Xand Technical White Paper

Transparent Financial Systems

April 27, 2022

Contents

Executive Summary and Problem Statement

Paul Allen, an American business magnate, investor, and philanthropist, had a vision to create better money. He found it confounding that he—with his billions—would pay less to transfer money than the poorest amongst us.

Paul wanted to make money more equitable by making it more efficient and independent of any one financial institution. His team at Vulcan, along with several experts in financial technology, distributed systems, software, and financial regulations, came up with a design they called Xand, playing off Alexander Hamilton's name, and spun out a new company, Transparent Financial Systems (Transparent) to develop it.[1] Xand brings more competition to a market dominated by just a few big players by making the financial system more efficient and thus dramatically unlocking possibilities for both businesses and the people they serve.

Further, existing payment solutions are varied but suffer from one or more issues such as:

- costly
- introduce new intermediaries
- concentrate settlement risk
- are slow
- close on weekends, holidays, or after business hours
- can be reversed even some time after payment has "settled"
- operate on limited amounts

Xand addresses **all** the above issues.

[1] See https://www.transparent.us for more information on the company.

Introduction

Xand is a novel implementation of a private settlement network developed by Transparent. It provides a **fast**, **24/7/365**, **non-reversible bank-agnostic** payments solution, at a **lower cost** than competitors. Xand provides **more control** to its users (known as Members), is designed to operate within **existing U.S. legal and regulatory frameworks**, and is developed using **modern, reliable** infrastructure.

Settlement Speed

In legacy payment systems, funds can be tied up for hours or days before becoming available.[2] Xand is designed to enable transactions of **digital dollars** (known as Claims) in real time and solves the problem of **efficiently deploying capital** to where it is needed by removing the opportunity costs of funds caught in the middle of a payment transaction. Settlement is completed in **under 60 seconds** and funds are **immediately available** for use.

Non-Reversible

Xand Claims are transferable records under the Uniform Electronic Transactions Act (UETA) and are fully backed by **US dollars** held in trust at the same banks used by the members of the network. Claims can be unconditionally redeemed at any time. Payments made on a Xand Network are **final** and are **irreversible**.

Bank Agnostic

Conventional solutions often concentrate all transacting parties at a single bank, adding significant bank risk to all parties. Xand integrates with the bank(s) that Members are already banking with to provide **real-time payments** capability. Xand integrates with existing Bank programmable interfaces allowing any bank that meets Xand's minimum technical requirements to be rapidly enabled on the Network.

Low Cost

Xand Networks do not typically charge membership or transaction fees, although the Members themselves may elect to change this if they wish.[3] Network operating expenses are **paid using interest** earned by the USD backing the claims and excess funds beyond this are **paid back to the Members** themselves.

Modern Technology

Xand provides the **reliability, security, and performance** that users expect from modern software. All transactions use **modern cryptography** to authorize payments to prevent fraud and secure the Members' financial information. Each individual entity on a network runs its own software, creating a **shared decentralized settlement** network.

---

[2] Economic Impact of Real-time Payments; Deloitte (2019) https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/financial-services/deloitte-uk-economic-impact-of-real-time-payments-report-vocalink-mastercard-april-2019.pdf

[3] See Governance section below for more information.

Technical Overview

To send digital dollars on a Xand network, Members need to create Claims. Once Members have Claims, any member can send some of or all of those Claims to any other Member. Finally, if a Member wishes to withdraw funds from a network, the member can redeem those Claims for US dollars.

Create

To create claims on a network, a Member first signs and publishes a Create request transaction to create the claims as Unspent Transaction Outputs (UTxOs). Included with this transaction is a one-time identifier, which is known as the Correlation ID.

The Member then transfers funds from its bank account to the trust's bank account using the bank's APIs (Application Programming Interfaces) to perform an intra-bank book transfer. The Trust software monitors the Network for Create transactions and upon finding one, will check that the corresponding funds transfer has occurred in the bank account. If found, the Trust software will publish a transaction that Confirms the receipt of funds, and the Claims (created earlier) will immediately become spendable.

If no matching funds transfer is found, the Create request will expire after 24 hours and the Claims will not be valid.

Send

To send Claims, the member publishes a Send transaction. This consumes existing UTxOs and outputs a new set of UTxOs. These transactions use advanced cryptographic techniques to keep the counterparties and value of the transaction private to only the sender and receiver.

Redeem

When a member wishes to withdraw money from a Xand network, they publish a Redeem Request to the network. This transaction locks up one or more UTxOs and contains encrypted payment instructions that only the Trust can read. Upon receipt of a valid Redeem Request, the Trust software performs an intra-bank transfer via the bank's APIs to deliver US dollar funds to the member.

The Trust will either Confirm the redeem—in which case the Redeemed UTxOs are consumed—or the trust will Cancel the Redeem and the UTxOs are unlocked. The Trust will only Cancel a Redeem if the payment instructions are invalid (e.g., do not match the list of registered accounts at the Trust).

Network Participants

There are four roles for participants in a Xand network: Members, Validators, the Trustee, and a Limited Agent. A Network exists for the purpose of providing Members with the ability to transact and settle while the other participants act to enable the proper functioning of the network.

Members
Members use a Xand network to transact with each other. They take Claims created on the network and Send them to each other as payment. Once a Member has Claims, the Member can then Redeem them at any Xand Enabled Bank that they have a bank account at. Members also participate in all Network Governance activities.

Trustee
The Trust that holds all the assets backing Xand Claims on a network. The Trustee oversees the Trust by running software that observes Create and Redeem activity on the Network Ledger.

During Creation, if the software detects a correlating deposit into a Trust account at a Xand Enabled Bank then it will issue a Cash Confirmation Transaction automatically. During Redeem, the software will transfer cash into the specified Member bank account at a Xand Enabled Bank.

Validators
Validators maintain a Xand Distributed Ledger in the form of a blockchain and ensure every transaction adheres to the Network rules before it can be added to the Ledger. Validators also run a consensus algorithm that decides which transactions are added to the Ledger and in what order and participate in Network Votes. Validators are rewarded with Claims for blocks they add to the Ledger. Note: These claims are not confidential and cannot be Sent to other Participants—they can only be Redeemed for US dollars.

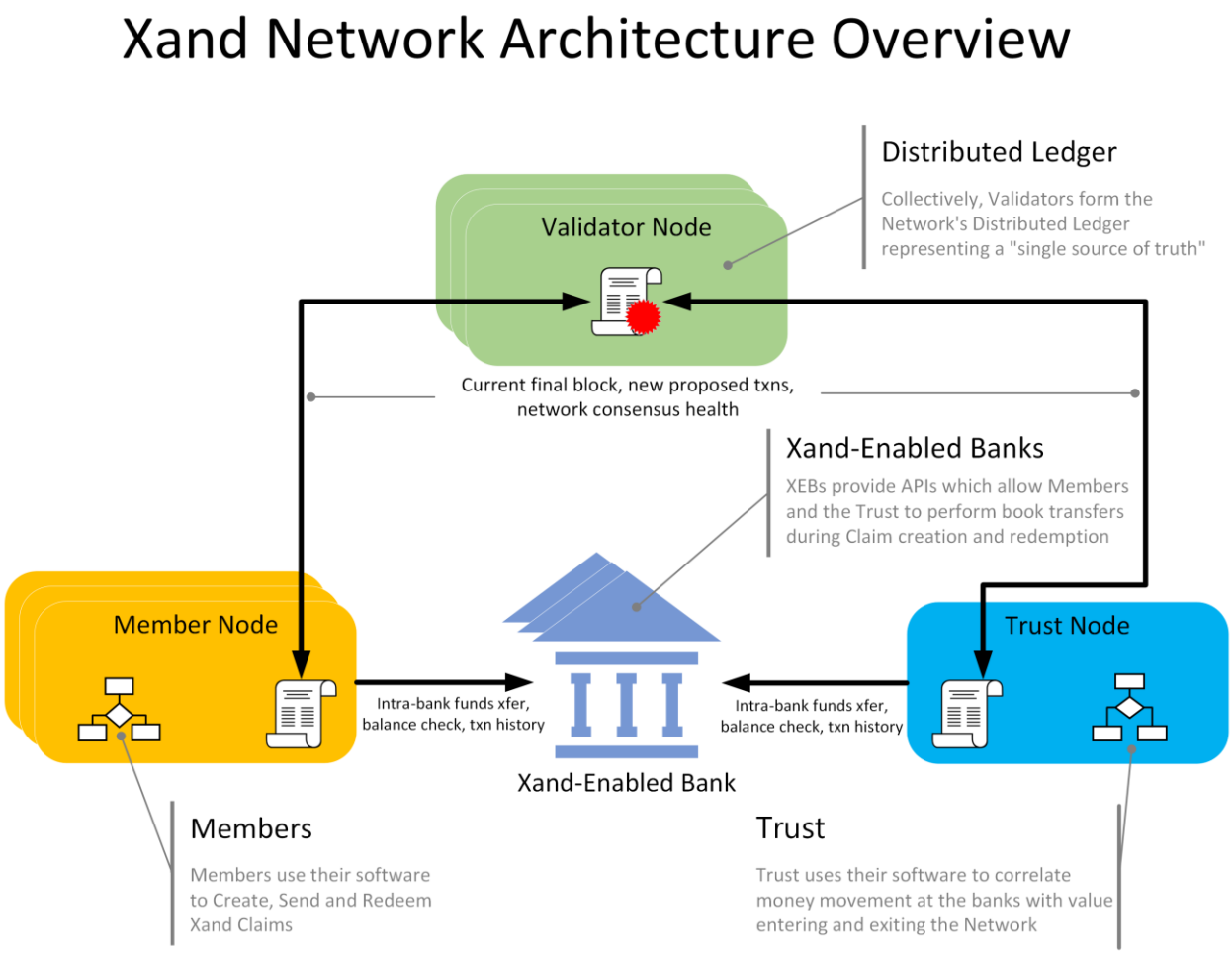
Limited Agent
The Limited Agent is appointed by XMCO Members and has a limited ability to act on their behalf by proposing Network Votes. The primary role of the Limited Agent is to provide certain corporate and operational services to facilitate the operations of XMCO. The Limited Agent itself has no ability to vote.

Xand-Enabled Banks
Xand-Enabled Banks do not run Network software or interact with the Ledger. To be Xand Enabled, a bank must provide an API (Application Programing Interface) that allows for real time book transfers, transaction details and balance checks. Once the Membership decides to enable a bank, the Trustee must open an account there on behalf of the Trust.

Governance
A Xand network is not a static system, it can change over time. Most obviously, members can join many Xand networks and leave a network at any time. In addition, parameters of the network—such as how much Validators are paid for their work—and even the network logic itself can be amended. To manage this, Xand has full-featured on-chain governance in which the participants of the network can vote on changes to the network.[4]

[4] See Appendix B for details.

Architecture



Distributed Ledger/Blockchain

The Xand Distributed Ledger is a blockchain. Xand uses a blockchain because no other technology offers the ability to build a decentralized trustless ledger.

There are critical areas of infrastructure where it is important not to "roll your own" solution[5]. We believe blockchain consensus, gossiping, chain upgrades and certain aspects of validation are among them. For this reason, Xand builds on top of Substrate, a well-vetted, open source, customizable blockchain framework. Substrate provides Xand with the foundational features needed for a blockchain system while allowing easy implementation of custom logic.

Most blockchain-based systems are difficult to evolve and upgrade because of their decentralized nature. Typically, every party needs to upgrade to the latest version of software at the same time or risk forking the chain. Xand leverages Substrate to provide

[5] You Really Shouldn't Roll Your Own Crypto: An Empirical Study of Vulnerabilities in Cryptographic Libraries arXiv:2107.04940 https://arxiv.org/abs/2107.04940

forkless upgrades through an on-chain mechanism that ensures the whole network stays coordinated.[6]

Services

Each participant runs software to allow it to connect to a Xand network as well as to facilitate actions on a network appropriate to its role. The software associated with Xand is broken up into units of functionality called Services. Each participant will deploy some subset of the services.

	Xand Service	Trustee Service	Member Service	Voting Service
Member	✓		✓	✓
Validator	✓			✓
Trustee	✓	✓		
Limited Agent	✓			✓
X-E Bank				

Xand Service

The Xand Service provides access to the blockchain. This service is run by all Participants as a part of their Node. The Xand Service is comprised of a few components:

- Substrate Node – This is the component that communicates with the rest of the network via gossiping and consensus. It stores a complete copy of the distributed ledger in the form of a blockchain. Only nodes run by Validators participate in consensus to add new blocks to the chain.
- Xand API – This Rust API built by Transparent provides for submitting transactions as well as searching transaction history.
- Indexing Component – This component built by Transparent stores the ledger transactions in a searchable way after decoding confidential transactions

Trustee Service

The Trustee Service is a fully automated system that observes the ledger for any pending Create or Redeem requests. On seeing a Create Request, it looks for a matching bank transfer and if it finds one issues a Cash Confirmation to the ledger. On seeing a Redeem request, it transfers the specified amount into the specified bank account and then confirms this action on the ledger. This service is run only by the Trustee. The Trust service is comprised of three components:

- Trust Application – This is a Rust application built by Transparent that automates all the Trustee's duties around creation and redemption. It talks to the Xand Service and the Bank APIs.

[6] For more on Transparent's selection of Substrate, see "Why We Built the Xand Network Using Substrate," Seth Paulson, December 10, 2021; https://transparent.us/post/why-we-built-the-xand-network-using-substrate

- Bank Transaction Repository – This is a Rust library built by Transparent that caches transaction history from the banks and ensures an unambiguous (ISO 8601) timestamp. This component talks to the bank APIs periodically, harvesting new bank transactions.
- Bank Transaction Repository DB – This is a SQL database used by the Bank Transaction Repository.

Member Service

The Member Service provides a convenient API for Members to write payment automation with. It makes creating, sending, and redeeming claims very straightforward. This service is run only by the Member. It is comprised of two components:

- Member API – This is a REST API with endpoints for creating, redeeming, and sending claims. It talks to the Xand Service and the Bank APIs.
- Member Service DB – This is a SQL database that stores bank and account information for the Members.

Network Voting Service

The Network Voting Service provides an interface for creating proposals, viewing existing proposals with their status, and voting on any open proposals. This service is run by Members, Validators, and the Limited Agent. It consists of only one component:

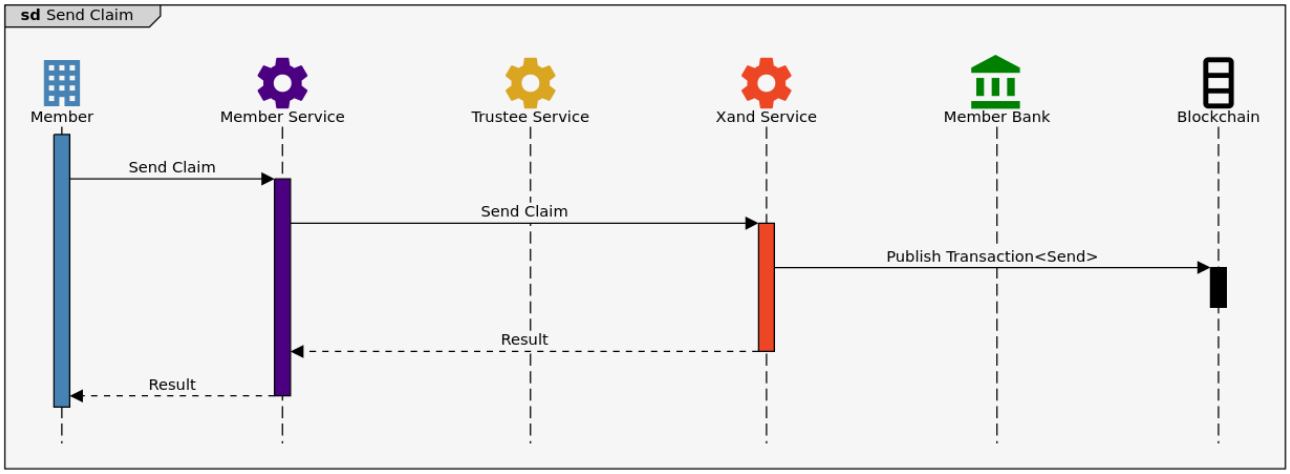
- Network Voting CLI - A Rust-based command line interface application written by Transparent. This component talks to the Xand Service.

Operation

In this section we will describe the operation of key workflows. Excluded from these diagrams are the Validator nodes that work on every block to validate and finalize the transaction on the blockchain. The service is resilient to Member or Validators being offline and a Member need not be online to receive Claims. If the Trustee is offline, then Claims can still be sent between Members but moving funds on and off the network may be impacted.

Send Claims

A Send Transaction allows a Member to transfer the ownership of Claims to another Member (i.e., make a payment). It is a simple one-step operation, with no Trustee interaction.

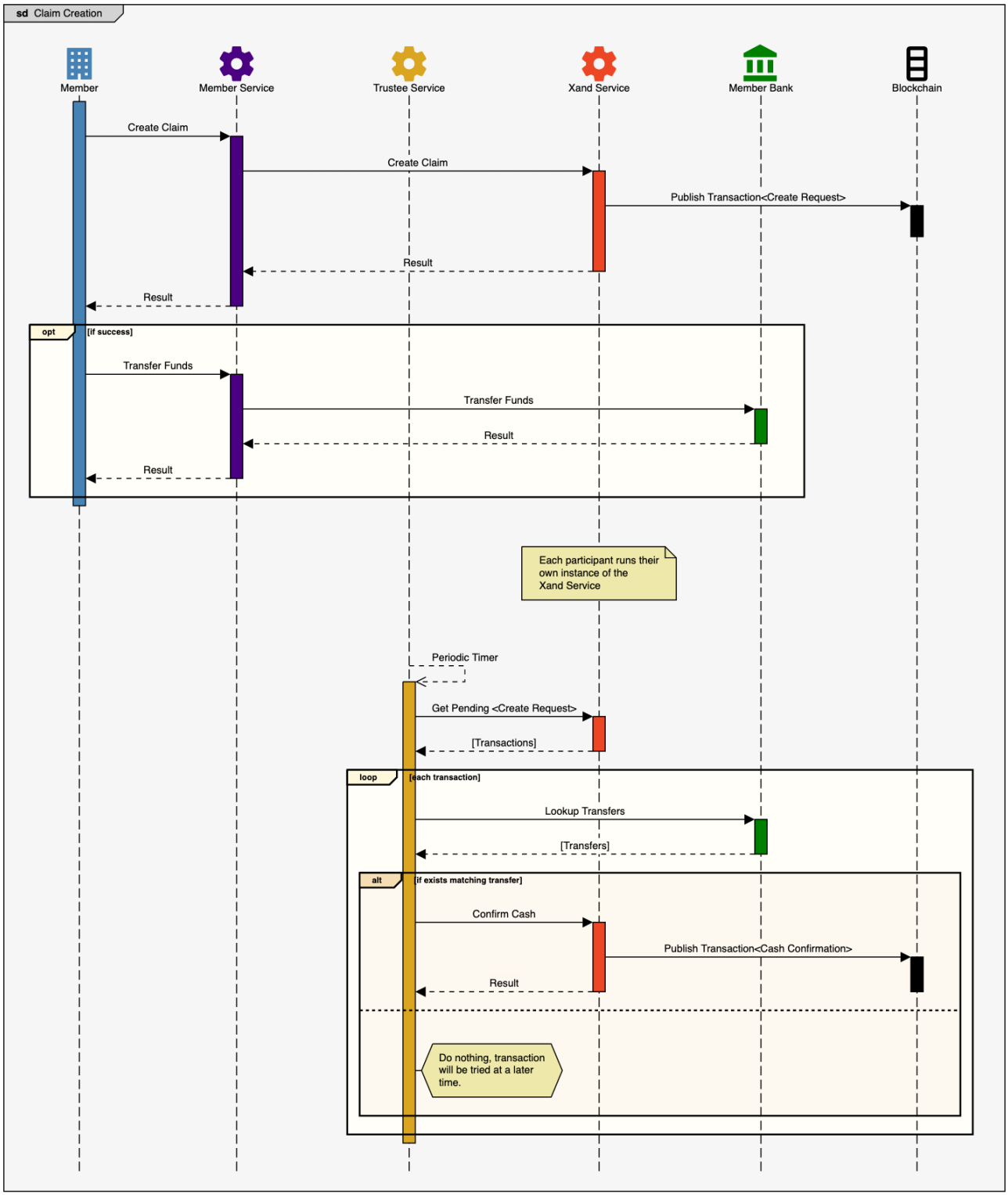


Member Actions

1. The sending Member instructs the Member Service to send Claims.
    a. The Member Service submits a send request to the Xand Service.
    b. Xand Service constructs a UTXO.
    c. Xand Service ring-signs the transaction.
    d. Xand Service submits the "Send Transaction" to the blockchain.
2. The receiving Member's Member Service observes the "Send Transaction" on the Blockchain.
    a. Wallet balance is increased to reflect the receipt of Claims.

Create Claims

Create Transactions are how Claims are created on a Xand network. A Member initiates the process by submitting a "Create Request" for a public amount. The Member must then send money to the trust's bank account, and that bank transaction must be marked with the Correlation ID specified on the create request. The Trustee Service sees the matching bank transfer and submits a "Cash Confirmation," which allows those Claims to be spent.



Member Actions

1. Member instructs the Member Service to Create Claims.

    a. The Member Service sends funds amount and bank account information to the Xand Service.
    b. Xand Service converts the funds amount into a new UTXO, attaching a new Correlation ID.
    c. Xand Service encrypts bank account information via authenticated encryption and view key for the new UTXO.
    d. Xand Service computes ring signature over the transaction.
    e. Xand Service submits the "Create Request" transaction to the blockchain.
2. Member instructs the Member Service to transfer funds.
    a. The Member Service calls the Bank API.
    b. Funds are transferred from the Member's Account to the Trust's Account.

Trustee Actions

3. Trustee Service receives the pending "Create Request" transaction from the Xand Service.
    a. Xand Service decrypts bank account info using Shared Key decryption algorithm and the Trustee and Member keys.
    b. Xand Service sends info to Trustee with decrypted bank account information.
4. In case of a malformed request (i.e., does not conform to the protocol), Trustee Service tells Xand Service to issue a "Create Cancellation" transaction and ends Create process.
5. Otherwise, Trustee queries Trust Account via Bank API to verify receipt of Member's deposit.
    a. Trust verifies that a bank account deposit matches the funds in the Create Request and the Correlation IDs match. If there is not a match over 24 hours, transferred funds are to be refunded.
    b. After deposit is verified, Trustee Services confirms transaction to Xand Service.
    c. Xand Service submits "Cash Confirmation" transaction to the blockchain.

Member Actions

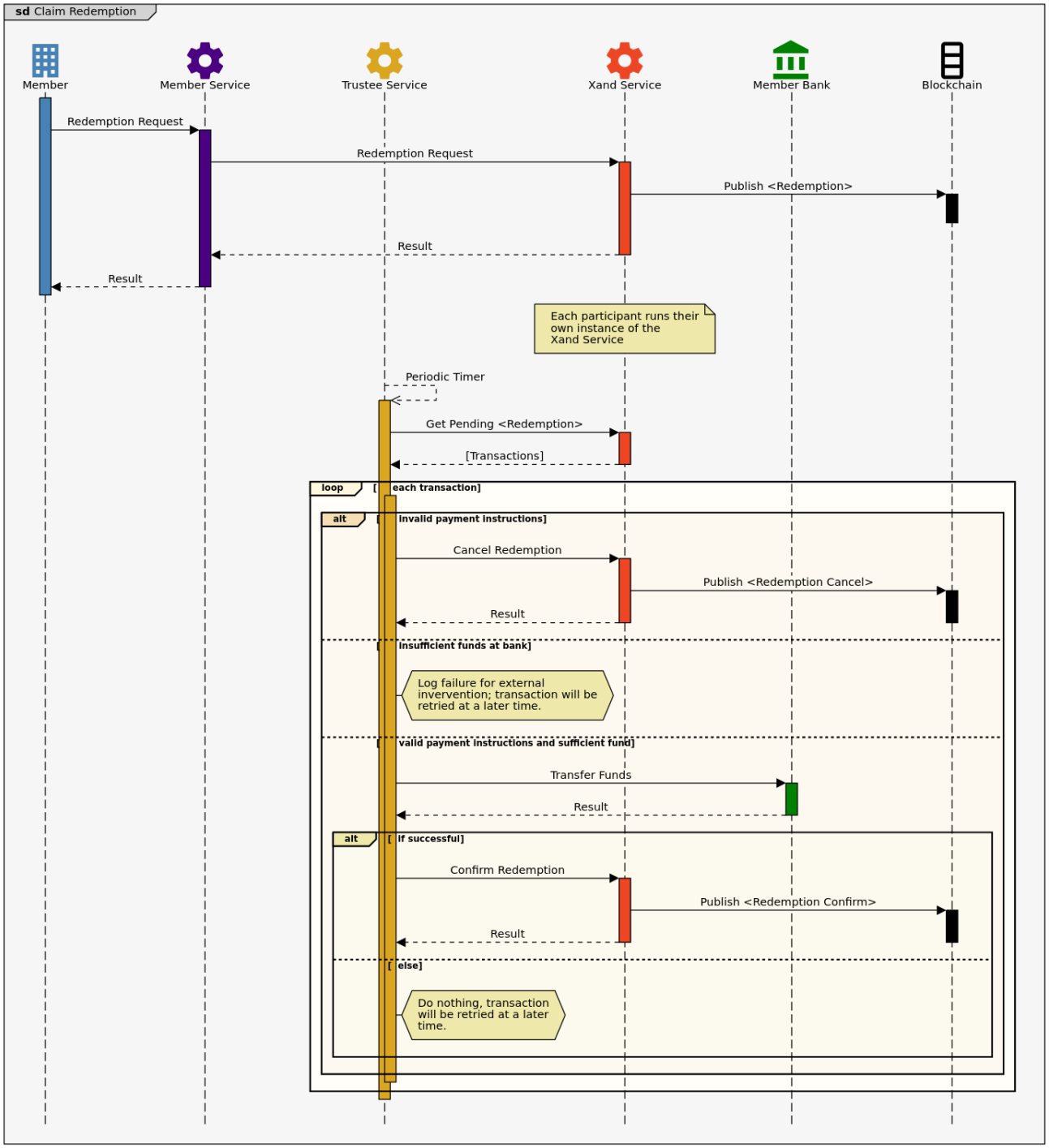
6. The Member Service observes the "Cash Confirmation" transaction.
    a. The Member can now send Claims to any other Member on Xand.

Redeem Claims

Redeem Transactions are how Members redeem Claims on a Xand network for funds. A Member initiates the process by submitting a "Redeem Request" for a public amount along with corresponding Claims that will be destroyed. The linked UTXOs remain in a pending state until the flow is completed. On observing the payment instruction contained in the "Redeem Request" transaction on-chain, the Trustee Service transfers money from the Trustee Account to the Member's Account. It then issues a "Redeem Fulfillment" to the Network, which finalizes the destruction of those Claims. If the Trustee Service is not able

to perform the bank transfer due to lack of liquidity in that Trust Account, it waits until it is able to do so[7].

[7] Funds are held in trust across a network of bank accounts and occasionally may not be immediately available where requested.



Member Actions

1. Member instructs the Member Service to redeem Claims for funds.
    a. The Member Service submits request to Xand Service with redemption amount and bank information.
    b. Xand Service selects UTXOs greater than or equal to redemption amount.
    c. Xand Service creates *redeemOutput* FixedKeyTXOs totaling the exact redemption amount.

d. Xand Service creates new UTXO for any change exceeding the desired redemption amount.
e. Xand Service encrypts the redemption bank account information using chacha20-poly1305-openssh and opened TXO details for all inputs.
f. Xand Service attaches a unique Correlation ID to the transaction.
g. Xand Service computes ring signature over the transaction.
h. Xand Service submits the "Redeem Request" transaction to the blockchain.
i. The linked Claim are marked for redemption, removing them from circulation.

Trustee Actions

2. Trustee Service receives the pending "Redeem Request" transaction from the Xand Service.
    a. Xand Service decrypts bank account info using Shared Key decryption algorithm and the Trustee and Member keys.
    b. Xand Service sends info to Trustee with decrypted bank account information.
3. In case of a malformed request, Trustee Service tells Xand Service to issue a "Redeem Cancellation" transaction and ends the redemption process.
4. Otherwise, Trustee Service calls the Bank API to transfer funds.
    a. The bank transfers funds from Trust Account to Member's Account.
    b. In the rare case where funds are not available in the local Trustee Account, the process will queue here, waiting for funds to arrive. They are serviced in a first-in first-out (FIFO) manner as funds become available.
5. Trustee Service calls the Bank API to confirm execution of the funds transfer.
6. Trustee Service confirms finalization of transfer.
    a. Trustee Service confirms funds redemption to Xand Service.
    b. Xand Service submits "Redeem Fulfillment" transaction to the blockchain, containing the Correlation ID specified by the redeeming Member.

Member Actions

7. The Member Service observes the "Redeem Fulfillment" transaction.
    a. Funds should now be posted to the Member's account per its bank's standards and practices.

Deployment

Most decentralized systems do not provide a good operational story. This can lead to difficulties with potential participants being put off from the challenge of setup or ending with poor visibility and resilience in their deployment. Additionally, if all parties standardize on a certain provider for deployment, it increases the risk to the whole network. With that in mind Xand comes with an automated deployment system that provides the following advantages:

- All the major cloud providers (AWS, GCP, Azure) are supported.
- Network Participants willing to run in a supported cloud and use Xand's automation can be connected to the Network and operational within a day.

- Network Participants unable to use Xand's automation can still use it as living documentation on how to correctly configure the software.

Xand's automation is built on Ansible,[8] which streamlines the setup process by combining it into one seamless process. Tooling generates keys and configuration files are templated. Provisioning is managed by Terraform,[9] which provisions Kubernetes[10] clusters and other cloud resources in the Participant's preferred cloud. Software is then distributed via Docker[11] images, with code deployments on Kubernetes further ensuring consistent behavior across clouds. Kubernetes deployments come bundled with Prometheus for metrics collection and FluentD for aggregating and shipping logs.

Xandbox

Transparent has developed a "Xand-in-a-box" system that is able to run an entire simulated Xand Network locally. The Xandbox uses docker and docker-compose to run all the components on a single machine. This will allow participants or potential participants to familiarize themselves with how the system works as well as build and test automation before running against a live network. If you would like to request access to the Xandbox simply contact Transparent.[12]

Confidentiality

In traditional financial systems one party owns and manages the ledger. The ledger owner has a view into all transactions where all other parties only have a view into transactions they are party to. On a Xand network the ledger is shared by all parties. This confers many of the advantages detailed above but could come with the downside that now all transactions would be seen by all parties. To alleviate any privacy concerns, Xand uses a confidential cryptography system that allows any party to verify the validity of a transaction without revealing confidential information like the amount and counterparties.

To accomplish this, the research team at Transparent developed the Xand Confidential Protocol with the following invariants:

Sending Claims:

- The signer is hidden from observers but revealed to the recipient
- The amount is hidden from observers but revealed to the recipient
- The recipient of the Claims is hidden from observers but revealed to the recipient
- The sum of the inputs always equals the sum of the outputs

Creation and Redemption:

- The signer is hidden from observers but revealed to the Trustee

[8] https://www.ansible.com/
[9] https://www.terraform.io/
[10] https://kubernetes.io/
[11] https://www.docker.com/
[12] See "Build a Castle in the Xandbox," Jeff Kramer, September 10, 2021; https://transparent.us/post/build-a-castle-in-the-xandbox

- The value of Claims created and redeemed is public knowledge such that any observer can know how many Claims exist in total on the network
- The bank account information is hidden from observers but revealed to the Trustee

Claims:

- Consumed Claims are owned by the signer
- Consumed Claims have not been spent previously
- Consumed Claims in a Redeem are of the amount publicly claimed by the transaction

General Invariants:

- Only Members are allowed to transact confidentially, but their identity is not revealed by proving their Membership
- Members can be added and removed from the network. Removed Members are not allowed to transact

The protocol uses a custom proof system developed by Transparent which is an evolution of the Ring Signature popularized by the CryptoNote protocol.[13] This proof system is a generalization of the ring signature that allows proving additional information. The protocol also makes use of bulletproofs, homomorphic encryption and deterministic shared key encryption to provide the capabilities outline above. For details on how the protocol works see the Xand Confidentiality Whitepaper.

[13] See CryptoNote repo: https://github.com/cryptonotefoundation/cryptonote

Appendix A: Glossary of Terms

Member. The primary users of Xand. These are business entities that maintain deposit accounts at Xand Enabled Banks and create, send, and redeem Claims, which are recorded as transactions on the Xand Blockchain.

Network Participant. Any entity that has a role on the network. The types of participants are Member, Validator, and Trustee.

Software Provider. The software provider, Transparent, develops and licenses Xand-related technology to Network Participants.

Trustee. An independent trustee named by XMCO (Xand Member Collective Organization) to administer the Xand Trust for the benefit of the Members.

Unspent Transaction Output (UTxO). A blockchain structure representing funds that are available. Only the keyholder may spend the UTxOs. Once a UTxO is consumed it may not be spent.

Validator. Network service providers that operate software nodes comprising the Xand Distributed Ledger infrastructure. They validate transactions, bundle the transactions into blocks, and vote to post them to the blockchain, which is the shared general ledger for tracking ownership of Claims. Once a transaction is included in a block in the blockchain, it is finalized. Validators are paid for their services on-chain with Claims.

Xand Enabled Bank (XEB). State or nationally chartered, FDIC-insured depository institutions. These banks provide deposit accounts for the Xand Trust and the Members and enable them to conduct balance checks and intra-bank transfers programmatically via bank APIs.

Xand Trust. A Delaware statutory trust established by XMCO as the trust sponsor and a Trustee who administers the trust. The Trustee controls and manages assets held in Trust Property and ensures that the aggregate value in USD of Trust Property is equal to the aggregate designated value of all Claims in circulation on the Network. The operating terms of the Xand Trust are directed by XMCO.

XMCO. The Xand Member Collective Organization (XMCO) is a limited liability company (LLC) collectively owned by the Members that serves as the sponsor of the Xand Trust.

Appendix B: Governance Details

A hallmark of decentralized financial systems is to empower users to determine the economic and governance rules of the systems in which they participate. As Members own XMCO, this is doubly important for Xand – they need to be able to not only manage the governance of the blockchain systems, but also of the LLC entity.

In Xand Governance, most actions happen on-chain[14]. There are two types of actions that occur on the network: Network actions and Member actions. They differ in who can vote and what percentage constitutes a passing voting.

Action Type	Voting Power	% For Passage
Network	51% Validators / 49% Members	> 2/3rds
Member	100% Members (No Validators)	> 50%

Network Actions

A Network Action is the most common governance mechanism, wherein Members and Validators collectively vote on configuration changes that affect the whole Network, including adding or removing participants. All Network Voting is currently weighted 49% Members, 51% Validators with a ⅔ majority required for passage. Members and Validators act as a check on each other's votes as either side scales.

Xand blockchain logic updates can redefine the rules of the Network, which may include, for example, adding transaction limits or removing the limitation that only Members can create or send Claims.

Member Actions

Member Actions are like Network Actions, but only for Members. A simple majority vote passes these measures. These actions relate to the financial or corporeal controls of the Network. For example, the Validator Emission Rate determines the per-block earnings rate for Validators – as discussed in the following section ("Economics").

Action	Vote Type
Permission a Validator	Network
Revoke Permissions from a Validator	Network
Modify the Xand Blockchain Logic	Network
Permission a Member	Network
Revoke Permissions from a Member	Network
Set Validator Emission Rate	Member
Permissions a Trustee	Member
Permissions a Limited Agent	Member
Add a Member to XMCO	Member

[14] Off-chain actions—known as Specified Company Actions—generally deal with XMCO corporate actions.

Appendix C: Network Transactions

Network operations are recorded as transactions on the Xand Blockchain to ensure permanence and equal access to all participants. There are seven types of Claims transactions supported by Xand and used by network participants, divided into three major categories: Create Transactions, the Send Transaction, and Redeem Transactions.

As noted below, the initiation of Create, Send, and Redeem Transactions are limited to activated Members and (in some cases) Validators. Non-Members or banned Members cannot create, send, or redeem Claims. This is supported by the Governance systems described in Appendix B.

Create Transactions

Create Request (Member). Initiates the creation of new Claims on the Xand network, as funds are transferred from the Member's bank account to a Trustee bank account. Metadata includes the amount of bank funds, bank account info, a nonce as Correlation ID, and the public key that will own the claims.

Cash Confirmation (Trustee). Confirms the receipt of an appropriate amount of bank funds from a Member. Metadata includes a Correlation ID linked to a Create Request.

Create Cancellation (Trustee or Validator). Cancels a current Create Request. A Trustee will issue Cancellation if a Create Request is malformed; a Validator will do so if it has not been confirmed in 24 hours. Metadata includes a Correlation ID linked to a Create Request.

Send Transactions

Send (Member). Transfers and assigns the right to redeem specified Claims from one Member to another permissioned Member as identified by their public key. Metadata includes recipient address and value of Claims.

Redeem Transactions

Redeem Transaction (Member or Validator). Redeems Claims, initiating the transfer of bank funds from the Trustee Account to the Member's Account. Validators also need to redeem Claims, which are the payments they receive for validation, stored in Redeem-only wallets. Metadata includes the amount of bank funds, bank account info, and a nonce as Correlation ID.

Redeem Fulfillment (Trustee). Confirms the transfer of bank funds from the Trustee Account to the Member's Account, finalizes the redeem, and burns the underlying Claims. Fulfillment is meant to occur in real-time, or if there is a liquidity issue at a Xand Enabled Bank, as soon as possible. A Trustee will always fulfill a Redeem unless it is malformed. Metadata includes Correlation ID.

Redeem Cancellation (Trustee). Cancels a current Redeem Transaction that was malformed.

Network Voting Transactions

Proposal (Member, Validator, or Limited Agent). A proposal transaction will create a new open proposal that Members and Validators can vote on. The proposal transaction must specify one of the possible governance actions (see Appendix B).

Vote (Member or Validator). A vote transaction specifies an open proposal and a yes or no vote. Once the vote transactions are added to the ledger then if the vote has passed the governance action takes effect immediately. If the vote causes the passing of the governance action to become impossible then the open proposal is closed immediately with no effect.

Operational Transactions

Set Encryption Key (Member, Validator, Trustee) In order for the counterparty of a transaction to receive information that should be non-public each party has a public encryption key on chain. This transaction can be used by any party to change their encryption key.

Add Allow-list CIDR Block (Any Participant) This allows any participant to designate a CIDR block to add to the list of allowed network identities.

Remove Allow-list CIDR Block (Any Participant) This allows any participant to designate a CIDR block to remove from the list of allowed network identities. This must be a CIDR block that the signing participant previously added.

Appendix D: Notable Cryptographic Keys

Xand uses cryptographic keys to represent identity, prove intent, and protect information. Each participant generates, stores and manages their own keys. This means they have full control over their actions on the network, but it also means that each participant must safeguard their keys carefully to avoid potential loss. Below are the important cryptographic keys for the network.

Validator Signing Key

This key represents the validator's identity and is used to sign during network voting and when redeeming block rewards. It is also used to generate session keys that are used during consensus.

Validator Session Key

Used to sign consensus messages. These are regenerated every few minutes by the Validator.

Member Signing Key

This key represents the Member's identity. It is used to sign all Member transactions allowing them to Create, Transfer and Redeem Claims as well as when making proposals and voting..

Limited Agent Signing Key

This key represents the Limited Agent's identity and is used to make network vote proposals.

Trustee Signing Key

This key represents the Trustee's identity and is used to confirm cash movement or issue cancellations for creations and redemptions.

Participant Encryption Key

Used to communicate encrypted data on chain to other participants (such as bank account data).

Changelog

2022-03-23: Initial White Paper release

2022-04-27: Add Appendix D with notable cryptographic keys