OmiseGO
Decentralized Exchange and Payments Platform

Joseph Poon
joseph@lightning.network

OmiseGO Team
omg@omise.co

June 17, 2017

Abstract

OmiseGO is building a decentralized exchange, liquidity provider mechanism, clearinghouse messaging network, and asset-backed blockchain gateway. OmiseGO is not owned by any single one party. Instead, it is an open distributed network of validators which enforce behavior of all participants. It uses the mechanism of a protocol token to create a proof-of-stake blockchain to enable enforcement of market activity amongst participants. This high-performant distributed network enforces exchange across asset classes, from fiat-backed issuers to fully decentralized blockchain tokens (ERC-20 style and native cryptocurrencies). Unlike nearly all other decentralized exchange platforms, this allows for decentralized exchange of other blockchains and between multiple blockchains directly without a trusted gateway token. Markets may be able to significantly reduce spreads and encourage market assurance via decentralizing custody and increased transparency of market activity. This is achieved using smart contracts, protocol tokens enforcing correct market behavior of orderbook matching, a new construction of Ethereum bonded external enforcement of clearinghouse activity, and commitments to historical exchange data for use with Ethereum smart contracts.

1 Introduction and Problem Statement

The primary role of blockchains are to solve coordination problems among multilateral agreements between a network of participants. By ensuring transparency, assurance, and enforcement, we can enable multilateral agreements where they were not previously possible. When all parties are assured that the operations are not only transparent, but also the mechanisms are guaranteed to not change without significant effort, parties are more willing to coordinate. Participants have significantly higher guarantees that a single party has difficulty forcing other parties in the future into usurious rent extraction via a change in business processes or information asymmetry. In other words, any single participant is more willing to use systems where the business processes and mechanisms itself are not owned by any other single participant.

There is a fundamental coordination problem amongst payment processors, gateways, and financial institutions. For instance, a customer of a bank wishes to pay a merchant on

Archived copy · cryp2nova.com

another network. Traditionally, there have been significant efforts in engineering around payment systems which are compatible across payment networks and financial institutions. These are usually constructed by creating a clearinghouse which manages the interchange, usually via a messaging network with either a central counterparty clearinghouse or nostro/vostro accounts. Examples include FedWire, CHIPS, SWIFT, consumer card payment networks, NSCC/DTCC, OCC, and ACH. These networks service different roles and functions, including local/national payments, international payments, credit, equities/asset exchange, and derivatives. These centralized networks allow for the controlling entity to arbitrarily change the mechanisms, which result in significant amount of transaction costs via information costs, due diligence, and contractual enforcement between all parties.

We believe that there is currently a large emerging market of disruption in digital payments with new payment platforms (e.g. Venmo, Alipay, etc.). These networks have significant aversion to interchange across networks, as it usually requires significant overhead costs in trust with the interchange facility. Parties are unwilling to use central counterparties, as neither party wishes to defer to the other, and use of nostro/vostro accounts require bespoke contracts between participants. While the larger networks have significant incentive around protection of their network effects, we believe that there is a long-tail of entities wishing to provide eWallet services which require greater coordination amongst multilateral participants. These mid-size participants will be able to cross value across networks in order to reach sufficient network effects in usability. The infrastructure and reference frontend for these providers will allow for the network effects to be encoded into this network, allowing for emerging eWallet participants to instantly create high network utility.

Blockchains allows society to externalize the world's business processes from single centralized corporations into open, decentralized computing networks. [1][2] OmiseGO (OMG) is a network which decentralizes market liquidity, orderbook matching and execution, clearinghouse custodianship, and high-scalability payments to help resolve payments across these emerging eWallet payment networks.

By shifting these business processes traditionally placed into a single corporation, it is possible to provide eWallet providers an entire interchange process in a decentralized high-performant open network.

2 Design Approach

The end-state requirement is a construction of a decentralized mechanism for eWallet platforms holding fiat-backed value (as well as native, opt-in, support for cryptocurrencies). The eWallet fiat tokens will have the ability to use Ether on the decentralized, public Ethereum[3][4] chain (or any other decentralized cryptocurrency) as the interchange/intermediary cross for maximum efficiency. We believe that this allows for significant more activity and value in decentralized cryptocurrencies, as it will serve as a useful venue for many eWallet platforms.

As it's a core function for this decentralized network to do eWallet interchange, a

Archived copy · cryp2nova.com

blockchain ledger on OmiseGO is necessary to hold the general balance of funds per eWallet service (or any user/node). This ledger must be able to hold funds across many assets/commodities. However, merely holding a ledger is insufficient for interchange. The mechanism must also allow to trade these assets/commodities.

In order to perform interchange, it requires an order to be placed across many different pairs on an open public market. This requires a decentralized orderbook and trading engine. The trading engine is built into the OMG blockchain, orders are published and matches are performed as part of every block when a matched order has reached sufficient number of validation confirmations. This results in a non-custodial decentralized exchange held by a single party where the eWallet platforms may exchange onto other eWallet platforms without centralized trust on a single entity.

However, direct crosses between eWallet fiat tokens may not be desirable, as there may be too many. It would be necessary to use cryptocurrency for a liquid market without single preference. By bonding Ethereum into a smart contract [5] (or Bitcoin-like tokens into bonded clearinghouses), it is possible to lock up Ether onto the activity of the OMG chain to allow for eWallet pairs to occur over Ether or other cryptocurrencies, creating a liquid market (if every pair crosses with ETH, spreads would be much smaller provided low currency volatility). For activity requiring very small spreads, it may emerge that some eWallet tokens will be used as interchange crossing; however, there's strong incentive to use decentralized tokens for settlement due to coordination/trust advantages related to programmatic adjudication. eWallet fiat tokens may also cross using other eWallet tokens if necessary, but bonding which don't affect short-term exchange rate fluctuations of smart contract activity will be primarily in ETH (e.g. HTLC clearinghouse, liquidity providing, and OMG chain enforcement). By allowing for cryptocurrencies to be the backing for eWallet platforms, the platforms can be assured of an even playing field between eWallet interchange activities.

This requires a greater degree of liquidity in funds locked up, and the OmiseGO decentralized exchange may not be desirable to transact for low-value interchange activity (e.g. for high-volume micropayments).

Not every payment between two distinct eWallets must be performed using a trade on the decentralized exchange. There is an expectation, that eWallets will hold some reserve of fiat tokens of other eWallets, ready to be used for smaller transfers in popular directions. Constructions such as Lightning Network[6] allow for payments to occur off-chain when eWallets hold balances to facilitate rapid payments. Implementations allow for payments across Bitcoin[7] and Ethereum[8], which can be easily ported to the OMG chain for eWallet balances.

The result of the OmiseGO blockchain construction is it allows for eWallet interchange, supported by a decentralized exchange, cryptocurrency (e.g. ETH) matching, orderbook, and clearinghouses without full-custody trust.

Archived copy · cryp2nova.com

2.1 Decentralized Liquidity Hub for Channels

The construction has the additional benefit of allowing for a decentralized liquidity pool to be created for use with payment channels on various cryptocurrencies, such as Bitcoin (and to some extent Ethereum).

For individual token payments on blockchains, there is a need to scale the underlying blockchain activity which does not affect the underlying chain to reduce computational pressure of validating/mining nodes. It is therefore necessary to conduct Lightning Network activities (or similar constructions using channels). However, Lightning Network faces significant pressure around network effects with capital, it's desirable to prevent liquidity pools from centralizing to a single trusted entity. By using the same mechanisms of the decentralized clearinghouse, we can create a Lightning Network hub which is not owned by any single individual on tokens which support more complex smart contracts (e.g. Ethereum, ERC-20-like tokens, etc.). For currencies with simple smart contracts, any node on the network (e.g. Bitcoin network) can act as a gateway into the OMG chain pool and cross back with any other participant. This allows the OmiseGO chain to offload a lot of on-chain activity, while encouraging decentralization.

We believe that the natural network effects of liquidity centralization can be mitigated by decentralized stake-chains with deterministic/known consensus rules.

For Ethereum in particular (and other full-featured smart-contract scripting blockchains), all participants set up channels into an ETH smart contract operating as a single pool of funds. The chain state of the OMG chain reflects the current balance of participants. This allows for any participant to supply liquidity onto this network which can be allocated in accordance to the OMG-chain consensus rules (limits may be in place early on to prevent this blockchain from sucking up all the spare liquidity from the cryptocurrency space if this construction is successful before robust testing/validation over time). These funds can thereby be used for any liquidity activity on the OMG chain.

3 Blockchain Overview and Mechanism

The above mechanisms require significant volume of activity (with a large amount of state), and is not at this time suitable for all activity to occur on the Ethereum main chain, however the construction would be to bond trading activity in the public Ethereum chain with contract execution input being provided by the OMG chain.

We are building a blockchain which hooks into other blockchains to allow for trading across token/asset classes, largely backed by Ether. From the perspective of any individual chain, we are building a scalable blockchain whose contract state is bonded by the activities of the OMG chain itself. Activity on other chains can interlink with this chain via inter-chain committed proofs similar (but constructed differently) to BTC Relay[9] on the OMG chain which can be submitted on Ethereum. The OMG chain validates the activity of the behavior of all participants (including activity on other chains). In other words, the role

Archived copy · cryp2nova.com

of the OMG token is providing computation and enforcement. The token itself acts as a bond for its activity on this blockchain, improper activity results in the token/bond being burned on the OMG chain. By creating a custom chain with deep enforcement, we are able to construct a system where consensus rules optimize for high-performant activity.

The design optimizes for rapid execution and clearing, with slower settlement. Future iterations may include sharding of the OMG chain, but the initial iteration will presume high-throughput capacity for block propagation.

Owning OMG tokens buys the right to validate this blockchain, within its consensus rules. Transaction fees on the network including (but not limited to) payment, interchange, trading, and clearinghouse use, are given to non-faulty validators who enforce bonded contract states.

The token will have value derived from the fees derived from this network, with the obligation/cost of providing validation to its users. This token must have value, to prevent low-cost attacks and is necessary to enforce this network.

It may be on our roadmap to allow for delegating validation to third-parties, whereby a limited amount can be slashed at a time before re-delegation is required (the exact mechanism is not yet specified for security modeling).

As this will be designed as a high-performant system, an linked-via-proof blockchain construction is necessary. We expect that this system will be able to handle extremely high volumes of transactions and hence, will only do final delivery over Ethereum. Clearing and settlement occurs over the OmiseGO blockchain. Consensus rules are enforced via this proof-of-stake network. As part of the consensus rules of this network, it is required that all OMG (Omise GO) validators also run the Ethereum network to validate in parallel, resulting in Ethereum as a first-class citizen with regards to inter-blockchain validation.

It is assumed for features such as Ethereum/ERC-20 bonding and withdrawals that BLS signature schemes (or alternatively Schnorr) will be enabled in Ethereum in the near future. For cryptocurrencies, these tokens are non-custodial and instead locked in smart contracts (unlike other exchange platforms such as Ripple, which requires trusted gateways representing the underlying). It also does not rely on named centralized validation sets (e.g. Ripple).

The OMG blockchain manages matching and managing order execution on the Ethereum chain. Activity on the OMG ensures the validator activity also may be enforced on the Ethereum chain via native Ethereum smart contracts. For Bitcoin and Bitcoin-like systems, we allow for trading via a clearinghouse network on the Lightning Network. The blockchain enforces activity on this network via committed proofs. While not as robust as Ethereum's network, it allows for near-instantaneous clearing and settlement of activity orchestrated on the OMG chain without full-node validation. We expect to do partial validation in the future for nodes which do not allow for blockchain reorgs; naive SPV validation with blockchains that support reorgs are not permitted on this network for security.

A detailed description of the consensus mechanism and security properties will be provided by Joseph Poon of Exonumia Labs, Inc in a (currently in-progress) forthcoming paper

Archived copy · cryp2nova.com

in Summer 2017. The construction of the paper (and subsequently with the implementation used by OmiseGO) will likely be useful for many future open source token protocol blockchain projects, and may provide novel constructions for emerging chains such as creating incentives for distributed data processing, and inter-blockchain financial activity. We hope OmiseGO and its distributed exchange will be a critical core in helping to lead the way in providing base-layer technologies/infrastructure which can spark and launch the entire protocol token ecosystem. Initial versions of OmiseGO may use aspects of Tendermint consensus.

3.1 Light Client Validation

While OmiseGO is constructed as a high-performance network capable of handling many transactions, it will become necessary to produce light client proofs for partial validation, as well as for external smart contract enforcement.

A merkle tree of committed transactions per block will be included, as well as a commitment to the recent block state. The current state can be acquired by any node by downloading the recent block state commitment and any blocks between then.

As the recent block state includes a tree of the recent state, clients are able to get a view of the recent commitment without downloading the entire chain. Note that this is only possible as there is sufficient economic incentive against reorganization and halting attacks; the OMG chain is designed to heavily disincentive block reorgs via bonded proofs, but does not provide guarantees around the need for block confirmations. Similar to current SPV Bitcoin validation implementations, there is some trust given to fullnodes with regards to censorship risk; we do not expect committed bloom maps to be feasible for the decentralized exchange given the transaction volume. Light clients can validate that a sufficient number of validators have processed the transactions, as well as any partial data acquired from fullnodes. It is heavily recommended for clients to validate activity on the Ethereum chain as well, due the OMG chain smart contract constructions.

CRYP2NOVA

4 eWallets

While OmiseGO supports payments, is not designed first and foremost a payment processor within a specific eWallet payment providers (EPP). It is our belief that there is no coordination problem within a single EPP, and the coordination problem lies primarily between EPPs. However, due to the need for transactions between EPPs, payment activity may be conducted over a blockchain. This blockchain allows for the EPP to provide token issuance on OmiseGO. This allows for fiat-denominated currencies backed by fiat on the platform, or for any asset class (such as loyalty points). OmiseGO is an open system allowing for anyone to issue assets, but it is up to individual users (or EPPs acting on behalf of the users) to ensure correct issuance/auditing. This is achieved by creating issuance attached to a script (with private keys) which allows for issuance. An alternative approach would

Archived copy · cryp2nova.com

be to issue ERC-20 tokens on Ethereum, lock them up in a smart contract and handle on OmiseGO chain - similar approach to what one would do to handle existing ERC-20 tokens on OmiseGO chain (REP, GNT etc.).

In the default configuration, it is presumed that an EPP holds funds directly on behalf of its users for ease-of-use. This is similar to full-custodian cryptocurrency wallets such as Coinbase or many centralized exchanges today. This allows for the EPP to construct fee-free transactions within their own network, as it doesn't result in blockchain activity. However, it may also be possible to withdraw directly from the EPP and transact their issued token (e.g. fiat currency) on the OmiseGO chain (but transfers may result in on-chain fees if not transferred within an EPPs custodial account on-chain). This allows for decentralized transfers, as well as serving the needs of some EPPs which need zero-fee transactions on their own network. The EPP may provide software which is centralized similar to many hosted cryptocurrency wallets, which significantly reduces deployment time, and only payments crossing networks is hosted on the EPP's infrastructure. Third parties may also in the future develop decentralized wallets which can hold EPP balances on-chain.

By building an eWallet platform as part of the blockchain, it will be possible to directly exchange fiat-backed tokens with decentralized currencies and protocol tokens on the OMG blockchain.

4.1 eWallet Compliance

Transfer restrictions requiring a certificate from the issuer of the token may be allowed for issued tokens (not decentralized cryptocurrencies) depending upon issuer policy. An EPP may require KYC validation before signing a certificate. Restrictions include limitations of transfers only to certificate holders and flow control (limitation of transfers per account in flow and maximum account balance for that particular issued token). This does not apply to tokens which do not flag these restrictions, nor decentralized crytpocurrencies. It is the responsibility of each EPP to ensure licensing and compliance with their issued token.

5 Decentralized Exchange

The central component for an eWallet interchange platform is a decentralized exchange. While this supports issued tokens from EPPs, it also supports trading between decentralized cryptocurrencies.

A decentralized exchange may be ideal for eWallet interchange, as they may have different underlying representations of value, and even when transacting with the same underlying, there's different counterparty risk and costs. eWallet A is different from eWallet B's, even if they are backed by the same thing. For that reason, a liquid market is necessary for proper market operation (even if the exchange rate differences are miniscule).

The decentralized exchange will initially use a batch-auction construction where every round exchange matching occurs. It is possible to buy into particular rounds (block-heights),

Archived copy · cryp2nova.com

or to leave open orders on rounds until the order is filled. A batch auction allows for orders to be placed and execution happens at once at a specific interval. This construction allows for higher assurance and performance over a decentralized network. Orders may be left on the orderbook, but execution can happen quick enough to be comparable to EMV card terminals (requires more research with the consensus mechanism). In the event there is insufficient speed for particular use cases, EPPs are responsible for holding balances of other EPPs they wish to support for fast transactions (they may charge a higehr spread), this can be used for things like small everyday purchases and larger value purchases are via the Decentralized Exchange.

While it is desirable to be able to perform low-latency high-frequency order execution, there are significant impediments to doing so in a decentralized network. It is a necessary function of order matching that execution is occurs at a single point. Without execution where an order occurs with a single "engine", it opens the possibility to either sybil attacks or trust in a single party. If one can make an order and have execution occur at many places, then no real order commitment has occurred – one can easily sybil the network and pretend to self-execute. Additionally, with untrusted execution venues, it's not possible to create a ticker for use externally with smart contracts – a necessary function of this network. The purpose of this network is designed with the goal of being the preeminent high-value exchange and settlement platform (not a high-volume low-value network).

An alternative which allows for fast execution with low-latency would be allowing for external centralized venues, however, this establishes trust in execution on a single entity. As trading liquidity naturally centralizes (far stronger than payment centralization), there are significant trust/coordination problems, which end up looking like current cryptocurrency exchanges (with the only difference being that it is non-custodial). This construction, however, does not resolve significant coordination problems around participants needing to resolve a coordination issue around not wanting to trade on a single trusted vendor. The goal of OmiseGO's decentralized exchange is to have transparent, known execution behavior. We believe that trusted non-custodial execution is a credible option as a complement to a decentralized execution engine and OmiseGO may support these platforms in the future as well. A mature decentralized exchange has the benefit over a non-custodial trusted execution environment of being able to use it as a decentralized oracle for smart contracts.

This decentralized exchange is designed to be high-performant where orders are propagated over the proof-of-stake network. When sufficient participants have the order with block confirmations, the order is then placed on the order book. The order book for a particular batch-execution point is a running tally of all orders which do not execute until the batch-execution point (so there are orders which are matched on the book). The initial configuration includes transparent orders, but it is possible to do a fauxcoin-like construction whereby blinded orders are placed, then no more orders are accepted, the blinding keys are released by the participants who placed orders, and finally execution occurs after a set time. Initial versions will use a fully transparent system (which a batch-execution format mitigates some amount of adversarial behavior).

Archived copy · cryp2nova.com

The result is a system where trade execution occurs on a single "engine", namely that of a proof-of-stake decentralized exchange, but with the assurance that the rules of execution is transparent and verifiable.

5.1 Ethereum Trading

As OMG requires fullnode validation of the public Ethereum blockchain for maximum efficiency and security, it's possible to create a contract on the Ethereum blockchain which locks up funds dependent upon the condition of the OMG chain. These funds are now bonded and locked and its activity is enforced by the OMG chain. When an order executes, a proof is provided to unlock the funds on the Ethereum side.

This construction presumes that Schnorr or BLS signatures will be available on Ethereum in the near future. A transaction tracks the activity of the OMG chain, and needs some level of maturity confirmations before payment is delivered on the Ethereum chain. Funds can still be settled on OMG and balances updated for continued trading, it is only for final delivery when the payment occurs on Ethereum. The behavior of the OMG chain enforces the behavior of payments on the Ethereum chain. In an non-adversarial environment, a Lightning-like construction is available where a user can provide a payment directly without proof, and if the payment is not disputed after a certain amount of block maturity, is paid out without needing blockchain proof/computation. In the event the payment does not match the state in the OMG chain, anyone can provide proof and the sender's balance would be slashed. This allows for greater computational and bandwidth efficiency on the Ethereum chain.

This construction on the OMG chain is for trading Ethereum, Ethereum-like chains, and Ethereum issued tokens similar to ERC-20 using bonded smart contracts.

5.2 Comparison With Other Works

Trade is a fundamental aspect of financial activity. It is to no surprise that there have been other efforts to build a cryptocurrency exchange structure.

Centralized full-custody cryptocurrency exchanges such as Poloniex are high-performant, but relies upon the trust of a single party to hold custody responsibly, and execute orders honestly.

Networks such as Ripple (XRP) rely upon trusted named validators to reach consensus, which game theoretically converge on an unchangable set. Additionally, Ripple's trading functionality relies upon trading issued assets on its own platform (with significant issues related to custody selection), the decentralized exchange cannot trade Ether or Bitcoin without creating an issued gateway.

Many decentralized exchange platforms using EVM smart-contracts rely upon either doing things directly on-chain (which forces everything on the Ethereum network and does not permit cross-blockchain activity), or they do things off-chain without a single execution

Archived copy · cryp2nova.com

engine. The OMG chain is designed to operate trading across chains (e.g. ETH-BTC) without using full-custody issued assets for native cryptocurrencies.

Emerging networks may also provide designs related to Decentralized Exchange, e.g. Cosmos. As these networks are not yet fully deployed, we cannot properly evaluate or compare the differences.

5.3 Bitcoin Clearinghouse

For Bitcoin and Bitcoin-like systems, on the other hand, it is possible to create a system where trading BTC and other similar blockchains are possible as well using assets bonded external to the system with clearinghouses.

Essentially, this construction allows for the clearinghouse to operate as an oracle[10] with activity bonded and enforced by the OMG chain to enable decentralized exchange with Bitcoin-like blockchains. This builds upon the work by Tier Nolan[11] to conduct rapid decentralized exchange based on an external exchange execution engine.

Clearinghouses are used to ensure that payments occur on the Bitcoin blockchain. We use clearinghouses instead of SPV proofs, to prevent adversarial incentives by Bitcoin miners to generate blocks which are incompatible with consensus but valid with SPV proofs in order to attack external systems (reorg attacks on one's own chain is costly, but external attacks are cheap).

For Bitcoin-like systems this system requires either a malleability fix (e.g. segregated witness) OR a combination of P2SH/BIP-66/CLTV/CSV available on only transparent addresses.

Clearinghouses are necessary as it's not currently possible for complex enforcement of contract state in Bitcoin. These clearinghouses are responsible for disclosing activity on the Bitcoin (or Bitcoin-like) chain by generating preimages and hashes. The hashes are committed to activity which the clearinghouse is responsible for, and are bonded. If they release incorrect preimages or refuse to disclose preimages to the OMG chain, anyone can provide proof of malfeasance and the clearinghouse gets slashed.

Note that this requires the clearinghouse to have funds available on the Bitcoin side, as well as funds available for bonding on the OMG chain. For the bonded amount, this only persists until the funds can be cleared and settled on the Bitcoin side, so ideally doesn't require extreme amount of funds.

Clearinghouses operate a Lightning channel, but they hold not only funds on their side in the channel, but a multiple of expected fund flows on the OMG chain held in ETH (e.g. 3x for what fund flows they are responsible for to account for exchange rate fluctuations).

Archived copy · cryp2nova.com

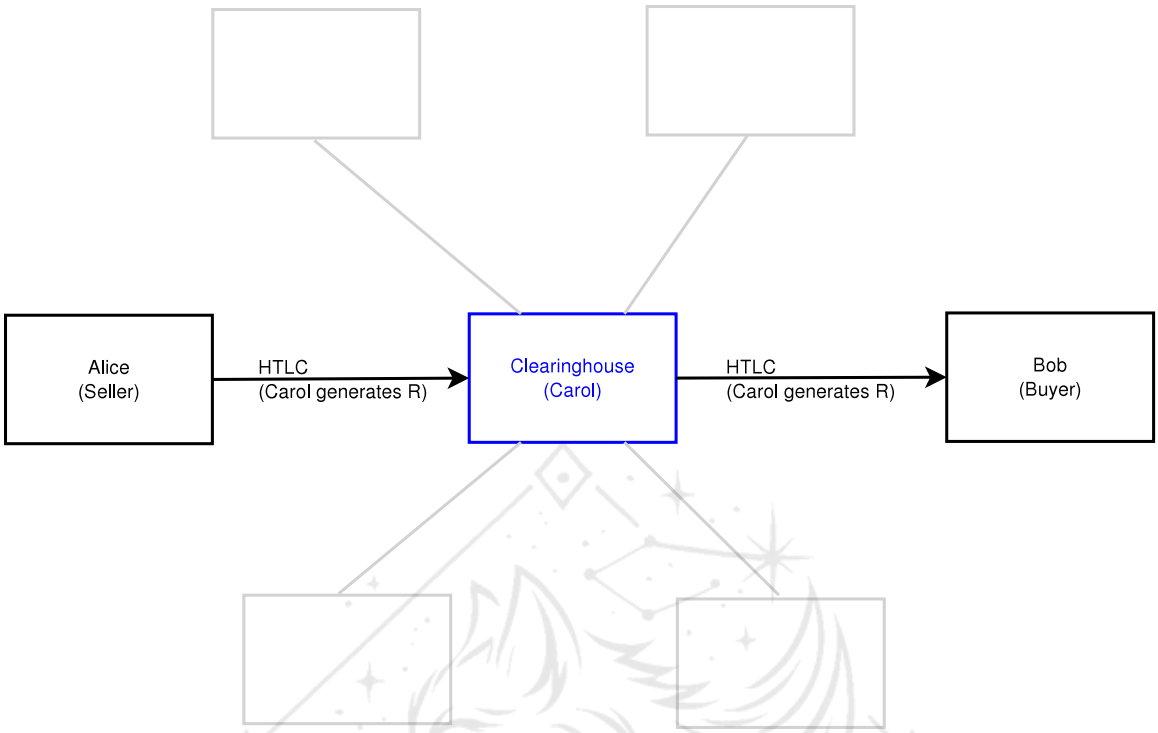


Figure 1: Alice and Bob have a Lightning Network channel with Carol the Clearinghouse on the Bitcoin blockchain. The payment preimage R is generated by Carol and release of the preimage is enforced by bonded commitments on the OmiseGO chain.

Presume Alice wishes to sell Bitcoin and Bob wishes to buy Bitcoin and they both have channels open with Carol the Clearinghouse. All 3 are on the OMG chain, and designate Carol as an acceptable clearinghouse intermediary. Note that transfers may occur over multiple clearinghouses if both parties designate it as acceptable, and that trades may only occur with an intersection of acceptable clearinghouses between trading participants.

Carol the Clearinghouse locks up funds in Ethereum in a smart contract determined by the consensus rules of the OMG chain and the Smart Contract. Carol provides a signed proof that particular hashes H (which were generated by Carol's preimages R which at this point in time only Carol knows). She provides the hashes H, with a corresponding value in BTC she is responsible for, and a signature. This can be used as a proof on the OMG chain (and the Ethereum Smart Contract in case Carol is faulty)[12].

When Alice wants to sell Bitcoin, she creates an HTLC payment contingent upon release of an H value that Carol provided. Similarly, when Bob wants to receive Bitcoin Carol sends an HTLC contingent upon release of an H value that Carol provided to Bob.

These H values are associated on the OMG chain with particular people, and the funds are now available to execute on the decentralized exchange.

When a trade executes on the OMG decentralized exchange, e.g. Alice sells BTC for ETH and Bob buys BTC for ETH, the trade is now cleared on the OMG chain. Everyone now has the responsibility and obligation to execute the trade.

Archived copy · cryp2nova.com

It is the responsibility for Carol to release the R preimages for the relevant H which Alice and Bob execute the trade onto the OMG chain. Bob can use this information to pull the funds on the Bitcoin chain, and Carol now has the right to pull the funds from Alice.

If Carol refuses to release the R preimages within the relevant amount of time to the OMG chain, her funds are slashed and the ETH is delieverd to Alice and/or Bob (with the penalties to mitigate exchange rate fluctuations and as a disincentive for Carol from acting faulty).

If Carol incorrectly releases R values she should not have, then a proof can be provided to the OMG chain by any party and Carol is penalized and funds given to the party which has the clearinghouse exchange contract locked with the H value.

Clearinghouses may not need to be directly connected to participants (Alice, Bob), they can pay over a routed network, hence they can maximize capital efficiency.

The clearinghouse is able to charge a fee for use of their clearinghouse for all activity.

There is some trust in the clearinghouse in being able to make payments, but there is trust-minimization in their activity (as their activity is bonded on the OMG chain).

Side note, this construction is also useful for rapid expiration of HTLCs via externalized bonding, and can be a way to construct payments with incredibly rapid timeout expiration measured in minutes. It doesn't require the clearinghouse to lock up bitcoin, only to have bonded release of information enforced by the clearinghouse. Further explanation of this construction forthcoming in a separate paper.

Note that this is only possible since the OMG chain heavily discourages reorgs.

The end-result is the ability to have a decentralized exchange outside Bitcoin. We believe this is a novel construction, as the activity of a participant on the Bitcoin network is enforced by an external decentralized exchange via a clearinghouse operated on Bitcoin with economic incentives, and that enforced release of preimages via external conditions allow for Bitcoin to be used for trade in protocol token blockchains.

5.4 Smart Contract Data Feed

A VWAP of recent trade executions is computed and published periodically on the OMG blockchain as a consensus rule.

This allows external contracts to use merkle-tree SPV proofs of trade execution prices and volume, hopefully creating greater viability in smart contracts.

Archived copy · cryp2nova.com

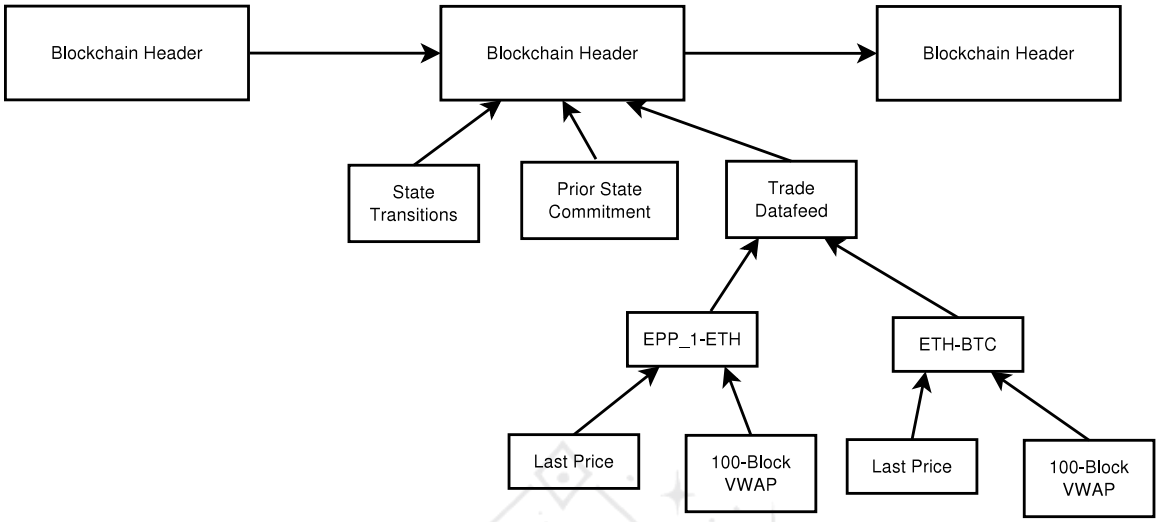


Figure 2: Periodic commitments to the datafeed will exist in the OmiseGO blockchain. This allows for external validation via merkle root commitments in the blockchain header. The trade datafeed includes popular exchange pairs with the last trade price, volume, and various VWAP conditions (various times and/or blockheights).

A primary function of any exchange is not only managing the orderbook and executions, but having a feed for use with 3rd party systems. It allows for 3rd party systems to be able to use this information and for participants to net out activity on a single venue. As the basis for a exchange-rate/pricing mechanism is necessary for all manner of (smart) contracts, access to this system allows for participants in these external contracts using the exchange as a data feed to have greater assurance and transparency in execution. This allows for participants in contracts to create contracts with knowledge of the behavior and access to the decentralized exchange. If participants use the price oracle feed on the OmiseGO chain as the basis for pricing on smart contracts, they can have greater assurance of execution by placing orders on the OMG chain, this creates significant network effects of the OMG chain with greater adoption of smart contracts.

6 Lightning Liquidity Provider

There is a fundamental concern around centralization pressures around the network effects of capital liquidity. Many are concerned that the Lightning Network allows for the potential to centralize around a handful of nodes which allows for rent extraction. Lightning Network is designed to avoid this type of rent extraction for nodes with a great deal of liquidity, however, there is some optimal benefit of having well connected nodes.

It is possible to construct mechanisms similar to the clearinghouse in the section above whereby a node can bond up activity on the OMG chain, and the OMG chain can act as a single Lightning hub with a great deal of liquidity.

For ETH and ETH-like channels, this is possible to lock it up in smart contracts directly.

Archived copy · cryp2nova.com

For BTC-based channels, this is possible, but channel participant activity is enforced by ETH-backed bonds on the OMG chain. Payments get sent into a participant on the OMG chain, and outgoing activity is enforced via commitments on this chain.

Limitations are necessary before OMG platform maturity in order to prevent too much capital being allocated into this system. This allows for the creation of a giant liquidity pool, which incentivize fund availability for clearinghouses and the decentralized exchange.

7 Economic Implications for OmiseGO Tokens

Transaction fees are native to the OmiseGO chain. The validators earn fees from validating the activity of this blockchain.

Payments and interchange fees are used to pay for activity on this network and to incentivize honest activity.

Bonding has a cost, those who bond on behalf of others on this network will likely charge fees, e.g. clearinghouses.

8 Limitations

This network is an open network, it is necessary for accurate trading activity to require activity on the decentralized exchange to eventually be public, even with blinded commitments/bids. While new cryptography is possible via SNARKS, it is currently too slow and resource intensive for a high-volume trading network. We are currently optimizing for performance and speed. Since this is a pseudonymous network natively (with optional AML/KYC constructions for issued tokens).

SPV validation of other chains is presumed to be insecure with blockchains that do not discourage reorganizations. For chains which allow reorgs, either full-node validation of that chain is required or an HTLC-clearinghouse construction is needed. It presumes that Ethereum will create greater reliability and guarantees around finality (current Proof-of-Stake research).

These technologies are new and not yet tested. While we will do our best to construct it with maximum security in an adversarial setting, we are modeling the security model of these mechanisms which require real-world use case with human behavior to properly understand. When interaction between chains, it is difficult to roll-back errors, one should only put the minimum necessary to transact at a time on this chain when doing significant decentralized cross-blockchain activities. Initial versions may have less robustness in adversarial settings, and we recommend lower values at stake, as often times attacks (especially Denial of Service attacks) are resolved over time as the software develops. Performance and real-world behavior implications of the design is not yet clear.

It is not yet clear what the long-term value participants of this network can derive, and may be affected by competition in this space, there are no guarantees provided by

Archived copy · cryp2nova.com

participating as a validator, as this is an area which is still being technically explored in this space.

The total value of cleared transfers (but not yet settled) at any one time must be below the total bonded value of the validators. It is possible to bond an additional amount, but may not be necessary if the total value of the token is sufficiently high. Further modeling is necessary of enforcement mechanisms inherent to the system.

Execution of this vision is ultimately the responsibility of the OmiseGO team, the authors not part of the OmiseGO team are principally only responsible for providing technical guidelines and the architecture.

9 Conclusion

With the emerging popularity of eWallet platforms, siloed networks are becoming a problem. This creates a unique opportunity for fiat tokens to interchange across a decentralized network, along with cross compatibility with cryptocurrencies.

In order to build this decentralized interchange network, it requires not only a blockchain well-suited for payments and interchange of issued tokens, but also a decentralized exchange which supports these activities, as well as incentives around creating well-functioning liquidity pools.

Eventually, these issued tokens may asymptotically get closer and closer to full decentralization (including user-owned keys) which maximizes agency of the individual. This can be achieved by creating not only transparency in the business process of payment interchange, but also removing the ownership of the business process itself from a single trusted entity. OmiseGO allows for stakeholders, from individuals to issuers, to have significantly greater assurance in the financial mechanisms of society.

10 Acknowledgements

Thanks to Piotr Dobaczewski for contributions to this paper, as well as Rick Dudley and Vitalik Buterin for input and feedback.

11 Licence

This document is licensed Apache 2.0.

References

[1] Fred Erhsam. Blockchain Tokens and the dawn of the Decentralized Business Model. https://blog.coinbase.com/app-coins-and-the-dawn-of-the-decentralized-business-model-8b8c951e734f.

Archived copy · cryp2nova.com

[2] Fred Erhsam. Tokens, Why How. https://www.youtube.com/watch?v=rktHO5R8Y9c.

[3] Ethereum. Ethereum. https://ethereum.org.

[4] Gavin Wood. ETHEREUM: A SECURE DECENTRALISED GENERALISED TRANSACTION LEDGER. http://szabo.best.vwh.net/formalize.html, Feb 2015.

[5] Nick Szabo. Formalizing and Securing Relationships on Public Networks. http://szabo.best.vwh.net/formalize.html, Sep 1997.

[6] Joseph Poon and Tadge Dryja. Lightning Network. https://lightning.network/lightning-network-paper.pdf, Mar 2015.

[7] Satoshi Nakamoto. Bitcoin: A Peer-to-peer Electronic Cash System. https://bitcoin.org/bitcoin.pdf, Oct 2008.

[8] Raiden. Raiden Network. https://raiden.network/.

[9] Joseph Chow. BTC Relay. http://btcrelay.org/.

[10] Bitcoin Wiki. Using external state. https://en.bitcoin.it/wiki/Contract#Example_4:_Using_external_state.

[11] Tier Nolan. Re: Alt chains and atomic transfers. https://bitcointalk.org/index.php?topic=193281.msg2224949#msg2224949.

[12] Ilja Gerhardt and Timo Hanke. Homomorphic Payment Addresses and the Pay-to-Contract Protocol. http://arxiv.org/abs/1212.3257, Dec 2012.

CRYP2NOVA

Archived copy · cryp2nova.com