Decentralized Bank for Migrants

Whitepaper v1.1.9
Last updated December, 4th 2018

Sean Patrick Braithwaite
Marco Muccini

Abstract

In this paper we introduce Topos, a decentralized bank built as a dApp on blockchain but used in the physical world. The first section of this paper outlines how it is possible to connect a decentralized network of Coin Desks to offer deposits on top of money remittance flows, fostering financial inclusion in any remote area of the world. The second section analyzes how the participants of such network will be able to form pools of collateral and manage their own deposits, creating value and financial self-determination.

Table of Contents

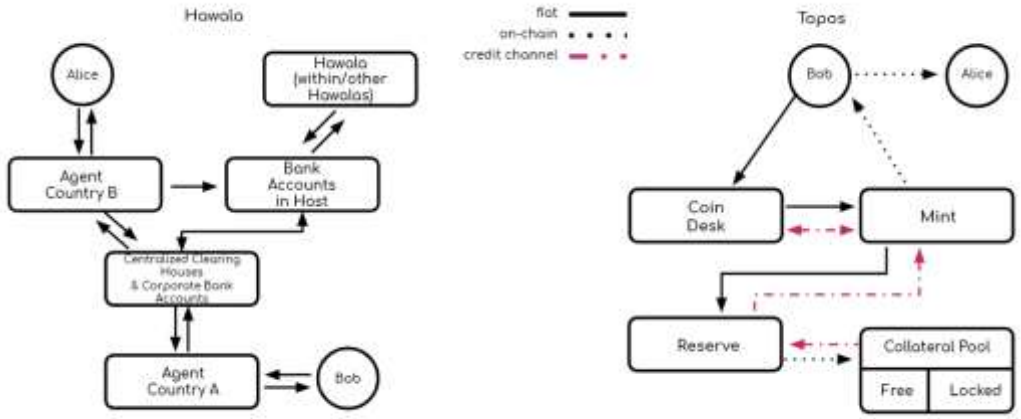
Section 1. Topos dApp for Financial Inclusion

In this section we present Topos dApp, a decentralized application that allows users to deposit, redeem and transfer money anywhere in the world, thanks to a network of merchants that extend credit to each other to service operations. Topos dApp aims at becoming the stepping stone to build the largest decentralized bank for migrants.
Users interact with local merchants known as Coin Desks to exchange fiat for value pegged tokens (V.P.T). VPTs have a value stabilized by the network and are redeemable from any participating Coin Desk around the world. Coin Desk maintain and extend credit with each other to ensure liquidity of fiat is available to service redemptions across the network. Users are incentivized by a censorship resistant, secure and stable store of value that provides almost free remittance, Coin Desks are incentivized by fees and interest they gain from loans.
Topos let's anyone be their own bank.

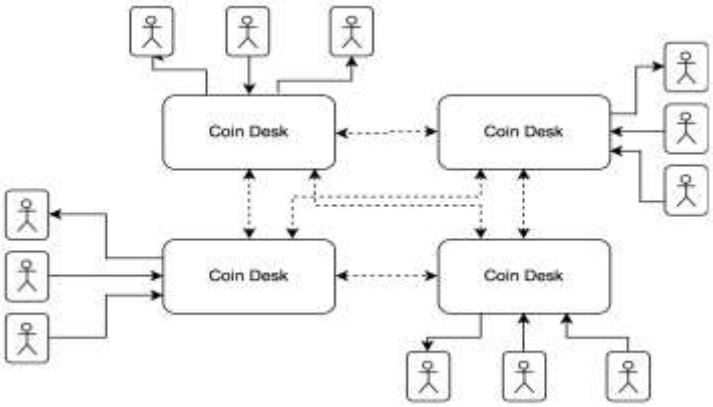
Introduction

Over a trillion dollars is transferred each year in remittances.
Remittances are money transferred across borders to the most remote areas that are for the most part unbanked. The remittance system forms a capillary network, thin and vulnerable connections to the financial world which serve as the lifelines for a decentralized population: migrants. Migrants form the 3rd largest economy in the world and are dependant on this capillary network to send small and frequent transactions. Of the 1.2 trillion $ in remittance sent every year, more than half flows through informal channels known as Hawala. The other half, through expensive -and often exploitative money transfer companies. Regardless of the medium, the average transaction is below 200$ and it has to be entirely redeemed by the recipient in order to be completed. At this price, profits from servicing this community are too low for traditional banks, therefore leaving room for exploitive and expensive remittance services. Western Union, Moneygram and other major money transfer services rely on network of local brick and mortar stores, operated by merchants acting as agents for foreign corporations, to cater their services to this community. These agents have often little to no brand loyalty but are instead motivated by price and the essential role they perform in their community. If given ownership, each agent would both benefit and better serve their community.

By creating an infrastructure that allows transactions not to be entirely redeemed upon reception, the goal of Topos dApp is to convert every remittance agent into a local branch of a decentralized bank, which they have ownership into.



Key to the transition between the old and new systems is the realization that remittance is not banking. As a business model (and incentive structure) remittance is limited to revenues it can extract from fees. By contrast, banks can take deposits, offer loans and profit from interest. This revenue is far greater than what could be captured by any remittance agent. If given the opportunity, local agents would accept deposits, offer community loans and pass on the revenue through lower fees to the community. Topos makes this possible in a trustless way, in which incentives between users and agents are aligned for community benefit.



Topos functions as a decentralized bank. Decentralization produces a robust an permission-less system in which anyone can participate and ensure trustless interactions motivated by common benefit. Thanks to a blockchain interconnected network and a dual token economy that balances incentives between Coin Desks and users, it is possible to ensure that people can perform an essential function: putting money in, and getting the same money out, anywhere in the world.

Alternatives

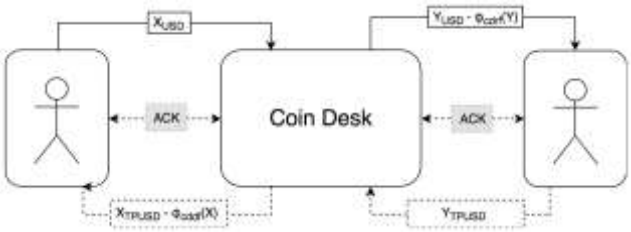
The cryptocurrency ecosystem has several stable stores of value. These solutions are often available on exchanges as a temporary store of value for speculators. None of them fits the migrants' peculiar needs for two main reasons: 1. The liquidity they provide is on exchanges and requires a bank account to access it. A large portion of the world is unbanked making the entire crypto economy inaccessible. 2. Reserves are centralized and invested exclusively to the benefit of token issuers instead of holder.

The innovation of Topos lays in solving the first problem -liquidity at the edges of a network- by making the second problem -reserve management- decentralized and equitable to all participants.

A Decentralized, Redeemable and Stable Store of Value

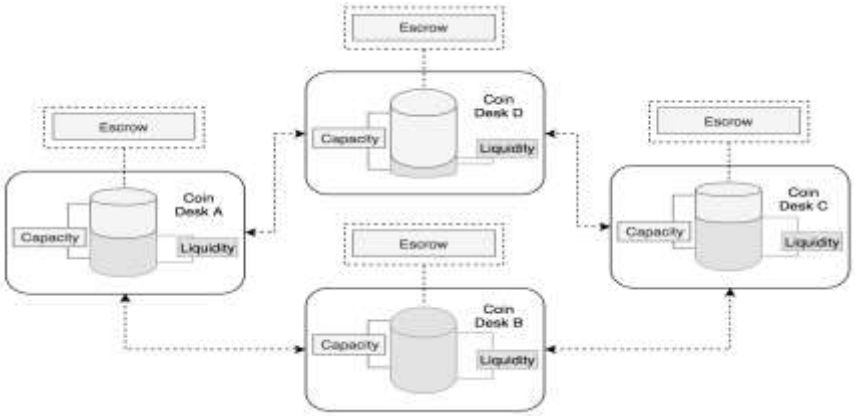
Topos is a decentralized application built on blockchain allowing permission-less peer to peer interaction in which economic agents coordinate without necessarily trusting each other. A mobile wallet application facilitates transactions between users and a merchant known as a Coin Desk to exchange value pegged tokens (V.P.T). The tokens acquired have a value pegged to the floating value of the currency used to mint them modulo fees. Once minted, VPTs can be sent to any wallet at a negligible cost. Users can convert those tokens to fiat in a redemption request with a Coin Desk. To ensure tokens are always redeemable, Coin Desks are incentivised to keep float of currency available. Float functions as a decentralized currency reserve, spread over each Coin Desk all over the world to produce a robust and decentralized bank.

Each Coin Desk is capable of accepting deposits and servicing redemptions. User provides Fiat, e.g. USD, and receives a VPT account in their currency of choice, in this case TPUSD. Balances are owned by the user as private keys, and are redeemable at any Coin Desk within the network.



Decentralized Reserves

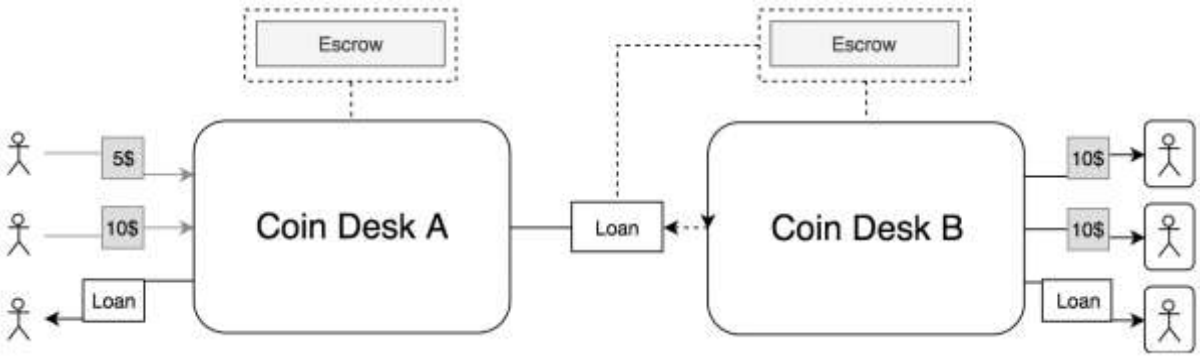
Each Coin Desk holds one portion of the total reserve. The Coin Desk secures its part of the reserve with on chain escrow denominated in a native token TPG. This escrow allows the Coin Desk to accept deposits, extract fees and manage liquidity up to a maximum capacity determined by the amount of tokens in escrow.



The capacity of any individual Coin Desk limits the overall risk taken by the network. Each Coin Desk is simply a node in a network. For the network as a whole to be robust, we must assume that any individual node can fail and the network remains operational. In the case of Topos, we assume that any Coin Desk can default on its obligations, but tokens are still redeemable. To ensure this is true, the amount each Coin Desk stores in escrow limits the overall risk it can pose to the network as well as how much money it can make it terms of fees.

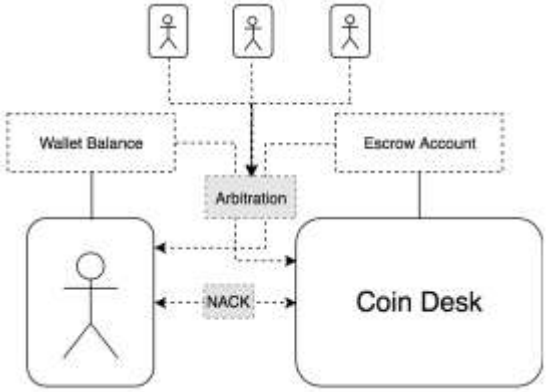
Coin Desks are incentivised by fees they receive on account openings and redemptions, which are lower than an OTC transaction but add up at scale. As Coin Desks service more deposits than redemptions, they accumulate float of physical currency which they can invest back into the community. Investments can be made off chain and bear the risk of being lost or stolen. The core mechanism of Topos is to ensure that Coin Desks are profitable while being reliable to service users, without controlling how the float is managed.

To ensure a trustless system, Coin Desks operate with a capacity of float they can manage determined by on chain escrow accounts. Coin Desks lock Topos native token TPG in a smart contract and are allowed to accept deposits in fiat up to a given counter value. The counter value is determined by deposits and based on TPG price, which gets determined by the average of a voted set of oracles.



Coin Desks which net more deposits than redemptions will have excess reserves and be unable to accept more deposits without increasing their escrow. Instead, they will be incentivised to loan such excess reserves to Coin Desks which net more redemptions. Loans are secured by escrow and rewarded with interest.

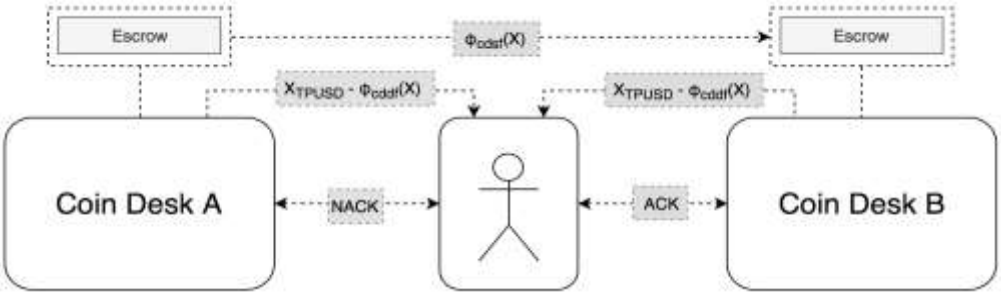
Users and Coin Desks must rely on a minimal amount of trust to coordinate. Transactions are in person as a User hands fiat to a Coin Desk for a deposit or vice versa for a redemption. These transactions are confirmed by both parties through the wallet app to verify the successful completion of the operation. In cases in which trust is broken, either party can dispute a transaction and the role of Topos is ensuring that each party has something to lose in case of malfeasance.



Users secure transactions with their wallets while Coin Desks secure transaction with their escrow. If a Coin Desk is unable to fulfill a redemption, users can raise a dispute. If the dispute is won, a portion of Coin Desk escrow becomes a bounty. The bounty is split between the user and any other Coin Desk able to service the transaction. The goal of the dispute mechanism is to ensure redeemability which is how the network ensures the value of each V.P.T remains stable, even with adversarial actors.

Ensuring Redeemability

The true value of any V.P.T token is based on its redeemability. If users can't redeem tokens for fiat currency by one Coin Desk, they will be incentivised to seek redemption at a lower exchange rate in another desk. To incentivise Coin Desks to service such redemptions, transactions which are disputed and won by users result in bounties for the next Coin Desk to service that users redemption.



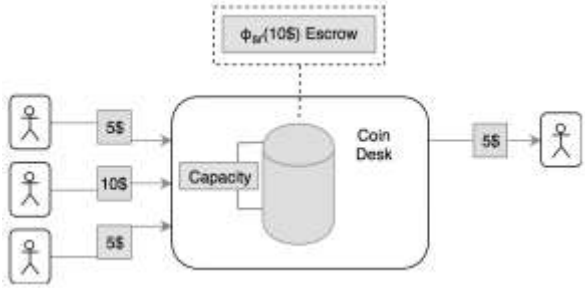
Bounties are extracted from the Coin Desk who fails to service the disputed redemption. In this way, the network is sensitive to the users' needs; Fiat redemption is always granted, in this case at a lower cost, while the network ensures that malfeasance by Coin Desks in penalised.

Given that Coin Desks are allowed to manage their fiat capacity as they wish, we provide this slashing mechanism to incentivise diligent investment. If a Coin Desk performs bad investments, unobserved through transaction made on-chain, it will be unable to fulfill redemption transactions and put its escrow in jeopardy. This mechanism provides a guard against

malfeasance and ensures that despite the profit motives of Coin Desks, users can always get their money out.

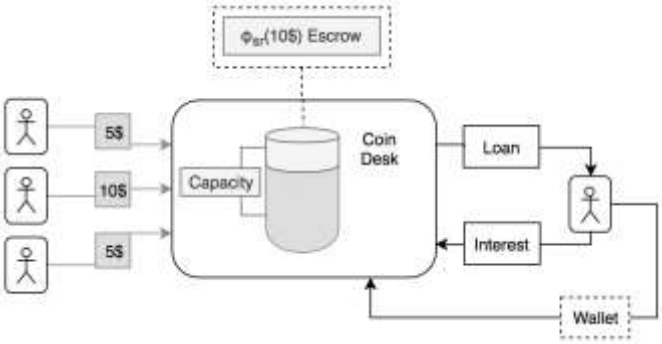
Incentives for a global Network

Coin Desks expand their reserve as they accept deposits and reduce their reserves as they service redemptions. If a Coin Desk consumes its total secured capacity,



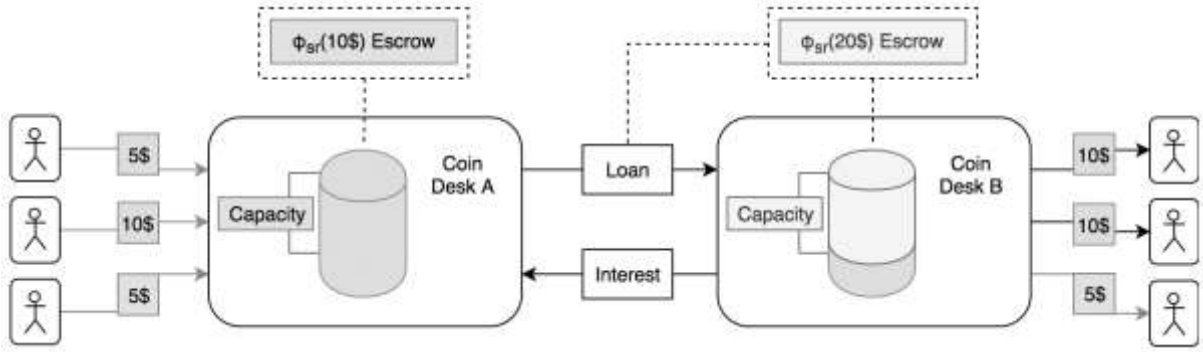
it cannot accept further deposits and give up on the corresponding fees.

To increase capacity to accept more deposits and accumulate more fees, Coin Desks can loan part of their reserve to users. Such loans can bear interests as negotiated between the parties.



Loans can be secured in part by the user's wallet holdings and rewarded with interest.
Coin Desks which net more deposits than redemptions will have excess reserves and be unable

to accept more deposits without increasing their escrow. Instead of increasing their



holding in escrow, Coin Desks will be incentivised to loan excess reserves to other nodes of the network which net more redemptions. Loans are secured by escrow and rewarded with interest.

Credit Channel

One of the most important principles in banking is “don’t move money”. Moving money is expensive as it incurs a frictional cost and often takes time as well as manual intervention to complete. The majority of transactions on financial networks are conducted by changing numbers on balance sheets while the underlying assets never move. These transactions are conducted by adding and subtracting from credit balances to keep track of how much is owed and to whom. Outstanding balances are settled periodically, effectively amortizing the frictional cost of individual transactions and clearing balances all at once, as a batch.

In Topos, credit channels are a smart contract driven mechanism which allows entities to exchange credit balance on-chain and minimize money movement. Credit balances are extended from a creditor to a debtor and have on-chain representations. Each channel has a credit limit which determines the maximum amount of credit that can be accumulated by the debtor. Once that credit limit is reached, the channel gets closed and no further credit is available from it until the outstanding debt is settled.

Credit Channel is a complex concept intended to minimize frictional or transactional costs. It exists between a debtor and creditor, affecting the balance sheet of both, and accrues debts through a settlement period. Credit channels structure can be described as follows:

```
type CreditChannel struct {
        ID          CreditChannelID
        Creditor    EntityID
        Debtor      EntityID
        Denom       Denomination
        Capacity    int64
        Utilization int64
        // ...
}

// CreditChannelID uniquely identifies a credit channel.
type CreditChannelID string

// ErrCapacity is returned when a credit channel doesn't have enough available
// capacity to service a credit request.
var ErrCapacity = errors.New("requested amount beyond current capacity")

// Request the amount from the credit channel, increasing its utilization.
func (c *CreditChannel) Request(amount int64) error {
        if c.Utilization+amount > c.Capacity {
                return ErrCapacity
        }
        c.Utilization += amount
        return nil
}

// ErrOversettled is returned when a credit channel receives a settlement
// request that's greater than the current utilization.
var ErrOversettled = errors.New("settlement amount greater than current utilization")
```

```
// Settle the amount in the credit channel, decreasing its utilization.
func (c *CreditChannel) Settle(amount int64) error {
        if amount > c.Utilization {
                return ErrOversettled
        }
        c.Utilization -= amount
        return nil
}
```

Balance Sheet

Balance sheets represent the financial state of every node in the network, at any given time. Balance sheets allow network nodes to inter-operate on credit and determine the minting-burning functions underlying deposits and redemptions. Balance sheets are composed of a string that enumerates the three core classes of accounts: Asset-Liability-Equity and a Debit-credit section enumerating classes of journal entry items, as well as kinds of accounts. Accounts carry crypto duals for the given fiat denomination.
Balance Sheets are influenced by journal entry items as follows:

```
//
DebitCredit
enumerates
classes of
journal
entry
items,
              // as well as kinds of accounts.
              type DebitCredit string

              // Debit and Credit.
              const (
                      Debit  DebitCredit = "Dr"
                      Credit             = "Cr"
              )

              // AssetLiabilityEquity enumerates the three core classes of accounts.
              type AssetLiabilityEquity string

              // The classes of accounts.
              const (
                      Asset     AssetLiabilityEquity = "Asset"
                      Liability                      = "Liability"
                      Equity                         = "Equity"
              )
```

Setup Process

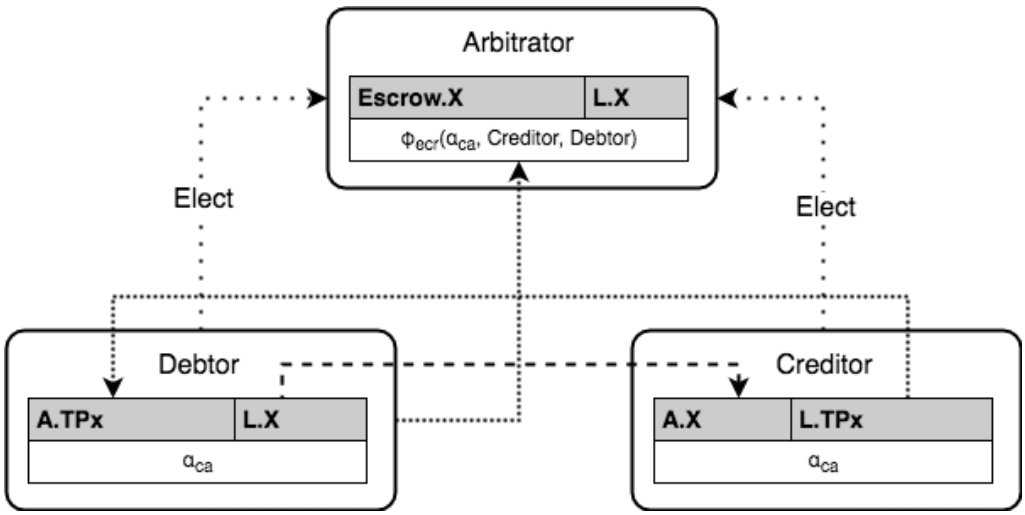
Credit channels are created through coordination between creditor and debtor. The creditor and debtor agree on a credit amount α_{ca} and elect an arbitrator. Election is completed when both the creditor and debtor submit the same public key to a smart contract.

To guard against credit risk an escrow account is created. The debtor must deposit an amount $\varphi_{ecr}(\alpha_{ca}, \text{Creditor, Debtor})$ which is a function of the credit amount, the creditors overall risk profile (calculated as a function of their balance sheet) and the debtors overall risk profile (calculated as a function of their balance sheet).

Credit Premium

To reward risk, balance settled include a credit premium defined by the function $\varphi_{cpr}(\alpha_{ca}, \text{Creditor, Debtor})$ which is a function of the credit balance, the credit risk associated with the debtor, as well as the credit risk associated with the creditor.

There is a relationship between the escrow amount $\varphi_{ecr}(\alpha_{ca}, \text{Creditor, Debtor})$ and the credit premium $\varphi_{cpr}(\alpha_{ca}, \text{Creditor, Debtor})$. When both debtor and creditor are in good standing, both escrow amount and credit premium should be low. If debtor is in bad standing, both escrow and premium amounts will increase to reflect the overall risk. The specific escrow function φ_{ecr} and credit premium function φ_{cpr} are to be determined in future work which analyses the specific economics and risk associated with the system.



Credit channels create accounts on the balance sheets of both the debtor and creditor. The debtor receives an asset account, denominated in TPx as well as a *_payable liability account represented the credit received. On the creditors balance sheet, an asset account denominated in TPx^1 (where x and x^1 can differ) as *_receivable as well as a liability account denominated in TPx representing the credit issued.

Settlement
Balances on credit channel are settled through off-chain transactions using means of payments agreed upon by both the debtor and creditor (ie: wire transfer). Settlement is conducted in the following sequence:

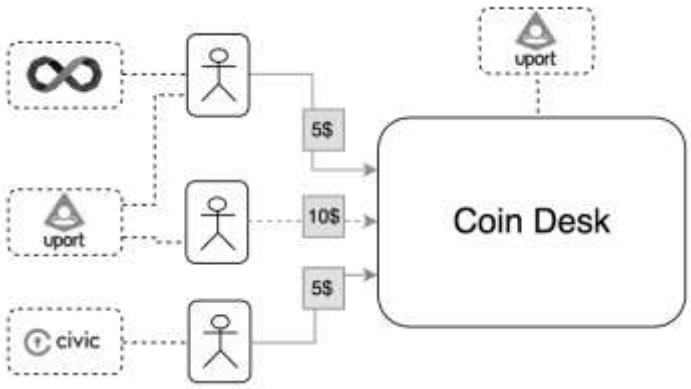
->Debtor Initializes a settlement claim to clear outstanding credit balance;
->Debtor sends off-chain settlement (e.g.: wire transfer);
->Creditor receives off-chain settlement transaction:
->Creditor sends settlement confirmation on-chain.

Once the settlement claim has been confirmed by the creditor, the balance on the credit channel is updated and the debtor once again has access to credit provided by the credit channel.

If the debtor does not send a settlement payment or the creditor does not confirm the settlement payment, either party can initialize a dispute. A dispute triggers a process in which the elected arbitrator verifies the validity of the claim. Once the outcome of the claim is determined by the arbitrator, the amount held in escrow is awarded to the winning party.

Decentralized KYC

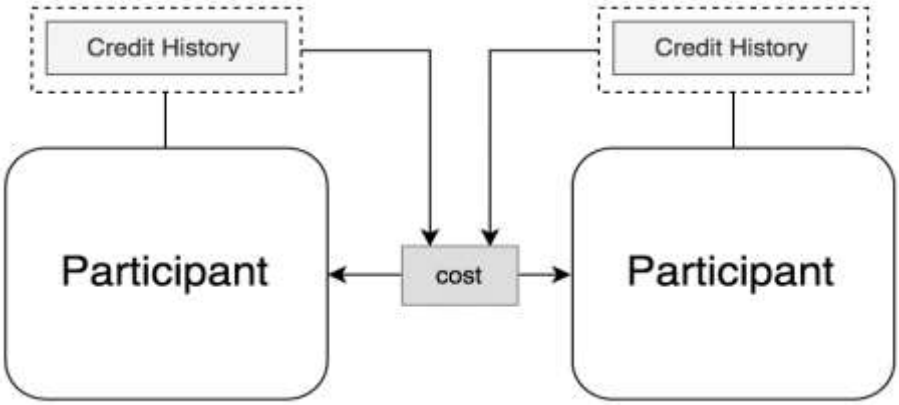
Each participant in the network decides any number of decentralized KYC providers. Coin Desks select which providers they accept. Identity protects the network from spam and sybil attacks. Ensuring that there is some consequence to spoofing one's identity makes measuring risk across the network feasible.



Coin Desks can facilitate KYC onboarding with 3rd parties allowing users to secure their identity in the network.

Eliminating Arbitration

As the network evolves, credit history of each participant can be used to price transaction fees,



reducing the frequency of arbitration until it becomes negligible.

Token Economy

TPG tokens are designed to prevent economic shocks and operate credit channels across the network.
As outlined above, TPG tokens are used to secure credit channels. By putting them in escrow, the system naturally reduces the amount of circulating supply. When credit channels are productive, TPG tokens securing the channel will remain out of circulation. When credit channels are unproductive, or debtors will fail to make payments, the channel will default and TPG will be liquidated to compensate the creditor. Even with a high default rate (50%+) we can assume the overall circulating supply naturally decreases as the network expands. Inflation will compensate for this reduction by rewarding creditors with additional tokens which they can use to establish new credit channels and continue to grow the network.
As the network expands, TPG Holders will be gaining additional benefit from its success.
In fact, they will be able support Coin Desks by collateralizing their credit, so that Coin Desks can extend their threshold to store fiat as liquid asset; TPG tokens bonded in credit channels become illiquid, reducing the overall supply. They get progressively released according to:
○ repayment installments from liquidity bonds (net of coupon);
○ credit depletion;
○ custodianship termination.

TPG supply is algorithmically adjusted based on systemic credit needs[1] to maintain 80-99% short term credit available across the network. Adjustments drive liquidity and participation based on:

$$s_C = \frac{D_C}{v}(\theta)$$

Where S_C represents the supply of TPG tokens, D_C represents the demand for credit within

[1] https://en.wikipedia.org/wiki/Credit_theory_of_money

the network, v, the current token value and the parameter θ expresses the relation between credit in escrow and credit defaults. Such credit defaults within the system are accounted for by default pools formed at Reserves level to cover up to 30% of liquidity shocks.

Implementation

Topos is a decentralized application running on top of blockchain networks, with an initial implementation on Tendermint. The underlying blockchain network allows permission-less participation and secures transactions against censorship. Computer nodes validate transactions and are incentivised by block rewards in a native token TPG. TPG is used to secure credit and enable liquidity of fiat currency at the edge of the network where it can be redeemed.

On top of the blockchain network, Topos maps a geographical network of financial hubs enabling anyone to: have a deposit account denominated in local currencies; store, share and transact at negligible cost; redeem tokens for local currency from brick and mortar stores (the equivalent of remittance agents). This seamless interaction mimics the existing Hawala (money transfer) customer experience, reducing the friction to onboard and fostering network scalability.

Each hub in the geographical network is represented on chain as a balance sheet. Each transaction between hubs is a double entry accounting entry. Entries keep track of outstanding loans and how different operations are financed providing transparency and trust to the payment network. Portions of the transaction are encrypted to maintain privacy while providing enough information to assess credit risk.

Credit checks will allow nodes in the network to lend to each other. Lending between nodes will push liquidity to the edge of the network to service redemptions. Credit risk is assessed through a smart contract providing fair and transparent credit check.

Conclusion

In this first section of the paper we presented the primitive mechanisms behind a system that allows deposits to be offered on top of existing remittances channels. The problem was motivated by the fractured financial system which leaves a large portion of the world unbanked and reliant on expensive remittance services. Building banking services whitin existing micro-economies presents a large economic opportunity but requires a complete re-think of the way financial systems balance risk and reward.
We designed Topos as decentralized and stable store of wealth with a more equitable incentive structure. Reserves are spread over a network of participants where they can be deployed productively to help the community.
Topos allows anyone to become their own bank by becoming Coin Desks and servicing their community to foster financial inclusion.

Section 2. Topos *de*Central Bank: Managing a federated set of collateral pools to create the decentralized economy of the future.

In this section we describe the mechanism allowing a decentralized bank to be built on a federated set of independently managed pools of collateral. Once the amount of deposits held within Topos network becomes relevant enough to require management and create added value for the underlying depositors, Topos protocol will be rolled out within the system to allow Users to group their assets in pools of collateral and invest it in ways that both prevent volatility and benefit communities.
Collateral is composed of a mix of assets and allocated semi-autonomously by the collateralized pools to generate profit. Stability is ensured through democratically developed monetary policies and a decentralized reserve of interest yielding bonds.
The time is right to create a banking protocol that could be applied to any decentralized economy in order to create value and financial self-determination.

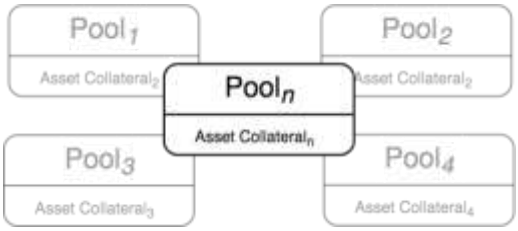
Preface

The degree to which a banking institution finances the real economy is evident from the portion of assets dedicated to lending, and the structural difference between ethical and systemic banks is how credit is extended to depositors[2]. Looking at the past ten years data, we can assume that access to credit and counter-measures preventing volatility represent key drivers for financial independence and sustainability of every developing economy. During times of recession or stagnation, access to credit inevitability shrinks, and in times of economic growth, inflation drives loss of buying power, leaving in both cases the lower tiers of society exposed to higher risks of marginalization.
To counter those threats, Topos proposes an independent and fully decentralized banking infrastructure, owned by its own participants (depositors), where assets can be collateralized and handled in community specific way, and where credit is made available based on community values and not sheer financial multiples.

In traditional economies, contrasting volatility is a role mainly undertaken by Central Banks. Such institutions are designed to provide stability by setting monetary policies and holding reserves to guard against sudden economic shock. There is a caveat though: A single central bank can only operate within specific borders and mostly on a single currency, given that its goal is to protect the corresponding national economy. Therefore, in a more complex system such the current global economy where currencies and liabilities are intertwined, central banks had to federate in larger entities such as the European Central Bank (ECB), or elect watchdogs like the international Monetary Fund (IMF) and delegate parts of their mandate in order to attain results more effectively through a higher level.

[2] ETHICAL AND SUSTAINABLE FINANCE IN EUROPE https://ebi-europa.eu/wp-content/uploads/2018/07/REPORT-on-Ethical-Finance-in-Europe-by-the-Ethical-Finance-Foundation-Banca-Etica-Group.pdf

Equivalent organizations will need to arise for the ecosystem around developing economies or marginalized populations to progress.
These organizations shall be transparent, decentralized and governed by their own participants.



We propose taking the institutions which govern our financial infrastructure, such as central banks and international monetary funds, and recreating them as a decentralized protocol. This protocol will connect a federated set of independently managed collateral pools, adhering to democratically developed monetary policies which will grant the ecosystem stability and growth. Each pool will accept deposits, maintain reserves and manage collateral as a portfolio of assets. Pools will differ both in how they allocate collateral as well as the services they provide. The Topos protocol will ensure proper incentives to maintain this careful balance of risk and reward. This will enable anyone to become their own bank.

Glossary

- Collateral*:* security pledged for the payment of a IOU
- Asset: Object of value like a cryptocurrency, commodity or security, priced by and traded on a market
- Appreciation: Increase in value of an asset
- Depreciation: Decrease in value of an asset
- Correlation: The tendency for two assets to increase or decrease at the same time
- Anticorrelation: The tendency for one asset to increase in value as the other decreases
- Diversification: The composition of a collection of anticorrelated assets to provide stable value
- Liquidity: Availability of an asset to be bought or sold
- Deposit: Transactions in which currency is exchanged for account balance
- Redemption: Transaction in which account balance is exchanged for currency
- Reserve: A set of liquid assets to service obligations
- Obligation: Outstanding deposits and interest payments
- Solvency: Ability to repay all obligations
- Bond: Loan to an organization with interest and maturation period
- Monetary Policy: the process by which a monetary authority controls either the cost of very short-term borrowing or the monetary base, often targeting an inflation rate or interest rate to ensure price stability and general trust in a currency.

Mechanisms for a Central Banking Protocol

We are building Topos on top of any existing blockchain. Smart contracts will operate in concert to provide transparent application of monetary policies. Transaction fees will be covered by the profits generated with the collateral appreciation, making it free and even cost negative for users to participate the system.

Token Issuance

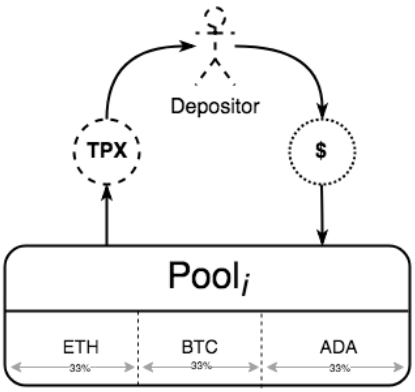
As covered in the previous section, two native tokens will be issued to power Topos network. *TPX*: a VPT[3] token with value pinned against a currency, where risk of solvency is secured by collateralizing deposits in a basket of assets. *TPG*: A governance token with floating value, designed to secure credit channels between network nodes and to be anticorrelated with other assets and used to stabilize the system in case of sudden economic shocks. Out of 1,062,500,000 *TPG* created, only 425,000,000 be progressively disseminated into the system to account for credit need. A pool consisting of 265, 625,000 TPG will be help as a Reserve Fund to counter liquidity or systemic shocks, and will be release on a consensus basis.

Users creating wallets will be able to associate them with one or more collateral pools to be granted their redeemability at any Coin Desk within the network. In fact, if Coin Desks represent bank branches, pools function as credit unions for users. Different pools will adhere to different monetary policies to drive different use cases.

Some examples would include: A pool focused on consumers with overall low risk tolerance and low return expectations. Users linked to this pool will perform frequent but small transactions forcing the pool to maintain adequate reserves. This pool will mostly be used as a store of value and limit the depositors' exposure to volatility of the underlying assets.

An alternative example would be an investment pool, carrying higher risk tolerance but also higher return expectations. This pool would be willing to sacrifice and take on higher risk for a potentially higher reward. Transactions would be less frequent but of larger amounts.
Users will be able to participate different pool, based on their risk profile and investment thesis, as well as partition their holdings and allocate them to several pools.

Accepting Deposits



Deposits are accepted in multiple currencies and trigger TPX tokens minting, with an hypothetical exchange rate against the peg determined by the basket in which the collateral underlying the chosen pool is held. A basket is comprised of multiple assets in different proportions to create a target value which varies as little as possible. An example would be 20% USD, 80% GOLD. If the value of the USD was to go down, the overall depreciation of the basket would be limited to the floatation of the percentage held in USD. If USD and GOLD are anticorrelated, the price of USD going down will be met with some proportion of the price of GOLD going up, effectively neutralizing the change to the overall value of the basket. This basket target insures stable exchange rate against as many currencies and assets as possible. Thanks to the system's real time visibility on asset value fluctuations, adjustments will be algorithmically triggered to liquidate depreciating assets and counter negative effects.

[3] https://cointelegraph.com/news/important-aspects-of-stablecoins-the-difference-between-pegging-collateralization-and-redeemability

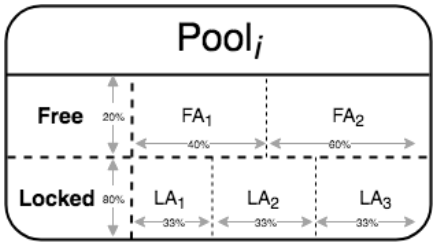
On receipt, a portion of deposits up to 88% is converted into a mix of assets. Each mix of assets is chosen by the collateral pool to reflect the predetermined investment strategy. Different mixes of assets carry different risk profiles as well as different rewards. Different pools will have different -higher or lower- risk tolerances and the assets they choose will reflect this. An example of allocation would be 80% USDT 20% ETH. As a stable coin USDT has a very low risk profile but the expected returns on such holdings will be equally negligible. ETH, by comparison, is a more volatile asset. The risk taken on by the pool exposing itself to the fluctuation of ETH prices could also be rewarded when the price goes up. The remaining portion is held as local liquidity to service redemption needs under the LCR guidelines[4].

Managing Collateral

A careful balance between risk and reward must be met to ensure responsible management of collateral throughout the system. Spreading the risk over a diverse federation of collateral pools makes the system more robust. In order to ensure that risk is managed appropriately across the system, collateral pools are subject to a composition of global and local monetary policies.

Each collateral pool is divided into a *locked* and a *free* portion. The locked portion inherits and is bound to a global monetary policy, developed democratically by all participants. The free portion instead, is allocated locally by the collateral pool specific participants. The ratio between free and locked portions gets calculated and adjusted via algorithm periodically, based on the overall risk profile and allocation performance.
On one hand, a pool designed for an investment consortium, with a very aggressive and speculative approach applied to the free part -for instance focused on purchasing high volatility new tokens- will automatically result into a higher locked portion until a proven track record of the locally managed free portion is built. On another hand, a pool formed by a community of pensioners, with a conservative investment thesis such as real estate loans, is most likely to achieve a perfect balance between locked and free portions, unlatching more collateral to be managed at local level.
Different assets will have different risk levels, calculated empirically based on volatility.
Volatility can be broken down into multiple components including *seasonal*, *trend* and *noise*.

The seasonal component can be considered a market cycle which is always evolving in itself.
The trend component represents the overall change over multiple cycles. Noise reflects recent price action.



The decomposition of volatility will classify different assets in terms of risk profiles. With a rapidly evolving ecosystem of cryptocurrencies, a careful selection of assets will be key to ensure stability. Selecting a new cryptocurrency without a pronounced market cycle may in fact expose the pool to too much risk.

[4] Liquidity Coverage Ratio (LCR) – Executive Summary https://www.bis.org/fsi/fsisummaries/lcr.htm

The volatility of assets will be assessed individually as well as collectively in terms of their correlations. Portfolios will maintain a level of anticorrelation ensuing the overall value is kept even if a subset of assets depreciate suddenly.

Reserve Requirements

Pools will maintain a reserve of liquid assets to ensure all redemption requests are serviceable. Monetary policy developed at global level will set the minimum liquidity thresholds for each pool, thresholds that can vary and be adjusted at local level based on historical data, real time demand and seasonal needs. Empirical redemption frequency will combine with pools specifical monetary policies to service a range of different use cases.

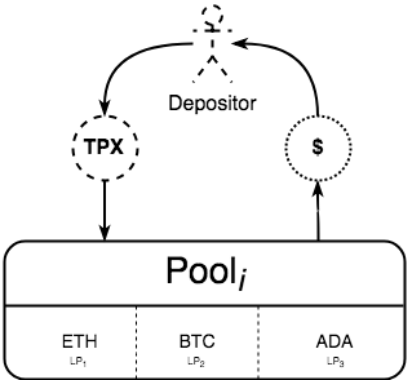
Different reserves requirements will evolve to service different use cases. For instance, a pool servicing commercial clients will need to maintain sufficient liquidity to withstand many small transactions. By contrast, a pool operating under a pension fund-like approach, will be required to service a lower frequency of redemption requests.

Servicing Redemptions and Liquidation

Depositors will be able to exchange TPX for fiat as a redemption request. Redemption requests will be handled either directly at collateral pool's level using built-in on/off ramping services or facilitated by Coin Desks networks, rewarded for holding liquidity. Redemption requests handled by coin desks will incur a small fee to incentivise expansion of the network.

Redemption requests will burn redeemed tokens on receipt, maintaining the collateral to TPX supply ratio.

Depositors can also denominate redemption requests in a number of cryptocurrencies. To service the requests, the collateral pool will liquidate a portion of its assets. Liquidation of collateral pool will happen in a liquidation order where more volatile assets will liquidate before less volatile assets. Over time Topos will evolve into a more dynamic liquidation orders protocol, to limit the amount of conversions and disruption to portfolios overall strategy. Progressively, the system will be able to balance liquidity needs internally, decluttering the value chain from middlemen.



Minimizing Asset Movement

Acquiring assets for pools' collateralization will come from various liquidity sources. Both centralized and decentralized exchanges will be an option. We assume that each transaction will incur fees and, once the system reaches a large scale, these fees will become a significant operational expense.

Being a protocol, Topos will benefit from economies of scale by acquiring and liquidating assets in batch through a settlement process. On transaction, changes in allocation will be recorded on the blockchain as a debit/credit. A settlement process will be run periodically to execute accumulated debit/credit and balance each pool with their actual desired allocation.

As TPX transactions volume increases, regularities in these transactions can be exploited to determine predicted demand for assets in the locked allocation. Liquidity pools of these assets can form within the topos network to service these operations to -again- reduce the overall cost of buying/selling assets.

The settlement process combined with liquidity pools will minimize the amount of transactions fees linked to the assets reconfiguration within all pools. The economy of scale will make the cost associated with managing a portfolio of assets in Topos orders of magnitude lower than what would be expected from manual management.

Profit Distribution

Profits generated from pools will be redistributed in the form of dividends. Dividends will be split amongst pool participants proportionately to deposits. The schedule of dividends issuance will be defined by each pool based on local monetary policy. Lower risk pools will issue rewards less frequently while higher risk pools will most likely issue more frequently.

A portion of profits will be held back in escrow. Held back profits will be used to pay interest on bonds and insure the pool against sudden influx of volatility.

Stability

A key objective of Topos is to serve as a stable store of wealth. In practice, this means that the system must, at all times, ensure that all issued TPX can be redeemed for their original value. With different pools allocating collateral in different ways and effectively taking different risks, we require a mechanism which can fulfill liquidity needs even as collateral depreciates.

Monitoring price movement and change

Collateral value will be monitored with regular frequency. Price feeds will come from voted in exchanges and an average between the 25th and 75th percentile will be taken to remove outliers. Price feed information will be used in combination with expected redemption history to calculate value at risk. As an asset depreciates or becomes more volatile, risk increases. When the risk rises above a certain threshold, pools with high value will need to find liquidity to ensure all redemption requests can be serviced.

Stability Bonds

Central Banks often operate as the “lender of last resort”[5] in times of economic shock. If a market was to crash, banks which are over exposed would require emergency funds to fulfill

[5] The lender of last resort and modern central banking: principles and reconstruction
https://www.bis.org/publ/bppdf/bispap79b_rh.pdf

their obligations. Without a central authority, Topos will require a decentralized alternative to respond to sudden changes in asset values.

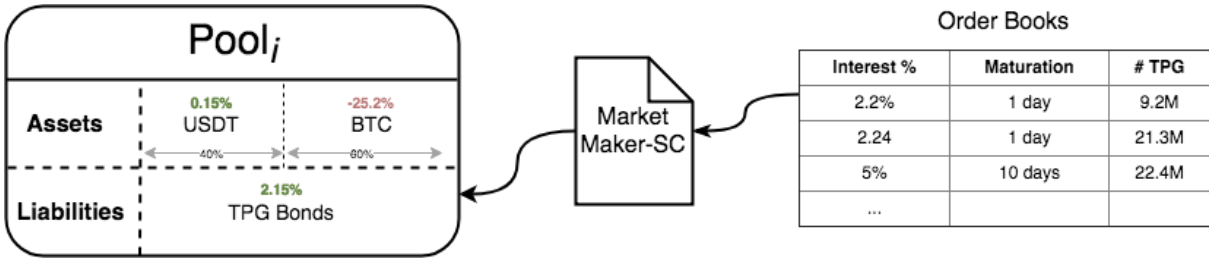
To provide a decentralized “lender of last resort”, TPG tokens can be composed into bonds and placed on a bond market. TPG token holders specify the minimum yield and maximum maturation they would accept to lock up their tokens in a bond. Bonds are placed as limit orders, and will be executed automatically via smart contract when their yield and maturation criteria are met by a buyer. For placing bonds on the market, TPG holders will be rewarded with a small interest payment paid weekly. This interest payment should exceed inflation and incentivise participation in stabilising the system,

The Bond market will serve as a transparent and decentralized reserve against sudden economic shocks. As part of the protocol, the depth of the market can be used to inform monetary policies in real time. Monetary policy enforcing smart contracts can adjust risk levels according to how many bonds are available and at what price. This mechanism can even be used in extreme cases to re-collateralize pools in a stability intervention process.

Stability Interventions

Pools collateralization levels will vary based on volatility of their underlying assets. This volatility will be handled by proper allocation and sufficient anticorrelation between the assets. With risk always being proportionate to reward, there is sometimes the chance that changes in economic conditions occur overnight and a rapid depreciation of overall asset value socks the system. In Topos the exposure, or value at risk, is monitored constantly. In cases in which the value at risk crosses a certain threshold, a stability intervention process automatically triggers to rebalance the system.

During any stability intervention, a collateral pool which has exceed it’s risk threshold gets assigned stability bonds automatically by a market making smart contract. The amount of interest rate (of such bond) is determined by a mix of factors, including bond current risk levels and bond supply.



Interest is granted by collateral pool profits, effectively punishing collateral pools for taking on too much risk.

Proof of Solvency

Each TPX issued constitutes an obligation. The state of the system will be monitored continuously to ensure that all obligations can be fulfilled. The Proof of Solvency smart contract will use redemption rates, current collateral value, collateral volatility and available bond reserves to assert the solvency of all collateral pools.

Price Dynamics of TPG bonds

TPG must maintain its value under overall market instability to be a suitable reserve currency. If TPG were to suffer depreciation in tandem with overall asset depreciation, the system would be at risk of becoming insolvent. The price dynamics, in terms of supply and demand determined by the stability intervention mechanism, are meant to ensure that TPG value is anti correlated with the other collateralized assets.

When the value of collateral pools falls, the stability intervention mechanism will start assigning bonds to collateral pools. This increased demand will be reflected in increased price. If no bonds at the current interest rate are available, the market maker smart contract will start assigning bonds at a higher interest rate. The higher yield from bonds will encourage more people to come into the market to lock in a better interest rate.

There is an additional dynamic between the duration of market cycle and the bond maturation period. A market crash will result in increased demand for bonds and this will drive TPG appreciation. As the market recovers, demand for TPG along with price will go down. However, even as the market recovers and the overall demand for TPG shrinks, some supply of TPG is still held in bonds. Care must be taken to match bond maturation period and expected market cycle to avoid over inflating the price of TPG.

Governance

Topos will require a system of governance which reflects the decentralised nature of the protocol. On chain governance will provide a path for wallet holders to shape the way the network is operated and ensure these operations align with their values. Specifically, the goal of the governance system is to evolve and enact transparent monetary policies. These policies will ensure the stable growth of all pools and limit system risk. By consequence, the governance system will need to be robust to:

1. *Corruption: Where malfeasance has recourse*
2. *Censorship: Censoring any one pool/agent would not bring down the network*
3. *Plutocracy: The slow shift towards governed exclusively by wealthy.*

Monetary policies will take the form of smart contracts defining the computational process and parameters for all monetary operations. Parameters defined by a monetary policy include interest rates, liquidity requirements, asset types and how risk is calculated. The monetary policy smart contract will be consulted in operations which jeopardise the stability of the collateral and reject operations which expose too much risk.

The governance protocol will happen at two levels:

Globally: as a *reverse-Lamfalussy process*[6] conservative monetary policy applying to all pools subject to participation by all users.

Locally: More dynamic monetary policies applied at the pool level subject to participation by pool members only

The system will be governed by participation across users performing different roles:

- Wallet holders
- Delegates
    - Vote Delegate
    - Stake Delegates
- Elected
    - Pool Manager
    - Global Policy Manager

Each wallet represents one vote, regardless to its assets size. Votes can be delegated to representatives with more knowledge on specific issues. Representatives are assigned votes that they retain for the duration of a term. The term should be sufficiently long to allow assessment of representative performance. Longer terms present larger risk while shorter terms will burden wallet holders with process and lower participation. Term lengths will be subject to votes and vary across roles.

Different wallets have different holdings. And risk is proportionate to their holdings. This risk should be mitigated by having an impact on how the system is governed, but this impact should not be disproportionate to other wallet holders, even when the risk is. A principle of Topos is that every wallet holder should have one vote and stake should be proportionate to risk. With this motivation we propose developing a two mechanisms system with voting and staking. The goal of the two mechanisms system is to have democratic outcomes while balancing risk and reward.

Certain democratic outcomes involve bigger risk. Electing a manager of global policy constitutes a large risk as the decisions may take affect everyone. Candidates therefore require a minimum stake. The minimum stake is determined per role democratically (1 wallet= 1 vote). The stake is used as insurance against malfeasance. The minimum stake can require some portion from the candidates themselves, ensuring they individually have something to lose.

Once elected, the stake is held in escrow for the duration of the term. If an elected official is voted out, through democratic process, the stake is transferred into a separate account controlled by the voters for the use of remediation.

Many roles in Topos will require multiple occupancy to be robust against single points of failure. These elected groups will participate in key rings allowing anyone in the group to sign operations permitted by their role. Within the group, different operations require different level

[6] https://en.wikipedia.org/wiki/Lamfalussy_process

of consensus, always proportionate to the impact. The number of minimum members required for a vote is defined as its quorum. Different groups require different quorums on a per issue basis.

The combination of the staking and voting system provides an augmented form of liquid democracy to balance risk and reward. The governance structure will develop alongside the protocol to put more control into the hands of wallet holders, while incentivising and enforcing the evolution of a stable monetary policy.

Protocol Implementation

Topos protocol will be implemented as a collection of smart contracts deployed to a blockchain network. A variety of networks are emerging, each with different tradeoffs. In the short term Tendermint[7] and Ethereum[8] are the most mature and offer easy integration with variety of on chain assets which can be used as collateral.

Smart contracts

In order to operate, several classes of smart contracts will be made available to the participants.

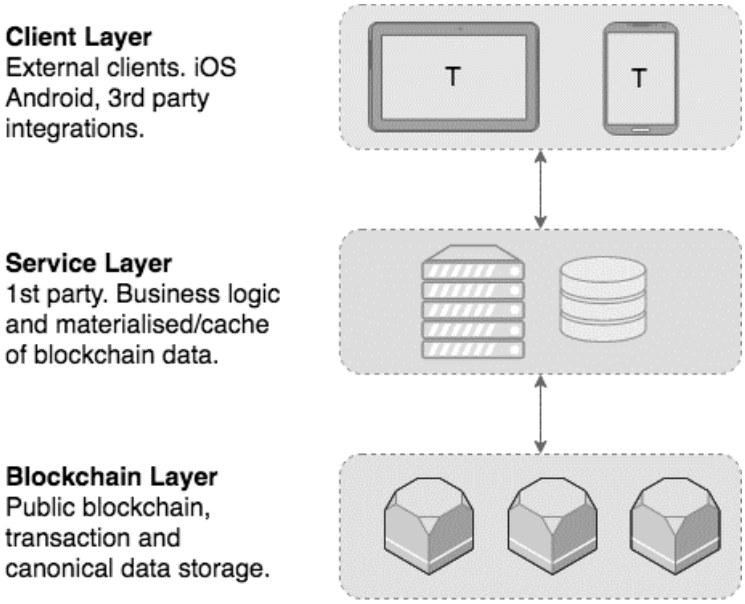
- GBSC: Governing body smart contract
    - Creates pools
    - Handles voting processes
- MPSC: Monetary Policy smart contract
    - Enforces risk limits
    - Sets Interest rates
    - Collateral pool allocations
- LNSC: Liquidity needs smart contract
    - Tracking deposits and redemptions for different pools
- VTSC: Volatility tracking smart contract
    - Uses a set of oracles to observe price movement in various crypto assets
- LMMSC: Liquidity Market Maker
    - Decentralize market of bonds to re-collateralize pools
- POS
    - Proof of Solvency Smart Contract
        - Assess solvency based on:
            - Collateralization levels
            - Collateral exposure
            - Bond rate & liquidity on the market

Full Stack Implementation

The architecture will follow a layered schema which splits the components into groups. These groups can easily be identified by ownership. The *Client layer* owned by users, the *Service layer* by Topos and the *Blockchain layer* being public.

[7] https://tendermint.com/
[8] https://solidity.readthedocs.io/en/v0.4.24/introduction-to-smart-contracts.html

Well defined interfaces will delineate boundaries between layers leaving room for both extension and integration.



The benefit of this approach is ensuring natural refinement of evolution by decoupling components along ownership boundaries. Specifically, the iOS/Android app should be able to be refactored without changing the service layer. Additionally, 3rd party wallets could integrate using the same protocol as native Topos clients.

The current Service layer is designed to be owned by Topos but will be released as open source software. An incentive scheme could be devised here to incite 3rd parties to operating their own stack providing a more robust and trustless interaction with the public blockchain. In the foreseeable future in which the architecture transitions to a more trustless design, components of the Service layer will be integrated into a Topos-Blockchain, enabling deeper integration with 3rd parties.

Components and Interaction

The architecture of Topos will be straight forward off-chain reliant design. The motivation for using a blockchain, comparison of options and centralization tradeoffs are detailed above.

The mobile application will connect to the Service layer to facilitate transactions and community network features over HTTPS. Topos API components will operate as Stateless relay services, mediating the connection between clients and the blockchain. Complex operations like fee calculation will be performed within the API service.
In order to optimize Topos interaction with Tendermint, we released an application on top of the Tendermint ABCI, implementing a key-value store with a compare-and-swap API in Go[9].

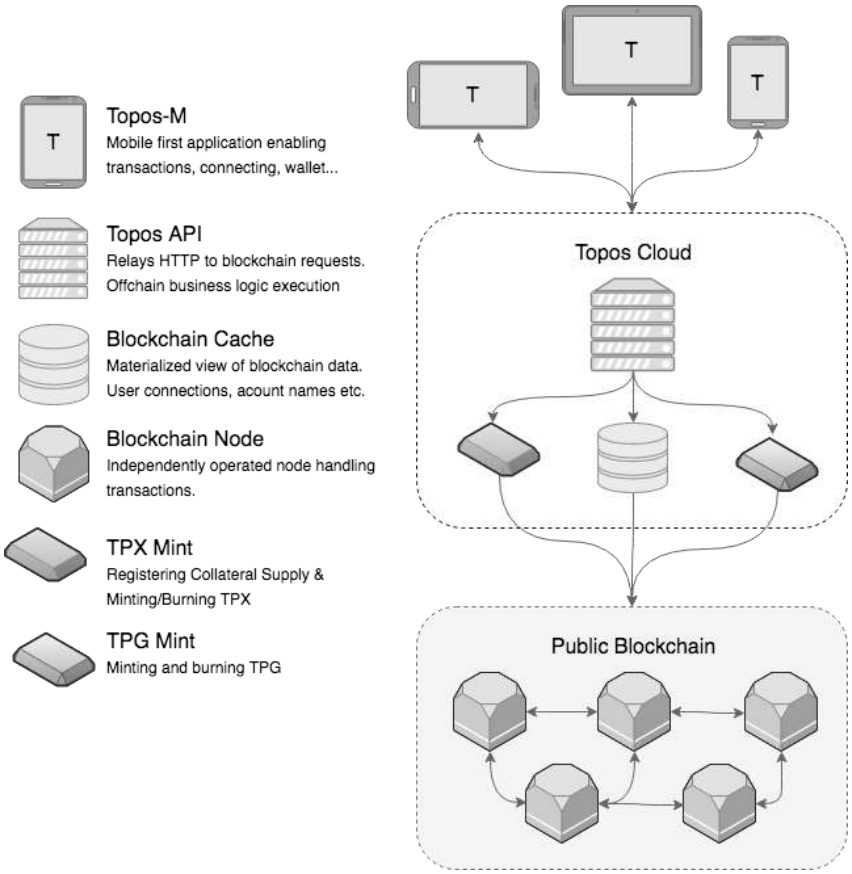
Each node will have an HTTPS API implementing compare-and-swap semantics for a key-value store. The keys and values will be reliably and consistently replicated between nodes by Tendermint, allowing greater scalability and lower frictional costs than the ones currently

[9] https://github.com/6thc/tendermint-cas-demo

available to projects built on top of this technology.

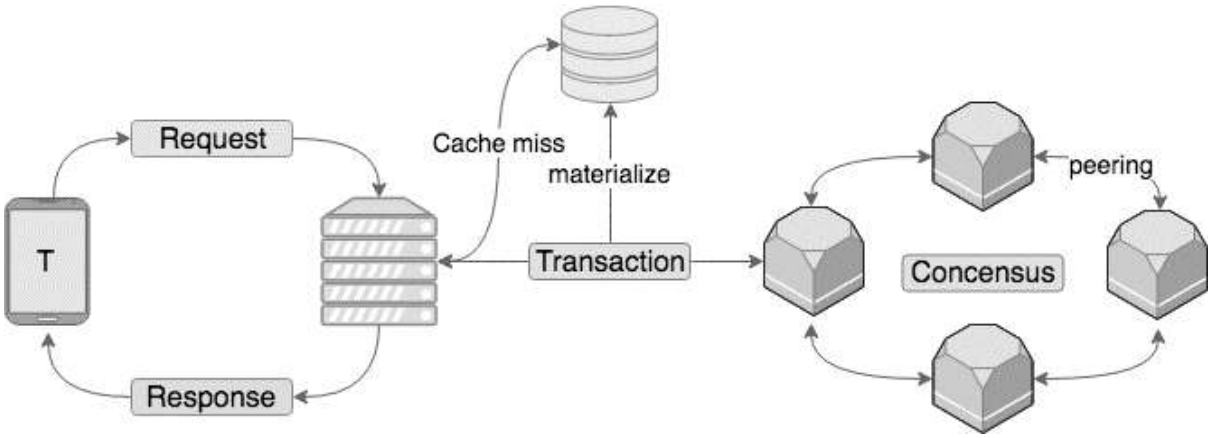
Data pertaining to user connections, account holdings and transaction history will be stored on the public Blockchain. The representation of the user connection on the blockchain will be limited by the storage facilities provided by the blockchain.

An efficient materialised version of the data model will be stored in a cache available within Topos cloud to ensure fast user interactions.



Request Flow

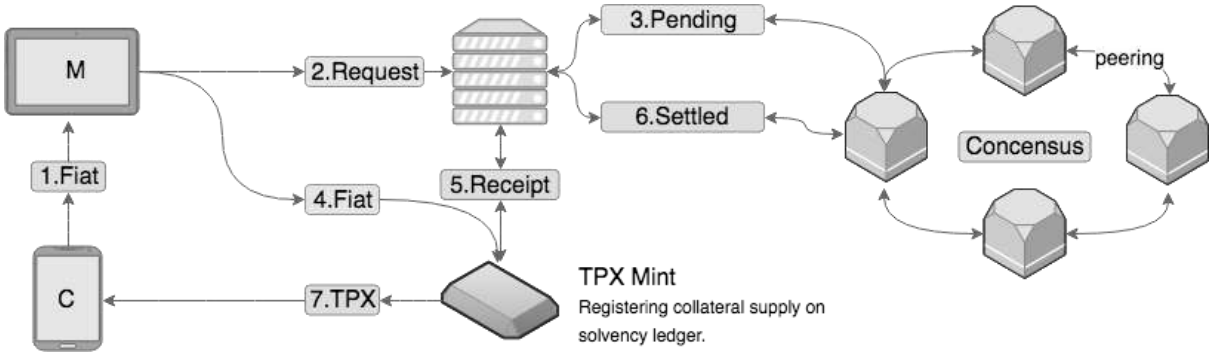
Interaction initiated on the mobile client will cause a chain of interaction throughout the stack terminating in transactions on the blockchain. HTTPS requests from the client to the API service will interact with the blockchain for writes and materialize a cached view for reads.



The Blockchain network will field transaction requests and trickle responses back up the stack to the client.

Deposit Flow

Deposits handled by merchants (M) will register pending transactions on the blockchain.



Upon receipt, a receipt event will be issued to the API triggering a settlement and the release of TPX tokens to the customer.

Conclusion

In this section we described how there is an opportunity to form a new decentralized financial institution that can provide a more democratic and transparent method of banking. We proposed a protocol for both applying and evolving monetary policies as a more democratic process. This protocol connects a federation of collateral pools which are managed independently, to offer a range of different financial products to a plethora of different customers. These pools will generate profit which is distributed amongst network participants.

Solvency of the pools is handled using a mix of preventive and reactive methods. Sane monetary policies insure that collateral is allocated balancing risk and reward. Smart contracts monitor the liquidity needs in terms of redemption history as well as available liquidity in the form of

bond markets, to assert the solvency under regular conditions. In edge conditions, stability interventions will assign bonds to pools forcing them to give up some of their profits to fulfill their obligations.

As a protocol, Topos allows anyone to become their own bank by forming or participating to a collateral pool. These collateral pools are managed independently but benefit collectively from economies of scale. The application of sane monetary policies binds them together, forming a financial platform on which any decentralized economy can be built.

Topos proposed protocol is set to become the *de*Central Bank for any emerging economy.

References

Remarks
IOM Director General, William Lacy Swing
Global Forum on Financial Inclusion for Development
International Conference Center, Geneva, Switzerland
24-25 October 2013
http://presentations.upu.int/index.php?get_action=open_file&repository_id=d3b3f8c3f2afaa966a35248d2c89057e&file=%2F2013%2FFinancial%20Inclusion%2F1st%20Day%2FSession%201%20William%20Lacy%20Swing%20IOM.pdf

United Nations, Department of Economic and Social Affairs, Population Division (2017). International Migration Report 2017: Highlights(ST/ESA/SER.A/404).
International Migration Report

The hawala alternative remittance system and its role in money laundering
Patrick M. Jost, United States Department of the Treasury