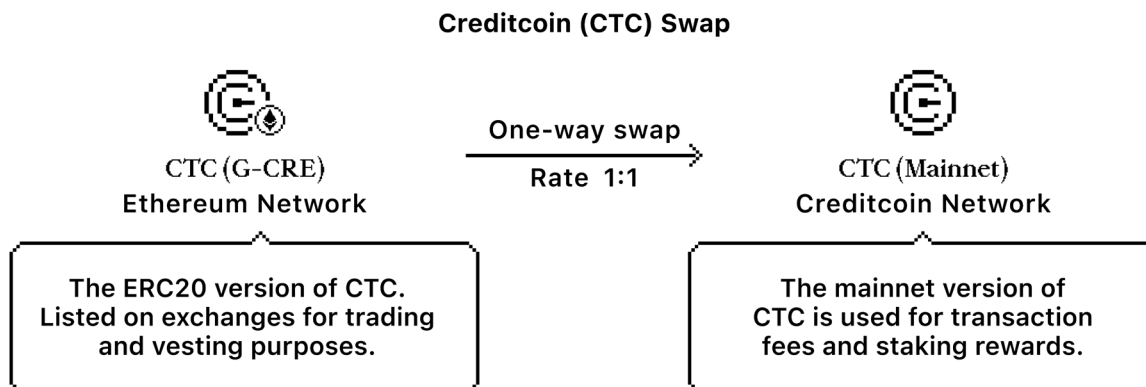
2. CTC (Mainnet) vs CTC (ERC-20)

The Creditcoin Network has two different types of tokens. Whilst these are both commonly called CTC, and represent two sides of the same coin, they actually have two different purposes. It's important you understand this difference.

CTC (Mainnet) - As the name implies, these are CTC tokens used on the Creditcoin mainnet, and represent the primary utility token of the Creditcoin Network. CTC (mainnet) tokens are used for transaction fees as well as staking rewards. The primary market for CTC (mainnet) tokens are financial institutions and RWA fintech lenders recording their transactions on the Creditcoin network. CTC (mainnet) tokens are burned when used.

CTC (ERC-20) - CTC (ERC-20) are the tokens listed on crypto exchanges and represent the trading and vesting token of the Creditcoin Network. On centralized exchanges, you will see CTC (ERC-20) represented with the CTC ticker, while on decentralized exchanges, you may see CTC as G-CRE. CTC (ERC-20) aka G-CRE can be swapped to CTC (mainnet) using a one-way 1:1 swap function.

Creditcoin (CTC) Swap

CTC (G-CRE)
Ethereum Network

One-way swap
Rate 1:1

CTC (Mainnet)
Creditcoin Network

The ERC20 version of CTC.
Listed on exchanges for trading
and vesting purposes.

The mainnet version of
CTC is used for transaction
fees and staking rewards.

	CTC (Mainnet)	CTC (ERC-20) AKA G-CRE
Purpose/Utility	Mainnet transactions and staking rewards	Trading and vesting
Staking Rewards	☑	✕
Acquisition Method	Swap or staking	Buy on exchange
Listed on Exchanges	✕	☑
Swappable	✕	☑

3. Validators and Nominators

Creditcoin is built on a Nominated Proof-of-Stake consensus (NPoS) algorithm that rewards validators and nominators for participating in good faith and penalizes bad actors who may damage the integrity of the network.

Validators participate in consensus by creating new blocks and finalizing previous ones. To be part of the active validator set, validator candidates must have stake behind them. It can be theirs or from third parties, which we call nominators. All elected validators have equal block production rights, no matter the stake behind them.

Nominators can participate in Proof of Stake consensus without running their own validator nodes. They do this by backing up validators with their stake. By doing this, they share rewards and slashing with elected validators.

Potential validators indicate their intention to be validator candidates. The candidate list is made public so that nominators can submit a list of their preferred candidates.

4. Validator Election

The validator election process involves three distinct steps; Nomination, Winner Selection, and Stake Distribution. These three steps are repeated for each **Era**. Each **Era** is composed of **2 Epochs** and **each Epoch is 12 Hours**. Therefore, Validators are re-elected every 24 hours. 50 Validators will be elected in each Era. This number will increase as the network grows and becomes more robust.

In the **Nomination step**, Validators mark themselves as candidates and nominators can decide to support them with their stake. One nominator can vote for several validators in the same Era. In the **Selection step**, winning validators are selected by summing up all the stake that is supporting them. Those Validators with the most votes/stake are elected and become part of the active set for the upcoming Era.

Once the network decides on the active validator set, it must decide who is responsible for producing each block in the Epoch. The slot distribution is achieved through a combination of 'Blind Assignment for Blockchain Extension' (BABE) and Aura.

BABE is the block production mechanism that runs between the validator nodes and determines the authors of new blocks. BABE assigns block production slots to validators according to stake and using a Verifiable Random Function. Slots are discrete units of time of approximately 15 seconds in length. Validators participate in a lottery for every slot, which will inform whether or not they are the block producer candidate for that slot. Due to the specifics of the lottery, multiple or no validators can be selected for a slot, resulting in either a race condition or an empty slot (inconsistent block time).

In order to ensure that any empty slots are assigned and produced, the **Aura** approach is used. Aura is a deterministic and much simpler process to distribute slots.

A given Validator is allowed a maximum of 512 Nominators.

5. Reward Distribution

Validators and Nominators are rewarded at the end of each Era, according to the number of Era Points a validator has earned by producing blocks. The total reward is calculated using the era duration and the percentage of staked tokens.

Assuming all validators are honest and are 100% online when required, block production slots for an era are distributed evenly among them, no matter their total stake. Ideally, they all earn a similar amount of Era Points and thus a similar amount of tokens.

Each block will offer a reward of 2 CTC that will be distributed between the Validator and the Nominators, proportionally to the amount of CTC Staked. Validators may set a commission fee that will be paid before the reward is split. For example, if a validator sets a commission of 10%, the total shared reward for a single block would be 1.8 CTC. If a particular nominator has staked 20% of the CTC for this validator, they would receive 20% of the 1.8 CTC from that block.

6. Slashing and Penalties

If a Validator shows harmful behavior, a percentage of their staked tokens will get Slashed as a penalty, meaning they will lose them. Any Nominators who are actively nominating a Validator that is Slashed will also be Slashed, and will be stripped of their tokens and rewards. This incentivizes thoughtful voting from nominators. Node operators can also send reports to the network when they detect a particular offense. If the report turns out to be valid, they are rewarded with a portion of the Slashed tokens.

Inactivity Slashing Penalty
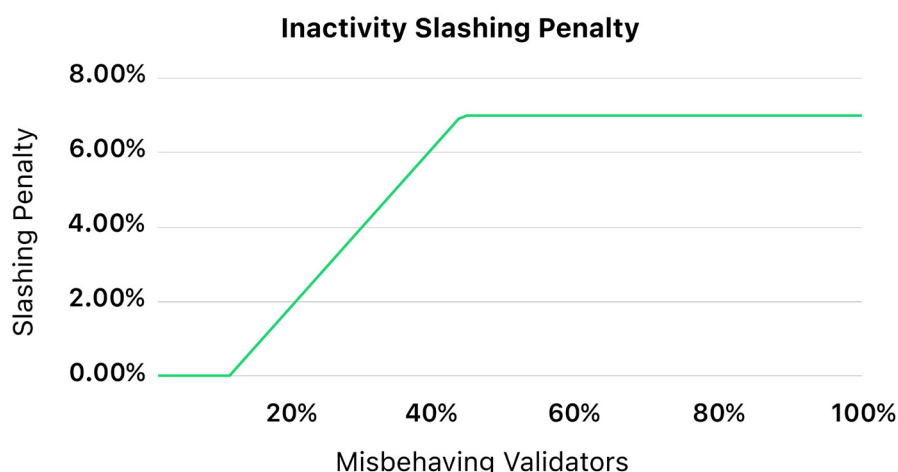
There are three types of offences in the Creditcoin network which can lead to a validator getting slashed: inactivity, block production, and block finalization.

1. Inactivity

If more than 10% of the network is offline, it is considered a coordinated attack. Slashing begins and climbs linearly up to 7% based on the percentage of the network that is offline. If less than 10% of the network is offline there is no slashing.

Inactivity Slashing Example

Here's an easy-to-follow scenario of how slashing works for inactivity. Based on the chart, you can see the slashing penalty increases linearly as a greater % of misbehaving validators are detected.

Slashing begins when 10% of validators are detected to be misbehaving and imposes a penalty of 0.021%. When the % of misbehaving validators reaches 44%, slashing linearly increases to 7%.

In the Creditcoin network, there are 50 validators, each responsible for securing the network, producing new blocks, and validating transactions. Each validator has bonded (or staked) a certain amount of CTC tokens as collateral.

For simplicity, we will assume that all 50 validators have staked 100 CTC each.

When the network detects that 10% of validators (or 5 validators) are misbehaving, slashing penalties will be imposed for those respective validators of 0.021 CTC (0.021% slashing penalty * 100 CTC tokens).

When the network detects that 44% of validators (or 22 validators) are misbehaving, slashing penalties will be imposed for those respective validators of 7 CTC (7% slashing penalty * 100 CTC tokens).

The slashing mechanism ensures validators are motivated to stay online and perform their duties efficiently by enforcing a tangible penalty.

It is also important to note that when a validator is oversubscribed during an

era, only the top 512 nominators receive staking rewards. However, when it comes to slashing, all active nominators of a validator found committing a slashable offense will be penalized.

2. Block Production

If a validator produces more than a single block in their assigned slot, they may be Slashed between 0% and 100%.

3. Block Finalization

If a validator finalizes two or more blocks in the slot on distinct forks, it can be reported and may be penalized using the same formula.

Slashing Calculations

Offence	Formula	Range
Inactivity	min((3 * (offending_validators - (total_validators / 10 + 1))) / total_validators, 1) * 0.07	0% (chill) – 7%
Block production offence	(3 * (offender_count) / total_validator_count) ^ 2	0% – 100%
Block finalization offence	(3 * (offender_count) / total_validator_count) ^ 2	0% – 100%

7. CTC Distribution

The CTC mainnet ecosystem reserve does not include vesting tokens. All mainnet tokens were distributed as mining rewards pre-Creditcoin 2.0+. With the upgrade to NPoS, CTC (mainnet) tokens are distributed as staking rewards.

The initial distribution of CTC (ERC-20) aka G-CRE tokens are as follows:

- Investors (Genesis allocation; 6-month to 3-year linear vesting) – 200M CTC, For funding network development, business development, partnerships, and support. Any unsold tokens were remitted to the Creditcoin Foundation with a vesting period of 6 years.

- Gluwa, Inc. (Genesis allocation; 6-year linear vesting) – 300M CTC, For R&D, deployment, business development, marketing, distribution, and administration costs.

- Creditcoin Foundation (Genesis allocation; 6-year linear vesting) – 100M CTC, For long-term network governance, partner support, academic grants, public works, and community building.

V. Epilogue – Designing Creditcoin

As James Rickards, the author of Currency Wars, said, "Currency is not only used to buy goods and services... people should be able to lend and borrow to make it a currency." Although cryptocurrency already has a significant portion of the market (more than $70 billion), it is true that the capital market infrastructure it provides is limited to payment. Cryptocurrency will eventually require a credit network.

People say, "If all you have is a hammer, everything looks like a nail." Just like with any other technology development project, before we get started with a blockchain project, we have to ask ourselves whether it is the best technology for solving the problem.

The problem we are trying to solve is the vicious cycle that unbanked people experience. We set the unbanked as our target group because they are the stratum that has reason to use cryptocurrency—even with some of the inconveniences associated with the premature ecosystem.

Many people can't get signature loans from the traditional banking system. As a result, they borrow money using other methods, and banks cannot record these transactions. So, credit records do not accumulate in the banks, which means that people cannot build credit—there is no reason for banks to believe the individual files of lenders. Eventually, the vicious cycle of receiving credit loans again in adverse conditions repeats. To summarize, the credit history of the unbanked does not get objectively accumulated.

The solution is to build a system that stores credit records objectively. As stated earlier, a blockchain is a technology specialized in keeping data objectively. The blockchain is the perfect technology to solve this problem.

Once you decide to use the blockchain, you need to make a choice: Are we using a smart contract, or are we building a new blockchain?

A smart contract is enough to store information on the blockchain. We can save significant time if we use a blockchain with a well-established ecosystem as a platform such as Bitcoin or Ethereum. Designing and building a proprietary blockchain is very time-consuming.

However, existing blockchain platforms are slow and expensive. A blockchain is a decentralized system that runs the same computation on many nodes across the world in exchange for security and availability in a byzantine environment. Therefore, the best performing blockchain is always less efficient compared to a centralized server. Also, multi-purpose systems like Ethereum are less efficient than single-purpose systems like Bitcoin. Platform blockchains will stay relatively slow and expensive for many years to come.

We have experienced the limitations of the existing blockchain platform.

We first built the Creditcoin network with a ERC-20 standard smart contract of Ethereum to make a proof-of-concept of Creditcoin. Something had happened by the time we finished building the smart contract. At that time, Cryptokitty on Ethereum was becoming popular, and transactions began to accumulate without being processed, which caused the cost of using Ethereum to increase considerably, making it economically impossible for the unbanked to use the smart contract. Our partner, Aella, gets over 1,000 loan requests per hour. We concluded that we could not operate Creditcoin as an Ethereum smart contract.

We finally decided to develop a proprietary blockchain. After reviewing the requirements, we found that Parity Substrate was the best for our needs.

We decided to develop a blockchain with a single purpose. Creditcoin is only intended for recording credit transactions. In the end, users who want to transact Cryptokitty and others who wish to trade file storage space don't have any reason to compete with each other for limited bandwidth. Blockchains with a single purpose will not interfere with each other's traffic since they are in different markets. User behaviors will determine the cost and the traffic of each blockchain.

During the design process, we were confronted with many questions. We started by defining what a loan is. A loan is essentially a conditional transaction. There are usually dozens of conditions you can set for a loan, and that means there are thousands of possible types of loans. As Creditcoin is not a smart contract platform, it should not support every kind of loan. Then, what is the most basic loan? It is borrowing money and paying it back with more money. In short, it is a contract saying, "I will repay $110 if you lend me $100." You will pay interest even if you pay back earlier than the expiry date. More specifically, it is a non-collateralized bullet loan with a prepayment penalty.

Next, we've defined the types of transactions in the order of creating a loan contract. First, there is a bid, offer, and deal at the stage where both users agree on the conditions of a loan. Then, there are two transactions: an investment transaction for a lender to send money to the borrower and a repayment transaction for a borrower to repay the money back to a lender. At this time, if the lender and the borrower have negotiated the reimbursement amount, the lender may receive only a portion of the money and exempt the rest. The lender may also transfer the receivables to another person as a creditor.

A difference between Creditcoin and Bitcoin is that Creditcoin needs to support a variety of different types of transactions.

There has been much discussion about supporting collateral. In reality, many loans have collateral. If security tokens mature, they will play a useful role as collateral for Creditcoins. For example, you can borrow money with the real-estate security tokens as collateral for loans. However, the standard for the security token does not exist yet, and we do not see any substantial traction of security tokens. Therefore, we have decided not to implement this idea until the security token establishes a mature ecosystem.

Bitcoin only supports a single type of transaction: transfer. However, Creditcoin needs to support seven types of transactions. Each transaction will have a different value depending on the user, and demand for transactions will also vary. What if users ask for extra fees for certain types of transactions? If validators get the transaction fee as Bitcoin miners do, a transaction with more transaction fee attached to it will be a priority for them. This might cause bottlenecks. For example, although users have made 100 loan agreements, no investment transactions get processed.

So, we decided to see how the market would respond to a wide range of transactions. The initial release of Creditcoin will have a fixed transaction fee. We will collect live usage data to make decisions for future development.

Ideally, users should be able to get a loan on any blockchain. How would Creditcoin know if investment or repayment transactions are done correctly on other blockchains? We use the transaction ID of other blockchains. Creditcoin node operators run nodes of different blockchains and enter transaction IDs to look up transaction details in other blockchains.

Creditcoin currently supports Bitcoin and Ethereum. Creditcoin can support a blockchain as long as a Creditcoin plug-in is developed.

Now Creditcoin is completed. With Creditcoin, you can get non-collateralized bullet loans with a prepayment penalty, and you can transfer loans as well. If you develop a plug-in, you can connect any blockchain to Creditcoin. Creditcoin matches loan orders in the blockchain and verifies the investment and repayment transactions in other blockchains. Welcome to the borderless credit market.

VI. Regulatory, Compliance, and Legal Considerations Section

Currently, digital tokens are being closely and regularly scrutinized by various regulatory bodies around the world, including but not limited to the SEC, European Securities and Markets Authority, and each individual state in the United States. Law regarding ICO's is an evolving area, and there is no clear guidance from regulatory agencies, courts, and laws regarding legally-compliant practices for ICO's. As a result, the future evolution of the law and potential consequences are too speculative for Gluwa to reasonably foresee and act upon. However, Gluwa has taken good-faith measures to account for the evolving law and rules on ICO's in an effort to comply with such law, but there is still substantial risk surrounding legal compliance for any ICO in light of the little legal guidance.

There is a substantial risk that in numerous jurisdictions, including the United States, Creditcoins may be deemed to be a security, meaning such tokens must be registered or comply with an applicable exemption from registration. For example, applicable securities laws may limit the ability to hold more than certain amounts of Creditcoins; restrict the ability to transfer Creditcoins; require disclosure or other conditions in connection with any sale of Creditcoins; and may restrict the businesses that facilitate exchanges or effect transfers of Creditcoins.

Every user, purchaser, and holder of a Creditcoin is required to make diligent inquiry to determine if the acquisition, possession and transfer of Creditcoins is legal in their jurisdiction, to comply with all applicable laws, and any of Gluwa's terms and conditions. Creditcoins and the Creditcoin network may be eliminated by future regulation or legal actions. In response to such action, Gluwa may take actions that adversely impact you and the Creditcoins you hold, including: (a) ceasing operations or restricting access in certain jurisdictions, (b) voiding, refunding or not processing token purchases, or (c) ceasing operations entirely.

Each token holder is: (a) if in the United States, or a U.S. Person (as defined in Regulation S under U.S. Securities Act of 1933 (the "Securities Act")), an accredited investor (as defined in Regulation D under the Securities Act) or (b) if outside of the United States, a non-U.S. Person who is not purchasing for the account or benefit of a U.S. Person (as defined under Regulation S under the Securities Act). Each token holder of Creditcoin is sophisticated in terms of investment, business, and/ or blockchain technology, or able to fend for themselves or have access to the information that can allow such purchasers to fend for themselves with regard to the subject matter of Creditcoins.