Interlay v2: Bitcoin Finance, Unbanked

Interlay Labs

Version 1.0 - 13 February 2023

Abstract

This whitepaper introduces Interlay v2, a decentralized network designed to provide DeFi tooling for Bitcoin. Interlay utilizes an already operational, decentralized bridge to connect Bitcoin with a lending protocol and AMM decentralized exchange, enabling Bitcoin holders to access basic financial services without relying on centralized exchanges. Its modular design and support for trustless, light-client bridge protocols allows Interlay to become a layer for connecting Bitcoin with the rapidly growing, multi-chain DeFi ecosystem.

Contents

1 Introduction

Bitcoin started a movement towards a decentralized, transparent, and censorship-resistant financial system. A decade later, Bitcoin has 300 million users and has penetrated every sector: internet giants, department stores, banks, and even nation-states have started to adopt Bitcoin as a method of payment or investment.

There is, however, a controversy - a chasm between adoption and innovation. While Bitcoin is the driving factor for cryptocurrency adoption worldwide, the majority of innovation happens on other, newer networks that support smart contracts. Smart contracts have unlocked novel decentralized financial products, community governance (DAOs), censorship-free identity systems, and new forms of ownership (NFTs), creating a multi-billion-dollar market under the umbrella term "web3".

While demand for Bitcoin in web3 applications is higher than ever, Bitcoin finance almost exclusively relies on centralized systems, controlled by a few institutions. Numerous players, including wBTC, renBTC, Liquid, RSK, attempted to fill this market gap, yet ended up with solutions that rely on a set of trusted parties to hold BTC in custody. On the other hand, attempts to engineer more complex financial products directly onto Bitcoin have struggled with limited programmability and resorted to centralization one way or the other. As such, strictly speaking, Bitcoin "DeFi" does not yet exist.

How can Bitcoin succeed as a global financial system if everything around it is centralized and controlled by a few, politicized institutions?

2 Interlay: From Trustless Bridge to BTC DeFi Hub

Interlay's vision is to help Bitcoin achieve mass adoption by unlocking decentralized financial use cases for BTC while removing the need for centralized exchanges. The idea for Interlay was born in 2018 with the publishing of the XCLAIM protocol paper [1] describing the first trustless and decentralized bridge BTC and blockchains that support smart contracts, including a prototype for Ethereum. In 2022, the Interlay network went live implementing a refined version of the XCLAIM bridge, improving over the academic paper in terms of security and usability. This paper outlines Interlay's next big step: native support decentralized financial tools tailored to Bitcoin.

Interlay v1: iBTC – Bitcoin for DeFi Interlay v1, as operational at the time of writing, offers Bitcoin holders to use their BTC for DeFi via a novel, trustless bridge design. By locking BTC on Bitcoin, users mint iBTC, a 1:1 representation of Bitcoin on Interlay, compatible with other networks. iBTC is a so-called *vaulted* asset: BTC is secured by a decentralized network of vault operators that combines a MakerDAO-like over-collateralization model [2] with cryptographic cross-chain verification of Bitcoin transactions. If a vault operator fails and loses BTC, affected iBTC holders can claim the operator's collateral as reimbursement, avoiding financial damage.

iBTC can be freely moved to other networks: Polkadot's built-in trustless cross-chain mechanism (XCM) has already made iBTC available on other networks within the ecosystem, including Acala, Moonbeam, Astar, and Parallel. Interlay's bridge itself is not limited to Bitcoin and can be expanded to support other networks, as well as different security models.

Interlay v2: DeFi for Bitcoin The next iteration of the Interlay network is centered around making DeFi primitives easily accessible to Bitcoin holders. While iBTC can already be used in DeFi protocols across multiple chains, cross-chain interactions are slow, expensive, and complex in terms of user experience. Further, specialized AMMs, lending, and other DeFi protocols each come with their own risk models and intricacies that require careful assessment. This poses a hurdle for the onboarding of non-expert users who are used to the simplicity of centralized exchanges.

Interlay v2 introduces *native* DeFi functionality to the network: a decentralized AMM-based exchange (Uniswap v2 model and Curve Stableswap) paired with a liquidity protocol for BTC borrowing and lending (Compound v2 model). By creating markets catering to Bitcoin holders and building deep liquidity in these protocols, Interlay will enable easy, one-click access to Bitcoin-centered DeFi use cases, ranging from simple passive liquidity provision to tailored long/short

leverage positions. Interlay's modular architecture and integration with (trustless) cross-chain bridge protocols such as Polkadot's XCM, enables users to leverage AMMs, lending markets and other DeFi protocols on external chains for maximum flexibility and cost optimization.

In parallel, v2 brings enhancements to cross-chain bridges. The addition of native DeFi primitives unlocks novel collateral re-utilization models for the iBTC bridge, significantly improving capital efficiency. Separation of concerns between technical vault operators and collateral delegators that only contribute capital reduces scalability bottlenecks and removes technical entry barriers for new capital. Integrations with (semi) trustless bridges to networks beyond Polkadot, including Ethereum and Cosmos, unlock new BTC use cases and position Interlay as a on- and off-ramp for Bitcoin in DeFi.

Outline Section 3 provides a deep dive into the new Interlay architecture, covering consensus, (bridge and oracle) infrastructure, DeFi, and application layers. Updates to the fee model are proposed in Section 4. Section 5 introduces updated economic models to the native INTR token (short "INTRnomics"). Finally, an outlook on upcoming product and feature improvements, as well as open "moonshot" problems is presented in Section 7.

3 Interlay v2 Architecture

Interlay is a modular network optimized to host decentralized Bitcoin finance protocols. The network consists of four layers as depicted in Fig. 1:

- **Consensus, Computation, and Governance**: The base layer provides security through consensus, functionality through computation, and community control through governance.
- **Infrastructure**: The infrastructure layer enables bridging between Bitcoin through Interlay's decentralized bridge as well as bridges to other DeFi networks.
- **DeFi**: The DeFi layer facilitates basic financial primitives including lending, borrowing, and exchanging assets.
- **Application**: The application layer provides easy access for end users via the UI as well as developer access via SDKs and APIs.

3.1 Consensus, Computation, and Governance Layer

Interlay is a decentralized layer-1 network, powered by and optimized for Bitcoin. Operated as a Polkadot parachain [3] the Interlay network achieves 12-second block times, up to 1500 transactions per second.

3.1.1 Computation: Substrate

Interlay is built on Rust using the Substrate framework [1] and features a *modular* WASM runtime with the following properties:

- **Customization**. Interlay is optimized for interoperating with Bitcoin. This includes re-using Bitcoin core's robust cryptography libraries and efficiently performing complex operations, which would be unfeasible on generalized virtual machines like Ethereum's EVM.
- **Extensibility ("Plug-and-Play")**. Additional functionality can be added without major changes to existing modules: new products can be deployed quickly, without halting ongoing operations - also in collaboration with partner projects.
- **Interoperability.** The modular architecture also works cross-chain: Utilizing XCM, IBC, or Snowfork, components of the protocol stack can be optimized. For example, if there are AMMs with deeper liquidity or less slippage, then the one-click strategies might opt to replace the Interlay AMM for specific assets with asynchronous cross-chain AMM calls.

[1] `https://substrate.io/`

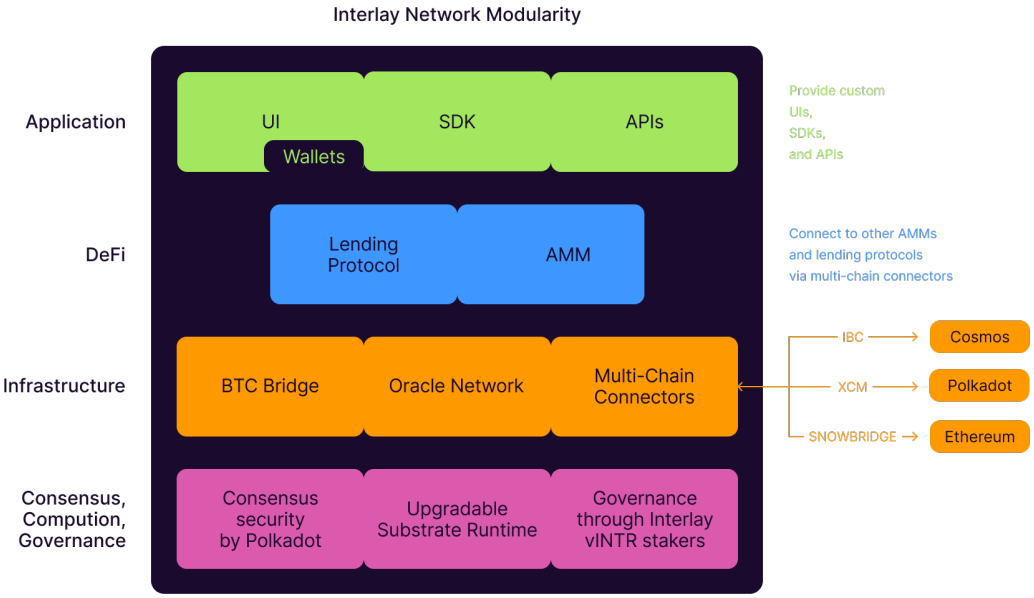

Figure 1: The four layers and main modular components of the Interlay network.

- **Scalability**. Sub-modules that require high throughput can be outsourced to additional Substrate chains, either operating as equivalent units to Interlay (as is the case for the Kintsugi canary network, cf. Section 6) or as hierarchically subordinate chains (the Interlay chain would assume a coordination role, similar to the Polkadot Relay Chain [3]).
- **Forkless upgrades** The Interlay runtime is a deterministic WASM code. As consensus nodes execute the WASM code that is stored in the network, the runtime can be upgraded independently of upgrading the consensus nodes. By accepting a new WASM runtime through governance, the consensus nodes simply execute the updated runtime without having to opt-in to any changes.

Automated and Off-Chain Computations. Smart contracts, e.g. deployed on Ethereum, require someone to call a function by creating an on-chain transaction - which may cause unfavorable delays for real-time processes, such as liquidations. Substrate solves this issue by allowing to define actions that are performed at the start of each block[2], guaranteeing that, e.g., security-related processes are reliably executed even under high transaction load (e.g., price oracle processing). In addition, critical but resource-heavy computations, e.g., complex liquidation checks over thousands of users, can be outsourced to consensus nodes, such that they are automatically performed off-chain with results submitted to the network upon completion [3].

3.1.2 Consensus: Polkadot Parachain

As of this writing, the Interlay network is deployed as a Polkadot parachain, and we refer the reader to the Polkadot technical paper for more details on the consensus architecture [3].

In summary, the Interlay network operates as an independent chain, secured by Polkadot's Proof-of-Stake consensus. So-called Collators produce blocks for the Interlay blockchain, generate proofs of state validity, and submit these to Polkadot validators, who verify the correctness and finalize the system state. Validators are shared across and achieve agreement over the state of all Polkadot parachains. Parachain slots are allocated for 2 years via an auction mechanism, with Interlay's next slot being subject to renewal in January 2024.

[2] https://docs.substrate.io/fundamentals/transaction-lifecycle/
[3] https://docs.substrate.io/fundamentals/offchain-operations/

By operating as a parachain, the Interlay network benefits from the security and decentralization of Polkadot's consensus, and built-in interoperability with other parachains, with the safety of cross-chain transfers enforced by Polkadot itself.

3.1.3 Governance: Interlay

Governance decides on the Interlay runtime: any rules of the network are subject to the changes proposed and voted on by its community. Importantly, governance is able to upgrade the network at any time by introducing a new WASM runtime. Section 5 explains governance in detail.

3.2 Infrastructure Layer

3.2.1 Decentralized Bitcoin Bridge: Vaulted BTC

The main building block of Interlay is a decentralized Bitcoin bridge that enables minting of iBTC - a multi-chain 1:1 Bitcoin-backed asset. The design follows the XCLAIM framework introduced in 2018 [1], with considerable functional and security improvements. We provide a high-level summary of the currently deployed system below, and summarize V2 extensions. The full specification can be found online[4].

Vaulted Bitcoin. The Interlay Bitcoin bridge introduces a new kind of "wrapped" asset: *vaulted* Bitcoin. iBTC is a fully fungible, tokenized representation of BTC on other blockchains that allows the owner to redeem it for BTC at a 1:1 ratio *or, in case of bridge failure, for insurance collateral in other digital assets at a premium rate.*

The Interlay bridge is maintained by an open (anyone-can-join) network of over-collateralized *vault* operators. Each BTC deposited by a user into a vault is insured by collateral provided by the operator. This collateral is used to automatically reimburse iBTC owners in case of operator failure.

Pre. **Vaults register**: Once at least one Vault has locked collateral on the Interlay chain, users can start minting iBTC.

1. **Mint iBTC**: User requests to issue and sends BTC (on Bitcoin) to the Vault address provided by the Interlay chain. The Vaults collateral is now locked and the Interlay chain issues iBTC to the user at a 1:1 ratio to the deposited BTC, minus fees.

2. **Use iBTC**: iBTC can now be used in Interlay DeFi and on other chains as a fully fungible asset.

3a. **Successful redeem**. The user returns iBTC to the Interlay chain and requests a redemption. One or more Vaults send BTC to the user (on Bitcoin), minus fees, and prove this to the Interlay chain. The Vaults collateral is unlocked. A user can redeem with any Vault they like.

3b. **Failed redeem**. If a Vault does not send BTC to the user within a pre-defined period (currently 48h), the user can decide whether to (a) retry with another Vault or (b) trade iBTC for the Vaults collateral. In both cases, the user receives a premium, slashed from the Vaults collateral.

From an economic perspective, the Interlay bridge functions similarly to a peer-to-peer lending protocol. Users deposit BTC to borrow iBTC at a 1:1 rate. Vaults receive the deposited BTC as a loan, in return for locking collateral. iBTC represents a claim on the deposited BTC at a 1:1 rate or the vault's collateral at a premium rate.

[4] `https://spec.interlay.io`

Collateral Following the MakerDAO model [2], each Vault has exactly one collateral asset, while an operator can open multiple different Vaults using the same account. Collateral assets must be white-listed by a governance vote. Each asset undergoes a risk assessment by the community and external risk teams, defining the ceiling (i.e., the absolute amount allowed in the system) and the following safety thresholds per collateral:

- **Secure threshold** (e.g. 160%). The target collateralization rate at the time of minting. The secure threshold defines how much iBTC can be minted with a Vault.
- **Premium Redeem** (e.g. 120%). Redeeming with Vaults below this threshold is incentivized: the redeemer claims a small, volume-based premium (e.g. 5%) charged to the Vault.
- **Liquidation** (e.g. 110%). Vault positions that fall below this threshold are automatically liquidated by consensus nodes.

Interesting collateral assets include BTC-correlated L1 tokens, fiat-backed stablecoins, and interest-bearing assets e.g., liquid staking and LP tokens (see "Extensions" below).

Liquidations Liquidations ensure that the following invariant between the amount of iBTC minted and collateral locked *COL* holds for each Vault:

$$iBTC \leq COL \cdot exchangeRate_{(BTC,COL)} \cdot liquidationThreshold \tag{1}$$

When a Vault is liquidated the bridge considers the BTC lost (the Vault is allowed to keep the BTC) and instead uses the liquidated Vault's collateral to temporarily back the value of iBTC. *Any* iBTC owner can then re-balance the bridge by "burning" iBTC to claim the collateral at a premium rate (e.g. 110%).

BTC Relay The Interlay parachain tracks and verifies the state of the Bitcoin blockchain using a built-in light client [4]. The so-called *BTC-Relay* verifies block headers and proofs of transactions being included in the Bitcoin blockchain, handling forks when needed. This allows the Bitcoin bridge to enforce correct behavior on participants and penalize malicious actions, making it *economically trustless*: both users and Vault must submit cryptographic proofs to confirm the correct execution of iBTC mint and redeem requests or incur penalties otherwise.

Bridge Security An in-depth security analysis is provided in the original, peer-reviewed XCLAIM paper [1] and the Interlay specification [4]. The open-source implementation [5] has been subject to multiple audits, with reports available online[6]. A detailed comparison to other, centralized bridges, can be found in the following peer-reviewed cross-chain systematization paper [5].

In summary, the two main properties of the Bitcoin bridge are decentralization and *economic* trustlessness.

- **Decentralization** is achieved by allowing anyone to register as a Vault operator, without requiring any form of permission. The bridge is also *censorship-resistant*: the minting process is *non-interactive*, meaning there is no action that must *or can* be taken by Vault operators to interfere with or prohibit the creation of iBTC.
- **(Economic) Security** is achieved by requiring Vault operators to over-collateralize their BTC positions and cryptographically prove correct redemption of BTC. Liquidations ensure that users can always redeem BTC or are reimbursed in collateral, facing no economic damage (cf. Equation 1).

We observe Equation 1 holds under the assumption that (i) the bridge is aware of the current exchange rate between BTC and collateral assets (i.e., assumes robust price feeds, cf. Section 3.2.2), and (ii) that the value of the collateral does not devalue faster than the time it takes a liquidator to complete a successful arbitrage trade, i.e., include the liquidation transaction in the Interlay chain and exchange the claimed collateral for BTC or iBTC.

[5] `https://github.com/interlay`
[6] `https://docs.interlay.io/#/about/audits`

v2 Feature Extensions We have described v1 of the Interlay bridge, as currently deployed on the Interlay network. The next iteration (v2) features significant improvements in terms of scalability and economic efficiency.

- **Operator-Delegator Model** Currently, Vaults combine two roles: First, they provide the collateral to secure the bridged BTC. Second, they run infrastructure to maintain the BTC-Relay and automate cross-chain transactions on Bitcoin and Interlay. In v2, these two roles are split into Operators and Delegators. Operators, like v1 Vaults, run the Vault software and can provide collateral to increase their capacity. Delegators, a new role, can stake their collateral with Operators *without* running software themselves. This feature will be rolled out gradually. In the first iteration, the Operator will still have access to the BTC but not to the Delegator's collateral. Delegators can pick Operators based on previous performance and other social scores, incentivizing honest and proactive behavior of infrastructure providers. In the final version, the Delegator will be able to parameterize how much BTC is stored in the Delegator's cold-wallet, and how much is held in the Operator's hot wallet, balancing security and usability[7].
- **Collateral Re-Utilization** Vault can use tokenized positions representing capital supplied into the Interlay 2.0 lending protocol (qTokens, cf. Section 3.3.1) as collateral to secure the bridge, earning interest on their capital from both protocols. LP tokens representing positions in the AMM decentralized exchange (cf. Section 3.3.2) can also be supported be as Vault collateral. The latter is particularly useful to represent baskets of different assets as single Vault collateral positions, unlocking more flexible risk management.

3.2.2 Oracle Network

To verify collateralization rates on the bridge, as well as in DeFi protocols, Interlay requires a robust price feed, reflecting (near) real-time exchange rates from across centralized and decentralized exchanges. By design, Interlay supports an unlimited number of exchange providers submitting price data into an on-chain medianizer. In v1, price data was medianized off-chain and fed to the network via a single provider.

In v2, the responsibility to provide price data is distributed among reliable ecosystem partners, including but not limited to infrastructure providers, dedicated oracle projects such as DIA and Chainlink, non-profit web3 organizations (incl. DAOs) and individuals who take up a stake in the network - subject to whitelisting by governance. In addition to medianizing price feeds, the on-chain oracle implements several safeguard mechanisms to mitigate manipulation. Most notably, instead of reporting the last traded price, the system uses an exponentially weighted average that smooths out temporary price fluctuations that do not necessarily reflect the true value of the asset. Further, a cap on the maximum price over a certain time period is introduced, based on the historic price movement of the underlying asset.

Work towards a dedicated oracle chain has already been initiated. The proposed oracle system can be shared across and operated by multiple projects and L1 networks, thus significantly improving reliability and making manipulation attempts much more costly [6].

3.2.3 Multi-Chain Connectors

Exporting iBTC, as well as importing collateral and trading assets is a central part of the Interlay network's product model. Ultimately, Interlay as a network places a bet on decentralized bridge protocols using *bi-directional light clients* that rely on cryptographic verification of blockchain state rather than trusted intermediaries [5]. Within the next 5 years, decentralized bridges are expected to become the dominant method of communication between major L1 networks. As of this writing, such protocols are operational between homogeneous chains: XCM [3] that connects Polkadot and Kusama parachains and IBC [7] used between Cosmos SDK chains. Snowbridge [8], the first heterogeneous light client bridge, is expected to connect Substrate and Ethereum-like chains in 2023.

[7] Delegators must manually sign transactions accessing their BTC cold-wallet

Expanding from XCM to IBC and Ethereum Today, Interlay already maintains decentralized connections to several other chains in the Polkadot ecosystem making use of XCM. Interlay v2 will add support for the IBC protocol standard to bridge assets from and to the Cosmos and Near ecosystems. Interlay will also integrate with Snowbridge and/or other decentralized solutions to connect to Ethereum. When connecting to chains that do not support trustless light-client bridges, nor exhibit sufficient demand for a native (BTC-like) integration with Interlay's collateralized bridge, the Interlay community may decide to rely on integration with one of the numerous (semi-)trusted providers that use threshold signatures or MPC protocols to distribute trust across a set of public actors. Establishing insurance funds to (partially) recover assets in case of bridge exploits is encouraged in such cases.

3.3 DeFi Layer

Interlay v2 features a set of financial tools, offering Bitcoin users decentralized access to trading, borrowing, lending, and other primitives.

3.3.1 Decentralized Liquidity Protocol

Interlay v2 introduces support for borrowing and lending of iBTC and other assets through a pool-based liquidity protocol, based on the design of Compound v2 [9], .

Lending Pools Assets supplied by lenders into a lending pool are represented by a fungible "qToken" balance. Subject to the supply of the pool exceeding the borrowed amount, qTokens can be redeemed for the underlying assets. As the protocol accrues interest, subject to borrowing demand, the amount of the underlying asset redeemable by each qToken increases. Thereby, generated interest is distributed among lenders of each pool on a pro-rata basis.

To borrow assets, users must deposit qTokens as collateral. Borrowing contracts are open-ended while rates follow the models encoded in the protocol. Each loan must be backed by collateral at a loan-to-value (LTV) ration below 1.0 to ensure that borrowers have an economic incentive to repay their loans. The interest accrued by a loan, payable in the underlying asset, continuously increases the LTV ratio.

Each asset that can be supplied into lending pools must be whitelisted by Interlay network governance. Assets (qToken representations) that can be used as collateral for borrowing require a separate vote. This is to ensure high quality of assets and proper risk management.

Subject to proper risk assessment by community governance, qTokens may also be used as Vault collateral in the BTC bridge. This allows Vaults to lend out their bridge collateral as an additional revenue stream, significantly improving the capital efficiency of the collateralized bridge model.

Liquidations If the LTV ratio of a position exceeds the borrowing capacity, as configured by network governance on a per-asset basis, all or part of the outstanding loan may be liquidated. During a liquidation, an arbitrageur repays (parts of) the outstanding loan in return for the borrower's qToken collateral at the current market price minus a *liquidation discount*. This process can be executed by any user and repeated until a healthy LTV ratio is restored.

Bad Weather Fund A fraction of the profits from each completed liquidation is routed to a "bad weather" fund, maintained by the network treasury. The sole purpose of this fund is to create a financial buffer to assist recovery from bad debt should timely liquidations fail, e.g. due to technical issues.

Interest Rate Model The Interlay liquidity protocol utilizes an interest rate model to balance lending supply and borrowing demand and incentivize liquidity. High demand for an asset leads to a decline in the liquidity of that asset. The protocol reacts by increasing interest rates, which makes borrowing more expensive and incentivizes supply (and vice-versa). The mathematical models for supply and borrow rates are described in Appendix A.

3.3.2 Decentralized Exchange Protocol

To unlock easy access to trading for BTC holders, Interlay v2 introduces a decentralized exchange (DEX). The DEX serves as a capital source for liquidations in the liquidity protocol. Further, the combination of lending/borrowing with trading transactions unlocks a variety of financial products for Bitcoin, including leverage and hedging. In the first iteration, the goal of the DEX is to create deep iBTC liquidity, pairing all major listed assets with iBTC: trades between any two assets should be able to be routed via iBTC.

The DEX supports the following automated market maker (AMM) functions:

1. Constant product AMM($XY = K$), following the Uniswap v2 design [10], which allows pairing iBTC with any other crypto asset.
2. Curve StableSwap AMM [11] for low-slippage swaps between assets that are expected to trade at the same value, e.g., iBTC and wBTC.

Liquidity positions in the DEX are represented through "LP-tokens", which can be transferred and potentially traded themselves. Subject to proper risk assessment by community governance, LP-tokens may also be used as Vault collateral in the BTC bridge.

Flash-Swaps An important feature of the DEX is the support for optimistic transactions, which allow a trader to temporarily borrow assets from the AMM pools and use them for swaps or in other protocols, as long as the loan is repaid in full at the end of the same, atomic transaction. This significantly increases market efficiency, as even small discrepancies can be arbitraged without upfront capital cost, and contributes towards more timely liquidations of under-collateralized loans in the liquidity protocol.

3.4 Application Layer

Building financial strategies and products in DeFi typically requires constructing a sequence of (cross-chain) transactions and interfacing with different protocols - posing a major hurdle to non-technical users. The key to "unbanking" Bitcoin finance lies in removing these complexities: Interlay v2 allows anyone to create tailored DeFi products that are accessible to users via "one-click" interactions.

As opposed to DIY smart contract platforms, Interlay's multi-layered setup prioritizes security over the ability to deploy arbitrary smart contracts[8]. Modular DeFi building blocks can be developed by anyone with Rust and Substrate - but are subject to a community-driven quality assurance process and governance approval that ensures best practices are adhered to and no hidden backdoors or centralization points are introduced. On top of the DeFi layer, the application layer provides a set of open-source APIs, developer tools, user interfaces, and wallet integrations. This design allows traders, product teams, and DeFi-hobbyists to build custom DeFi products without the overhead of forking and maintaining security-critical blockchain or smart contract code.

3.4.1 Tooling

The vision of the Interlay network is to be decentralized on every layer of the stack. To this end, already today, there is a set of open-source tools and interfaces that can be self-hosted and customized by developers and users alike.

SDKs To encourage the development of custom tools and products on top on the Interlay network, both Typescript[9] and Rust[10] SDKs are made available as open-source.

APIs Apart from coding custom integrations, interaction with the Interlay network can be done via the `wss` network node endpoints or GraphQL query endpoints[11], e.g. using Subsquid.

[8] EVM or WASM smart contract support can be added on demand given Substrate's plug-and-play extensibility.
[9] `https://github.com/interlay/interbtc-api/`
[10] `https://github.com/interlay/interbtc-clients`
[11] `https://docs.interlay.io/#/developers/api`

User Interfaces Anyone can self-host a version of open-source the front-end [12] that interfaces with the Interlay network, freely customizing it to their needs. Secure and reliable UX access can be ensured through integrations with data-sharing networks such as IPFS [12], accompanied by governance-driven code authenticity checks (hash pre-image check of the uploaded front-end code).

3.4.2 Composability without Smart Contracts.

Being a Substrate chain, Interlay supports combining multiple blockchain interactions into a single transaction without writing custom smart contract code. Via `utility.batchAll(`tx_0`,` tx_1`,` ...) [13], any user can craft complex financial products within the *synchronous* environment of the Interlay chain, utilizing the Bitcoin bridge, lending protocol, the decentralized exchange, as well as advanced features such as flash-swaps.

When interacting with multiple applications across different chains, *asynchronous* handling of transactions typically requires users to wait and come online multiple times to complete even a simple set of actions. As a Substrate chain, Interlay offers a greatly improved user experience: off-chain workers can listen to cross-chain events and, once detected, automatically submit pre-signed transactions to complete any desired sequence of actions. For example, assume a user wishes to deposit BTC into the lending protocol directly from their Bitcoin wallet. Normally, the user would first have to mint iBTC, wait for the Bitcoin transaction to finalize (up to 1h), then come online again to complete the deposit. Instead, the user can pre-authorize the iBTC lending deposit at the same time as sending BTC to the bridge, letting the off-chain worker do the rest.

3.4.3 Bring Your Own Fees

One of the most cited pains of using new blockchain networks is acquiring the "gas" token to pay for fees, even prior to the first interaction. Interlay v2 follows a "bring-your-own-fees" strategy: while the underlying fees are paid in the native INTR token, users can pay in a set of whitelisted external assets, which are swapped into INTR on the fly using the decentralized exchange.

4 Fee Model

The Interlay network brings together Bitcoin users with service and capital providers to create a decentralized value network. At the core, the v2 fee model builds on iBTC volumes across DeFi products deployed on Interlay, as well as BTC bridge and cross-chain transactions. By default, fee revenues are distributed primarily among providers of each product, while cross-funding of common-good components (e.g. infrastructure) as well a network treasury ("DAO") share may be introduced by community governance.

During the bootstrapping phase of the network, fees are likely to be kept low, prioritizing adoption over revenue generation, and the network treasury may hence subsidize capital and service providers in INTR (cf. Section 5).

4.1 Consensus and Governance Layer

Collators receive transaction fees (base fee plus optional tip specified by the user) in INTR, paid by users of the Interlay network. In addition, Collators receive INTR fees for processing cross-*para*chain transactions via Polkadot's XCM (and in the future potentially Cosmos' IBC and other decentralized bridging protocols). Specified by Polkadot's design, Collator fees are shared across multiple blocks: half of each block's *TransactionFees*, which include cross-chain and off-chain processing fees, go into a Pot. Half of this Pot is paid out at the start of each block. The fees earned by a Collator proposing a block b are hence computed as:

$$CollatorFees_b = \frac{Pot_{b-1}}{2} + \frac{TransactionFees}{2} \tag{2}$$

where Pot_{b-1} refers to the Pot value after block $b-1$.

[12] `https://github.com/interlay/interbtc-ui`
[13] `https://polkadot.js.org/docs/substrate/extrinsics/#batchallcalls-veccall`

Outlook: Off-chain computations Collators can offer auto-execution and computation services to users via off-chain workers. Examples include automated loan repayments and batching together multiple asynchronous cross-chain transactions. In the future and subject to demand, an off-chain execution marketplace may emerge, where Collators advertise paid execution and automation services.

4.1.1 Governance: vINTR stakers

Currently, stakers earn staking rewards in INTR based on the amount of vINTR they hold (vINTR represents the amount of INTR staked and the lockup duration, cf. Section 5). The amount of INTR distributed to stakers is determined by governance - at launch, this parameter was set to 5% of the initial 4-year supply. In v1, the share of each staker was proportional to their share of the total vINTR in existence. In v2, active governance participation is added to the calculation via a *participationFactor*: stakers must vote on a target amount of governance proposals during a rolling interval. The staking rewards of a staker s are hence calculated as follows:

$$StakingRewards_s = StakingRewards_{total} \cdot \frac{vINTR_s}{vINTR_{total}} \cdot \frac{\max(Votes_s, Votes_{target})}{Votes_{target}} \tag{3}$$

This model strengthens the resilience of Interlay's governance against manipulation. Incentivizing higher staking ratios and lock-up periods makes governance attacks expensive, amplified by the fact that vINTR is non-transferable. Additionally, the participation factor combats the lazy voter problem, minimizing the probability of proposals going unnoticed.

4.2 Infrastructure Layer

4.2.1 BTC Bridge: Vault Fee Model v2

Vault revenue is composed of volume-based bridging fees (issue and redeem) and block rewards in the native INTR token, as operational subsidy while bridge revenue is growing. The issue and redeem fees are fixed, volume-based parameters set by governance.

In v1, both income streams were distributed among all Vaults, *proportional to how much iBTC was minted with each Vault*. This model presented itself as non-optimal, leading some Vault operators to fill up their own iBTC capacity to maximize their reward share, without the iBTC necessarily going into circulation. This in turn hindered non-technical users, who cannot run Vaults themselves, from using Bitcoin.

In v2, the revenue distribution hence only takes into account the *available iBTC minting capacity* of each Vault. The capacity of a Vault is thereby a function of locked collateral, collateral thresholds, and whether the Vault is actively accepting new issue requests:

$$VaultCapacity = \begin{cases} \dfrac{Collateral_{BTC}}{\max(CustomThreshold, SafeThreshold)} & \text{if accepting new issue requests} \\ 0 & \text{otherwise} \end{cases} \tag{4}$$

where the *CustomThreshold* optionally set by Vaults is always greater or equal to the protocol-defined *SecureThreshold* for each collateral asset respectively[14]. The revenue of a Vault v is then defined as

$$VaultRevenue_v = (Fees + Subsidies) \cdot \frac{VaultCapacity_v}{\sum_{i=1}^{n} VaultCapacity_i} \tag{5}$$

where n is the total number of Vaults in the system. Higher reward shares are allocated to Vaults that lock up more collateral, follow the (lower-bound) recommended collateral thresholds and continuously service issue requests. The capacity-based fee model hence aligns Vault and protocol interests: The protocol rewards Vaults for allowing as much BTC as possible to securely flow into the system.

[14] Vaults can set more conservative collateral thresholds to reduce risk of liquidation.

Outlook: Market-based and continuous fee models With the increasing demand for iBTC as an on- and off-ramp solution, introducing a market-driven fee mechanism may be more capital efficient for both Vaults and users. Models currently under consideration include (a) a (bounded) open fee market where Vaults can compete among each other for processing volume, (b) dynamic fees along a supply-demand curve (higher demand and liquidity crunches incurring higher fees), and (c) tips paid by users to Vaults for fast/instant iBTC issue processing (Vault takes up the low risk of a Bitcoin blockchain fork in return for higher fees).

Another model being explored, yet in early stages, is the introduction of continuous fees charged to inactive iBTC accounts, e.g. DAOs diversifying their assets into iBTC for long-term holding or iBTC used as liquidity on cross-chain DeFi products. This can, for example, be realized as a subscription fee payment for continuous collateral insurance by Vault operators, deducted directly from the subscriber's iBTC balance.

4.2.2 Oracle Network: Operator Subsidies

Operators whitelisted as oracle providers by Interlay governance can request funding from the treasury to cover maintenance costs, including server infrastructure. In the future, if the Interlay oracle network starts being used by on-chain applications, data requests can be monetized via a flat fee per on-chain read access.

4.2.3 Multi-Chain Connectors: Routing fees

The Interlay network acts as the central hub for iBTC routing within the Polkadot ecosystem via XCM - and in the future, potentially other ecosystems via decentralized bridges, e.g. Cosmos's IBC. In v2, a volume-based fee is added for such trustless cross-chain iBTC transfers. This fee serves to subsidize BTC bridge operations, i.e, the capital costs of the Vault operators' collateral that acts as safety insurance for iBTC holders.

4.3 DeFi Layer

4.3.1 Decentralized Liquidity Protocol: Lenders

The income of capital lenders (cf. Section 3.3.1) comes from the loan repayment fees paid by borrowers, determined by the *SupplyRate* of the borrowed asset as defined in Appendix A. The income of liquidators, i.e., protocol participants that bring up capital to liquidate under-collateralized loans to restore healthy loan-to-value ratios, is determined by a governance-set liquidation premium parameter.

4.3.2 Decentralized Exchange: AMM LPs

The income of DEX LPs is based on the volume-based trading fees generated by each pool of assets a and b, and is distributed proportionally to each LP's share in that specific pool. Trading fees are parameterized per asset pool and set by governance.

4.4 Application Layer

Projects operating of custom front-ends to interact with products on the Interlay network may charge transfer and execution fees, implemented via the `utility.batchAll` functionality. This model can be also used by developers of custom and automated DeFi strategies and portfolio management tools.

Data, Platform, and API Providers The Interlay network is supported by a range of infrastructure providers including block explorers, governance front-ends, and high-throughput API endpoints. These providers submit requests to the network treasury to fund their work, subject to review by the community.

5 INTRnomics: Governance, Revenue, Sustainability

The Interlay economic model derives the following utility for INTR:

- **Transaction fees.** INTR is used to pay transaction fees in the Interlay network, creating a market-driven pricing dynamic based on network utilization.
- **Governance.** INTR must be time-locked (obtaining vINTR) to participate in the network's governance. Voting power increases proportional to the locked-up amount and duration, assigning more voting rights to long-term stakers. Interlay is fully decentralized and governed by community governance, meaning every code and parameter change is subject to vote. Moreover, projects that wish to list specific collateral assets, launch lending/trading markets, or incentivize specific AMM pools are encouraged to participate in vINTR voting.
- **Feature access.** vINTR is a prerequisite for assuming roles in the network and gaining access to features that require having "skin in the game" including running Collators, oracle nodes, and operating Vaults that can receive collateral delegations.
- **Liquidity bootstrapping.** Vaults, lenders, LPs, governance participants, and other users of the Interlay network face capital costs for providing capital and resources. While Interlay's fee and collateral models focus on revenue-generated sustainability, bootstrapping mechanisms can be activated by governance to incentivize early liquidity and accelerate growth.
- **DAO revenue.** Fees accumulated by the DAO from the various decentralized services and products can be distributed to stakeholders, subject to criteria and approval by a governance vote.

Emission and Distribution Interlay v2 makes no explicit changes to the emission and distribution schedules themselves (cf. Appendix C): 70% of the supply are allocated to the treasury. Instead, v2 proposes to remove static schedules (e.g. block subsidies to BTC bridge Vaults, pre-scheduled years in advance) in favor of a continuous, governance-driven review and adjustment process.

5.1 Governance Basics: Liquid, Optimistic, Stake-to-Vote

vINTR stakers act as guardians of the Interlay network by making governance decisions, including but not limited to:

1. **Economic administration.** Proposing and voting on changes to economic parameters (e.g. collateral thresholds), fee rates, and distribution of revenues (bridge fees, lending fees, AMM fees, ...) and subsidies (continuous and ad-hoc treasury spending).
2. **Technical stewardship.** Proposing and voting on technical changes to integrate new features or resolve issues.

A full and up-to-date overview of Interlay's governance system can be found online[15]. Interlay's governance follows a liquid, stake-to-vote model:

Liquid Liquid governance means that every vINTR staker can create and vote on proposals, and all accounts have equal voting rights, i.e., there is no elected board or council.

Stake-to-Vote To create and vote on governance proposals users must lock INTR, minting vINTR - a non-transferable token representing each user's voting power at any given point in time. The more and longer INTR are locked, the more vINTR are minted, assigning more voting rights to long-term stakers. As time progresses, vINTR balances of stakers decrease linearly on a per-block basis. At the end of the lock time, INTR can be withdrawn, all at once. A similar model was first implemented by Curve[16].

[15] `https://wikibitimg.fx994.com/attach/2020/10/189869321/WBE189869321_21425.pdf`
[16] `https://curve.readthedocs.io/dao-vecrv.html`

$$vINTR = INTR \cdot \frac{remainingLockTime}{maxLockTime} \tag{6}$$

Optimistic Governance During the early days of the network, regular code and parameter updates are expected, each requiring governance approval. To promote an active governance process early on and avoid the lazy voter problem, Interlay implements optimistic governance: at low turnouts, proposals require a heavy super-majority of "nay" votes to be rejected. As turnout increases towards 100% (of the vINTR stake) the system moves to a simple majority-carries vote.

$$\frac{vINTR_{nay}}{\sqrt{vINTR_{total}}} < \frac{vINTR_{aye}}{\sqrt{vINTR_{nay} + vINTR_{aye}}} \tag{7}$$

As the Interlay network matures and the financial value at risk increases, it is expected that the community transitions to more conservative, majority-based voting, introducing minimum vote participation for critical decisions.

Technical committee A technical committee (TC) can be (continuously) elected by the community. Its only ability is to fast-track (prioritize in proposal queue and/or shorten voting periods) security-critical proposals, e.g. in case of emergencies. The TC has no other powers.

5.2 Governance v2: Dynamic Governance

So far, INTR block subsidies for Vault operators (and other network participants) were pre-scheduled for years in advance. Such a static mechanism stands in stark contrast to the needs of networks to adapt to the ever-changing macroeconomic, technical, and regulatory environment.

Governance v2 makes exercising vINTR governance power more accessible, following a paradigm shift towards dynamic management of economic subsidies and revenue distributions.
The modular design of the Interlay network creates an ecosystem of various stakeholders with different goals and interests, aligned by the goal of the good economic performance of the overall system.

Stakeholder groups At the launch of this model, we propose the following stakeholder groups.

- **Vaults**: Lock collateral to safeguard iBTC and service mint/redeem requests.
- **Lenders**: Provide capital to the lending market.
- **DEX LPs**: Provide capital to AMM pools.
- **Collators**: Produce blocks and submit them to Polkadot validators.
- **vINTR stakers**: Steer the Interlay network through governance.
- **DAO treasury**: Interlay network economic reserve, i.e., stakers can also vote to temporarily reduce emissions.

Stakeholder groups can be added (e.g. when new products are released) and removed via governance votes.

Pooling block emissions Instead of fixed multi-year emission schedules for stakers and Vault operators, all INTR block emissions are pooled and defined by a single emission function *Emission*() that is determined and can only be changed by a governance vote.

Dynamic emission allocation vINTR stakers use their voting power to determine the distribution of INTR block emission among stakeholder groups using a score voting system. Each vINTR staker independently votes for their preferred distribution among stakeholder groups in the Interlay network. The final distribution percentages are computed as weighted averages across all vINTR participating in voting.

$$Emission_{StakeholderGroup} = Emission \cdot \frac{Votes_{StakeholderGroup}}{TotalVotes}$$

where each vINTR counts as one vote. vINTR stakers can reallocate their voting power on a continuous basis if they wish to change it. If votes are not updated, the vINTR vote allocation remains as per the last vote.

The emissions allocated to each stakeholder group are then distributed among individual stakeholders following the respective fee models of each component as outlined in Section 3.

Encouraging Responsible Governance. It is of genuine interest to every vINTR holder to compensate each stakeholder group in a fair and competitive manner, similar to how a company must pay their employees and suppliers a competitive wage for their work and prices for their goods to remain a functional and profitable entity. Additionally, the requirement for a prolonged locking period in order to attain increased voting power offers robust protection against attacks on governance.

5.3 Protocol Revenue

With the introduction of v2, the Interlay network is making significant progress toward achieving economic independence. The network's treasury will benefit from the revenues generated by various products and accumulate a diverse portfolio of assets. Upon reaching economic sustainability, where fees surpass operational and development expenses, vINTR stakeholders will be able to cast their votes on how to distribute the funds, including options such as implementing new features, providing subsidies to certain stakeholder groups, incorporating the funds into DeFi protocols as protocol-owned liquidity, executing buyback strategies, or simply accumulating long-term reserves.

6 Canary Network Model

Kintsugi is Interlay's canary network, an experimental network with real economic value deployed on Kusama. Kintsugi and Interlay share the same design and architecture - with the difference that parameters on Kintsugi will be riskier to test system boundaries and discover edge cases. New features will first be rolled out to Kintsugi, tested in a real environment, and only then deployed to Interlay.

Kintsugi features its own governance, currently independent from Interlay. In the long-term, a connection between the two networks is possible, where Kintsugi stakers are able to vote on Interlay and vice-versa, establishing synergies similar to those observed between companies and their in-house research labs.

7 Outlook: Decentralized BTC Finance in 10 Years

Bitcoin is the single most important financial invention of the 21st century and has been adopted by hundreds of millions of users. With tens of millions of active users each month, Bitcoin is at the forefront of driving the widespread acceptance of decentralized protocols globally. There is no doubt it has become the core building block of the open and transparent financial system that our industry strives to create.

Interlay envisions a future where Bitcoin holders can effortlessly access a diverse range of BTC-based decentralized financial products and services with just one click, directly from their (mobile) wallets. Users should be able to focus solely on the applications they use, without worrying about the complexities of cross-chain transactions or the underlying networks. Interlay wants to make using Bitcoin in DeFi as convenient as withdrawing cash from an ATM.

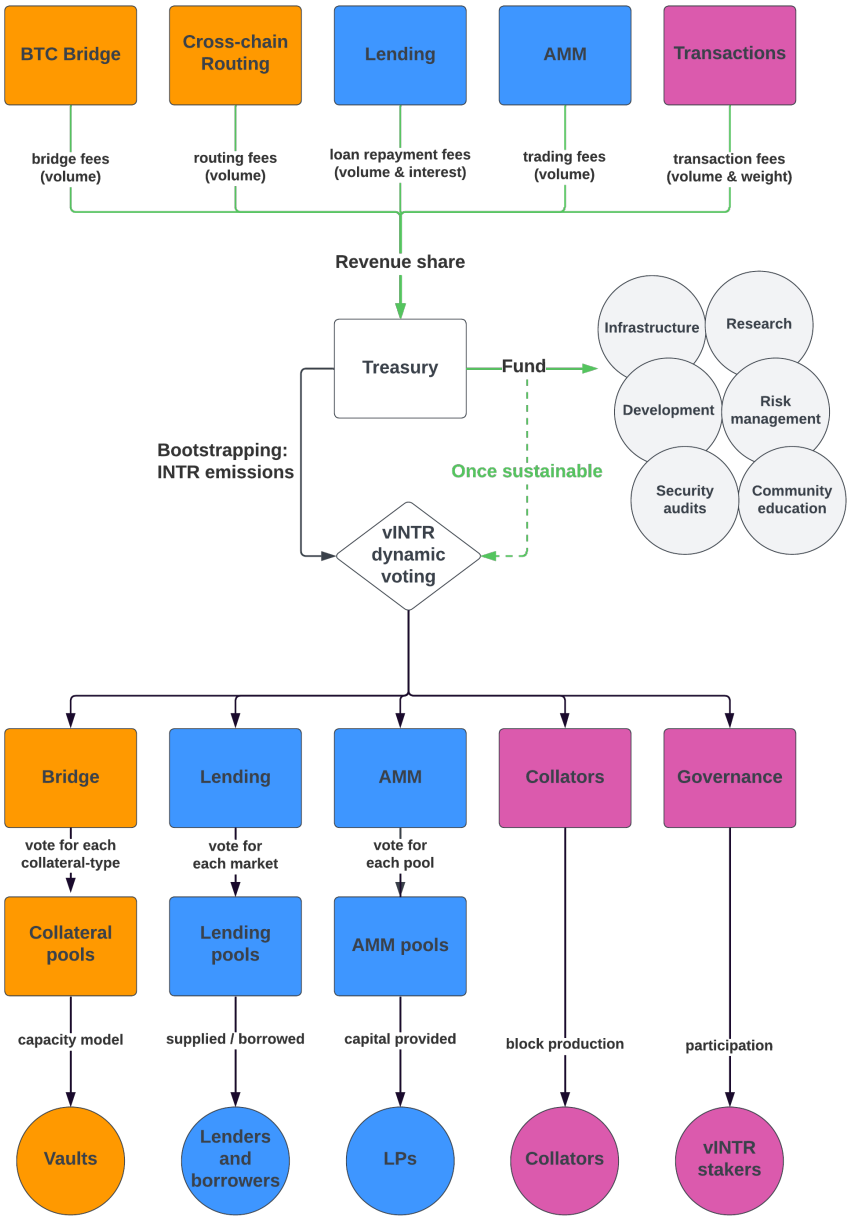

Figure 2: Visualization of the Interlay value network. vINTR stakers determine subsidy emissions, as well as any other treasury spending plans.

Outlined below are possible next steps, beyond v2, that the Interlay community can take toward realizing this vision. We divide them into two categories: product improvements, which have well-defined objectives and advantages, and open research problems, which are currently unresolved but have the potential to lead to groundbreaking innovations if successful. These open research problems represent ambitious projects that have the potential to create zero-to-one innovations.

Product improvements

- **Mobile and Universal Wallet support**. Integrate Interlay with all major multi-chain, mobile, and hardware wallets to ensure accessibility to a wide range of users without requiring them to change their habits.
- **More DeFi primitives**. Swaps and lending markets already enable a variety of use cases, ranging from portfolio diversification, passive income, leverage, and long/short bets. Structured financial products such as futures and options are tools widely used on financial markets, already today accounting for significantly higher daily volumes than spot markets. Synthetics and perpetual swaps are popular products used on Ethereum and centralized exchanges. Expanding the Bitcoin DeFi toolkit on Interlay is hence one of the logical next development directions.

  A more niche use case today, Bitcoin-backed synthetic loans, most commonly USD-pegged stablecoins, have been gaining more interest among the Bitcoin community as a means to use BTC in day-to-day business. Stablecoins rely on wide adoption and use cases beyond speculation that take time to develop, and are hence easier to deploy once the network has built up a solid "core" DeFi ecosystem.
- **Multi-party/Threshold Vaults**. Improving the resilience of the Bitcoin bridge remains a high priority on the path to mass adoption. By design, Interlay's Vaults do not rely on or require complex cryptographic primitives such as threshold signatures or multi-party computation (MPC). However, with recent improvements to these cryptographic primitives [13–15] adding support may enable multiple operators to join forces and jointly maintain Vaults, improving resilience against hacks, which in turn might attract more collateral delegations from external capital providers.
- **Regulated DeFi Subsystems**. Decentralized finance today operates under the radar of most regulators, making it difficult for both institutional and retail users of certain legislation to access decentralized products. Following the example of fore-runner regulated DeFi offerings, such as Aave Arc [17], creating a sub-system within the Interlay DeFi network which requires KYC/AML compliance may present itself as an opportunity to claim significant market shares among institutional players. In the end, decentralized financial tools should be accessible to everyone, which includes residents of areas with stricter regulations.

Open research problems

- **Hybrid Bitcoin Bridging**. Under the hood, iBTC is a combination of a multi-collateral synthetic (like Maker's DAI) and a Bitcoin IOU ("I owe you"), i.e., a physically redeemable BTC debt position. These two products can be separated, allowing DeFi users to borrow BTC synthetics against diverse collateral assets for quick BTC price exposure, while still being able to settle for BTC on Bitcoin through the purchase and redemption of tokenized Bitcoin IOUs. Sellers of IOUs commit to trading BTC on Bitcoin against the collateral underlying BTC synthetics for a fee, acting as a settlement service. Similar to failed iBTC Vault redeems, failed settlements would be subject to penalties. While the technical possibilities are somewhat clear, the economic benefits and risks remain a subject of ongoing research.
- **Zero-Collateral Bridges & Non-custodial Bitcoin DeFi**. Being able to earn passive income on Bitcoin without the risk of third-party custody or wrapping is a vision that comes close to the holy grail of Bitcoin DeFi. The first steps in this direction have already been made with the release of the XCC protocol [16] - a combination of layer-2 commit chains and Interlay's Bitcoin bridge. The biggest challenge, namely finding a good balance between non-custodial security and limitations to fungibility and hence usability in DeFi, is subject of ongoing research.

[17] `https://github.com/aave/protocol-v2/blob/feat/permissioned-market/aave-arc-whitepaper.pdf`

References

[1] Alexei Zamyatin, Dominik Harz, Joshua Lind, Panayiotis Panayiotou, Arthur Gervais, and William Knottenbelt. "Xclaim: Trustless, interoperable, cryptocurrency-backed assets". In: *2019 IEEE Symposium on Security and Privacy (SP)*. IEEE. 2019, pp. 193–210.

[2] MakerDAO. *The Maker Protocol: MakerDAO's Multi-Collateral Dai (MCD) System*. URL: `https://makerdao.com/en/whitepaper/`.

[3] Jeff Burdges, Alfonso Cevallos, Peter Czaban, Rob Habermeier, Syed Hosseini, Fabio Lama, Handan Kilinc Alper, Ximin Luo, Fatemeh Shirazi, Alistair Stewart, et al. "Overview of polkadot and its design considerations". In: *arXiv preprint arXiv:2005.13456* (2020).

[4] BitcoinWiki project. *Simplified Payment Verification*. URL: `https://en.bitcoinwiki.org/wiki/Simplified_Payment_Verification`.

[5] Alexei Zamyatin, Mustafa Al-Bassam, Dionysis Zindros, Eleftherios Kokoris-Kogias, Pedro Moreno-Sanchez, Aggelos Kiayias, and William J Knottenbelt. "Sok: Communication across distributed ledgers". In: *International Conference on Financial Cryptography and Data Security*. Springer. 2021, pp. 3–36.

[6] *Open Runtime Module Library: Oracle*. URL: `https://github.com/open-web3-stack/open-runtime-module-library/tree/master/oracle`.

[7] Christopher Goes. "The interblockchain communication protocol: An overview". In: *arXiv preprint arXiv:2006.15918* (2020).

[8] *Snowbridge: A trustless bridge between Polkadot and Ethereum*. URL: `https://github.com/Snowfork/snowbridge`.

[9] *Introduction to Compound v2*. URL: `https://docs.compound.finance/v2/`.

[10] Hayden Adams, Noah Zinsmeister, and Dan Robinson. "Uniswap v2 core, 2020". In: *URL: https://uniswap. org/whitepaper. pdf* (2020).

[11] Michael Egorov. "StableSwap-efficient mechanism for Stablecoin liquidity". In: *Retrieved Feb* 24 (2019), p. 2021.

[12] Juan Benet. "Ipfs-content addressed, versioned, p2p file system". In: *arXiv preprint arXiv : 1407.3561* (2014).

[13] Rosario Gennaro and Steven Goldfeder. "One round threshold ECDSA with identifiable abort". In: *Cryptology ePrint Archive* (2020).

[14] Rosario Gennaro and Steven Goldfeder. "Fast multiparty threshold ECDSA with fast trustless setup". In: *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*. 2018, pp. 1179–1194.

[15] Chelsea Komlo and Ian Goldberg. "FROST: flexible round-optimized Schnorr threshold signatures". In: *Selected Areas in Cryptography: 27th International Conference, Halifax, NS, Canada (Virtual Event), October 21-23, 2020, Revised Selected Papers 27*. Springer. 2021, pp. 34–65.

[16] Theodore Bugnet and Alexei Zamyatin. "XCC: Theft-Resilient and Collateral-Optimized Cryptocurrency-Backed Assets". In: *Cryptology ePrint Archive* (2022).

Appendix

A Liquidity Protocol Interest Rate Model

At launch, the Interlay liquidity protocol will feature an interest rate model inspired by Compound v2 - a model that is well-tested in practice. Improvements and optimizations are expected in future versions of the protocol.

Utilization Rate The utilization rate is defined as the percentage of the total supply that is currently borrowed and is a central parameter in determining the supply interest rate.

$$UtilizationRate = \frac{TotalAmountBorrowed}{TotalCash + TotalAmountBorrowed - TotalReserves}$$

where *TotalCash* is the amount of supply that is currently not lent out, *TotalAmountBorrowed* is the total outstanding debt, *TotalReserves* is the number of unharvested reserves which accrued in the pool.

Internal Exchange Rate When a supplier adds tokens to the lending pool, they are credited qToken based on the initial exchange rate. Since the qTokens accrue interest as the n *TotalAmountBorrowed* continuously increases, the number of tokens they will receive at redemption will change based on the internal exchange rate. This can be represented as:

$$InternalExchangeRate = \frac{TotalCash + TotalAmountBorrowed - TotalReserves}{TotalSupply}$$

where *TotalCash* is the unborrowed supply and *TotalSupply* is the total available supply in the pool.

Borrowing Rate The function below describes the borrowing rate depending on the demand and supply for a given asset, represented as the utilization rate U.

$$r_{borrow} = \frac{BaseRate + U * (JumpRate - BaseRate)}{U_{target}} | U \leq target \tag{8}$$

$$r_{borrow} = \frac{JumpRate + (U - U_{target}) * (FullRate - JumpRate)}{1 - U_{target}} | U > target \tag{9}$$

where *BaseRate* is the intercept (when utilization is zero), *JumpRate* is the borrow rate when $U = U_{target}$ and *FullRate* corresponds to the rate when $U = 100\%$.

Supply Rate The relationship between the supply and the borrowing rates is then calculated as:

$$SupplyRate = \frac{BorrowRate * TotalAmountBorrowed}{TotalSupply} * (1 - DAOFee)$$

where *DAOFee* is the percentage fee that is collected by the protocol. Note that the supply rate is reduced by the fees that are attributable to the protocol.

B AMM Curves

Non-stable Pools Exchange prices on the DEX are determined by the constant function market maker. For non-stable pools, prices are determined via a constant product function in the form of

$$K = x * y$$

where K is a constant, x and y are the supplies of tokens X and Y, respectively.

Stable Pools For stable pools, the DEX determines the exchange price of an asset using the stable swap invariant first proposed by Curve [11]

$$An^n \sum x_i + D = ADn^n + \frac{D^{n+1}}{n^n \prod x_i}$$

where A is the amplification coefficient that determines the liquidity concentration towards the middle of the curve, D is the constant (determined as the product of the number of tokens and is

comparable to the constant K in the constant product function), n is the number of coins in the pool and x_i is the respective token.

When a trade is being executed on such a pool, the above equation must hold. This requires finding a solution for either D or x, when all other variables are known, via iterative convergence.

C INTR Emission and Distribution

A more detailed overview of the INTR emission, distributions, and vesting schedules can be found online[18]

INTR has an unlimited supply, with a pre-defined emission schedule over the first 4 years after network launch. Note that these are merely initial parameterizations and can be adjusted by governance.

- 1 billion (1,000,000,000) INTR over the first 4 years.
- 2% annual inflation afterwards

The Interlay network followed a fair launch approach. INTR were/are distributed to (early) network participants, builders, and supporters in two forms: gratuitous airdrops and block rewards. No form of public sale was conducted. 70% of the initial 4-year INTR supply is distributed to the network treasury from where it can be distributed as airdrops and block rewards to community and service providers, subject to governance vote. 20% of the initial 4-year INTR supply is airdropped to the Interlay team, and early backers, who funded the initial development of the protocol - subject to lockup & vesting. 10% of the initial 4-year INTR supply is airdropped to a Foundation Reserve, to be used for funding ecosystem growth and future development.

Starting with year 5, 100% of the annual inflation is allocated to the treasury, to be spent as determined by the community via governance.

D Vault Fee Model Math

D.1 Vault Income

The revenue of Vault is composed of the following components:

- **Mint and redeem fees, paid in BTC**. Currently, these are static set to 0.15% for minting and 0.5% for redeeming. The fees can be changed by governance. In the future, these fees will be changed to dynamic fees, based on supply/demand.
- **During bootstrapping: Token subsidies, paid in INTR** by the protocol treasury to subsidize capital costs while bridge volumes are not high enough to cover operational costs.
- **Outlook: DAO revenue share**. The protocol DAO takes a cut from the volume-based fees earned by the DEX and lending protocols, paid in the traded assets. In the future, Vaults may be allocated a share of the DAO's revenue as a "service fee" instead of the token subsidies.

The revenue of a Vault i is hence defined as:

$$VaultRevenue_i = (Fees + Subsidies) \cdot VaultShare_i \tag{10}$$

D.2 Individual Vault Share

The current Vault fee model considers the BTC locked with a Vault, compared to the total BTC locked in the Interlay bridge:

$$VaultShare_{v1} = \frac{VaultBTCLocked}{TotalBTCLocked} \tag{11}$$

[18] `https://docs.interlay.io/#/interlay/tokenomics`

In v2, also referred to as the "capacity-based" model, the revenue share of each Vault is determined by the amount of BTC a Vault *could* accept, i.e., its *capacity*. Capacity is a function of the total amount of collateral locked, and the over-collateralization threshold. The lower bound for the collateral threshold is defined by the protocol (*SecureThreshold*) but Vaults can set more conservative thresholds (*CustomThreshold*) as part of their risk management strategy (e.g. 200% instead of the required 155%).

$$VaultCapacity = \begin{cases} \dfrac{CollateralLocked}{\max(CustomThreshold, SafeThreshold)} & \text{if accepting new issue requests} \\ 0 & \text{otherwise} \end{cases} \tag{12}$$

$$VaultShare_{v2} = \frac{VaultCapacity}{TotalCapacity} \tag{13}$$

Disclaimer

This paper is a collaborative effort by many members of the Interlay community. It outlines a proposed direction for the Interlay Network. However, the contents do not entail a commitment by any authors or their respective organizations. The Interlay community is responsible for the adaptation and adoption of the measures proposed in this paper. The success of any proposal will depend ultimately on the hard work of the wider community and those building within the Interlay Network. The information presented herein is being provided by the parties listed above (the PARTIES) for information purposes only. Neither the PARTIES nor any of their affiliates, nor any of their respective directors, officers, managers, employees or representatives make any representations or warranties, express or implied, with respect to any of the material or information contained herein. Neither do the PARTIES or any such person assume or otherwise have any responsibility or any liability whatsoever to you or any of your affiliates, or any of your or your affiliates' respective directors, officers, managers, employees, or representatives resulting from the use of the information and material contained herein. Information provided here is supplied in good faith based on information believed but is not guaranteed to be accurate or complete. The information provided in this paper does not constitute investment advice, financial advice, trading advice, or any other sort of advice and you should not treat any of the paper's content as such. The PARTIES recommend you conduct your own due diligence and consult your financial advisor before making any investment decisions of any kind.

Although this paper does not constitute investment, financial, or trading advice, a regulator may determine this paper includes "forward-looking statements" under U.S. federal securities laws. If such a determination is made, please note that the PARTIES have based any such forward-looking statements on current expectations and projections about future events. These forward-looking statements are subject to risks, uncertainties, and assumptions about the PARTIES and their related business objectives. The PARTIES caution readers of this paper that, although PARTIES believe that the assumptions on which such forward-looking statements are based are reasonable, any of those assumptions, current expectations, and projections could prove to be inaccurate and, as a result, the forward-looking statements also could be materially incorrect. Readers of this paper are cautioned not to put undue reliance on any such forward-looking statements. The PARTIES disclaim any intent or obligation to update publicly such forward-looking statements, whether as a result of new information, future events, or otherwise. All forward-looking statements attributable to the PARTIES or persons acting on their behalf are expressly qualified in their entirety by these and any other cautionary statements and risk factors contained herein.