RaidenX Yellow Paper

Off-blockchain token trading

Introduction

This yellow paper describes in more detail the technical aspects of RaidenX. It specifically addresses architecture of the features of RaidenX in the use case of it's account state-channels as a centralized order book management system, or trading exchange.

Abstract

Blockchain technology has made possible revolutionary and disruptive new interrelationships in the management and distribution of financial data. The consequential demand for the ability to trade new crypto-assets has created an industry based on centralized crypto-exchanges. These services have faced tremendous challenges in account security due to the nature of blockchain technology and the strict internal security of Decentralized Applications. The track record of this industry is infamous, and the resulting losses trending into the hundreds of millions of USD worth of crypto-currency.

RaidenX is an approach to alleviating the accounts risk of a centralized exchange through restricted multi-signature accounts made possible by off-chain state channels using smart contracts. This limited co-operation between the trading service and the user removes the risk of the service through restrictions on its authority over the account, by limiting the service keyholder authority on the account to merely matching signed market orders.

This is a powerful solution to an industry and segment of the blockchain ecosystem which will only see increasing demand as the volume and variance in the types of financial assets

being offered and tracked using blockchains will only increase as further innovations and market inroads are made.

Foundation

Core blockchain
With Bitcoin, for the first time a new and revolutionary approach to the problem of centralized control over, and access to, information was created. By combining public key cryptography with an accounts and value system, economic incentives could add the missing security link in closing the loop to eliminating the need for centralized control.

Given the need for a value store in the creation of a Decentralized Application to manage a blockchain, and that the greatest benefit of any new information management system is in the management of financial data, DApps are therefore naturally best fitted to manage the financial data of an economic or financial system.

The values stored within the blockchain ledgers are operated on through strict adherence to the protocol which support for all basic financial account interactions. As such all manner of financial assets and relationships are able to be represented in a blockchain. The leading use case being in new “crypto-currencies”.

It is these new types of relationships through decentralized distribution and restriction of access to the transfer of value measure in the secure blockchain state of the system which can be leveraged to further improve services developed for blockchains.

Embedded Value Tokens
After the advent of blockchain technology and DApps, innovators and developers sought new ways to use the technology. Along with experimentation on different consensus algorithms and transactions protocols during the “alt-chain” boom, an innovative way of tracking arbitrary values within a host blockchain was developed by the Mastercoin project.

With Mastercoin the first commonly understood “token” was created in the Bitcoin blockchain and the ICO concept was given form. Many other projects and tokens have been creating in as ever increasing use of the method of arbitrary value tracking within the notarization system of a decentralized application continued to gain momentum.

Smart Contracts
Blockchain accounts can also have logic attached to their execution. This allows for the arbitrary definition of conditions to the execution of the transaction, creating in essence a financial contract. When combined with the arbitrary value measures of embedded tokens, these smart contracts [r] could be used to represent any type of financial asset or relationship.

As such the demand for a flexible and standardized way of providing so called “turing complete” conditions to transaction execution led to the development of a DApp protocol to specifically support this: Ethereum. This approach more easily facilitated the publishing of

smart contracts in blockchains, and it's success has led to the explosion of token values embedded into the main Ethereum blockchain, as well as many competing projects offering similar function (references).

Together, the core blockchain technology as extended by both embedded tokens and contract logic make new types of financial relationships and account operations to be automated in ways previously not possible. This new type of management is enabled further in the functioning of services for blockchain technology in the latest application of blockchain technology.

Off-Chain Transactions

With development of tokens and smart contracts all manner of assets were definable in the blockchain ledger, but DApps have limitations. Security and integrity of the blockchain is paramount, and the primary function of a blockchain network. This is not well suited to the expected functions of traditional financial services which have been operated with the ease and benefit (and risks) of a centralized service to this point.

However, as mentioned the unique security challenges and risks when applied to blockchain technology created intolerable amounts of risk. It is interesting to note this unique ability of decentralized applications to prevent externalization of system risk, is what creates many challenges for existing business and financial models to coexist with blockchain technology..

However, another feature offered by blockchain technology is the ability to operate on a transaction before it has been published to the blockchain. Conceptually so called "off-chain" transaction management and manipulation has been well known of and even possible for quite a while, beginning with Bitcoin's support for "transaction mutability" and "transaction chaining" [r].

Transaction Mutability
Beginning with Bitcoin, the vast majority of Decentralized Application protocols have supported transaction mutability. This serves a technical purpose, as specific transaction aspects (such as the final transaction ID), can not be determined until the actual validation, reconciliation, and publication of the transaction in the main blockchain ledger by the authoritative validator.

The ability of transactions to be mutated before they are reconciled in the blockchain enables enormous flexibility and "chaining" of transactions. This functionality is a means to add additional functionality to blockchain transactions in managing its "state" prior to validation and publication by the main blockchain network.

State Channels
Using transaction mutability in order to maintain an running mutated state of a transaction "off chain" is referred to as a state channel. This transaction and associated rules logic or smart contract governing its operation, is able to be defined and operated on by parties in

the continuing adjustment of the state of the transaction, prior to its publishing to the main blockchain network, and it's reconciliation in the blockchain.

These state-channels can be used for several different types of transactional relationships as needed in order to gain the value and speed of centralized systems of high speed sub networks.

Raiden

Raiden is a cutting edge recently released and funded project which aims to provide a suite of core tools to use in creating state-channels using off-chain transaction "mutations". These changes to the channel off-chain are used to adjust the … balance between the two parties operating the state-channel transaction.

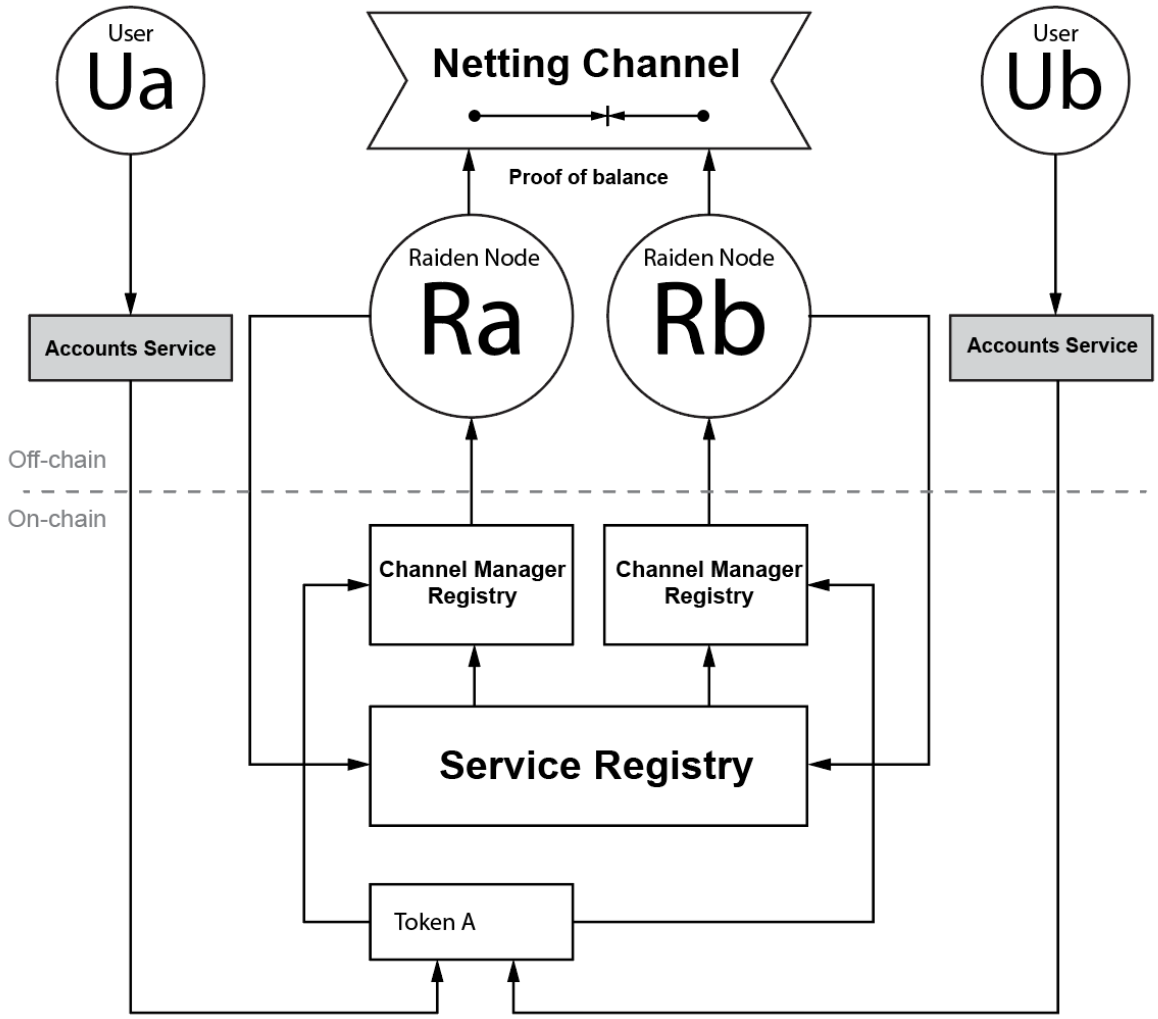
Raiden operates state-channel between delegated authoritative nodes on it's transaction network. These authorities can automatically adjust balance of funds in the channel output to the account initiators (users).

These counter-parties have been delegated authority to operate on the funds in the state-channel by the end users who have deposited funds into the channel. These state-channel managers then adjust the balances between themselves as a means to represent micro-transactions between parties using this service.

With this use case for state-channels, the intent of Raiden is to facilitate and micro-transactions between these services acting as counterparties to micro transactions. This allows for automatic transaction initiation by the Raiden node without the need for user input, an important reduction in friction in the user experience in using blockchain technology for micro transactions.

Raiden supports common ERC20 type tokens [r] in its smart contracts. It also provides existing state-channel service and management software. It's existing networking functions of the Raiden payment network allow for seperate channel manager nodes to operate the micro-transaction payment channels across a network. The functions of the Raiden payment network are not crucial to the function of RaidenX.

Raiden Payment Channels



Delegation of authority over funds among entities using the Raiden "micro-transactions" state channel. Management functions are based on both the main service registry, channel manager, and netting channel smart contracts.

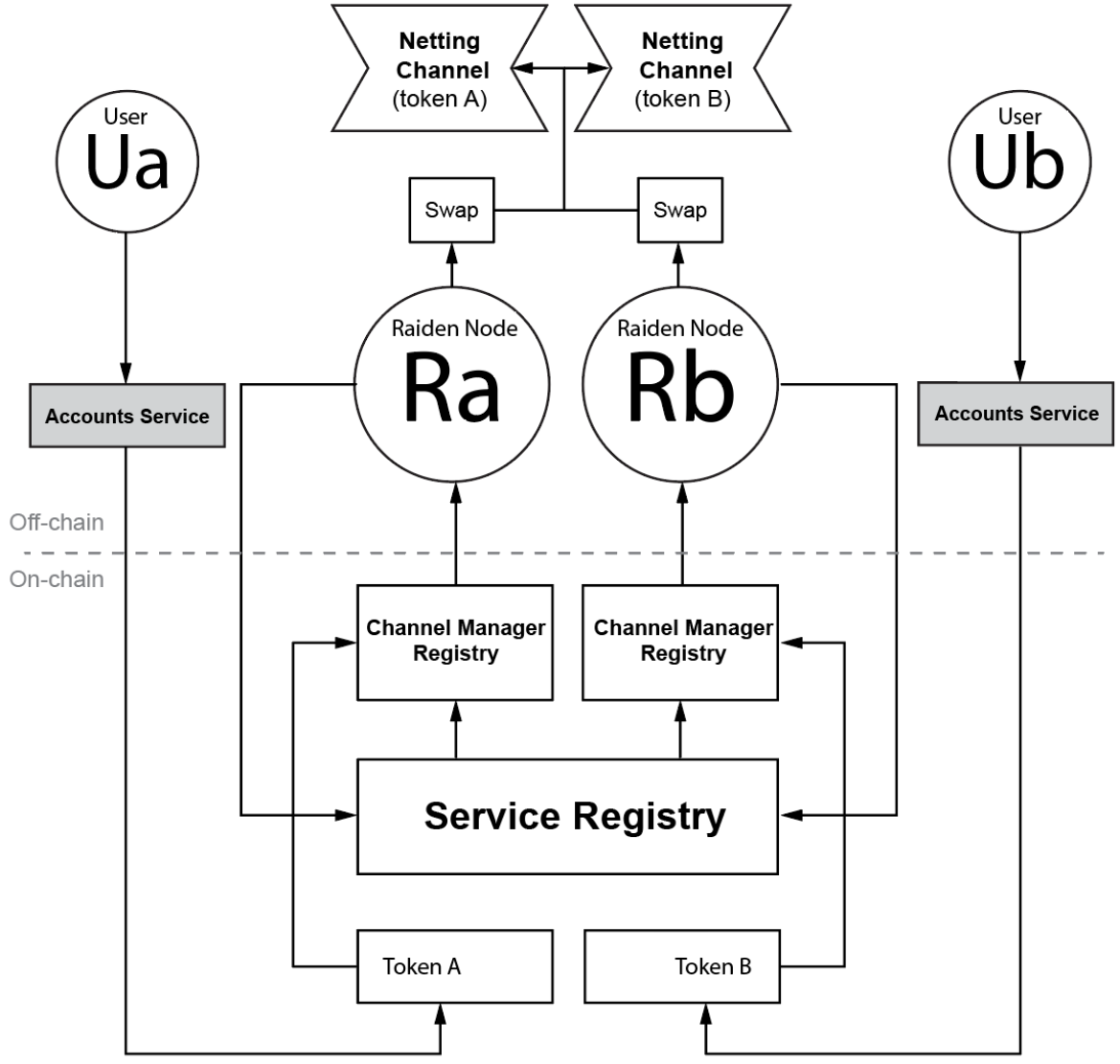
Proof Of Balance

These state channels in Raiden use the Proof of Balance to allow for verification of it's state not only by stakeholders on the account, but of course for validation and processing in the main network. The method by which state channels can provide a proof of balance is through the resulting merkle tree created through the continual hashing of the transaction state into subsequent transaction mutated states [r].

Channel Management
Raiden provides the smart contracts defining roles and operations of state channels based on the channel manager contract. Additionally core software developed by the Raiden project provides standard API access to core contract methods.

Token Swaps
With the existing payment channels Raiden also provides a rudimentary feature to allow for basic token swap. With Raiden swaps, the payment channel parties are the Raiden nodes themselves, who have full authority to execute on transactions and therefore “swaps” of value measures between channels. This authority is delegated in the same way the authority of the netting channel contract is delegated. This method of synchronized state-channel operation allows for a sequential atomic exchange for full balance of swap requests.

Raiden Token Swaps



In this case we see the raiden nodes must operate on swaps directly on the channels they control. This is a consequence of the delegation of authority of the Raiden state-channels.

Limitations
Delegating full authority over the state channel to nodes incurs some risk over the funds in the state channel. In the instance of micro payments, only small amounts of funds are expected to be put at risk. This may be acceptable in this use case for off-chain channels, however with larger deposits and value expected to be put onto a trading exchange, this recurrence of centralized risk is not tolerable in an exchange.
Delegating full authority of state channel to nodes incurs some risk for the account. In the instance of micro payments, only small amounts of funds are expected to be put at risk. This may be acceptable in this use case for off-chain channels, however with larger deposits and value expected to be put onto a trading exchange

Other limitations as well prevent the original Raiden network as functioning as a true market:

1. Nodes have full control over state channels
2. Token swaps are controlled by Raiden nodes
3. Raiden token swaps are atomic on demand synchronization of state channels, and do not support market type “order book” management.

Cooperative Centralized Services

By combining the core blockchain functions of smart contracts and multi-signature transactions, in off-chain state channels, RaidenX offers new types of relationships between a decentralized authoritative accounts ledger, centralized services, and their users.

These cooperative centralized services are able to offer of both the benefits of blockchain technology and centralized financial services.Their restricted operational authority on the “accounts” of their users in performing only the intended pre-determined function of the service secures users funds regardless if the service security is even fully compromised [proof]. The primary function of the state-channel and off chain mutable transaction features is to allow restricted cooperative management of the account state channel by designated parties.

Not only is this important to the function of RaidenX, but certainly other financial services will be able to leverage this same approach to de-risk their own financial operations. It remains to be seen if the potential for account state channels ends up being as successful a use case of state channels as in micro-payments, certainly there is demonstrated demand for centralized exchange services.

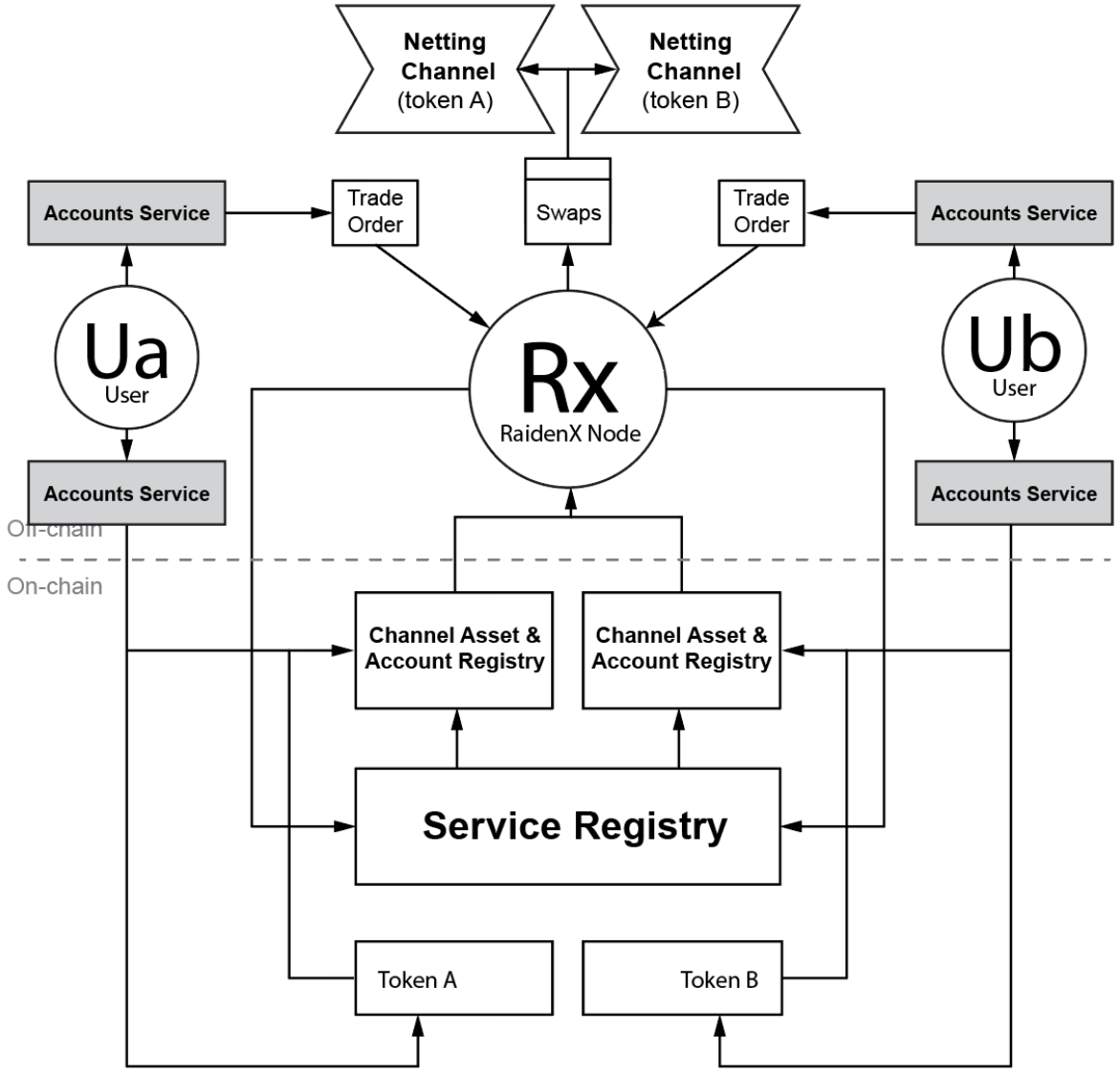
Introducing: RaidenX

With RaidenX we introduce a new use case for the Raiden state-channels. We do this to address the above limitations of Raiden in it’s support for a trading type exchange market. In this case, we modify account restrictions on the channel, as well as which parties can operate on the channel.

Instead of a channel between two nodes (“payment channel”), RaidenX operates the state channel to reprsent the state balance between an account holder and a service, hence the term “account channel”.

RaidenX makes it possible to co-operatively manage smart contracts off the blockchain with the attached conditions for the account execution of market functions written into smart contract logic itself. Designating within the blockchain registry, the service has only the restricted authority to operate on the account for these market functions.

RaidenX Account Channels and Trade Orders



Representation of fund and authority delegation and functional execution the account-channel between the trader and the RaidenX market exchange. Added user registry and signed swap orders facilitate traditional market and order book functions.

Differentiation

The fundemental difference between the two is which private keys are required to operate on the net balance of the state channel. In RaidenX, every action occuring on the account channel is initiated with the primary account holder (the RaidenX service is the “account channel service”).

On the trader’s behalf, every action on the balance of the channel is only possible through either a signed transaction on the main-net for the token asset, or as a signed message including trade order details. This signed trade order allows, as delegated to the account service by the account channel contract, allows the account service to modify account balances on the account channel only when the service has a pair of signed orders on behalf of the users.

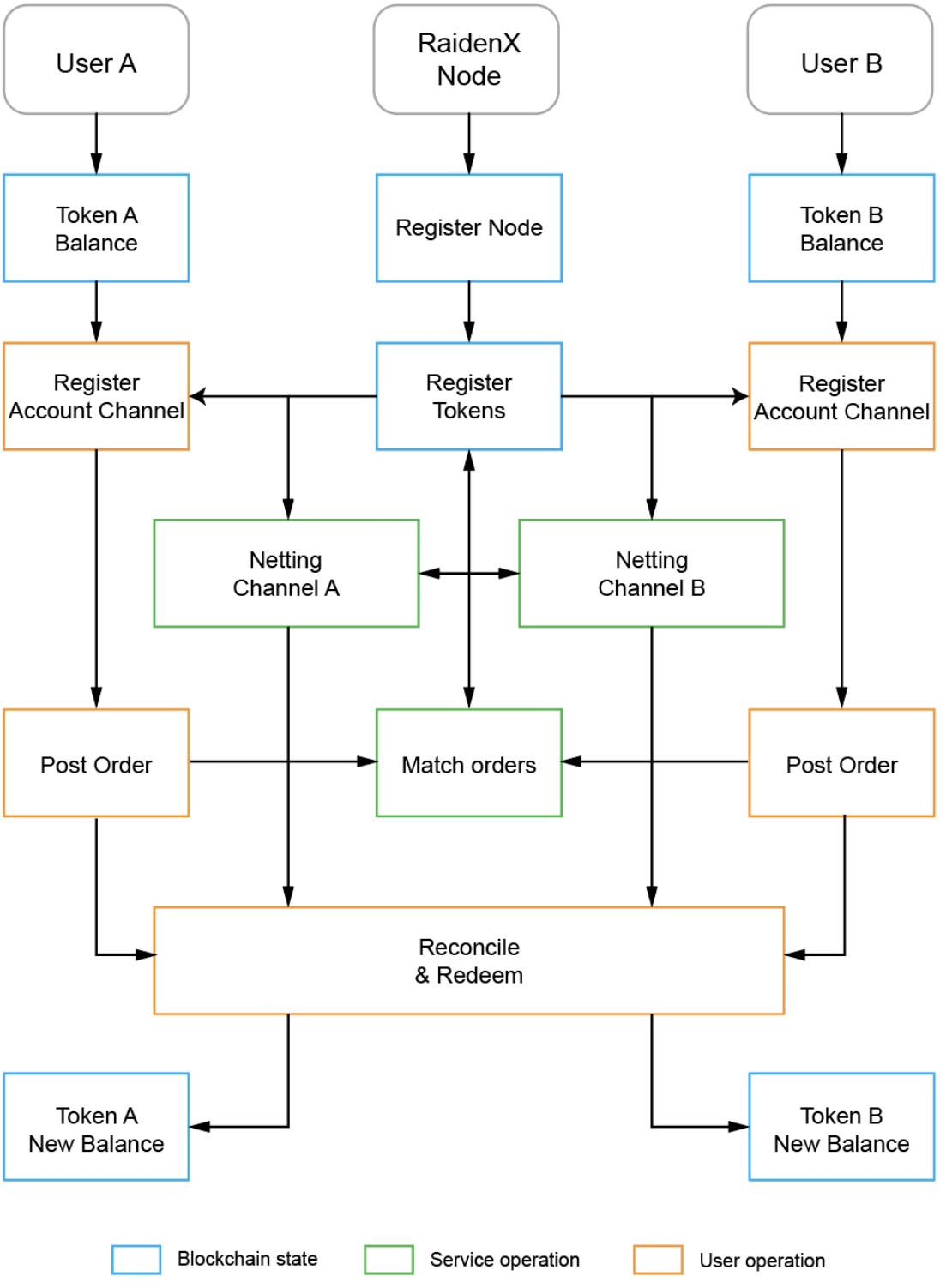
A new purpose of “state channels”. Trader “account channels”.
Instead of tracing balance of accounts between payment services raiden nodes), we make the channel.
Cooperatively manages restricted trading accounts

Market Functions

The state channel therefore manages an “account channel” which is cooperatively managed by an initiating party as “primary account holder”, and the service being requested as registering such party as an account holder on the services contract registry, referred to as “accounts service”. The accounts service is considered to be the primary channel operator, as the netting of balances withing the channel are expected to be operated on primarily by the “accounts service”.
The RaidenX approach to account channels provides all market functions in the cooperatively managed accounts with the accounts service:

Importantly it is the attempt of RaidenX to accurately represent the typical and expected functions of a trading market. This not only facilitates the value and benefits of a traditional trading market, but importantly provides a use case and potential user experience that will be a seamless transaction for traders moving from any existing legacy financial market or asset class.

RaidenX Service Functions

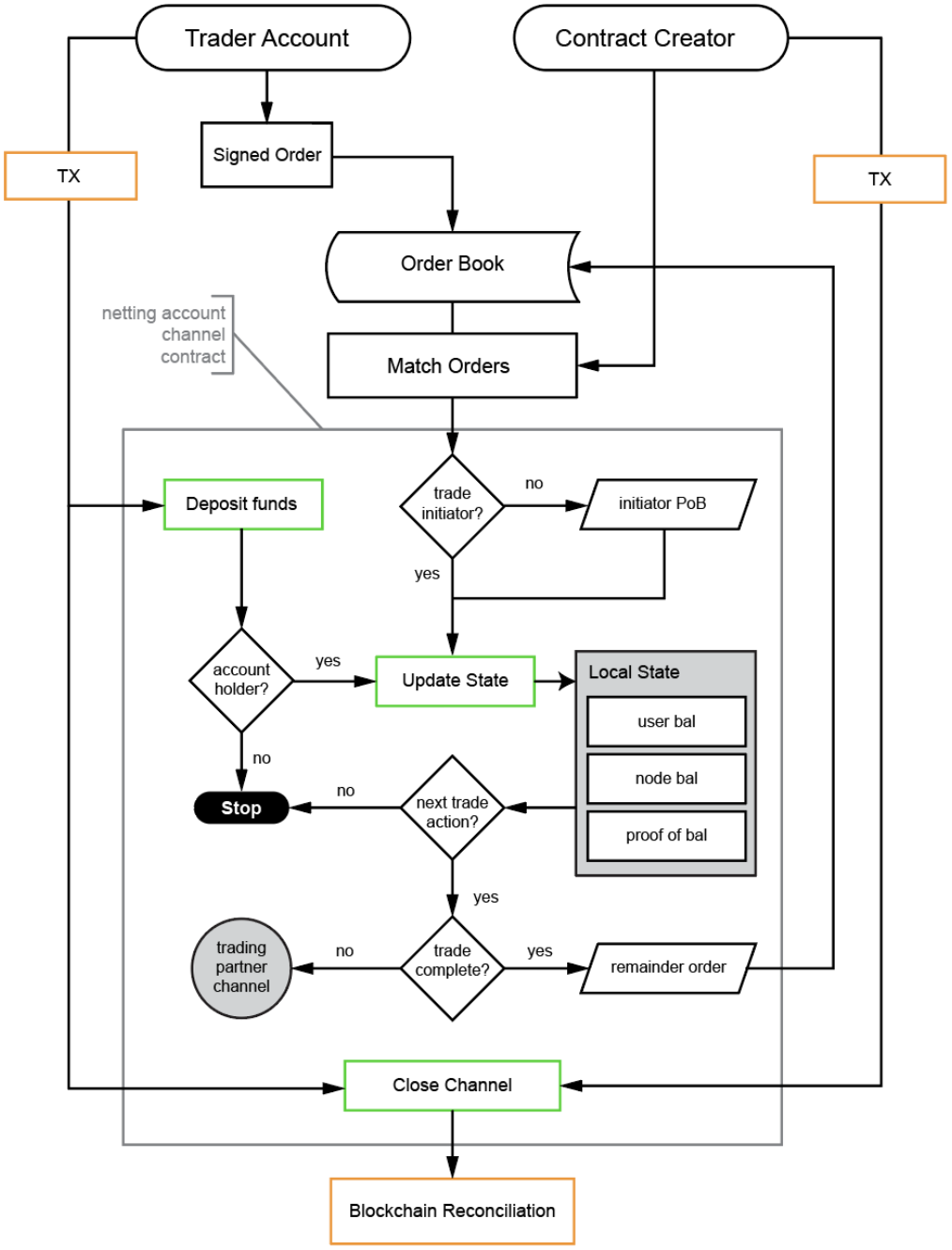


In this case the processes of the RaidenX system show processes of parties and services participating in the RaidenX trading platform. The process flow for operations and interactions on the RaidenX account state channels.

At the core of the unique function of RaidenX is the modified Raiden state channel contract. This contract applies additional restrictions on the parties operation of the channel, and

crucially, integrates the end use into the process flow for initiation of market functions. Importantly this allows for operation of accounts and making of trade orders by the users of the service remotely, directly over the internet and blockchain network.

Account Netting Channel Contract



The account netting contract functional flow chart demonstrating the channel methods. Inherent is the restriction of authority over accessing channel methods as delegated to respective key holders.

Exchange service & account channel operations schematic:
Then: The process leverages existing “swap” functions of Raiden, but modified to support the signed order triggers for channel synchronized swaps.

The contract will output back to the RaidenX node a “remainder” order in the event one of the orders remains unfilled. Therefore the trade execution method of the smart contract will accept either a signed order, OR, a previously outputted “remainder” order. This remainder order should be executed out of the channel contract to incorporate a validatable proof of previously signed order.

It is considered that for the future development of this concept into an implementable and functional technology that the appropriate designation of authority on the contract in it’s ability to output valid “remainder” orders WITHOUT the input or requirement of the traders private key should be carefully evaluated and developed with a awareness of the potential security exploits which could potentially arise. With proper account authority delegation to begin with, risks are already well averted. The remaining riskk would be whether the accounts service

Conclusion

RaidenX shows the potential for advanced usage of blockchain technology in developing lower risk account based state-channels. Explicit restriction of the account netting channel demonstrates the limited risk potential of multi-key or shared access transactions and accounts on the blockchain.

A fundemental bridge builder between financial services instustry and the blockchain industry, as well as a bridge between blockchain tracked assets.

We can show this is true, and see how many other ways of doing this will be possible.

References...