Regulated
Decentralised
Finance

The path to fair and responsible banking.

ReDeFi Blockchain whitepaper

Nov 2023, Draft v0.1

Rushd Averroes, Bulat Kaliev

“ReDeFi restores financial freedom and inclusion in a decentralised and compliant manner.”

- Rushd Averroes,
ReDeFi Founder

Table of Contents

Abstract

In an era marked by fast technological advancements, we've observed ambitious initiatives from the likes of electric vehicles to space exploration. However, even as the world sets its sights on space travel, fundamental challenges remain on Earth, particularly within the financial sector.

ReDeFi aims to revolutionise the blockchain and finance industry, placing its emphasis on empowering banks and regulated financial institutions on a global scale. With a vision to offer a universally accessible platform, ReDeFi is poised to become a catalyst for change, providing a secure network for these institutions but not limited to them. A variety of services will be available: from B2B payments, facilitating seamless e-commerce transactions, to streamlining foreign exchange operations and finding insurance-related opportunities.

ReDeFi taps into the crypto asset market with untapped potential. This paper will further explain the ReDeFi blockchain, showcasing this initiative in reshaping the banking and finance sector by offering unique opportunities to access refined services.

Introduction

According to research by the World Bank, the costs of sending money abroad (remittances) accounted for 6.8% of overall costs in 2020[1]. Every time a payment of $200 is made, $13.60 in fees are deducted from the total amount sent abroad. According to the survey, the average cost of international transfers varies substantially by region and country, ranging from 3.9% in South Asia to 8.7% in Sub-Saharan Africa.

Global remittances reached close to $540 billion in 2020 and global costs for foreign money transfers amounted to around $36.7 billion. Note that the exact figures may differ depending on current foreign exchange rates, financial institution fees, and the method of cash transfer chosen.

1 https://www.worldbank.org/en/news/press-release/2020/04/22/world-bank-predicts-sharpest-decline-of-remittances-in-recent-history

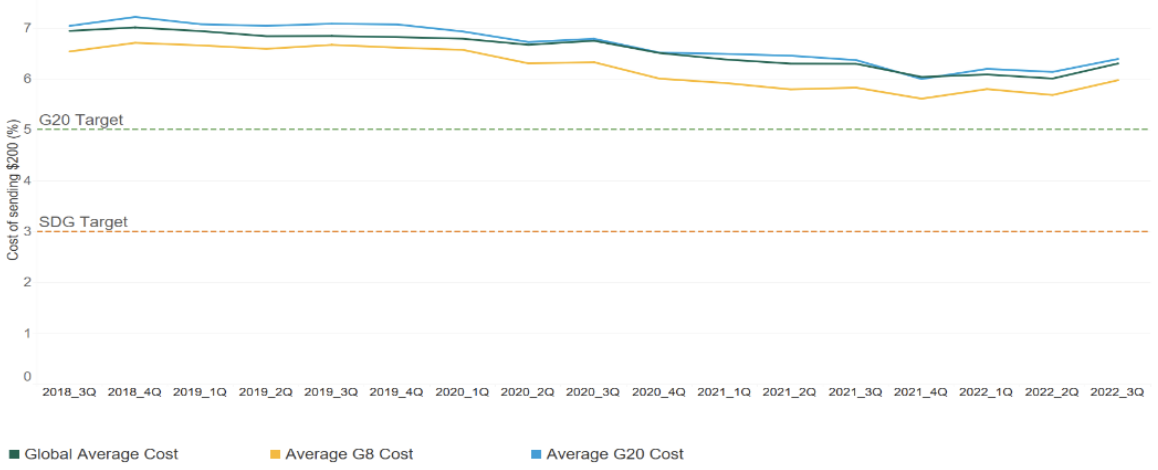


Figure 1. Average cost of sending $200 from G8 and G20 countries[2].

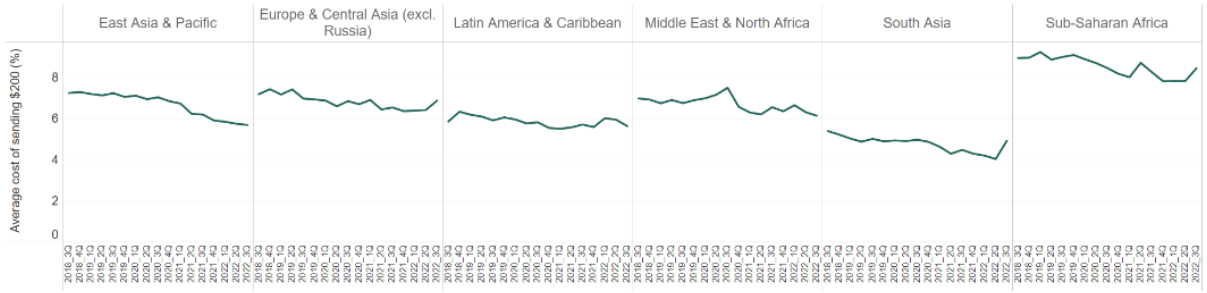


Figure 2. Average costs over time by region of the world[3].

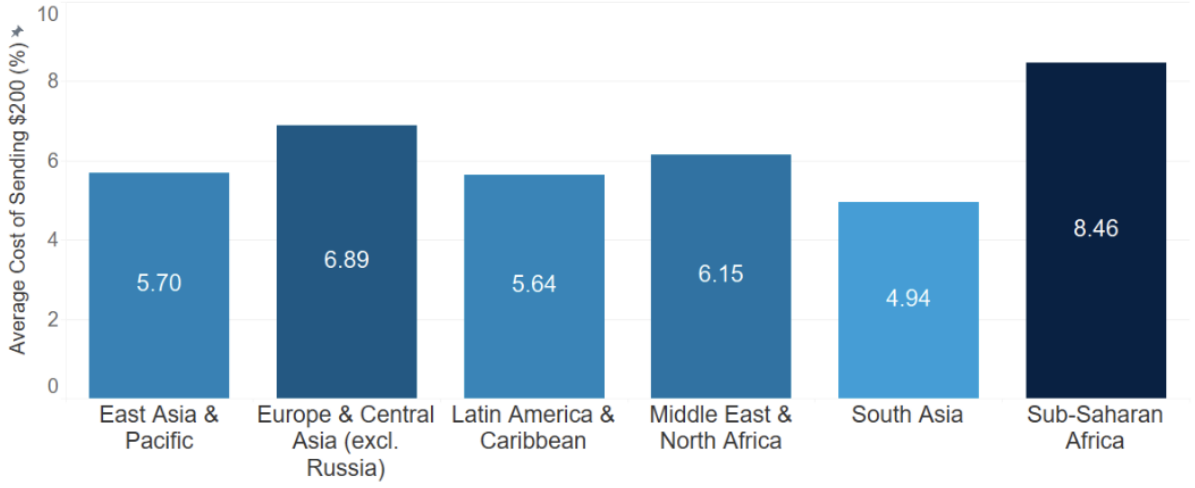


Figure 3. Average costs by region of the world[4].

[2] https://remittanceprices.worldbank.org/sites/default/files/rpw_main_report_and_annex_q322_final.pdf
[3] https://remittanceprices.worldbank.org/sites/default/files/rpw_main_report_and_annex_q322_final.pdf
[4] https://remittanceprices.worldbank.org/sites/default/files/rpw_main_report_and_annex_q322_final.pdf

ReDeFi's goal is to ensure that businesses and individuals around the globe have the same access to financial services. The higher the cost of using money, the less money remains with the individual in the economy to buy food and medicine for example.

By cutting the cost of doing business and using money, as well as lowering cross-border fees, the ReDeFi project will help to save billions of dollars compared to the current financial system. The money saved can be used to increase the availability of loans in developing economies, giving access to more resources and encouraging growth.

At ReDeFi we believe that a regulation-friendly and decentralised monetary system should be fair and accessible to everyone. By providing a platform that is both scalable and subject to constant improvement, we enable endless opportunities for banks, businesses and individuals in obtaining a better system through blockchain technology whilst complying with all the relevant rules and regulations.

ReDeFi is designed with regulatory compliance in mind because we understand it's important to success in the global economy. ReDeFi combines the accessibility and independence of decentralised finance with the safety and security of complying with regulation bodies. By taking into account specific frameworks across jurisdictions, we create a cutting-edge financial solution.

ReDeFi does not seek to replace the current financial system. Instead, it acts as an internationally accessible and universally regulated entry point into the financial markets. We believe that each country should be allowed to control its own economy and issue its own currency based on its needs. As part of being internationally compliant and connected, nations should have the authority to preserve and advance their monetary and fiscal policies through their own currency.

The ReDeFi platform is beneficial to banks, financial institutions, and Virtual Asset Service Providers (VASP) who seek to innovate whilst adhering to their local rules. We are offering a platform that allows financial institutions to utilise blockchain technology in accordance with local regulation, as we believe this technology will play an important role in the future of finance. Each financial institution can tailor the ReDeFi network to its unique environment while enjoying the advantages of an open and progressive monetary system where each currency has its own set of rules and can be designed in a variety of ways.

To summarise, ReDeFi is an innovative technology that is transforming the financial industry. We are discovering practical answers to pressing issues by combining the openness of decentralised financial systems with the security and compliance provided by regulatory frameworks. In the following sections, we are explaining how the ReDeFi blockchain works, the various components of the network with step-by-step examples to showcase each feature.

ReDeFi Blockchain

ReDeFi is a Layer-1 blockchain protocol capable of replicating traditional banking account functions on-chain. While efficiently mitigating issues such as high gas fees and slow transaction times, its primary innovation lies in integrating day-to-day bank accounts with blockchain technology.

ReDeFi introduces a comprehensive framework, tailored to support diverse scaling solutions and facilitate interoperability across multiple blockchain networks. It integrates key components, including dedicated testnet and mainnet infrastructures. The main features of our ecosystem are: Onchain Money, the Self-Custody Wallet, a cross-chain bridge, a block explorer, a naming service, and an advanced FX exchange protocol.

ReDeFi operates on a Proof-of-Stake (PoS) consensus mechanism, along with a peer-to-peer (P2P) identity verification method. This ensures fast and secure transactions with low costs. The system's integrity is further enhanced by requiring validators to undergo a strict KYC process. This amplifies ReDeFi’s security and promotes responsible nodes by rewarding the validators for maintaining the security of the network.

ReDeFi's interoperability is achieved by its bridge solution, which fosters seamless integration between blockchains like Ethereum, Binance Smart Chain, Avalanche, and Polygon. The ReDeFi Bridge acts as a conduit for the seamless transfer of assets between these blockchains, expanding opportunities in DeFi, introducing innovative cross-chain applications while introducing on-chain banking.

PoS Consensus & Security Control

PoS mechanisms have remained on the periphery of blockchain deployments, contributing to a mere 2% of the digital currency market capitalisation. The hesitancy towards PoS adoption can largely be attributed to inherent vulnerabilities, particularly susceptibility to notable security threats such as nothing at stake and long-range attacks.

The nothing at stake attack circumvents traditional deterrents, allowing nodes to create conflicting blocks without endangering their stakes. This vulnerability not only amplifies system forks but also extends consensus achievement times. Conversely, the long-range attack, colloquially termed the history attack, is characterised by a malefactor's intent to retroactively modify the blockchain's history, potentially going back to its genesis block. This type of breach is conceivable when, for instance, a bad actor procures the private keys of erstwhile substantial accounts, now devoid of stakes, and then fabricates a branching pathway from a historical block utilising these credentials. Existing remedial measures encompass deposit-based PoS and checkpoint methodologies.

The former mandates each validator to lodge a deposit, which stands to be confiscated by the system upon detection of conflicting block generation by said validator. Checkpoints, conversely, represent historical points on the blockchain, post which forks are disallowed.

This strategy somewhat circumscribes the long-range attack, as any modification attempt must ensue post the last established checkpoint. Yet, these measures are mere palliatives and do not extirpate potential misdeeds.

In ReDeFi, validators are chosen to create new blocks based on the quantity of RED tokens they hold and are willing to stake. This staking mechanism emphasises energy efficiency and ensures that those actively involved in the network take an active role in its operation.

Compliance

ReDeFi integrates an Identity Verification, or KYC natively. At its core, it hinges on a distributed verification approach through various industry partners to fortify the PoS mechanism, ensuring a safer network environment with contributor verifiability.

Multi-layered KYC process begins by offering users to create Digital Wallets including their full names, date of births and residency. For further service depth, users can undertake a more comprehensive KYC process through industry partners, sharing requisite identification documents to verify their identity and residency. However, the most innovative facet of this model is its blockchain component. Recognised and fully KYC'ed users within the network can authenticate basic account details followed up by KYC verifications provided by industry partners to enable higher transaction volumes.

This strategy ensures that ReDeFi not only reduces potential vulnerabilities by intertwining identity verification with network trust but also fosters expansive growth. By amalgamating traditional PoS with Multi-layered KYC, ReDeFi emphasises that consensus security is not solely reliant on mathematical deterrence but also harnesses the power of contributor trust and accountability.

ReDeFi Naming Service

The ReDeFi Naming Service (RDFNS) provides a decentralised naming system for the assignment of human-readable aliases to the intricate hexadecimal addresses of blockchain entities, including but not limited to smart contracts and dApps. This service is designed to significantly improve user interaction within the ecosystem, streamlining the transaction process by mitigating the inherent complexity of direct address utilisation.

The RDFNS adopts a hierarchical nomenclature system, analogous to the established Domain Name System (DNS) employed within the broader internet infrastructure. This design choice facilitates an intuitive mapping from the user-friendly domain names to the corresponding blockchain addresses. The management of the primary domain host is maintained by the ReDeFi team, whilst allowing the delegation of subdomains to the broader user community, thereby promoting a distributed administration model.

The integration of the naming service is deeply intertwined with the blockchain's underlying smart contract framework. This amalgamation ensures that the operations of assigning and resolving domain names are embedded within the blockchain's immutable ledger, affording a level of transparency and security characteristic of decentralised technologies. The execution of these operations through smart contracts enforces an autonomous and trustless environment for the naming service.

Accessibility has an interface designed to facilitate user engagement with the domain registration process. This interface enables individuals and entities to seamlessly associate their unique blockchain addresses or deployed smart contracts with a chosen domain name.

Efficiency is a byproduct of the naming service, as registered domain names can be utilised as references within the context of dApp interaction and as facilitators for transactional activities. This utility eliminates the conventional reliance on protracted addresses and improves accessibility.

Moreover, the RDFNS system is engineered with flexibility in mind, allowing domain owners the freedom to transfer ownership rights. This capability extends to the creation of subdomains, providing users with additional customisation and hierarchical management. Such features are intrinsic to the RDFNS system, ensuring that it remains an adaptable and user-centric component of the ReDeFi blockchain

Red Tokenomics

- **Staking:** RED token holders can engage in staking by becoming a validator or delegate their tokens to a specific validator address of their choice.
- **Security and Incentives:** Tokens staked are locked within a smart contract, ensuring validators or staking pools have a vested interest in the network's well-being. This stake acts as a guarantee for their performance and ethical conduct.
- **Reward System:** Staking rewards are a function of transaction fees and minted tokens. The distribution is proportional to the stake's size relative to the total network stake.
- **Unstaking Process:** To unstake, users must request and undergo a predefined waiting period, designed to prevent malicious activities and protect the network's stability. Post this period, tokens can be reclaimed and transferred back to the user's wallet.

Token Distribution

- **Token Standard:** RDF20 protocol standard.
- **Initial Supply:** 100 million RED tokens.
- **Inflation Model**: An annual inflation rate of 5% is set in the beginning.
- **Token Burn Mechanism:** Plans for a future mechanism to burn a set percentage of transaction fees, creating scarcity.
- **Distribution Phases:**
    - Private Sale: Exclusively for BAX token holders.
    - Presale: Details TBA.
    - Public Sale: Initial Exchange Offering (IEO).

Utility and Value Proposition

- **Transaction costs**: RED will cover gas fees and other on-chain activities.
- **Subscription Access:** Grants access to specific features on the ReDeFi platform.
- **Staking and Delegation:** Users can either run nodes or delegate tokens to validators, earning rewards.

Fee Mechanisms

- **Fee Structure:** Fees collected in RED tokens ensure the self-sufficiency and ongoing maintenance of the protocol.
- **Community Redistribution:** A portion of performance fees is earmarked for the treasury and ecosystem development, promoting long-term community engagement and protocol advancement.

BAX Tokenomics

Overview

BAX token is the primary token of the BABB Layer-2 and the ReDeFi ecosystem. It is designed to enhance transaction efficiency, reduce costs and boost the utility within the network.

- **Staking:** BAX holders can participate in staking by transferring tokens to a staking address or delegating to chosen validators. The ReDeFi Self-Custody Wallet, compatible with EVM, facilitates this process efficiently.
- **Security and Reward Structure:** Staked BAX are secured in a smart contract, aligning stakeholder interests with network health. Stakers and delegators are rewarded, reflecting their contribution to network security and operations.
- **Rewards and Distribution:** Rewards for staking BAX will come from staking bax (as a validator) or from delegation (delegate BAX tokens to a chosen validator).

Token Distribution

- **Token Standard:** Adheres to the RDF20 protocol standard, ensuring compatibility and functionality within the ReDeFi ecosystem.
- **Supply Details:**
  - Current Supply: 80 billion BAX tokens.
  - Maximum Supply Cap: 100 billion BAX tokens.
  - Allocations: (1), (2), (3)
- **Multichain Functionality:** BAX will function on both Ethereum ERC20 and ReDeFi Layer-2, maintaining a collective supply cap across both chains.

Utility and Value Proposition

- **Operational Utility:** BAX is integral for transactional operations on L2, covering gas fees and other network functionalities.
- **Access to Features:** BAX grants access to unique features and services within the BABB App and the broader ReDeFi platform.
- **Staking Benefits:** Staking BAX allows users to participate as network validators or earn rewards through delegation.
- **Ecosystem Integration:** Central to BABB App operations, facilitating transactions, offering exclusive discounts, and unlocking special access for holders.

Fee Structure and Ecosystem Growth

- **Network Fees**: Transactions within the BABB L2 network require BAX tokens, creating a consistent demand and utility for the token.
- **Ecosystem Support:** A portion of transaction fees in BAX is reallocated to support ecosystem development, treasury, and community initiatives.

Onchain Money

Key takeaways:

- *Onchain Money is a tokenised deposit that is settled in central bank money and does not break the "singleness of money" principle.*
- *Onchain Money provides enhanced functionality by utilising smart contracts' ability to introduce fast execution, traceability, near-zero cost of operations, and transaction composability.*
- *Onchain Money has certain characteristics of stablecoins, but there is no mechanism for issuing a token IN EXCHANGE for a fiat deposit. Instead, Onchain Money mirrors GBP settled in traditional bank accounts. This enables deposits and withdrawals from and to any bank account using standard bank account details such as sort code, account number, SWIFT, IBAN, and so on. These accts can be FSCS protected as direct Central Bank deposits with BOE.*

Introduction

The "singleness of money" is a fundamental part of the modern monetary system.[5] Singleness of money assures that monetary trade is not susceptible to variable exchange rates between different forms of money, whether privately issued (for example, deposits) or publicly issued (for example, cash). With monetary singleness, there is a clear unit of account that underpins all economic transactions in society.

To be clear, the singleness of money does not exclude variable credit risk among intermediaries. The value of private liabilities as repositories of value could range among intermediaries in the same way that bank bonds or negotiable certificates of deposit (CDs) can trade at differing spreads in the current two-tier monetary system. Rather of private liabilities as a store of value, singleness is a property of the payment. The perspective provided by the singleness of money is useful in talks on the tokenisation[6] of privately issued money and digitally representing claims using smart contracts[7].

Problem statement 1: Can the Onchain Money model be viewed as a tokenised deposits conducive to “singleness of money”?

[5] Padoa-Schioppa, T (2004): “Shaping the payment system: a central bank’s role”, speech at the Bank of Korea’s Conference on Payment Systems, Seoul, 13 May.
[6] Tokenisation is the process of digitally representing claims in order for them to be transacted on programmable blockchain platforms utilising smart contracts.
[7] Smart contract is a combination of data and code that can behave automatically.

Problem statement 2: Can the Onchain Money model expand the functionality by enabling programmable ledgers and introducing contingent execution and composability of transactions?

Problem statement 3: Can the Onchain Money model break the "singleness of money" principle?

The Onchain Money model

Onchain Money model represents the issuer's liabilities, and the holder has a claim on the issuer for redemption at par value in the sovereign unit of account.

The transfer process does not involve a direct transfer of claims and liabilities and Onchain Money cannot be transferred to individuals outside the KYC border. The model envisages participants to be customers of regulated financial institutions such as banks, and transfers are logged at the individual bank level and settled automatically and balance sheets are updated at the time of a transaction. An individual or business knows that when they receive an Onchain Money payment from their customers, the money will be credited to their own account at face value under this model of non-transferable liabilities.

The use of central bank money for settlement is the main aspect that supports singleness. The payment process is similar to the present two-tier monetary system's practice of debiting the sender's account and crediting the receiver's account, with settlement on the central bank's balance sheet. The payment is carried out by lowering the sender's Onchain Money and conventional GBP balances at their issuing institution and creating a new debt for the receiver that is issued by their institution. Meanwhile, central bank funds are being transferred utilising conventional money. This design does not require, but does facilitate, the availability of both Onchain Money and conventional GBP on the same platform.

The issuance (mint) process does not involve an exchange of Onchain Money for a fiat deposit. Instead, Onchain Money mirrors a conventional GBP settled in the user's (owner's) name in a traditional bank account. This model allows money to be sent to and received from any bank, even if it is not connected to the ReDeFi blockchain network, using traditional standard bank account details such as sort code, account number, SWIFT, IBAN, and so on.

In general, any asset that can be exchanged will have an exchange rate, which can move away from par for a variety of reasons. Divergence from par may be due to variances in settlement frictions associated with the cashing out procedure. Discounting and value fluctuation could also arise as a result of variances in issuers' perceived credit risk, differences in holders' risk-bearing capacity, and higher order uncertainty associated with doubts about whether others have concerns about the token's worth. Even a modest seed of uncertainty (whether warranted or unjustified) has the potential to weaken money's role as a medium of exchange. Finally, major issuers' market power could be used to devalue tokens issued by smaller issuers.

Because the Onchain Money does not circulate as transferable issuer liabilities, it is excluded from financial assets with a market price. Money transfers under the Onchain Money model are immediately settled in central bank money and follow the two-tier monetary system's practice. The singleness of Onchain Money and all users' shared confidence in the value of money is assured in the same manner that conventional fiat money is.

It is also important to note that the Onchain Money model has no AML[8] or KYC[9] compliance flaws because liabilities are indirectly transferred to individuals with verified identities.

The table below depicts the distinctions between the Onchain Money model and stablecoins, using USDT as an example.

	Onchain Money	Stablecoins
Name	Onchain Money	USDT
Issuer	Bank with a node on the ReDeFi blockchain	Tether
Organisation behind	Bank-issuer, BABB, ReDeFi	Tether
Are they onchain tokens?	Yes	Yes
Are they backed by conventional money?	They are not backed, but mirrored in both traditional bank accounts and the ReDeFi blockchain	Supposedly yes, but it is not possible to verify.
Who is in control of the money?	Money is stored on the bank's acct under the user's (owner's,) so the account holder's is the owner	The issuer controls the token and money.
Is there a mint and burn mechanism for them?	When it comes to the movement, no. Tokens are mirrored.	Yes
Is there an exchange of crypto assets for money?	No, since they are mirrored in a bank	Yes
Is there a need to redeem for cash or conventional deposits?	No, since they are mirrored in a bank	Yes
Does the pricing fluctuate?	No, it is an equivalent to conventional GBP	Yes
Does the payment process mimic the two-tier monetary system model of debiting and crediting accounts?	Yes, since they are mirrored in a bank	No
Does the payment process mimic the two-tier monetary system model of settlement on the central bank's balance sheet?	Yes, since they are mirrored in a bank	No

[8] Anti-money laundering (AML)
[9] Know-your-customer (KYC)

Does the payment process work with 3rd party banks (e.g., that do not enter the ReDeFi environment)?	Yes, since they are mirrored in a bank	No
Does the payment or a transfer a direct transfer of claims and liabilities?	No	Yes
Are they regulated?	Yes, since they are mirrored in a bank	Can be regulated to a certain degree
Are they FSCS protected?	Yes, since they are mirrored in a bank	No
Can they be approved by regulators?	Yes, since they are mirrored in a bank	Can be registered and controlled to a certain degree
Do they weaken the AML/KYC compliance?	No, since all ReDeFi environment users have gone through KYC	Yes
Is there commonly shared confidence in the value among all users?	Yes	No
Can cost or delays be imposed by the issuer?	No	Yes
Can they be credited to an account at face value automatically?	Yes	No
Can they be settled using Central Bank money with any bank?	Yes	No

Table 1. Difference between the Onchain Money model and stablecoins.

Use cases

Bank 1 and Bank 2 are participants of the ReDeFi environment.

Use cases and graphs below depict a specific technique of executing the Onchain Money model utilising blockchain technology procedures and terminology. The dotted lines reflect the four partitions of the model maintained by the two private tokenised money issuers (Banks 1 and Bank 2) and the central bank and the ReDeFi blockchain. The arrows indicate the issuers of the liabilities.

To be explicit, "Current acct" means a current bank account in conventional or modern banking with account details such as IBAN, BIC, sort code and account number. "Current mirroring acct" means a current bank account with account details such as IBAN, BIC, sort code and account number as well as a wallet address in the ReDeFi blockchain.

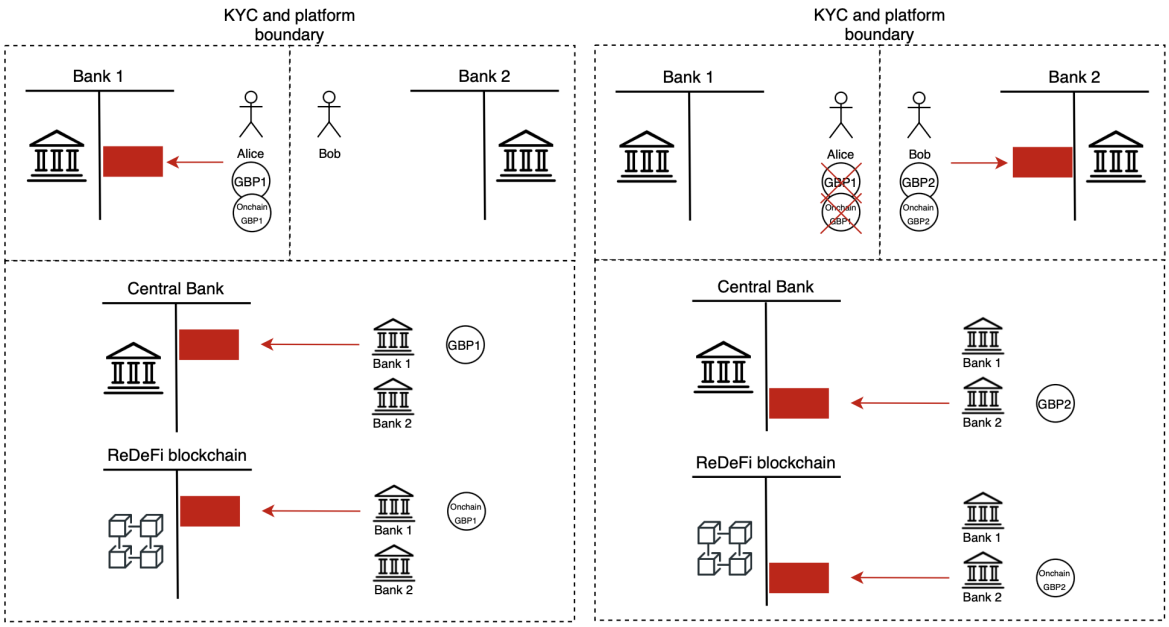
Both accounts provided by Bank 1 or Bank 2 are “everyday banking” accounts that give access to money for daily spending and can be linked to debit cards and can be protected by the FSCS.

Use case 1. Alice sends money from her Current mirroring acct to Bob’s Current mirroring acct.

The left-hand panel portrays the circumstances preceding Alice's payment to Bob. Alice has 1 Pound sterling in her Current mirroring acct with Bank 1, which is mirrored and represented by 1 Onchain GBP in the ReDeFi blockchain. Alice sends money from her Current mirroring acct to Bob’s Current mirroring acct.

The right-hand panel depicts what happens when Alice sends money to Bob:

a) Onchain GBP tokens are transferred (rather than burned and issued) from Alice to Bob since both banks are within the ReDeFi environment. If required, one Onchain GBP token held by Alice can be deleted ("burned") by Bank 1, and one Onchain GBP token can be assigned ("minted" or “issued”) to Bob by Bank 2.
b) The movement of onchain money tokens is accompanied by conventional GBP movement from Current mirroring acct at Bank 1 to Current mirroring acct at Bank 2 and the central bank's partition. One Pound sterling is moved from Bank 1 to Bank 2 and settled on the central bank's balance sheet. This is demonstrated by the fact that both Onchain GBP tokens and conventional GBP in the right-hand panel belong to Bank 2 after transaction.



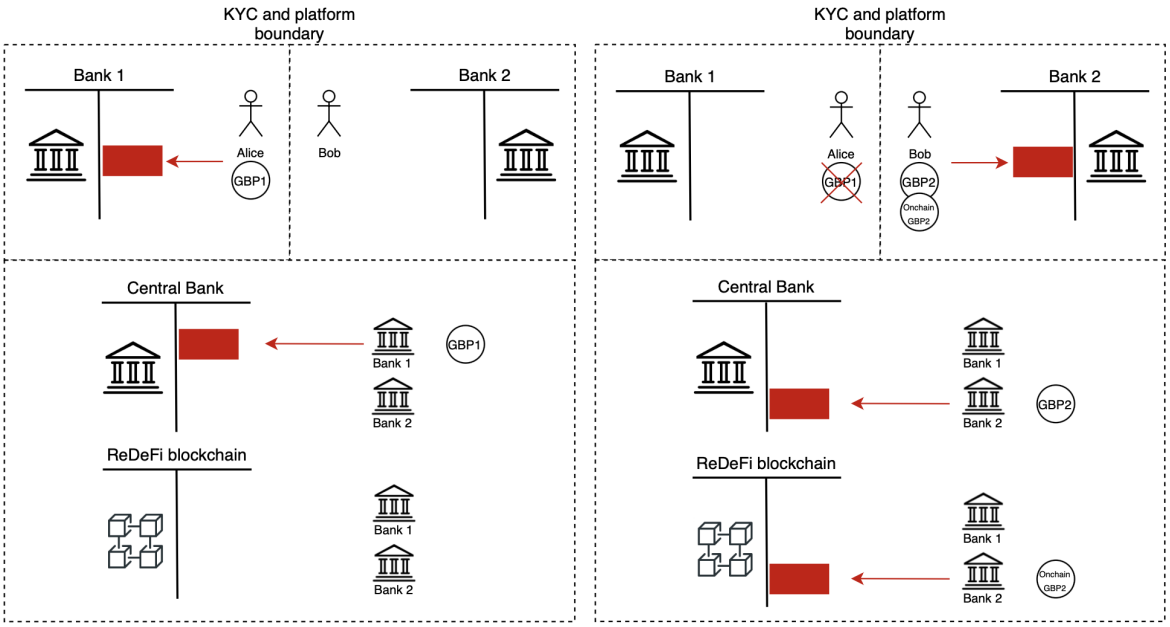
Graph 1. Alice sends money from her Current mirroring acct to Bob’s Current mirroring acct. Both banks are participants.

Use case 2. Alice sends money from her Current acct to Bob's Current mirroring acct.

The left-hand panel portrays the circumstances preceding Alice's payment to Bob. Alice has 1 Pound sterling in her Current acct with Bank 1. Alice sends money from her Current acct to Bob's Current mirroring acct.

The right-hand panel depicts what happens when Alice sends money to Bob:

a) Because Alice utilised her Current acct with Bank 1, there was no Onchain GBP mirroring conventional Pound sterling from her end. But, once Pound sterling landed at Bank 2 at Bob's Current account, Bank 2 also assigned ("minted" or "issued") one Onchain GBP to Bob's Current mirroring account.
b) The creation of onchain money tokens is accompanied by conventional GBP movement from Current acct at Bank 1 to Current mirroring acct at Bank 2 and the central bank's partition. One Pound sterling is moved from Bank 1 to Bank 2 and settled on the central bank's balance sheet. This is demonstrated by the fact that conventional GBP in the right-hand panel belongs to Bank 2 after transaction.



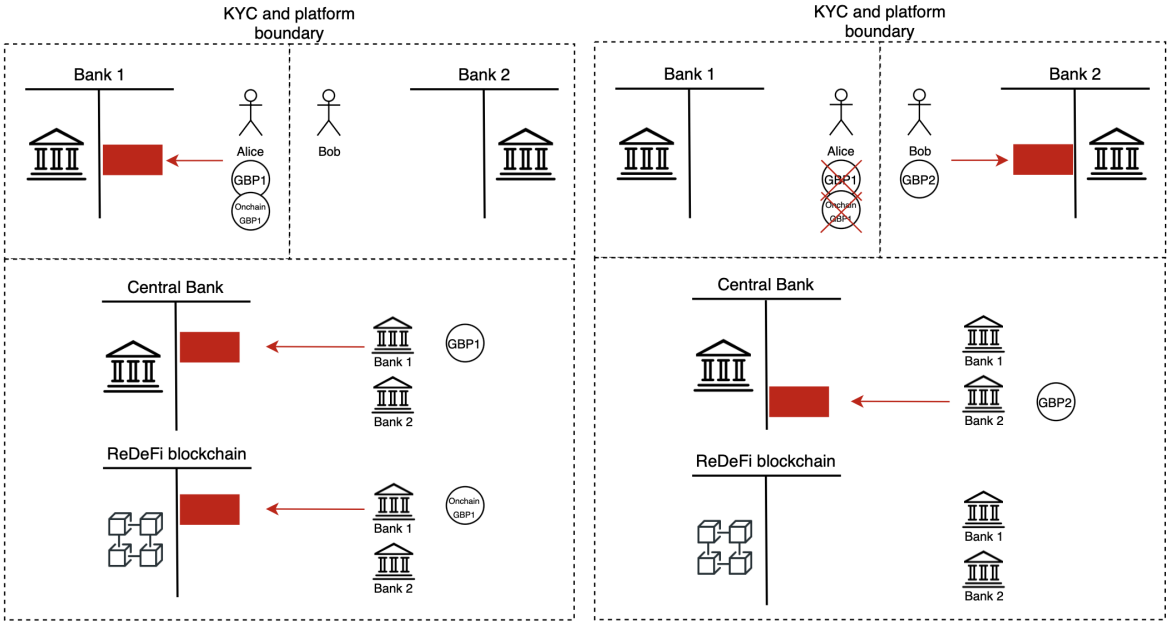
Graph 2. Alice sends money from her Current acct to Bob's Current mirroring acct. Both banks are participants.

Use case 3. Alice sends money from her Current mirroring acct to Bob's Current acct.

The left-hand panel portrays the circumstances preceding Alice's payment to Bob. Alice has 1 Pound sterling in her Current mirroring acct with Bank 1, which is mirrored and represented by 1 Onchain GBP in the ReDeFi blockchain. Alice sends money from her Current mirroring acct to Bob's Current acct.

The right-hand panel depicts what happens when Alice sends money to Bob:

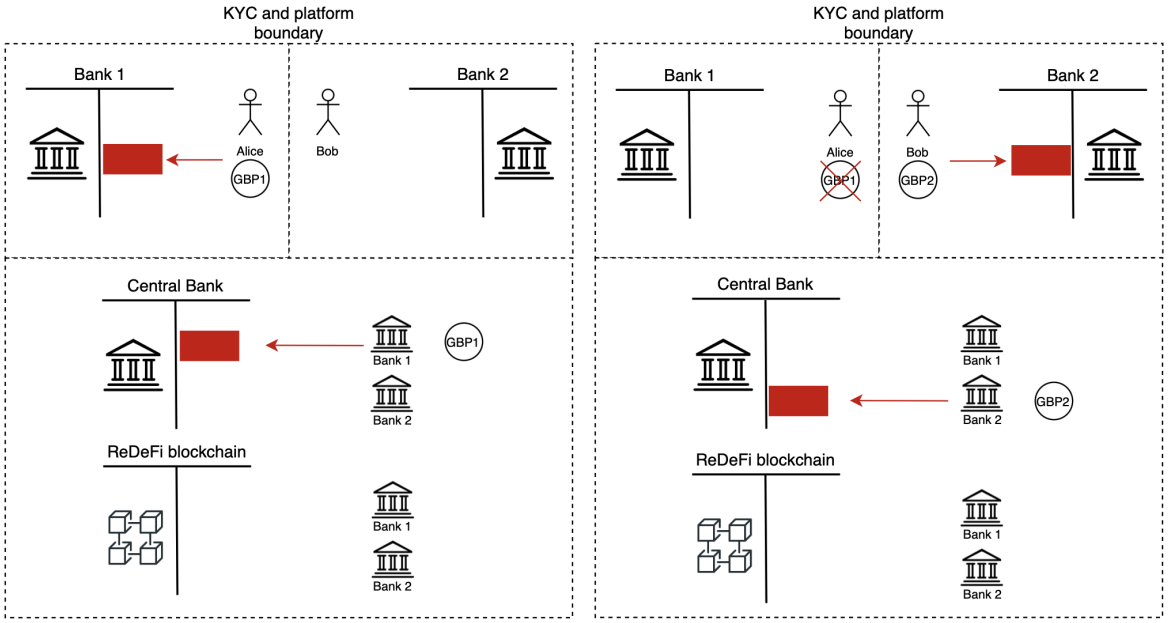
a) One Onchain GBP1 token held by Alice is deleted ("burned") by Bank 1. Because Alice sent to a Current acct at Bank 2, no Onchain GBP tokens were assigned ("minted" or “issued”) to Bob by Bank 2.
b) The deletion of onchain money tokens is accompanied by conventional GBP movement from Current mirroring acct at Bank 1 to Current acct at Bank 2 and the central bank's partition. One Pound sterling is moved from Bank 1 to Bank 2 and settled on the central bank's balance sheet. This is demonstrated by the fact that conventional GBP in the right-hand panel belongs to Bank 2 after transaction.



Graph 3. Alice sends money from her Current mirroring bank acct to Bob’s Current acct. Both banks are participants.

Use case 4. Alice sends money from her Current acct to Bob’s Current acct.

The left-hand panel portrays the circumstances preceding Alice's payment to Bob. Alice has 1 Pound sterling in her Current acct with Bank 1. Alice sends money from her Current acct to Bob’s Current acct.



Graph 4. Alice sends money from her bank acct to Bob's bank acct. Both banks are participants.

The right-hand panel depicts what happens when Alice sends money to Bob:

a) Because both accts are conventional, there are no onchain money tokens involved.
b) Conventional GBP moves from Current acct at Bank 1 to Current acct at Bank 2 and the central bank's partition. One Pound sterling is moved from Bank 1 to Bank 2 and settled on the central bank's balance sheet. This is demonstrated by the fact that conventional GBP in the right-hand panel belongs to Bank 2 after transaction.

Bank 1 is a participant of the ReDeFi environment, while Bank 2 is not.

Use cases and graphs below depict a specific technique of executing the Onchain GBP model utilising blockchain technology procedures and terminology. The dotted lines on the platform reflect the four partitions of the model maintained by one private tokenised money issuer (Banks 1) and Bank 2, which is not a ReDeFi network participant, and the central bank and the ReDeFi blockchain. The arrows indicate the issuers of the liabilities.

To be explicit, "Current acct" means a current bank account in conventional or modern banking with account details such as IBAN, BIC, sort code and account number. "Current mirroring acct" means a current bank account with account details such as IBAN, BIC, sort code and account number as well as a wallet address in the ReDeFi blockchain.

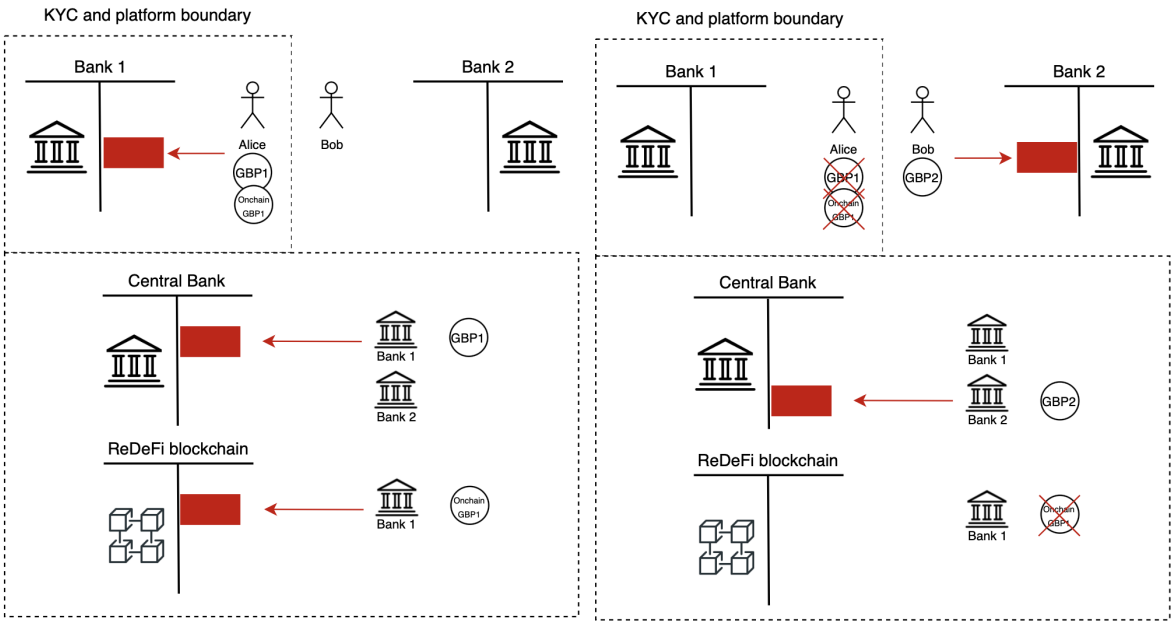
Both accounts are "everyday banking" accounts that give access to money for daily spending and can be linked to debit cards and can be protected by the FSCS.

Use case 5. Alice sends money from her Current mirroring acct to Bob's 3rd-party bank Current acct.

The left-hand panel portrays the circumstances preceding Alice's payment to Bob. Alice has 1 Pound sterling in her Current mirroring acct with Bank 1, which is mirrored and represented by 1 Onchain GBP in the ReDeFi blockchain. Alice sends money from her Current mirroring acct to Bob's Current acct.

The right-hand panel depicts what happens when Alice sends money to Bob:

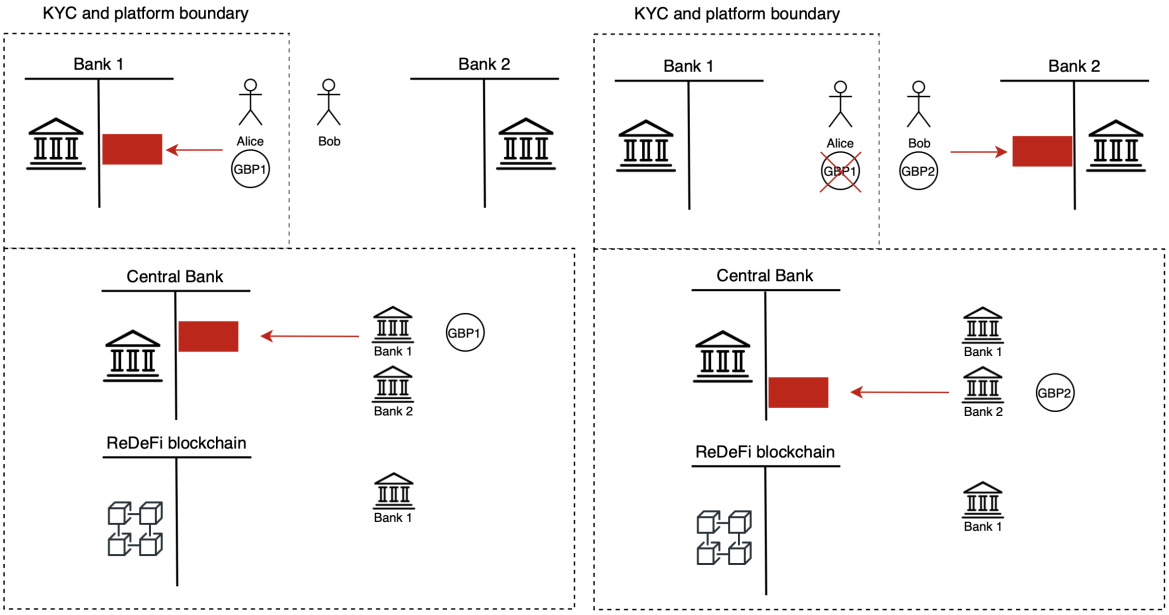
a) One Onchain GBP token held by Alice is deleted ("burned") by Bank 1. Because Bank 2 is not a participant of the ReDeFi network, it cannot deal with the onchain money tokens so no tokens are assigned ("minted" or "issued") to Bob by Bank 2.
b) The deletion of onchain money tokens is accompanied by conventional GBP movement from Current mirroring acct at Bank 1 to Current acct at Bank 2 and the central bank's partition. One Pound sterling is moved from Bank 1 to Bank 2 and settled on the central bank's balance sheet. This is demonstrated by the fact that conventional GBP in the right-hand panel belongs to Bank 2 after transaction.



Graph 5. Alice sends money from her Current mirroring acct to Bob's 3rd-party bank Current acct. Bank 1 is a participant.

Use case 6. Alice sends money from her Current acct to Bob's 3rd-party bank Current acct.

The left-hand panel portrays the circumstances preceding Alice's payment to Bob. Alice has 1 Pound sterling in her Current acct with Bank 1. Alice sends money from her Current acct to Bob's Current acct.



Graph 6. Alice sends money from her Current acct to Bob's 3rd-party bank Current acct. Bank 1 is a participant.

The right-hand panel depicts what happens when Alice sends money to Bob:

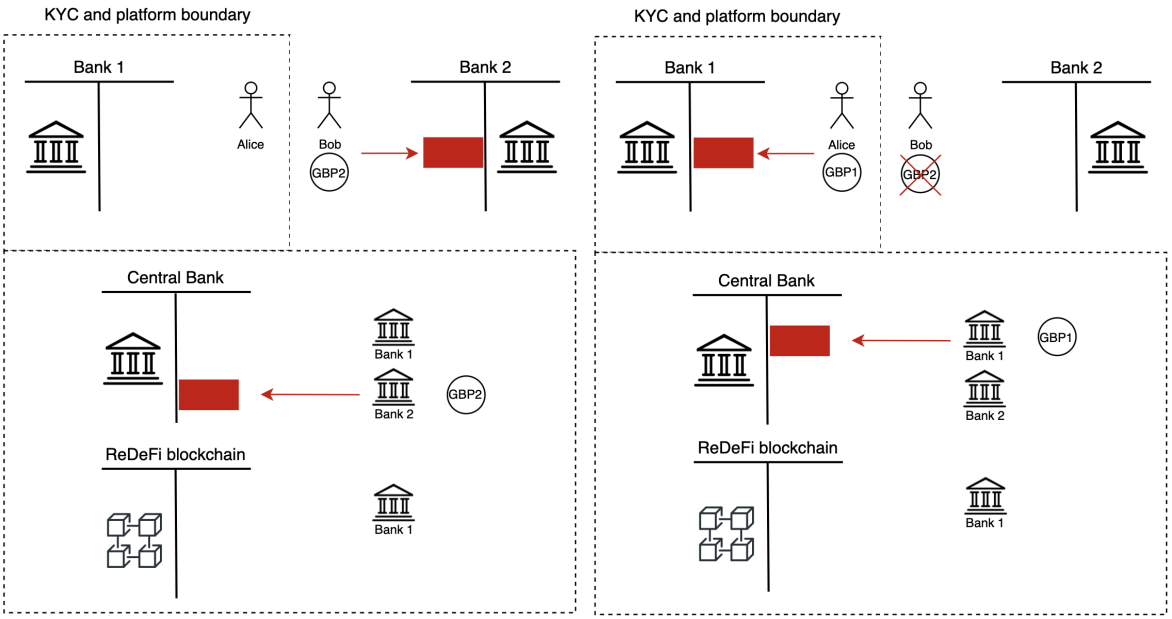
a) Because both accts are conventional, there are no onchain money tokens involved.
b) Conventional GBP moves from Current acct at Bank 1 to Current acct at Bank 2 and the central bank's partition. One Pound sterling is moved from Bank 1 to Bank 2 and settled on the central bank's balance sheet. This is demonstrated by the fact that conventional GBP in the right-hand panel belongs to Bank 2 after transaction.

Use case 7. Bob sends money from his 3rd-party bank Current acct to Alice's Current acct.

The left-hand panel portrays the circumstances preceding Bob's payment to Alice. Bob has 1 Pound sterling in his Current acct with Bank 2. Bob sends money from his 3rd-party bank Current acct to Alice's Current acct.

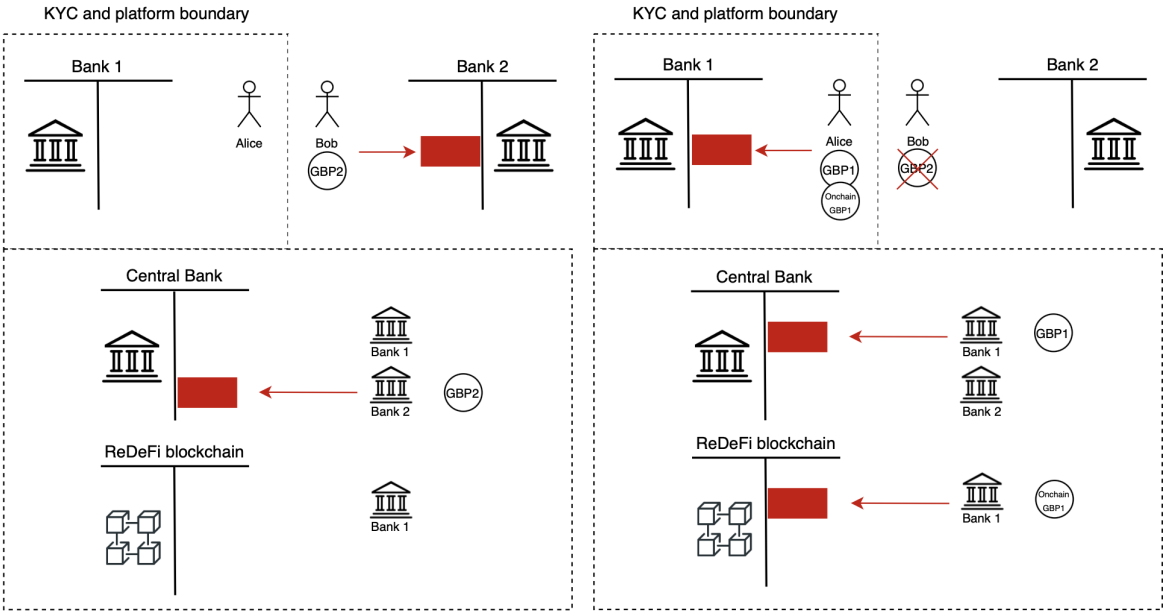
The right-hand panel depicts what happens when Bob sends money to Alice:

a) Because both accts are conventional, there are no onchain money tokens involved.
b) Conventional GBP moves from a 3rd-party bank Current acct at Bank 2 to Current acct at Bank 1 and the central bank's partition. One Pound sterling is moved from Bank 2 to Bank 1 and settled on the central bank's balance sheet. This is demonstrated by the fact that conventional GBP in the right-hand panel belongs to Bank 1 after transaction.



Graph 7. Bob sends money from his 3rd-party bank Current acct to Alice's Current acct. Bank 1 is a participant.

Use case 8. Bob sends money from his 3rd-party bank Current acct to Alice's Current mirroring acct.



Graph 8. Bob sends money from his 3rd-party bank Current acct to Alice's Current mirroring acct. Bank 1 is a participant.

The left-hand panel portrays the circumstances preceding Bob's payment to Alice. Bob has 1 Pound sterling in his Current acct with Bank 2. Bob sends money from his 3rd-party bank Current acct to Alice's Current mirroring acct.

The right-hand panel depicts what happens when Bob sends money to Alice:

a) Because Alice provided Bob with her Current mirroring acct at Bank 1, once Pound sterling landed at Bank 1 at Alice's Current mirroring acct, Bank 1 assigned ("minted" or "issued") one Onchain GBP to Alice's Current mirroring acct.
b) The creation of onchain money tokens is accompanied by conventional GBP movement from Bob's 3rd-party bank Current acct at Bank 2 to Current mirroring acct at Bank 1 and the central bank's partition. One Pound sterling is moved from Bank 2 to Bank 1 and settled on the central bank's balance sheet. This is demonstrated by the fact that both Onchain GBP tokens and conventional GBP in the right-hand panel belong to Bank 1 after transaction.

User interfaces

The user interfaces depicted below are simplified versions of an end user's mobile interface. For greater clarity, the mobile app has two distinctive tabs for Onchain money and Conventional money.

To be explicit, "Conventional money" means a Current acct in conventional or modern banking with account details such as IBAN, BIC, sort code and account number. "Onchain money" means a Current mirroring acct with account details such as IBAN, BIC, sort code account number as well as a wallet address in the ReDeFi blockchain.

Both accounts are "everyday banking" accounts that give access to money for daily spending and can be linked to debit cards and can be protected by the FSCS.

Interface 1. Sending money tabs.

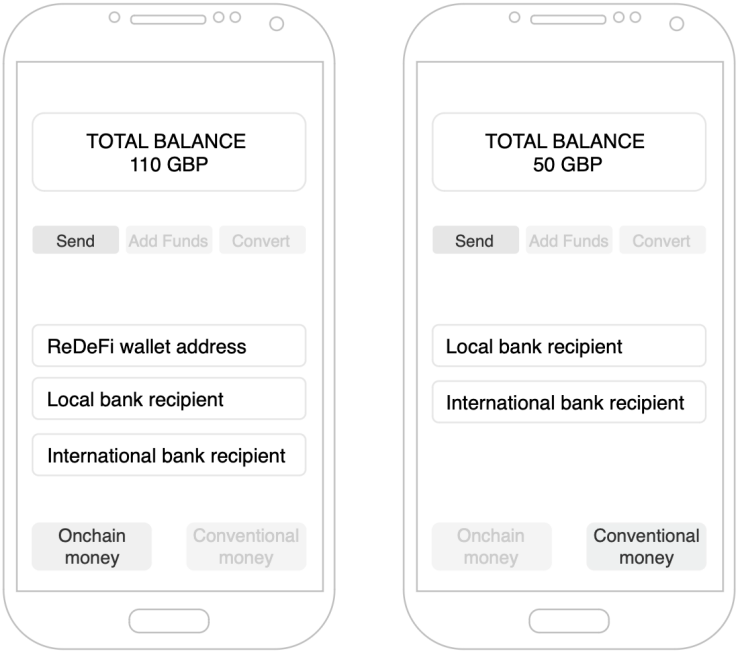
The Onchain money account is depicted on the left interface, with the following options:

1) To send money to a ReDeFi wallet address;
2) To send money to a local bank acct recipient using CHAPS, SEPA (e.g., the Sort code and Account number) or similar;
3) To send money to an overseas bank acct recipient using SWIFT (e.g., the IBAN and BIC) or similar.

All outbound onchain transactions from the Onchain money account to an external blockchain wallet address will be visible in the ReDeFi blockchain, but will not include the sender's or recipient's name or other account details.

The Conventional money account is depicted on the right interface, with the following options:

1) To send money to a local bank acct recipient using CHAPS, SEPA (e.g., the Sort code and Account number) or similar;
2) To send money to an overseas bank acct recipient using SWIFT (e.g., the IBAN and BIC) or similar.



Interface 1. Sending money tabs.

Interface 2. Receiving money tabs.

The Onchain money account is depicted on the left interface, with the following options:

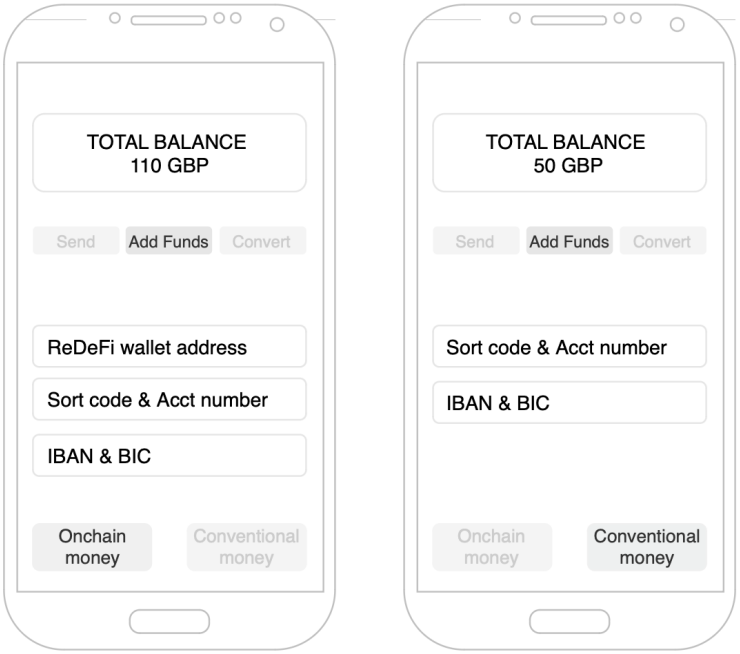
1) To receive money from a ReDeFi wallet address;
2) To receive money from a local bank acct using CHAPS, SEPA (e.g., the Sort code and Account number) or similar;
3) To receive money from an overseas bank acct using SWIFT (e.g., the IBAN and BIC) or similar.

All inbound onchain transactions from an external blockchain wallet address to the Onchain money account will be viewable in the ReDeFi blockchain, but will not include the sender's or recipient’s name or other account details.

The Conventional money account is depicted on the right interface, with the following options:

1) To receive money from a local bank using CHAPS, SEPA (e.g., the Sort code and Account number) or similar;

2) To receive money from an overseas bank using SWIFT (e.g., the IBAN and BIC) or similar.



Interface 2. Receiving money tabs.

Interface 3. Converting money.

The Onchain money account is depicted on the left interface, with the following option:

1) To convert money to Conventional GBP.

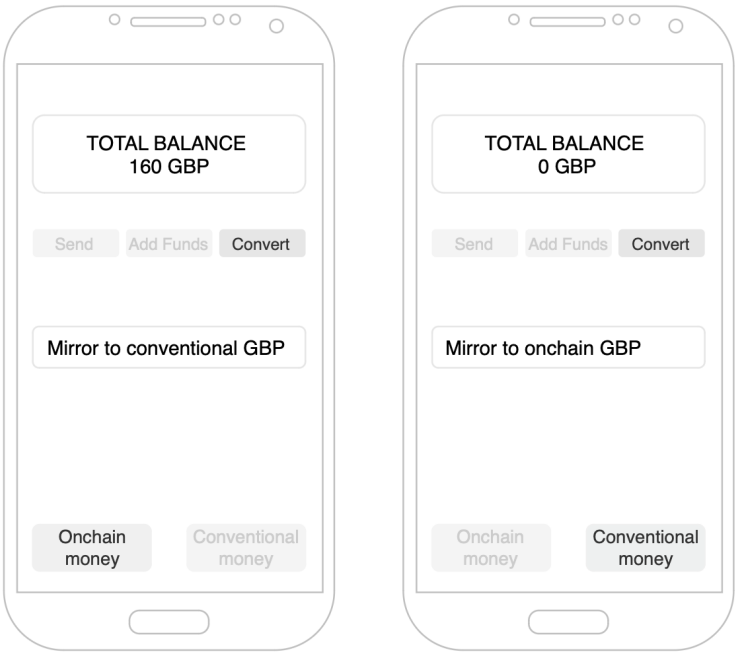
The Conventional money account is depicted on the right interface, with the following option:

1) To convert money to Onchain GBP.

In the interfaces below, its user transferred 50 GBP from their Conventional money tab (Current acct) to their Onchain money (Current mirroring acct), resulting in 160 Onchain GBP.

(The user had 110 Onchain GBP and 50 Conventional GBP on the interfaces 1 and 2).

Because both accounts are "everyday banking" accounts that provide access to funds for daily expenditure, can be connected to debit cards, and are FSCS-protected, this user can spend 160 Onchain GBP from their Current mirroring acct.



Interface 3. Converting money.

Conclusion

Onchain GBP model represents a tokenised deposits that do not break the “singleness of money” principle and expands the functionality by enabling programmable ledgers and introducing contingent execution and composability of transactions.

Thus, the Onchain GBP model is appropriate for use by banks and other financial institutions, as well as individuals and businesses, who want to benefit from the enhanced functionality and smart contracts' ability to introduce instant execution, traceability, near-zero cost of operations, and transaction composability while remaining on the regulated side of the financial system.

ReDeFi Self-Custody Wallet

Key takeaways:

- *ReDeFi Self-Custody Wallet is a decentralised wallet that allows users to retain complete control over their digital assets, including Onchain money, and access their funds online from different devices.*
- *ReDeFi Self-Custody Wallet allows its users to take advantage of mirroring safeguarding[10] accounts that hold the same amount of traditional fiat currency that users have Onchain money in their wallets..*
- *ReDeFi Self-Custody Wallet provides users with bank acct information such as sort code and account number, IBAN and BIC, and others, allowing them to send traditional fiat currencies from regulated institutions like banks and receive them as Onchain money in their ReDeFi Wallets.*

The ability to keep total control over owned assets is a fundamental human right. Existing non-custodial, or decentralised, hot and cold wallets allow users to own the wallet's private keys (a secret seed phrase that functions similarly to a very strong password) and retain ownership of their cryptocurrencies and tokens. As well as participate in smart contracts or blockchain protocols. The problem with the existing non-custodial wallets is that they do not fit the regulations such as FATF[11], and so cannot be completely incorporated into the financial sector.

The ReDeFi Blockchain is a decentralised network that is regulated. Thus it allows its active users to create decentralised apps and services that can be active participants in the regulated financial sector. The ReDeFi Self-Custody Wallet is a hot wallet that allows users to keep control of their cash in the network by controlling private keys and seed phrases.

Problem statement 1: Can the ReDeFi Self-Custody Wallet fit the existing regulation while also providing its users with an ability to retain complete control over their assets?

Problem statement 2: Can the ReDeFi Self-Custody Wallet work with the existing financial system and provide users with an enhanced utility via smart-contrat interactions?

The ReDeFi Self-Custody Wallet model

[10] https://www.fca.org.uk/firms/emi-payment-institutions-safeguarding-requirements
[11] https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Targeted-update-virtual-assets-vasps.html

The ReDeFi Self-Custody Wallets represent the issuer's liabilities, and the holder has a claim on the issuer for redemption. Depending on the asset, the claim could be at par value in the sovereign unit of account (for example, Onchain money) or not (for example, stablecoins or other tokens).

When using Onchain money, the ReDeFi Self-Custody Wallet represents tokenised deposits that do not violate the "singleness of money" principle. Moreover, the wallets are linked to individual safeguarding accounts in a bank. As a result, the ReDeFi Self-Custody Wallet can be used within the traditional banking system: individuals and businesses, for example, could send traditional money from or to traditional bank accounts while benefiting from enhanced functionality such as instant execution, traceability, near-zero cost of operations, and the ability to interact with smart contracts while remaining on the regulated side of the financial system.

It is also important to note that the ReDeFi Self-Custody Wallets have no AML[12] or KYC[13] compliance flaws because liabilities are indirectly transferred to individuals with verified identities.

The table below depicts the distinctions between the ReDeFi Self-Custody Wallets and other wallets.

	ReDeFi Wallet	Other decentralised wallets
Organisation behind	Regulated Decentralised Finance LTD	Anyone
Who is in full control of the assets?	User, they keep the private/public keys and the seed phrase	User, they keep the private/public keys and the seed phrase
Can wallets hold tokens?	Yes	Yes
Can wallets work with Onchain money such as Onchain GBP, Onchain EUR and so on?	Yes	No
Do tokens represent the issuer's liabilities?	For Onchain money, the claim is at par value in the sovereign unit of account. For other tokens, it works in the same way as other wallets.	Supposedly yes, but it is not possible to verify.
Is Onchain money in the wallet backed by conventional money?	Onchain money is not backed, but mirrored in a safeguarding accounts in a traditional bank by ReDeFi LTD	No
Is Onchain money in the wallet protected?	Yes, since Onchain money are mirrored in a safeguarding accounts in a traditional bank by ReDeFi LTD	No

[12] Anti-money laundering (AML)
[13] Know-your-customer (KYC)

Can conventional money be sent to the wallet?	Yes, they will arrive as the Onchain money	No
Can Onchain money be sent from the wallet to a bank acct?	Yes, users can send Onchain money to their bank accounts	No

Table 2. Difference between the ReDeFi Self-Custody Wallets and other wallets.

Use cases

Use cases and graphs below depict the work of ReDeFi Wallets utilising blockchain technology procedures and terminology. The dotted lines reflect the five partitions of the model maintained by the one private tokenised money issuers (ReDeFi LTD) and the central bank and the ReDeFi blockchain. The arrows indicate the issuers of the liabilities.

To be explicit,
"Current acct" means a current bank account in conventional or modern banking with account details such as IBAN, BIC, sort code and account number.
"Current mirroring acct" means a current bank account with account details such as IBAN, BIC, sort code and account number as well as a wallet address in the ReDeFi blockchain.

Both accounts are “everyday banking” accounts that give access to money for daily spending and can be linked to debit cards and can be protected by the FSCS.

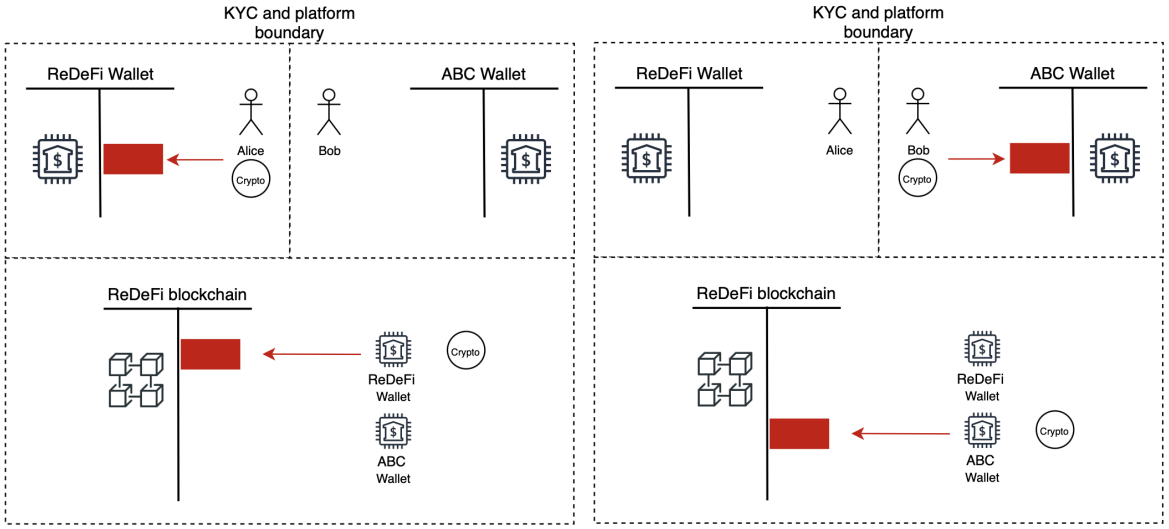
"Mirroring ReDeFi sub account" refers to a bank sub account under the ReDeFi LTD account. The funds in these sub accounts do not belong to users, but rather to ReDeFi, and are kept in segregated safeguarded sub accounts. This design allows to avoid double spending issues while also unlocking Mirroring current accounts for Onchain money. Every ReDeFi Wallet is linked to a Mirroring ReDeFi sub account that contains bank acct details such as IBAN, BIC, sort code, and account number, allowing users to send money from traditional banks and receive it as Onchain money in a decentralised wallet or send money to traditional banks directly from their decentralised ReDeFi Wallets.

Use case 1. Alice sends cryptocurrency from her ReDeFi Wallet to Bob’s ABC wallet.

The left-hand panel portrays the circumstances preceding Bob's transaction. Bob has 1 cryptocurrency token in his ABC Wallet in the ReDeFi network.

The right-hand panel depicts what happens when Bob sends funds:

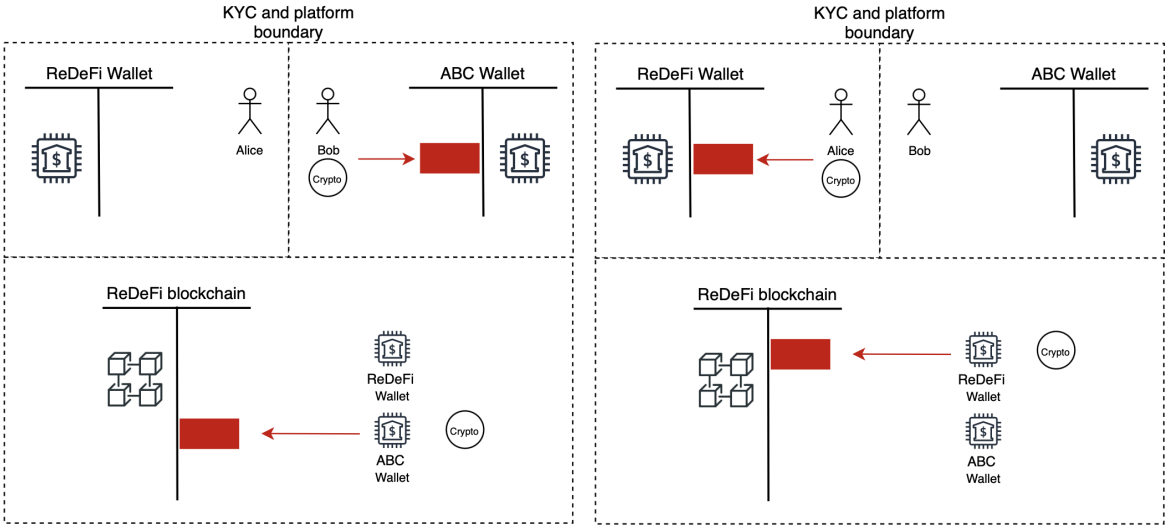
a) Cryptocurrency token held by Bob is transferred to Alice after network confirmations.



Graph 9. Alice sends cryptocurrency from her ReDeFi Wallet to Bob's ABC wallet.

Use case 2. Alice receives cryptocurrency to her ReDeFi Wallet from Bob's wallet.

The left-hand panel portrays the circumstances preceding Alice's transaction. Alice has 1 cryptocurrency token in her ReDeFi Wallet in the ReDeFi network.



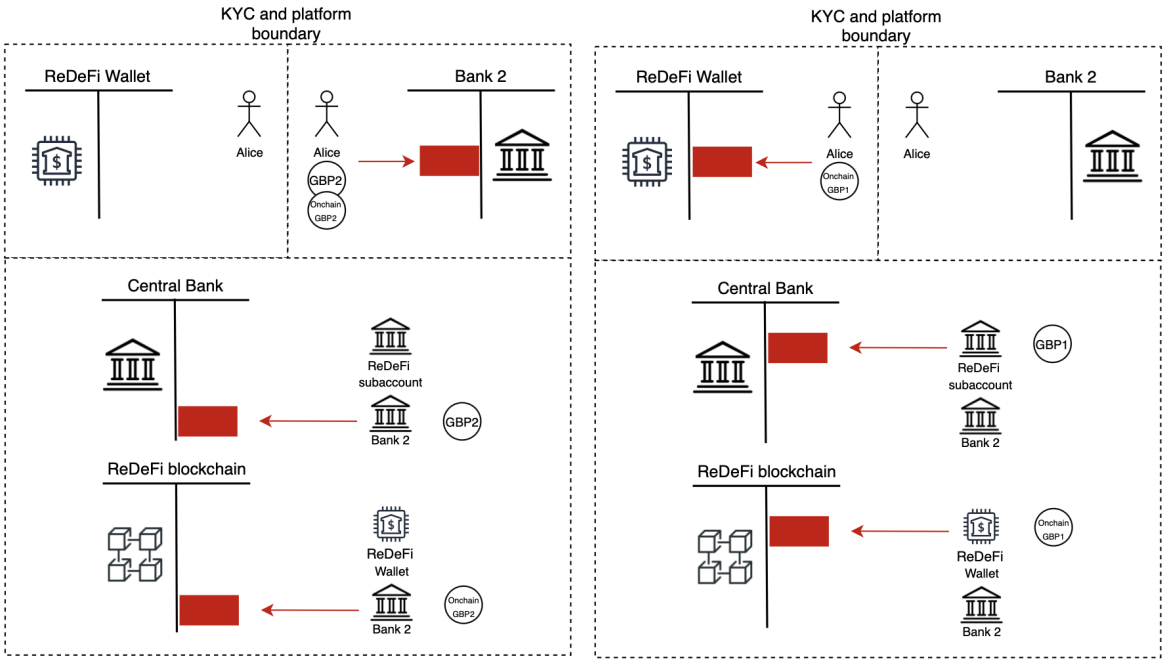
Graph 10. Alice receives cryptocurrency to her ReDeFi Wallet from Bob's ABC wallet.

The right-hand panel depicts what happens when Alice sends funds:

a) Cryptocurrency token held by Alice is transferred to Bob after network confirmations.

Use case 3. Alice sends Onchain money from her Current mirroring acct in a ReDeFi network bank to her ReDeFi Wallet.

The left-hand panel portrays the circumstances preceding Alice's transaction. Alice has 1 Pound sterling in her Current mirroring acct with Bank 2, which is mirrored and represented by 1 Onchain GBP in the ReDeFi blockchain. Alice sends money from her Current mirroring acct in a ReDeFi network bank (Bank 2) to her ReDeFi Wallet.



Graph 11. Alice sends Onchain money from her Current mirroring acct in a ReDeFi network bank (Bank 2) to her ReDeFi self-custody Wallet.

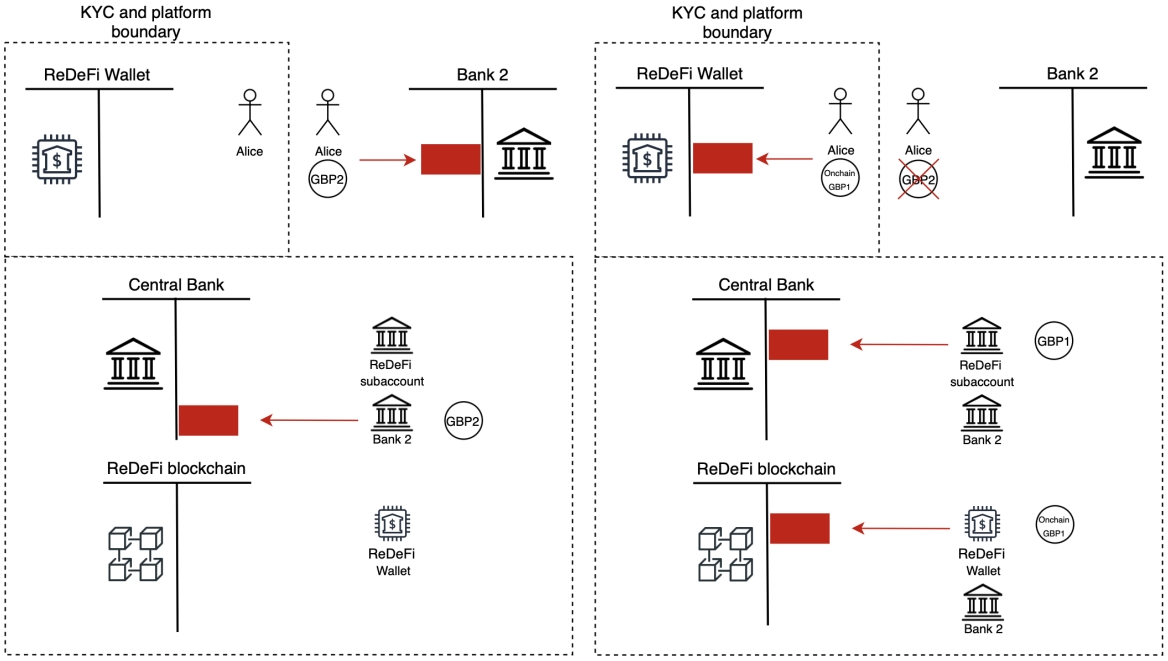
The right-hand panel depicts what happens when Alice sends money:

a) One onchain GBP token held by Alice is deleted ("burned") by Bank 2, and one onchain GBP token is assigned ("minted" or “issued”) to Alice by ReDeFi. Onchain GBP tokens can be transferred (rather than burned and issued) since both Bank 2 and ReDeFi are within the ReDeFi network.
b) The deletion and creation of onchain money tokens is accompanied by conventional GBP movement from Current mirroring acct at Bank 2 to Mirroring ReDeFi sub account and the central bank's partition. One Pound sterling is moved from Bank 2 to the ReDeFi sub account and settled on the central bank's balance sheet. This is demonstrated by the fact that onchain GBP tokens in the right-hand panel belong to Alice’s ReDeFi Wallet and conventional GBP belong to Mirroring ReDeFi Sub account after transaction.

Use case 4. Alice sends money from her Current acct in a 3rd party bank to her ReDeFi Wallet.

The left-hand panel portrays the circumstances preceding Alice's transaction. Alice has 1 Pound sterling in her Current acct with Bank 2, because it is not a ReDeFi network

participant, there is no Onchain GBP. Alice sends money from her Current acct in a 3rd party bank to her ReDeFi Wallet using Mirroring ReDeFi sub account details.



Graph 12. Alice sends money from her Current acct in a 3rd party bank (Bank 2) to her ReDeFi Wallet.

The right-hand panel depicts what happens when Alice sends money:

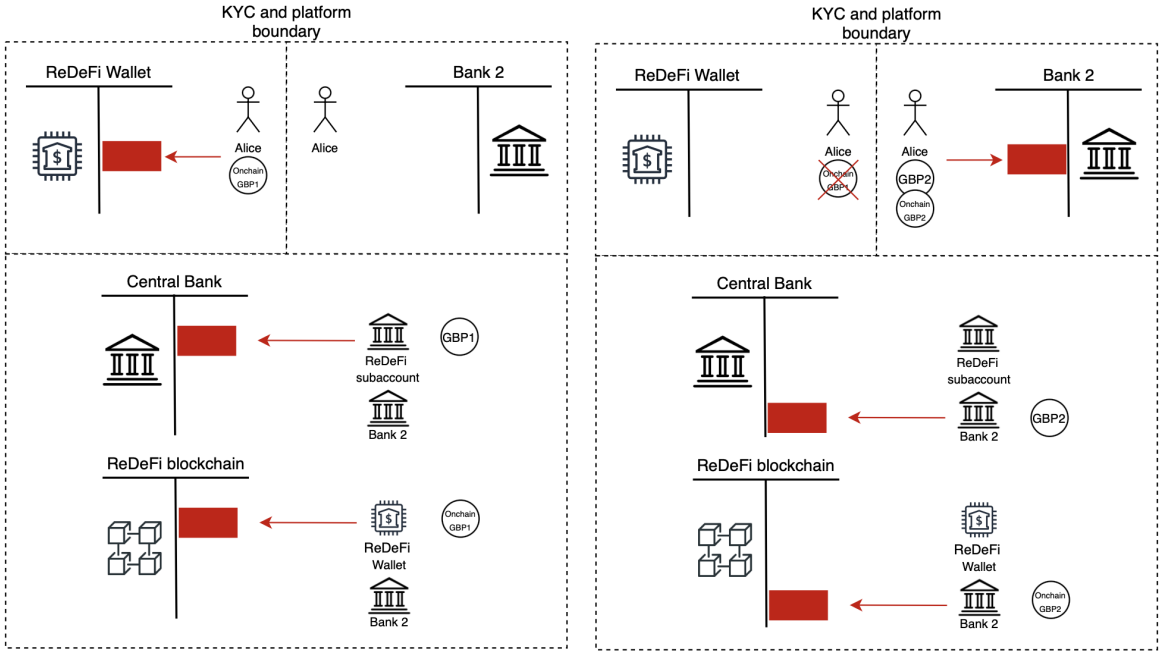
a) Because Alice uses account details of a Mirroring ReDeFi sub account linked to her ReDeFi Wallet, once 1 Pound sterling landed at Mirroring ReDeFi sub account, ReDeFi assigned ("minted" or "issued") one onchain GBP to Alice's ReDeFi Wallet.
b) The deletion and creation of onchain money tokens is caused by conventional GBP movement from Current acct at Bank 2 to Mirroring ReDeFi sub account and the central bank's partition. One Pound sterling is moved from Bank 2 to the ReDeFi sub account and settled on the central bank's balance sheet. This is demonstrated by the fact that onchain GBP tokens in the right-hand panel belong to Alice's ReDeFi Wallet and conventional GBP belong to Mirroring ReDeFi Sub account after transaction.

Use case 5. Alice sends Onchain money from her ReDeFi Wallet to her Current mirroring acct in a ReDeFi network bank.

The left-hand panel portrays the circumstances preceding Alice's transaction from her ReDeFi Wallet to her Current mirroring acct in a ReDeFi network bank. Alice has 1 Onchain GBP in her ReDeFi Wallet. ReDeFi LTD stores 1 Pound sterling under the sub account linked to Alice's wallet. These funds do not belong to Alice but they are required to keep the "singleness of money" principle. Alice sends tokens from her ReDeFi Wallet to her Current mirroring acct in a ReDeFi network bank (Bank 2).

The right-hand panel depicts what happens when Alice sends money:

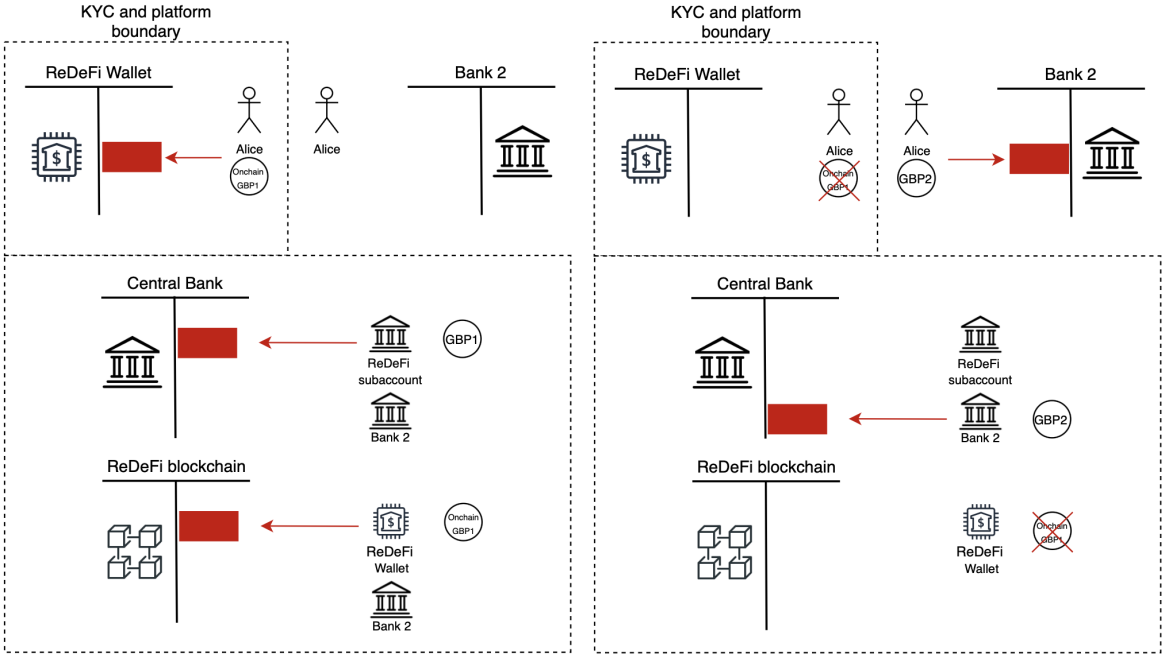
a) One onchain GBP token held by Alice is deleted ("burned") by ReDeFi blockchain, and one onchain GBP token is assigned ("minted" or “issued”) to Alice by Bank 2. Onchain GBP tokens can be transferred (rather than burned and issued) since Bank 2 is a ReDeFi network participant.
b) The deletion and creation of onchain money tokens is accompanied by conventional GBP movement from Mirroring sub acct at ReDeFi LTD to Current mirroring acct at Bank 2 and the central bank's partition. One Pound sterling is moved from ReDeFi LTD to Bank 2 and settled on the central bank's balance sheet. This is demonstrated by the fact that both onchain GBP tokens and conventional GBP in the right-hand panel belong to Bank 2 after transaction.



Graph 13. Alice sends Onchain money from her ReDeFi Wallet to her Current mirroring acct in a ReDeFi network bank (Bank 2).

Use case 6. Alice sends Onchain money from her ReDeFi Wallet to her Current acct in a 3rd party bank.

The left-hand panel portrays the circumstances preceding Alice's transaction. Alice has 1 Onchain GBP in her ReDeFi Wallet, and the ReDeFi keeps one Pound sterling in the corresponding Mirroring ReDeFi sub account. Alice sends her Onchain GBP from her ReDeFi Wallet to a 3rd party bank account (Bank 2).



Graph 14. Alice sends Onchain money from her ReDeFi Wallet to her Current acct in a 3rd party bank (Bank 2).

The right-hand panel depicts what happens when Alice sends money:

a) One onchain GBP token held by Alice is deleted ("burned") by ReDeFi blockchain, and because Bank 2 is not a ReDeFi network participant, no onchain GBP is assigned ("minted" or “issued”) to Alice by Bank 2.
b) The deletion of onchain money tokens is caused by conventional GBP movement from Mirroring ReDeFi sub account to Current acct at Bank 2 and the central bank's partition. One Pound sterling is moved from the ReDeFi to Bank 2 and settled on the central bank's balance sheet. This is demonstrated by the fact that conventional GBP belongs to Bank 2 after this transaction.

User interfaces

Simplified versions of mobile user's interfaces are shown below. The actual interfaces themselves could differ. ReDeFi Wallet may also offer web interfaces.

Interface 1. ReDeFi Wallet main tabs.

On the left, the main tab displays the available Onchain money, cryptocurrency and tokens. The two buttons above the balances allow users to Send and Add funds to their wallets.

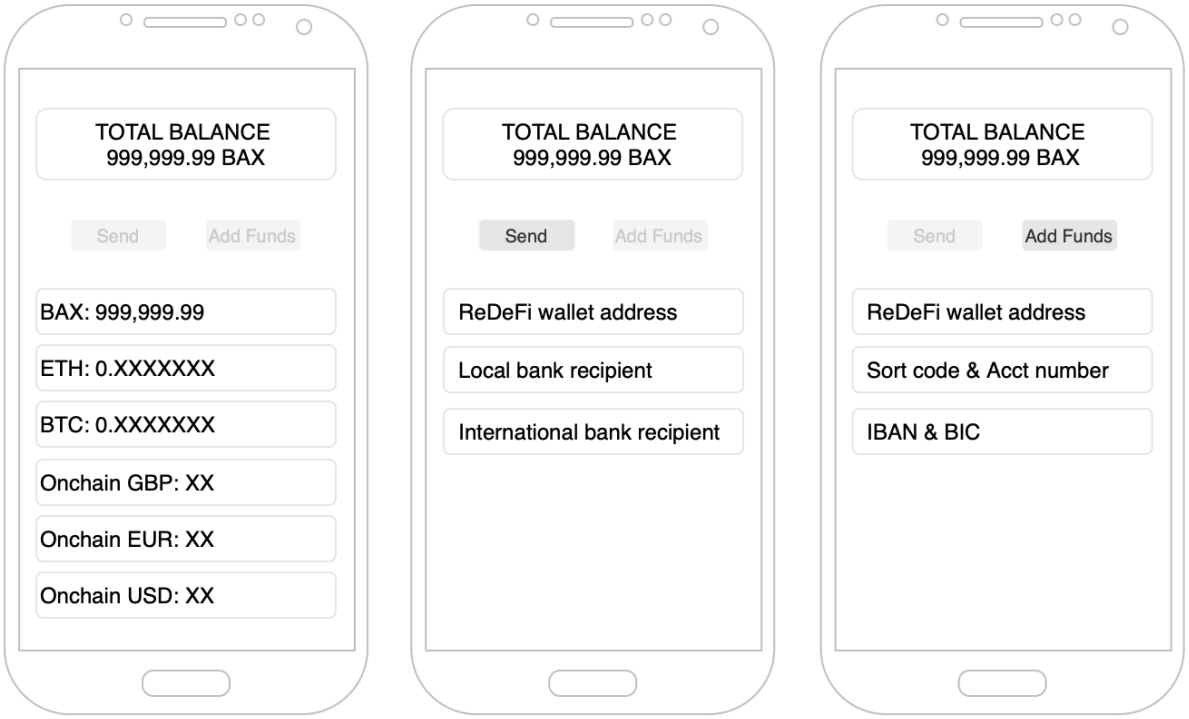
The Send tab is shown in the centre. Depending on the asset, a user can:

1) Send funds to a ReDeFi Wallet address;

2) Send funds to a local bank acct recipient using CHAPS, SEPA (e.g., the Sort code and Account number) or similar;
3) Send funds to an overseas bank acct recipient using SWIFT (e.g., the IBAN and BIC) or similar.

Cryptocurrencies like BAX, ETH, and BTC will only have wallet address options, however Onchain money like GBP, EUR, and USD will have two more options for sending straight to a bank. This action will be carried out from the Mirroring ReDeFi sub-account associated with this wallet.

The Add Funds tab is shown on the right.



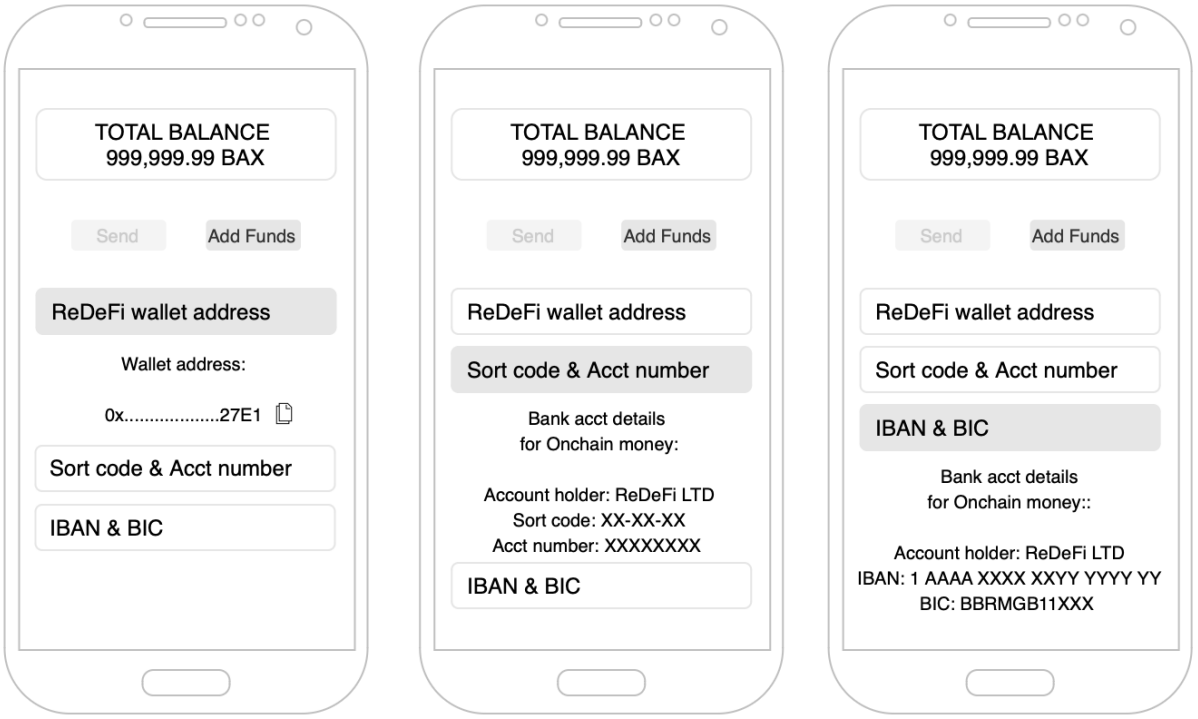
Interface 4. ReDeFi Wallet main tabs.

Interface 2. Add funds options.

The main tabs for Add Funds are shown below. Depending on the asset selected, a user can:

1) Receive funds from a ReDeFi Wallet address;
2) Receive funds from a local bank acct using CHAPS, SEPA (e.g., the Sort code and Account number) or similar;
3) Receive funds from an overseas bank acct using SWIFT (e.g., the IBAN and BIC) or similar.

Which is seen below, from left to right.



Interface 5. Add funds options.

Cryptocurrencies like BAX, ETH, and BTC will only have wallet address options, however Onchain money like GBP, EUR, and USD will have two more options for receiving funds. This action will be carried out using bank acct details from the Mirroring ReDeFi sub-account associated with this wallet.

Conclusion

ReDeFi Self-Custody Wallet complies with current regulations and can use the Onchain GBP model, which represents tokenised deposits that do not violate the "singleness of money" principle. Furthermore, users have complete control over their assets in the wallet.

The ReDeFi Self-Custody Wallet extends the capabilities of existing decentralised wallets by enabling programmable ledgers and smart contracts while remaining on the regulated side of the financial system.

FX Swap Protocol

The FX Swap Protocol introduces a DEX tailored specifically for the exchange of Onchain Money. It facilitates the conversion and settlement of Onchain Money among participants within the prescribed KYC border.

The Onchain Money Paradigm

Onchain Money, representing liabilities of the issuing entity, assures holders redemption at par value in the sovereign unit of account. It exists within a controlled environment, wherein participants are clients of regulated financial institutions. This design precludes the direct transfer of liabilities outside the KYC boundaries, ensuring compliance and integrity within the financial ecosystem. Settlements occur in real-time, with the bank's ledger balance sheet as the fulcrum, maintaining the singularity and confidence akin to conventional fiat money.

Functionalities

This protocol operates on the premise of facilitating foreign exchange transactions within the ReDeFi blockchain, mirroring traditional banking systems. It leverages the stability of Onchain Money, as it is pegged and settled against central bank reserves. The swaps do not engage with transferable liabilities, thereby preserving the integrity of the monetary system and maintaining the value parity anchored to the sovereign currency.

Operational Integration

The DEX offers an interface for banks to conduct foreign exchange transactions in a decentralised manner. It recognises the dual presence of Onchain Money - as reflected in the traditional banking accounts and simultaneously on the ReDeFi blockchain. The exchange operates under strict adherence to the regulatory framework, thereby negating concerns related to Anti-Money Laundering (AML) and Know Your Customer (KYC) compliance.

Distinction from Conventional DEX Models

The core differential of the FX Swap Protocol lies in its exclusion from market price-driven financial assets, remaining impervious to volatility typically associated with other cryptocurrencies or tokens. It functions under the protection of regulated financial entities, with each transaction underpinned by conventional GBP settlements.

The FX Swap Protocol provides a regulated, stable, and efficient DEX for foreign exchange within our network. It underscores the innovative potential of blockchain technology to operate within the boundaries of existing financial regulations while offering enhanced efficiency and security to every-day transactions between participants.

Sustainability and UN's SDG

Social impact

Reducing inequality, particularly financial inequality, and spurring economic growth has been at the heart of ReDeFi since the beginning. As a result, ReDeFi, as a responsible player seeking to pave the way towards fair and responsible banking, has joined the 2030 Agenda for Sustainable Development[14] which was adopted by all United Nations Member States in 2015. The agenda lays out a shared vision for people and the planet's peace and prosperity today and in the future. The 17 Sustainable Development Goals (SDGs)[15] are at the heart of everything, and they represent an urgent call to action by all governments AND businesses in a global partnership.

We at ReDeFi think that focusing on less and achieving more is preferable to focusing on more and missing out. As a result, ReDeFi has chosen four targets from three objectives, by priority:

Goal 10, Target 10.c: "By 2030, reduce to less than 3 per cent the transaction costs of migrant remittances <...>".

Goal 10, Target 10.2: "By 2030, empower and promote the social, economic and political inclusion of all, irrespective of age, sex, disability, race, ethnicity, origin, religion or economic or other status".

Goal 1, Target 4: "By 2030, ensure that all men and women, in particular the poor and the vulnerable, have equal rights to economic resources, as well as access to basic services, ownership and control over <...> appropriate new technology and financial services <...>."

Goal 8, Target 10: "Strengthen the capacity of domestic financial institutions to encourage and expand access to banking, insurance and financial services for all".

ReDeFi is committed to ending financial exclusion in all of its forms and dimensions, so that all people can reach their full potential in dignity and equality, live wealthy and meaningful lives, and economic and technical progress can occur in harmony.

[14] https://sdgs.un.org/2030agenda
[15] https://sdgs.un.org/goals

As a result, ReDeFi is dedicated to achieving sustainable development in a balanced and integrated manner. We will combat financial inequities within and among countries, as well as create conditions for inclusive, sustainable and long-term economic growth.

Environmental impact

ReDeFi is a blockchain that is environmentally friendly. To secure the network, ReDeFi's PoS-A consensus mechanism uses RED rather than energy. It is too early to say how much energy ReDeFi consumes across the entire global network though. The bottom-up estimates of the ReDeFi network's electricity consumption and carbon footprint will depend on the electricity consumption of different nodes as well as differences in hardware and client software configurations. As nodes join and exit the network, the annual electricity usage and carbon emissions values will change. ReDeFi will make every effort to make emissions data and energy use reports available as soon as practicable for individuals who want to inspect its findings or utilise it for their analyses.

It is worthwhile to compare estimates for different industries in order to contextualise ReDeFi's predicted energy consumption. This will help us determine whether the PoS-A estimate is high or low.

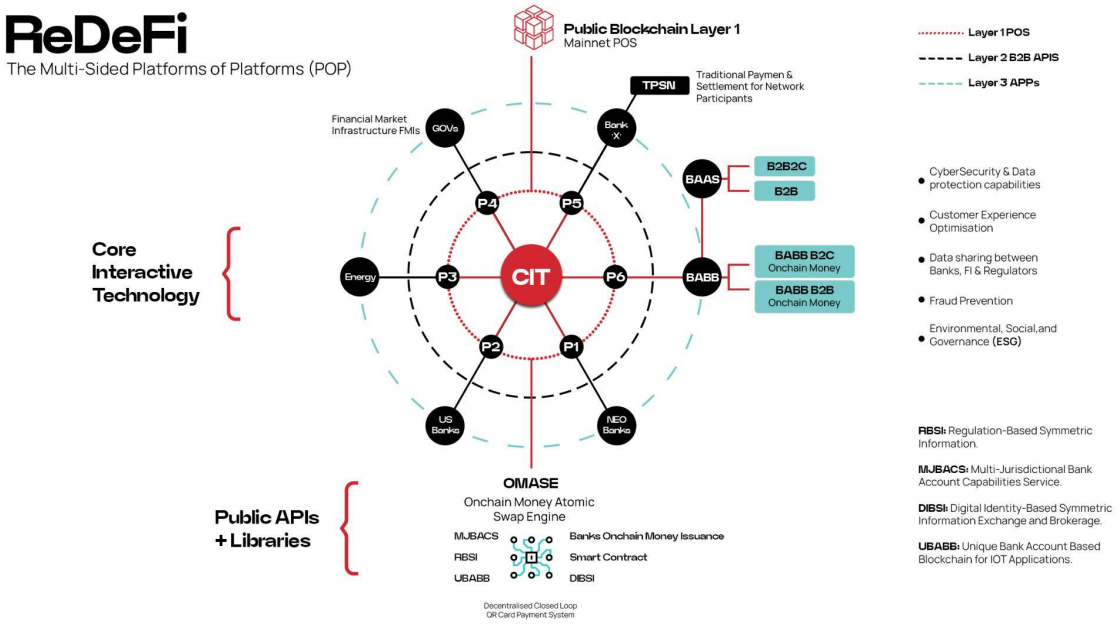
	Annualised energy consumption (TWh)
Data centres[16]	200
Bitcoin's Proof-of-Work [17]	131
YouTube[18]	12
Netflix[19]	0.451
ReDeFi's PoS-A estimated	0.002 - 0.004

Table 3. Predicted annual energy consumption for the ReDeFi comparison table.

ReDeFi's PoS-A consensus is both energy-efficient and environmentally-friendly. A staking mechanism that uses validators chosen from the staking pool to validate transactions, thereby gaining incentives and contributing to the network's growth, aids in the maintenance of a clean and energy-efficient blockchain and lowers its carbon footprint.

[16] https://www.iea.org/commentaries/data-centres-and-energy-from-global-headlines-to-local-headaches
[17] https://ccaf.io/cbnsi/cbeci/comparisons
[18] https://www.gstatic.com/gumdrop/sustainability/google-2020-environmental-report.pdf
[19] https://ir.netflix.net/governance/ESG/default.aspx

Core Interactive Technology



The Core Interactive Technology (CIT) facilitates a range of services from traditional banking systems to innovative financial market infrastructures. Within the ReDeFi ecosystem, distinct points from P1 to P6 *(image above)* represent interfaces for multifaceted interactions among banks, regulatory bodies, and energy sectors, each connecting to ReDeFi. This integration can support the seamless execution of complex financial operations such as on-chain settlements, regulatory compliance checks, and cross-institution data sharing.

The Onchain Money Atomic Swap Engine (OMASE) has the capability to execute real-time transactions across different banking entities. By enabling atomic swaps, OMASE reduces dependency on intermediaries, thereby minimising settlement time and associated risks. Similarly, the Regulation-Based Symmetric Information (RBSI) and Digital Identity-Based Symmetric Information (DISBI) systems embed compliance into the transaction pipeline, ensuring adherence to financial regulations and secure information exchange.

The Multi-Jurisdictional Bank Account Capabilities Service (MJBACS) streamlines cross-border banking operations, fit for the complex regulatory landscapes and diverse customer needs. It simplifies the creation and management of bank accounts across different jurisdictions, enhancing the global reach of financial services.

For Internet of Things (IoT) applications, the Unique Bank Account Based Blockchain (UBABBI) provides a secure and traceable platform, blending financial transactions with the IoT infrastructure. This integration paves the way for financial applications that align with the evolution of smart devices and their role in transaction facilitation.

ReDeFi's Public APIs and Libraries extend its utility beyond the core blockchain functionality, empowering developers to create custom solutions that tap into the platform's robust capabilities. This opens avenues for innovation in cybersecurity, data protection, and the broader scope of Environmental, Social, and Governance (ESG) considerations within the financial sector.

In essence, ReDeFi's blockchain serves as a versatile and scalable platform, enabling a multitude of applications that transcend traditional financial models, fostering the growth of decentralised financial services that are more accessible, secure, and compliant with global standards.

About ReDeFi

ReDeFi Blockchain is a product owned by Regulated Decentralised Finance Ltd (ReDeFi Ltd).

ReDeFi Ltd is a company registered and incorporated in England and Wales with company number 10803612 and registered office at Level 39, One Canada Square, Canary Wharf, E14 5AB, London, United Kingdom.

ReDeFi Ltd is a registered crypto asset firm with the United Kingdom Financial Conduct Authority (RRN 849446) under the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (as amended) in respect of its activities in crypto assets.

Contacts

Please, send any correspondence to BABB, Level 39, One Canada Square, Canary Wharf, E14 5AB, London, United Kingdom.

Questions and Answers

Onchain Money

Q: *Why and how is the Onchain Money model better than stablecoins?*

A: *Onchain Money model does not imply departures in their exchange values away from par, which would violate the "singleness of money". Under this model, a person or firm knows that when they accept and receive a payment from a customer of any bank, the payment will be credited to their account at face value. The use of central bank money for settlement is the main aspect that supports singleness. Furthermore, Onchain Money is not issued in exchange for a fiat deposit, but rather mirrors GBP settled in the user's (owner's) name in a traditional bank account.*

Q: *Why and how is Onchain Money model better than CBDCs[20]?*

A: *Onchain Money model enables any bank to join the ReDeFi blockchain by running a node in the network and benefit from the enhanced functionality of smart contracts, while also allowing money to be sent to and received from any bank that is not connected to the network using traditional standard bank account details such as sort code, account number, SWIFT, IBAN, and so on. The Onchain Money model provides for the preservation of existing financial market infrastructure and monetary policy while growing the use of blockchain and smart contracts.*

Furthermore, CBDC requires all banks to join the network at the same time and it's difficult to attain widespread adoption, but the Onchain money model allows institutions to join whenever they wish. The model will continue to function.

Moreover, the current CBDC design is intended to be managed by central banks, which are not designed to deal with customers directly.

Q: *How does a bank join the ReDeFi blockchain and participate in the Onchain Money model?*

A: *A bank should set up a node in the ReDeFi blockchain network, link to the Onchain Money smart contract, and set up mirroring bank accounts for its customers. Following that, a bank can freely use and benefit from the Onchain Money model.*

Q: *When two banks join the ReDeFi network, do they have to "mint" and "burn" onchain money, or can it be sent to treasury accounts?*

[20] Central bank digital currencies (CBDCs)

A: When two banks are the ReDeFi network participants, Onchain Money tokens can be transferred (rather than burned and issued). They also can keep their accounts and use treasury accounts instead.

Q: *Can Onchain Money be sent to unKYCed users onchain?*

A: *The Onchain Money model follows a targeted update on implementation of its Standards on virtual assets (VAs) and virtual asset service providers (VASPs), with a focus on FATF's Travel Rule*[21].

Q: *How does a bank receive Onchain Money without being a participant?*

A: *Because the payment method is comparable to the current two-tier monetary system's practice of using central bank money for settlement. The payment is made by debiting the sender's Onchain Money and conventional GBP balances at their issuing institution and crediting the receiver's conventional GBP balance at their institution. The Onchain Money is deleted ("burned") by the sender's bank because the receiver's bank is not a participant.*

Q: If a non-bank financial institution has a safeguarding*[22] *arrangement with a bank, can it join the ReDeFi network?

A: Yes, if a non-bank FI has a safeguarding arrangement with a bank, it can also join and benefit from the ReDeFi network. In this situation, its customers will use virtual IBANs (vIBANs), but the rest is the same.

Q: Why do users need to have double fiat accounts?

A: To illustrate, the mobile app in the preceding examples (User interfaces section) contains two unique tabs for Onchain money and Conventional money. However, this is simply for demonstration reasons, and the actual user interface may differ from this example. For example, the user interface can only have Current mirrored fiat acct and not Current acct - a "traditional" ones.

Q: *Is it possible to create Onchain EUR, Onchain USD, Onchain GBP or something else?*

A: *Yes, everything that has been said about Onchain Money is applicable and possible for any existing 180*[23] *sovereign fiat currency.*

ReDeFi Self-Custody Wallet

[21] https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Targeted-update-virtual-assets-vasps.html
[22] https://www.fca.org.uk/firms/emi-payment-institutions-safeguarding-requirements
[23] https://en.wikipedia.org/wiki/List_of_circulating_currencies

Q: ***To clarify, there will be two distinct decentralised ReDeFi Wallets, one containing bank account details issued by regulated banks and FI and the other without?***

A: *No, there will only be one ReDeFi Wallet with bank account information. ReDeFi LTD will open a standard bank account and create sub accounts for each ReDeFi Wallet it created.*

Others are free to develop their own versions of decentralised wallets on the ReDeFi blockchain. It can look like MetaMask wallets (no bank account, just a wallet) or like ReDeFi Wallets, in which case, they would need to establish their own agreements with banks in order to generate sub accounts and provide users with acct details such as sort code, account number, BIN, IBAN and so on.

Q: ***Why do you need Mirroring ReDeFi sub-accounts for each wallet?***

A: *This what makes ReDeFi Wallet innovative and unique compared to any other decentralised self-custody wallet. Having dedicated sub-accounts for every wallet, users will be able to send conventional money to and from any 3rd-party traditional bank regardless whether this bank participates in the ReDeFi network or not. Next, having dedicated sub-accounts allows for better accounting and audit.*

Furthermore, the Onchain Money model offers tokenised deposits that do not violate the "singleness of money" principle, making it suitable for usage by banks and other financial institutions, as well as individuals and businesses. As a result, even with a ReDeFi Wallet, it is critical to keep this model active.

Q: ***What will happen if a user loses their private keys?***

A: *This is an unfortunate event. Self-custody, by definition, means that only the owner of the private keys has access to the funds in the wallet. Fortunately, ReDeFi Wallet will have a feature that will allow users to designate a secondary wallet address to withdraw funds after a specified period of inactivity. The ReDeFi Blockchain provides expanded functionality through smart contracts while remaining on the regulated side of the financial system.*