RaidenX White Paper

What it is, what it does, what it means.

Outline:

1.Introduction

Blockchain technology has become an incredibly disruptive trend[1] in financial technology. It’s combined security[2] with the resilience of it’s incentivized P2P approach, have led to large organic growth in the broader ecosystem around it. This has led to proven and sustainable markets, a growing industry and expanding technology infrastructure.

Both the technology and the industry are very much in an early stage of development and market demand has shown a strong appetite for innovation and investment opportunities in the space. The resulting state of the art technology now allows for blockchain applications to be created which were previously not possible.

A new and growing segment of the blockchain ecosystem is “off-chain” transactions[3]. These types of blockchain transactions solve the rather limited capacity of the peer-to-peer networks managing the blockchain to allow for faster processing and higher transaction volumes by using independent services operating on account balances outside of the main network through smart-contracts, with periodic reconciliation on the blockchain. Raiden[4] is a

---

[1] "How blockchains could change the world | McKinsey & Company." https://www.mckinsey.com/industries/high-tech/our-insights/how-blockchains-could-change-the-world. Accessed 28 Nov. 2017.
[2] "Blockchain Security in Cloud Computing: Use Cases ... - MDPI." 18 Aug. 2017, http://www.mdpi.com/2073-8994/9/8/164/pdf. Accessed 1 Dec. 2017.
[3] "Off-Chain Transactions - Bitcoin Wiki." 11 Jun. 2016, https://en.bitcoin.it/wiki/Off-Chain_Transactions. Accessed 28 Nov. 2017.
[4] "Raiden Network." https://raiden.network/. Accessed 28 Nov. 2017.

leading edge technology project which facilitates micro-transaction payment channels using such off-chain transactions.

RaidenX is proposed as an extension to the Raiden payment-channel[5] technology, and its experimental token swaps feature. It adds support for the processing of token exchanges through normal market functions. This application of blockchain technology will allow for crypto and token exchange services to use RaidenX as the “backend” for their trading platform. These off-chain multi-signature[6] transactions allow a service to co-dependently manage blockchain based trading accounts in coordination with their registered users, with limited authority to execute co-signed trade orders on behalf of their users.

This offers a prime solution to the so-called “MtGox” problem[7] where a centralised service has control of funds on behalf of traders in executing market functions. Importantly, RaidenX is **not** attempting to decentralize market functions, but de-risk the benefits of a centralised exchange. The limited risk of operating through blockchain based accounts, and the added transparency for the reconciled state of the market in the blockchain, allows for an otherwise centralised system to operate in a strictly controlled, transparent and limited capacity. This makes the RaidenX approach to blockchain asset trading extremely attractive when compared to the risky, yet still popular, fully centralized attempts at crypto-exchanges to date.

As a new use case for off-chain transaction channels to solve an important problem in the blockchain ecosystem, RaidenX has the potential to disrupt the entire crypto-currency and blockchain asset trading industry. It's support of frequency and volume trading as well as the more efficient price-discovery afforded by centralised markets, gives exchanges and traders the **best of both worlds**.

2.Background

Blockchain Overview

Blockchains have clearly revolutionised applications for financial technology and the way financial relationships, as well as assets, can be defined. This is accomplished through ingenious and unique solutions to fundamental problems in the security and management of distributed data.

Importantly, it is crucial to recognize that the blockchain data is managed by a decentralized application[8] (DApp). Regardless of the form of the decentralized application, access and use of the system is governed by a set of rules designed to ensure integrity of the system and prevent its exploitation. The added security of the decentralized approach is one of it’s

---

[5] "Payment channels - Bitcoin Wiki." https://en.bitcoin.it/wiki/Payment_channels. Accessed 28 Nov. 2017.
[6] "Multisignature - Bitcoin Wiki." https://en.bitcoin.it/wiki/Multisignature. Accessed 28 Nov. 2017.
[7] "Mt. Gox - Wikipedia." https://en.wikipedia.org/wiki/Mt._Gox. Accessed 28 Nov. 2017.
[8] "Decentralized Applications White Paper and Spec - GitHub." https://github.com/DavidJohnstonCEO/DecentralizedApplications. Accessed 28 Nov. 2017.

unique values. Additionally decentralized applications and services can also be operated in limited or permissioned capacity, as is the case with RaidenX.

Core to the function of the DApps that manage blockchains, is the replacing of system of centralized authority with a system of balanced authority. This “rock paper scissors” approach distributes incentive and costs over a P2P computer network without centralised control through consensus mechanisms which are commonly agreed to by all participants on the network.

Unique Features

Consensus across these networks is reached by sharing a common transaction protocol, and common software which operates on transactions shared over the resulting network. This allows all systems connected to the network to be able to generate an identical result based on the protocol, to which all other participants can agree on with mathematical certainty. The core of this consensus is often referred as a “proof”[9].

This means of distributing authority is dependent upon several unique characteristics of blockchains. Most importantly is the usage of public key cryptography directly for addressing of transaction values. The resulting numbered accounts[10] tracked in the blockchain ledger are openly accessible through a public encryption algorithm (the account number doubles as a public key[11]), thus removing virtually all permissive barriers to access.

There are two widely accepted approaches for delegating authority among account holders for transaction validation. Unrestricted or permission-less[12] DApps allow any account holder to compete for rewards through contribution some type of computing resource, which incentivises participants to self-regulate their own system. Permissioned[13] DApp networks rely on an organised consensus among an explicit quorum of predetermined account holders through processes similar to casting votes. The incentive is similar but more indirectly tied to the traditional profit incentive of stakeholders to gain market trust and adoption.

Unique Value

The unique function of DApps create new and unique value for both users and participants, and also opportunity in further use cases and applications of the technology. A successful blockchain project is one that utilises one or more of the unique functions of a DApp to bring the value of blockchains to their target market or user base.

---

[9] "Proof-of-work system - Wikipedia." https://en.wikipedia.org/wiki/Proof-of-work_system. Accessed 28 Nov. 2017.
[10] "Help:Accounts explained - Bitcoin Wiki." 29 Dec. 2015, https://en.bitcoin.it/wiki/Help:Accounts_explained. Accessed 28 Nov. 2017.
[11] "Public-key cryptography - Wikipedia." https://en.wikipedia.org/wiki/Public-key_cryptography. Accessed 28 Nov. 2017.
[12] "Types of Blockchains & DLTs (Distributed Ledger Technologies)." https://blockchainhub.net/blockchains-and-distributed-ledger-technologies-in-general/. Accessed 28 Nov. 2017.
[13] "The difference between public and private blockchain - IBM." 31 May. 2017, https://www.ibm.com/blogs/blockchain/2017/05/the-difference-between-public-and-private-blockchain/. Accessed 28 Nov. 2017.

The primary value of a DApp is it's ability to securely automate and govern direct participation in it's system between those who provide resources and functionality, and those who wish to use the system or its resources. The resources used for its function, along with access fees, can create directly attributable value to the information stored in the blockchain from resulting security and integrity of the system. Although this value is fiat in form as a financial measure, it is also often perceived by markets as real value, with potential credibility given to their argument based on current authoritative legacy options such as central banking.

Additionally, tremendous reduction in cost, friction, and barriers to access create the opportunity for open and self-regulated free markets in the development of new innovations in financial technology, assets, and services. Existing norms in conventional thinking towards finance will be challenged in what is a truly borderless and boundless financial system. Virtual immediate access to a global market and all types of assets is available for any blockchain application or service.

Of course given the nature of the technology, it's borderless access, and it's self-incentive, many new opportunities for fundraising (so called "ICO"[14] crowd funding) and monetisation are available for offering "in demand" utility or services for blockchain technology. This new area of fundraising is sure to expand as the ecosystem of the free market naturally grows around the opportunity to support it, and share profit from doing so.

Monetising Blockchain

RaidenX leverages blockchain technology to create the exchange service in both permissioned and permissionless. Participation in transaction validation or trade execution for these systems has shown to be a profitable business model, especially when combined with other services. RadienX offers the same revenue model as traditional trading markets, and all the flexibility of blockchain technology for additional revenue potential.This is the primary incentive model which has driven the growth of the physical blockchain networks themselves.

Technology Evolution

Blockchain technology has also evolved substantially since it's inception. This progression follows a path of least resistance to marketable and monetizable opportunities in technology development and innovation. The overall direction of this innovation trends towards the eventual standardization of blockchain protocols in breaking down remaining friction and barriers between new digital blockchain assets, and eventually blockchains themselves. RaidenX is designed and developed to capitalise on and support this trend.

Phase 1: Basic Blockchain

Originally, the first blockchain networks were partially functioning DApps, and processed simple transactions with slow transaction committals, and unintuitive interfaces. Initial

[14] "Initial Coin Offering (ICO) Definition | Investopedia." https://www.investopedia.com/terms/i/initial-coin-offering-ico.asp. Accessed 30 Nov. 2017.

blockchain technology was also expensive to operate, costly to use, and awkward to understand. However later innovations such as Ripple[15] and NXT[16] brought lightweight and energy efficient consensus mechanisms.Open sourced nature of blockchain technology made possible many clones of these early systems allowed for competing avenues of innovation.

Phase 2: Sub-assets and smart contracts

The second wave of blockchain innovation came from projects like Mastercoin[17], and then Ethereum[18], which sought to create more flexibility in the tracking of arbitrary measures and value in a blockchain. They leveraged the original function of the secure DApp to notarize and distribute authority over transactions as defined by the issuers of these new asset measures, essentially allowing a decoupling between these secondary assets and the core asset of the decentralized application's incentive system. This was expanded and supported in a specific protocol offering the ability to define smart-contract[19] based on account logic added to blockchain transactions.

Phase 2.5: Off-chain Transactions (current stage)

In concurrence with the leading edge in the evolution of blockchain technology, multi-asset trading and exchange will increasingly become a larger and growing part of the technology and markets and asset ecosystems managed and built by and on blockchain technology. lightning technology[20] and state channels[21] using smart contracts, allow for tracking through a proof of balance adjustments between the parties on the transaction before it is reconciled into the ledger. These "netting channels" can then be operated off-chain, separate from the main network of the blockchain by services.

Phase 3: Inter-blockchain network synchronisation (future)

With the various competing blockchain ledgers and decentralized applications, strong demand has always existing for exchange of value between these ledgers, and between asset values tracked in them[22]. The bridging of these gaps that has begun during the current phase (2.5), will extended further into the blockchain ecosystem, and into the core protocols of Decentralized Applications themselves.

This newest wave addresses many issues with synchronizing transaction processing across multiple blockchain networks in order to facilitate decentralized core asset exchange. With

---

[15] "The Ripple Protocol Consensus Algorithm." https://ripple.com/files/ripple_consensus_whitepaper.pdf. Accessed 28 Nov. 2017.
[16] "Whitepaper:Nxt - Nxt Wiki." https://nxtwiki.org/wiki/Whitepaper:Nxt. Accessed 28 Nov. 2017.
[17] "GitHub - OmniLayer/spec: Omni Protocol Specification (formerly ...." https://github.com/OmniLayer/spec. Accessed 28 Nov. 2017.
[18] "Ethereum Homestead Documentation." http://www.ethdocs.org/. Accessed 28 Nov. 2017.
[19] "Smart contract - Wikipedia." https://en.wikipedia.org/wiki/Smart_contract. Accessed 28 Nov. 2017.
[20] ""The Bitcoin Lightning Network": Paper." https://lightning.network/lightning-network-paper.pdf. Accessed 28 Nov. 2017.
[21] "What are State Channels? – Stephan Tual's Blog." 4 Jan. 2017, https://blog.stephantual.com/what-are-state-channels-32a81f7accab. Accessed 28 Nov. 2017.
[22] "Bitcoin trading volume - Bitcoinity.org." https://data.bitcoinity.org/. Accessed 29 Nov. 2017.

this synchronization of DApps across networks, true inter-blockchain[23][24] transactions can allow for exchange of asset value between core blockchain assets using the base consensus engine's of all participating blockchain networks. Ultimately all measure of value interconnected in this way, will allow for near "currency agnostic" transactions.

Common transaction and account formatting conventions, inter-ledger transaction protocols, and standard off-chain transaction channels facilitating high-speed and high-volume functions will supply a full technology stack to support virtually any imaginable use blockchain based application, asset, or service.

With this significant development, blockchain technology is nearing the final stages of it's evolution into a global standard platform for value exchange. The eventual emergence of the "Internet of Value"[25] becomes to possible as a global interconnected financial transactions protocol. This platform will allow any business, asset, organization, or relationship to be defined openly and explicitly without barrier or restriction to either their creation or their use and participation, by any individual, organisation, service, or market.

De-risking (hybrid) centralized exchange

In evolution of financial technology, it is not so much the changing of these relationships, for certainly many variations of these relationships exist in many financial markets and assets, but the ability to more rapidly increase the automation of increasingly complex and compound financial relationships.

With DApps, we can automate more complex relationships than ever before. What is also uniquely revolutionary with blockchain technology is that through various means of distributing access and automating processes of the system, not only is this possible through the Decentralized Application which governs and manages blockchain data, but with shared authority at the account level, new types of co-operations in the management of financial relationships can be automated as never before.

This new form of technology for finance is in the early phase of development, with much fixing and improving needed before it can sustainable, effectively and securely manage users financial data if broader distribution and usage of blockchain technology is to have a chance.

---

[23] "Whitepaper - Cosmos - Internet of Blockchains - the Cosmos network." https://cosmos.network/whitepaper. Accessed 29 Nov. 2017.

[24] "Aion To Facilitate Communication Between Different Blockchain ...." 5 Sep. 2017, https://kryptomoney.com/blockchain-news-aion-facilitates-communication-between-blockchain/. Accessed 29 Nov. 2017.

[25] "The Internet of Value-Exchange - Deloitte." https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/Innovation/deloitte-uk-internet-of-value-exchange.pdf. Accessed 29 Nov. 2017.

3.Disruption

The full disruptive value of the blockchain technology revolution is based removal of barriers between market participants in peer-to-peer systems. The broader view of blockchain technology is as a primary component in the continuing trend towards a more “Uber” or “gigging” economy[26]. And as a transaction processing and accounts reconciliation system, is the "meta-uber" system which will lend itself to further supporting the trend.

This new phase in information revolution bears similar disruptive potential as the innovation of the mechanized printing press[27]. In both instances, forms of storing information were themselves turned into a platform for the processing and distribution of information. The vast improvements in efficiency, as well as the reduction in costs and barriers to participation in this new market, opened a never before seen opportunity for the expression and distribution of new ideas, and forever altered the course of human history.

With blockchain technology, and Decentralized Applications, we have the ability to not only realized the same magnified disruptive value, but it is additionally directly effective on management of financial information, and without direct or centralized control. Many have speculated as to the fully realized scope of the disruptive potential of blockchain technology, and it will likely be so disruptive as to create many broad and unpredictable effects[28].

The incredible advantage is of course in what function these systems provide in reducing the cost related to manual administration of current legacy payment networks and banking or asset account tracking systems. Namely the secure accounting for the ownership and assignment of measures of value within it’s ledger is immune to direct and arbitrary influence outside of the given open protocol standard and as enforced and agreed upon by the co-operating validators on the network.

This similar historic disruption is now open us with blockchain. As with previous historic time periods, significant disruption of both economic and sociological consequence will occur during a major power-shift in the control and access to financial information and services. While the effects are broad, and direct consequences can be mapped, the full disruption and resulting effect is a long way from being realised, and sure to introduce many unexpected consequences and effects during the disruptive process.

3.Philosophy

Any project seeking to maintain sustainability over a longer period of time during this disruption needs to be strategically aligned to benefit from opportunities, and also avoid the

---

[26] "Uber, Airbnb and the New Gig Economy - Business.com." https://www.business.com/articles/philip-kushmaro-gig-economy/. Accessed 29 Nov. 2017.
[27] "The Invention of the Printing Press and the Rise of Bitcoin - The Daily ...." 8 Aug. 2017, https://dailyreckoning.com/the-invention-of-the-printing-press-and-the-rise-of-bitcoin/. Accessed 29 Nov. 2017.
[28] "Beyond Bitcoin - Blockchain is coming to disrupt your industry - Deloitte." https://www2.deloitte.com/mt/en/pages/financial-services/articles/mt-banking-alert-019-blockchain-is-coming-to-disrupt-your-industry.html. Accessed 30 Nov. 2017.

many pitfalls and challenges along the way. Certainly the blockchain industry rightfully has a less than stellar reputation, as vast amounts of funds have been lost in various system failure, hacks, and scams[29].

It is important in financial technology to respect the real value users are expected to attribute to the information managed in blockchain applications. Ethical representation of values and distribution of authority are necessary to avoid even the wastefulness of first generation blockchain networks still in operation. Additionally there is immense pressure and demand to build solutions and take advantage of profit opportunity with blockchain technology, even to the point of challenging these ethics, or governmental regulations.

However large multi-national corporations and financial platforms are beginning to experiment with blockchain technology. As industrial and commercial grade solutions are developed, large stake holders and distributions channels in the legacy banking system will be able to offer the benefits of blockchain technology to large numbers of existing users.

The key differentiation between this phase of adoption, and previous phases of adoption, is that corporate entities with established market trust, brand recognitions, existing user bases, and distribution channels, will be able to bring blockchain technology to market much more rapidly than has happened to this point.

It is important for the RaidenX project to follow the trend towards ethical and compliant blockchain applications as regulators and industry begin to dominate the technology.

This more appropriate to markets approach will be the delineation between previous projects in the blockchain space, primarily operated and founded by technology teams or engineers themselves, and have lacked a certain financially appropriate perspective to the technology, and has resulted in a “technology first” philosophy of blockchain projects to date.

Technology First:

The existing challenges facing the blockchain industry are in no small way related to the “Technology First” approach of many early designers and developers of Decentralized Applications using blockchain technology. The background of these innovators was necessarily more heavily focused in the technology area, rather than in working experience or knowledge of business and finance.

As such many issues have resulted the technology conventions attributed to financial conventions. Terms such as “coins” and “mining” are arbitrary conventions to merely denote a recognisable financial function or asset. An unfortunate consequence of this misrepresentation is that these conventions are viewed as the source and representation of value, rather than the differing financial reality.

As a consequence, many blockchain applications and services do not directly or accurately represent their value or functions.

---

[29] "List Of High Profile Cryptocurrency Hacks So Far (August 24th 2017)." 24 Aug. 2017, https://storeofvalue.github.io/posts/cryptocurrency-hacks-so-far-august-24th/. Accessed 30 Nov. 2017.

Finance First:

With the many confusing and quirky buzzwords derived from these unconventional terms, compliance is only complicated further when financial relationships tracked in ledgers can be redefined. In finance it is not the form of the representation of a transaction that defines that transaction, but the relationship between the parties to the contract which is attempted to best be described in that form.

This is the primary principle of the Finance First philosophy, that values and transactions in data form, should best describe and represent the transfer of value actually occurring in the real world.

Compliance:

In the grey areas around blockchain, of which there are many pitfalls, the future support of mass market adoption must include the support regulatory compliance. Regardless of the nature of either the blockchain industry, or of the authorities who are surely less than perfect in their application or enforcement of them, regulations are intended to protect citizenry and should be respected as such if blockchain is to have wider acceptance in the market. Many ongoing reviews of technology be regulators and governing bodies have resulted in varying initial attempts to address blockchain technology[30], with more sure to follow.

The ethical approach and a “Finance First” philosophy is what will ensure that our best intentions with the development of the RaidenX technology will keep our project and partners free of unknown or unnecessary risk, and engender the trust of the industry and regulators not only in our project and approach, but in a broader perception the project and developing blockchain technology.

4.Opportunity

The current trend in the development of blockchain technology has resulted in an explosion of competing value measures commonly referred to as “tokens”[31]. With a virtual infinite capacity to support varying approaches and models to management and measure of value, the capacity for blockchain technology to support further “tokenization” is nearly limitless. As with the earliest phases of evolution in the blockchain ecosystem, the first greatest service demand is for exchange of these assets.

However a continuing and great challenge with blockchain technology comes in secure services providing access to blockchain funds. This is of particular issue for trading markets, the earliest of blockchain services. Typically markets depended on centrally controlled and closed sourced service facilitating the operation of market functions with full counterparty risk

---

[30] "Blockchain & Cryptocurrency Regulations in US & Abroad - Business ...." 20 Oct. 2017, http://uk.businessinsider.com/blockchain-cryptocurrency-regulations-us-global-2017-10. Accessed 29 Nov. 2017.

[31] "Digital Tokens: Colored Coins and Ethereum Tokens | Draglet.com." https://www.draglet.com/blockchain-applications/digital-tokens. Accessed 29 Nov. 2017.

on behalf of users. RaidenX poses the opportunity to finally solve a big problem in the exchange industry: How to prevent from being “MtGox’d”.

This situation where users funds have been put at risk on a centralized exchange, has infamously resulted in numerous hacks and loss of users funds, to the detriment of the blockchain industry. Yet this is where the majority of market priced trading of blockchain assets occurs.

The recent innovations in blockchain technology involving off-chain transactions have just recently provided a platform on which to develop a solutions to problems with centralized services. The Raiden project continues to gain interest and has a bright future.

The convergence of opportunities to use cutting edge technology in solving large problems by taking advantage of proven market demand is the full opportunity of RaidenX.

5.Solution

Raiden

Raiden is an application for blockchain technology to support the operation and management of a micro-transactions platform. Raiden leverages off-chain transaction channels to manage the netting of balances between parties to the transactions prior to reconciliation in the blockchain. The intended application of Raiden is in the facilitation of micro transactions between payment nodes. who have been delegated authority to accessing and managing funds in the payment channel on behalf of the user.

These state channels between Raiden nodes maintain a proof-of-balance in the resolving of bi-directional micro transactions between counterparties on the independent Raiden network. Users funds and authority over transactions to the nodes/counterparties who then need no further authentication for transactions, and can then resolve the resulting “net balance” between the two payment channel operators on the blockchain.

This delegation of authority is necessary for supporting micro transactions with little or no user interaction such as a web-browser plugins automatically submitting payments on behalf of users for instant access to content through a “paywall”, and automate.

RaidenX

RaidenX as a project is aimed at creating a centralised and trusted blockchain asset exchange service using the security of a decentralized application and leveraging new Lightning transaction technology.

It is offered as an extension of Raiden, and adds support for operating a restricted state channel between a trader and the service. The resulting off-chain token trading platform will be able accessible by remote wallets and keystores. This allows account holders on the main blockchain to open jointly operated the limited accounts held between the RaidenX.

As an extension of Raiden, RaidenX is a blockchain service designed to provide a trusted backend to crypto-currency trading markets. RaidenX is not a decentralized exchange. It is a centrally controlled service which co-dependently manages trading accounts and orders in off-chain “state-channels”. RaidenX handles management of account and order creation, as well as service and user registration on the blockchain. The RaidenX service itself only holds the order book and matches orders on behalf of its blockchain registered users.

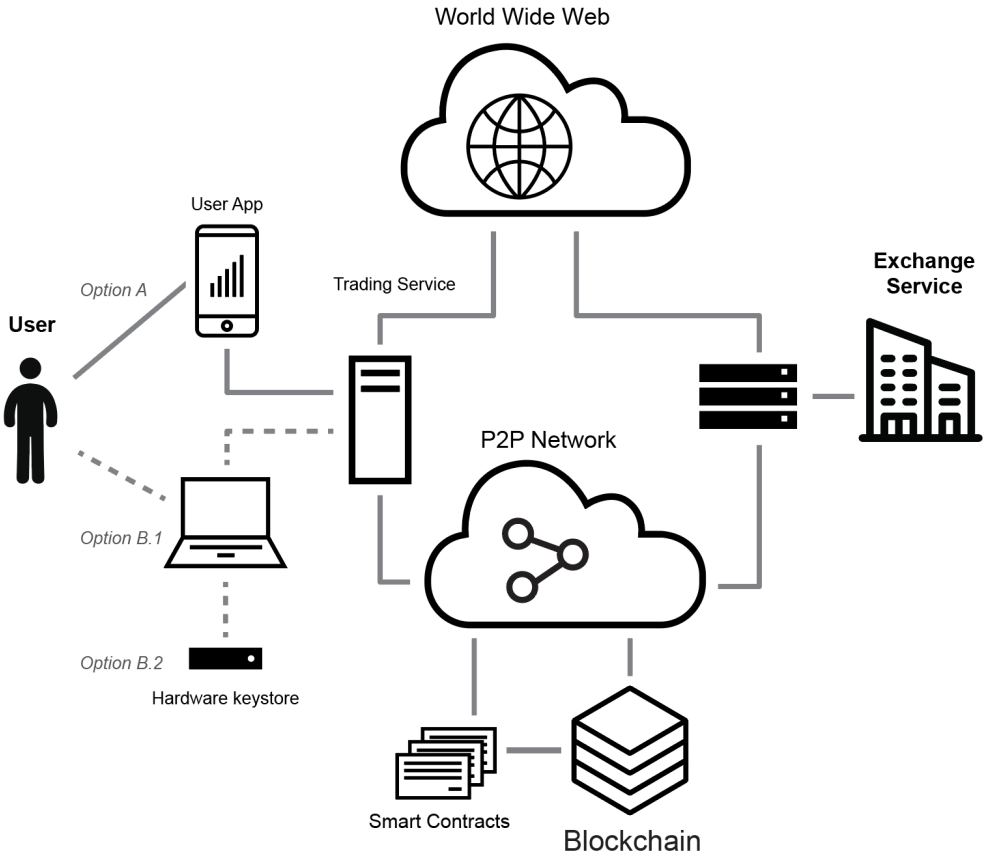
The RaidenX service operates similarly to a Raiden node. It is registered in the blockchain in a pre-published service registry contract. From this the service can then publish its channel management contract. This channel manager contract differs from the original Raiden channel manager contract in that is adds support for a user registry. This now fully registered service can now provide RaidenX functions through these smart contracts.

The functioning RaidenX service can now accept requests to its service through it’s interface of choice, although most likely this will be through API endpoints. From here users can submit requests to open accounts, post orders, and close accounts.

To open an account, a prospective user can register their key with the RaidenX channel manager contract, and upon doing so, the RaidenX service can open a state channel between their own service account, and the user's registered account. This state channel also differs from the existing Raiden state channel contracts in the added limitations placed on it. Specifically the RaidenX services operating the state channel may only submit signed orders to it in order to adjust its state and subsequent proof of balance. This is an acceptable and required limitation for operation of trading accounts in this manner.

This differentiation from the micropayment state channels of the base Raiden service is possible because there is a requirement that each end user or trader themselves initiate trade requests to the state channel. This also significantly reduces the risk exposure to the trader. Since technically their key is required to initiate a trade, and the service can only either execute trades or close out the account, netting respective balances to account of the initial depositors.

Network & Services Diagram



Services and systems which market participants use the access the RaidenX service. User's can choose between supported wallet software, or online services to access the exchange.

Account operations:

The RaidenX service is operated independently from the trading accounts service or software, allowing two options for operating a trading account on a RaidenX service:

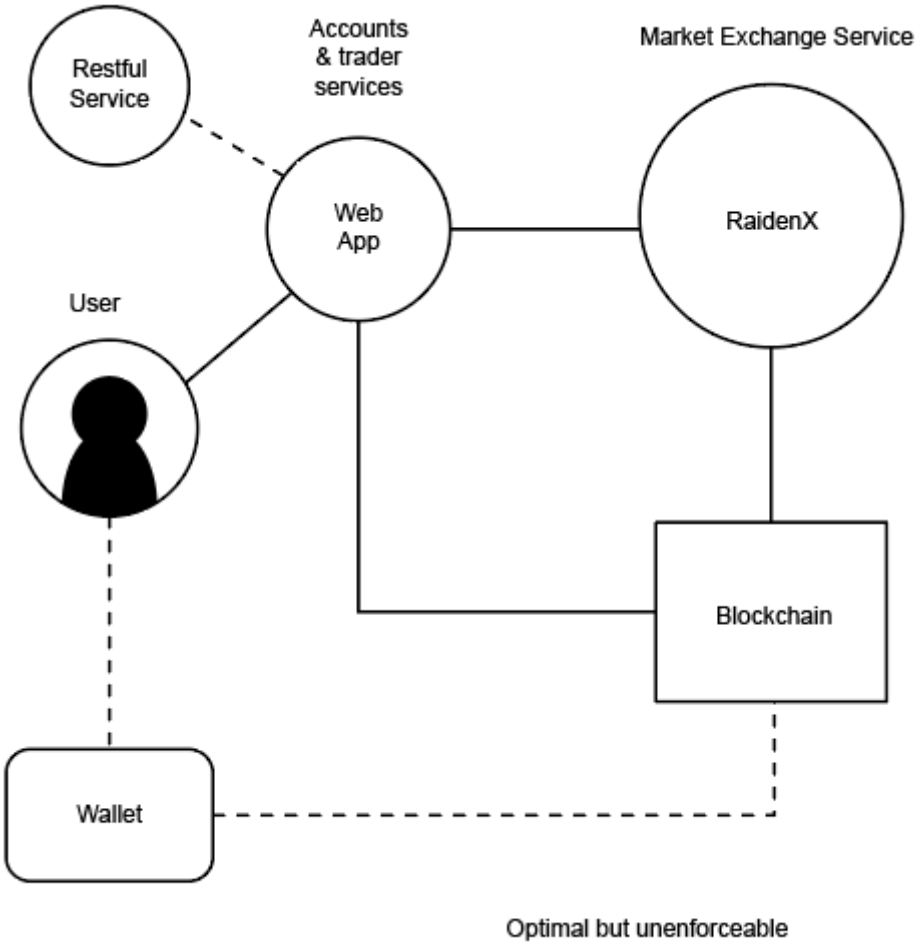
1. Independent Wallet - Trader can open a trading-channel (account) directly with the RaidenX service over the blockchain network and deposit funds into their account. The trader can also close their account in the same manner.
2. Account Service - The trader can use a wallet or trading platform service which will perform the same functions as above, as well as other optional or value-add services.

Market Operations:

The RaidenX service allows for direct market access in the same two ways, but over a Web API.

3. Independent Wallet - Supported wallet software will allow independent wallet operators to sign trade orders, and submit them off-chain to the RaidenX service.
4. Account Service - Traders who are managing their trading account through a trading accounts service, can use that service's trading features to use the RaidenX service.

Authoritative Entities



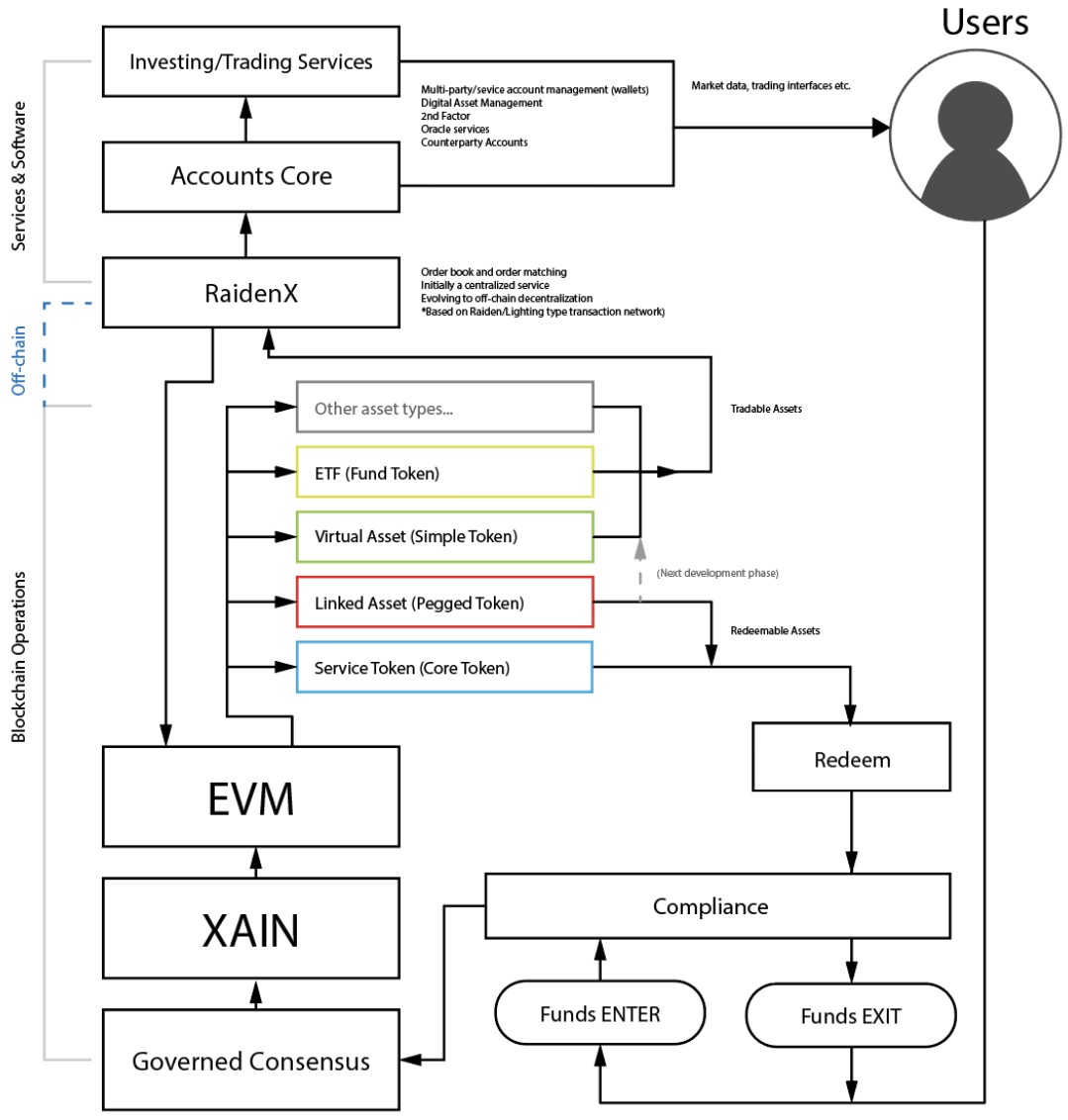
The RaidenX node operates an order book and and executes trades as a limited authority on a 2-of-2 multi-signature account between the trader and the service operator.

The “hybrid” exchange distribution of authority is design ed to eliminate centralized risk. All trades are executed as 2/2 signatured trading messages matched on the RaidenX platform. The initial order message are signed by the wallet or service of choice by the trader and submitted to the service’s server or network.

This de-risking of the exchange service through this method can be further enhanced through accounts or wallet services, multiple hardware devices, and 3rd party oracle services. In essence the hybrid approach to centralized trading or book management services allows for further distribution of risk of access or holding accounts, providing a much more scalable solution as well as the benefits of both the blockchain, and the centralized service.

Example Use Case

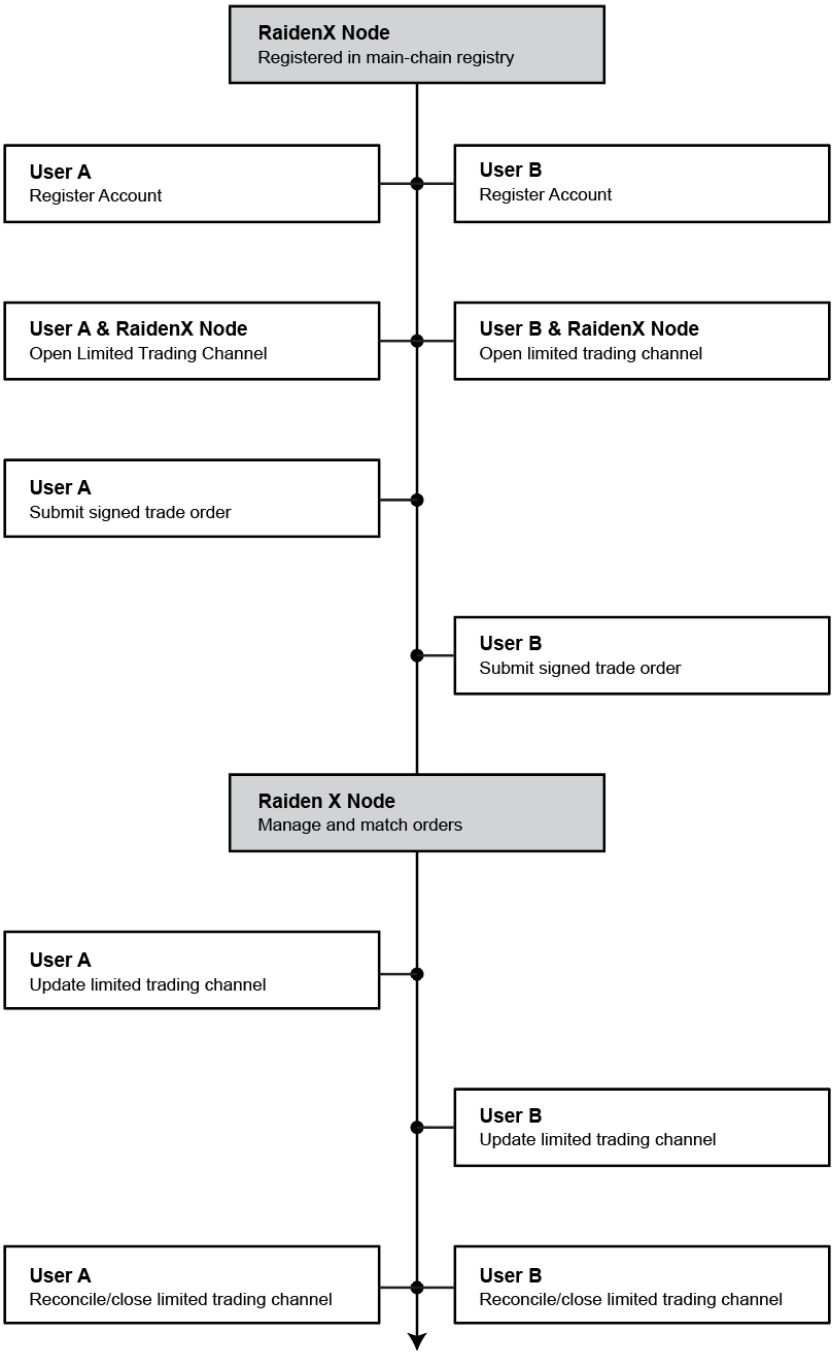
Compliant Crypto-asset Exchange



Example use case of assets architecture managed by service operating RaidenX exchange. Note potential for users enter and withdraw funds through compliance system operated by the central service.

With the RaidenX approach, compliance and safeguards for secure access, and secure assets can be leveraged to develop and service the full spectrum of asset trading opportunities. The RaidenX service is again able to leverage its de-risked model to operate all manner of various typical functions of an exchange.

Sequential timeline



Users initiate a trade by sending a signed order message to the RaidenX service. The RaidenX service will then either match that order with an existing order in its current state, or hold that order for further potential matching against new orders.

If a matched order for the signed order is found, then the RaidenX node has the authority in conjunction with this pair of signed orders to adjust the corresponding state of each trader's account. In the case that a full order is not fully filled by another order it matches, then the

state manager contract will return a “change” order for subsequent matching until the full balance of that order is executed.

At any time either key holder on the original state channel may call for the reconciliation of the current state balance into the main blockchain. This functions as the original Raiden channel close methods. At this point the trader account is considered closed with the service.

Why Now

Demonstrated demand

With the initial success of the Mastercoin/Omni ICO through to the Ethereum ICO, several subsequent projects were initiated and incubated, with the culmination of these efforts made apparent with the flourish of ICO offerings during 2017. Again with this latest round of funding success for blockchain based technology projects, certainly more will following in the wake of this latest wave. Increasingly standards, tools, services, and platforms will be in demand for the execution of all variety of market and services functions for these new blockchain based assets, and will certainly be one of the largest areas of growth over the next 18-36 months.

Opportunity Gap

As there are many people wanting to do ICO’s but they are coming to be seen as very risky. Certainly it cannot be argued that many if not most new blockchain or “ICO” projects offer far from significant technical innovation, and rather seek more to prioritize fundraising over initial technology development.

One of the more underdeveloped areas on the blockchain industry are trading markets or exchanges. Do to the extremely restrictive nature of securely self-regulated blockchain consensus of Decentralized Applications (those distributed transaction processing networks which manage blockchain ledgers), exchange of value between differing types of value are facilitated by a counterparty, which is delegated full control of the funds tradable on it’s platform.

New Exchange Opportunities

Prior to the new “hybrid”[32] approach to centralized exchanges, olders of crypto-based assets on blockchain ledgers wishing to trade or speculate on the value of those assets in trading markets, have had to rely on either centralized exchange, or limited risk, but non-price competitive “atomic” markets whose volume does not contribute to or is measured in the pricing of assets derived from the centralized trading markets.

The node operator can choose which assets to allow listing in its order book. Orders are manually matched by the node, as its primary service. The ability for RaidenX to leverage the underlying p2p transaction sharing protocol as a means of distributing this order book.

---

[32] "A provably fair centralized exchange using ... - Legolas Exchange." https://legolas.exchange/static/public/legolas-whitepaper.pdf?v=9. Accessed 1 Dec. 2017.

Additionally, adding a consensus engine to the RaidenX nodes on this network, would allow a distributed consensus on order matching and execution for trades on the channel accounts with the node. This would be a consensus on trades, based on a proof of balance. The output of this distributed consensus engine could also itself register these trades in a blockchain (depending on output limitations of such a network).

However the optimal operational conditions would be that of several RaidenX nodes working in concert initially to match orders as a services, while being able to operate such a service as very high through put.

6.Roadmap

1. ~~Design completed to support limited authority market executors & smart contract functions.~~
2. ~~Platform design for multiple token trading for single blockchains~~
3. Develop POC as testing platform
4. Iterate through development to MVP stage
5. Additional support for more asset and order types
6. Distribution of order book across P2P network
7. Lightweight permissive distributed consensus mechanism for service management

7.Limitations

It is not the intent of RaidenX to facilitate trading between separate different blockchains or blockchain platforms. The project and blockchain technology will continue to evolve in this regard, and more likely other approaches will be more adept at solving this issue.

Additionally, a trustless hybrid-exchange needs to ensure the integrity of the state of the order book, as well as the order of execution of trades that generated that state. This proof of state will be derived as demonstrated in the Plasma[33] approach to multi-channel state management, allowing for the proof of balance of accounts, and the proof of state of the order book.

8.FAQ:

Does RaidenX support inter-chain or cross-chain exchang?

At this time it does do not. The primary aim of the RaidenX project is to facilitate trading of assets on a centralized service, for all types of tokens or crypto-assets on a single blockchain. However there is certainly opportunity for evolve further and inter-ledger transactions are developed and evolve.

---

[33] "Plasma: Scalable Autonomous Smart Contracts." 11 Aug. 2017, https://plasma.io/plasma.pdf. Accessed 1 Dec. 2017.

Is RaidenX different from Raiden?

RaidenX is a project to extend Raiden. The intent is to support full existing Raiden network functions. Specifically it creates a new type of state channel, with new restrictions, for operation between a user and service provider, creating the so-called “hybrid”, or “de-risked” centralized exchange model. RaidenX is not at this time officially affiliated with Raiden.

What is the difference between RaidenX and Raiden.

RaidenX is an extension for the Raiden technology.Also the “swaps” executed by the service must be initiated by a signed message from the user/trader.

Which tokens does RaidenX support trading/exchange in?

Any standard token which is registered on the same blockchain and with the service running RaidenX can be traded on that service. There may be also be multiple RaidenX services running on the same blockchain, and it is up to each one to choose which blockchain based assets they will support.

Does RaidenX support “short” positions?

At this point, it does not, as this is not a purely technical function. Most likely assets representing short positions themselves will be available to trade as tokens on a RaidenX market.