The Wyvern Exchange Protocol

Project Wyvern Developers

Abstract

The Wyvern Exchange Protocol is a specification for the decentralized exchange of digitally representable non-fungible assets. A wide variety of real-world and virtual assets can digitally settle ownership through the use of secret information or a record on an immutable ledger. Existing solutions for the trade of assets so represented are dependent on rent-seeking, fallible centralized gatekeepers, unnecessarily split along market verticals due to interface constraints, and, being designed solely or primarily for human end-users, are fundamentally ill-suited to automation. The introduction to the digital ecosystem of smart contracts provides the fundamental tool — trustless execution of code — necessary to address these issues. This document outlines a protocol designed to provide such a solution and describes an initial instantiation structured as a set of smart contracts deployed to the Ethereum blockchain.

Contents

1 Motivation **2**

2 A Brief Historical Note **3**

3 Desiderata **4**
- 3.1 Responsibilities of the Protocol . . . 4
- 3.2 Practical Decentralized Governance . . . 4
- 3.3 Category Agnosticism . . . 4
- 3.4 Frontend Incentivization . . . 5

4 Initial Instantiation **5**
- 4.1 The WYV Token — token.projectwyvern.com . . . 5
  - 4.1.1 Purpose . . . 5
  - 4.1.2 Supply . . . 6
- 4.2 The Wyvern DAO — dao.projectwyvern.com . . . 6
  - 4.2.1 Usability . . . 6
  - 4.2.2 Exchange & Protocol Governance . . . 7
  - 4.2.3 Activist Shareholders . . . 7
  - 4.2.4 Upgradability . . . 8

4.3 The Wyvern Exchange — exchange.projectwyvern.com 8
4.3.1 Protocol 8
4.3.2 Initial Frontend 9

5 Risks **9**
5.1 Execution Risk 9
5.2 Platform Risk 10

6 Future Directions **10**
6.1 Automation 10
6.2 Interfaces 10
6.3 Derivatives 10

References **11**

1 Motivation

N.B. "Digital item" refers specifically to individually identifiable, non-fungible assets. This protocol will not support fungible assets such as currencies, shares of stock, or derivative contracts.

The expected market for digital item exchange is both wide and deep. A class of purely digital items already exists: virtual gear in videogames, gift cards for ecommerce sites, coupon codes for restaurant deals. All physical entities with representative ownership, such as a deed to a property, can in principle translate their present ownership settlement process onto a distributed ledger, and the benefits provided by doing so renders this likely to become commonplace. Digital settlement enables easy, cheap, and fast transfer, comprehensive auditing, and incontrovertible proof of ownership.

Existing marketplaces for the trade of digital items have mostly resembled their physical precursors in operational structure. Virtual agglomeration spaces, almost exclusively websites, take the place of physical ones — market stalls grouped in a city square. Buyers and sellers, still primarily human, trade one-on-one, often through an intermediary agent which ensures representational accuracy of the goods being exchanged (such as the validity of a gift card, or the presence of requisite balance in a buyer's Paypal[1] account) — replacing the regulatory body checking for food contaminants and the bank validating a check.

Economically, however, the situation has deteriorated. Gatekeepers — Ebay[2],

[1] 'Send Money, Pay Online or Set Up a Merchant Account - PayPal' (https://www.paypal.com/us/home).

[2] 'Electronics, Cars, Fashion, Collectibles, Coupons and More | eBay' (https://www.ebay.com/).

G2A[3], or Amazon[4] — connect buyers and sellers and take a fee proportional to the amount of each transaction. In the absence of physical scale limitations, digital gatekeepers can maintain locks on distribution and thus extract rent far beyond their marginal cost in executing transactions, often in excess of 10% of the purchase amount. This costs buyers and sellers dearly and precludes the existence of whole classes of otherwise viable business models whose profits are eaten up by the exorbitant transaction fees.

These marketplaces survive despite this inefficiency because the immediate incentive equilibrium is stable. Sellers must sell on Amazon, even if it costs them dearly, because Amazon has far more buyers than any other platform. New markets with lower fees must wage a steep uphill battle. To attract any kind of userbase at all competitors must target a niche specific enough that they can provide vertical utility more valuable than the potential revenue of Amazon's larger userbase. In the rare case that this strategy works, the larger marketplace simply acquires the new entry, integrates whatever novel technology they had developed, and then extracts more rent from their newly expanded userbase. The occaisional startup to refuse acquisition stands virtually no chance against the incumbent, which can borrow against future profits and abuse their financial might with predatory pricing strategies.

Smart contracts provide a new fundamental tool which may enable a different technical and economic approach. Trustless code execution allows essential functionality to be performed by a protocol owned by no one, thus immune to corporate M&A, and permits the explicit construction of incentive structures designed to properly align the long-term goals of market participants and avoid globally suboptimal Nash equilibria. Through the exclusive focus on digital items, a protocol run by smart contracts can also support new kinds of automated commerce and secondary markets. This document outlines a first stab at a protocol specification and governance structure designed with these aims in mind.

2 A Brief Historical Note

Intrepid Googlers will no doubt find traces of a previous Wyvern cryptocurrency. This was, in fact, a precursor to the Wyvern Exchange. A member of the present development team encountered that Wyvern by chance and thought that the concept (the original stated plan related specifically to videogames) held promise as a more general decentralized application.

The development team of that Wyvern, for their own reasons, chose not to continue with the original project, so we offered to take the ledger over and

[3] 'Buy and Sell Online: PC Games, Software, Gift Cards and More at G2A.COM' (https://www.g2a.com/).

[4] 'Amazon.com: Online Shopping for Electronics, Apparel, Computers, Books, DVDs and more' (https://www.amazon.com/).

pursue our own design concept. Our motivation in continuing the existing ledger was twofold. First, we thought it was nice to credit the original source of the idea. Second, and more importantly, we wanted a distributed set of stakeholders to implement decentralized governance — but we did not want to conduct an ICO, as we are primarily interested in experimenting with the technology and prefer not to spend time and effort raising funds. Continuing the original ledger served this purpose nicely.

3 Desiderata

3.1 Responsibilities of the Protocol

The protocol will be responsible for the full exchange process and all associated state.

- Allow parties to list items for sale
- Allow parties to register intent to purchase listed items
- Match buyer and seller intent
- Settle the item transfer once a buyer and seller have agreed to terms of purchase
- Interface to dispute resolution mechanisms, some possibly external, should a disagreement arise
- Provide a comprehensive audit trail of all transactions for future use

3.2 Practical Decentralized Governance

The present developers will bootstrap protocol development, implement the first frontend(s), and serve a very active initial role in directing the project, but the protocol should eventually be a commonwealth, not subject to the whims and execution risks of a single team. Protocol governance, and eventually funding, should be the responsibility of a decentralized autonomous organization with incentives correctly aligned so that short-term profits funnel back into development and the long-term success of the protocol is in the best interest of the organization's shareholders. This decentralized organization must be accorded sufficient power over the protocol to execute necessary alterations over time, and must be practical and quick enough to run that it can react effectively to evolving market requirements.

3.3 Category Agnosticism

The Wyvern Exchange protocol is not restricted to a particular *kind* of digital item. Rather, the protocol should support any item with one of two particular ownership representations: a record on a ledger representing ownership of an

asset transferable with a call to a smart contract, or a piece of secret information, where possession of the information constitutes ownership of the asset. Different exchange frontend interfaces will focus on particular asset categories (such as gift cards, video game cosmetics, or smart contracts themselves), but the protocol itself should be category-agnostic and focus on encapsulating and implementing the common functionality required by the various asset categories.

3.4 Frontend Incentivization

The protocol will only handle the "backend" layer of exchange. A diverse set of frontends will be required to support the expected diversity of digital assets — all of which will settle transactions using the backend protocol, but provide user-facing interfaces and additional API abstraction layers tailored to their particular niches. These frontends must be incentivized proportionally to transacted exchange volume in order to provide a convincing rationale for independent parties to pursue frontend development. The protocol should eventually have a strong agglomeration effect, as new frontends can provide access to existing listed assets, but initial frontends may be more likely to succeed if they focus on particular markets which are uniquely well-served by the protocol's capabilities.

4 Initial Instantiation

4.1 The WYV Token — token.projectwyvern.com

4.1.1 Purpose

The WYV token exists not as a fundraising vehicle for an ICO but rather as an attempt to create an aligned incentive structure: a mechanism to maximize the likelihood that the actions in the best immediate interests of WYV tokenholders are also in the long-term strategic interest of the Wyvern Exchange protocol, and to maximize the likelihood that external parties whose interests are aligned with the protocol's interests are the most likely to accrue substantial token holdings over time. Contrast this, for example, with the Bitcoin protocol, which we would argue currently has a misaligned incentive structure: Bitcoin holders who wish to maximize their expected return are best served by evangelizing Bitcoin's potential future status as a digital reserve currency traded primarily by existing financial institutions (in derivative contracts which involve no actual Bitcoin[5]), not the peer-to-peer digital cash originally envisioned in the Bitcoin whitepaper[6].

[5] 'XBT-Cboe Bitcoin Futures' (http://cfe.cboe.com/cfe-products/xbt-cboe-bitcoin-futures).
[6] 'Bitcoin: A Peer-to-Peer Electronic Cash System' (https://bitcoin.org/bitcoin.pdf).

This is a complex goal. The requirements for incentive alignment will change over time — originally, Bitcoin's incentives were much more aligned, as without functional use cases driving demand the network would likely not have acheived speculative velocity, but once speculative velocity was acheived it quickly took precedence as a use case due to far stronger network effects. The initial token structure ties expected token dividends to future exchange protocol revenue and requires a small amount of WYV to use the protocol (thus making it likely that end users will be exposed to the token), but the Wyvern DAO may need to make adjustments over time.

Initially, the WYV token will be used for:

- Protocol governance: WYV tokenholders will have voting rights in the Wyvern DAO proportional to their token holdings
- Protocol dividends: The core protocol will charge a small proportional transaction fee, paid to the Wyvern DAO in the token used to conduct the transaction, which can then be distributed as dividends or reinvested into development as the shareholders decide
- Exchange protocol antispam fees: In addition to a proportional transaction fee, which is expected to make up the majority of the revenue, the Wyvern Exchange will charge a small fee in WYV for specific actions to prevent spam

4.1.2 Supply

Capped at 20 million. About ten percent of supply is initially allocated to the Wyvern DAO, and the remaining ninety percent is distributed according to the previous Wyvern ledger's final UTXO set. We expect token holdings to diffuse across the Ethereum userbase over time. Generating tokens to pay for network security is unnecessary, as the token is secured by Ethereum's network, and a capped supply provides strong incentives for early developers and evangelists.

4.2 The Wyvern DAO — dao.projectwyvern.com

The Wyvern DAO is a distributed autonomous organization, operated through a smart contract on the Ethereum blockchain, responsible for administration of the present Wyvern Exchange instantiation and long-term development of the exchange protocol.

4.2.1 Usability

The DAO is structured as a delegated shareholder association. Shareholders, with voting weight proportional to their WYV token holdings, can propose transactions for the DAO to execute, which are carried out if the total voting

stake after a specified period exceeds a required quorum and a majority of the votes approve of the transaction. Shareholders can choose to delegate their shares by locking tokens in the DAO smart contract. These tokens then count as voting stake for the delegator's chosen delegate address until the delegor chooses to undelegate their tokens. This is intended as a practical measure: small shareholders are unlikely to want to spend a lot of time evaluating proposals, and in any case may prefer to delegate their voting stake to a party they trust to make informed decisions. Should their chosen delegate take a stance on a proposal that the delegator does not like, the delegator can undelegate their votes at any time, which will immediately no longer count as votes belonging to the delegate.

One additional tweak is put in place to prevent spam: a small stake requirement (initially 0.1% of the WYV supply) is required to be a "board member", where only board members can propose transactions. This threshold (along with the other configurable parameters, required proposal debate period and minimum quorum) can be changed by the DAO should adjustment be required.

4.2.2 Exchange & Protocol Governance

The Wyvern DAO controls the Wyvern Exchange directly: it can collect and adjust fees, arbitrate disputes, and upgrade the exchange's smart contracts.

Initially, the present development team will follow the will of the DAO's shareholders, but eventually the DAO will be expected to fund and decentralize exchange and protocol development. The DAO can contract developers, directly through platforms such as Ethlance[7], or indirectly by funding bounties (Bounties Network[8], Gitcoin[9]) or sponsoring distributed hackathons which can be administered through smart contracts. As the DAO can interact with any other smart contract on the Ethereum blockchain, it should be able to utilize future platforms as they are added to the ecosystem.

4.2.3 Activist Shareholders

This governance structure is explicitly intended to provision for "activist shareholders". Anyone who thinks the current direction of the Wyvern DAO is suboptimal could buy up a fraction of WYV tokens, submit a proposal, convince a majority of shareholders to support their initiative, and profit should their hypothesis prove correct. The ownership threshold required to create proposals is initially set at 0.1% of total supply (although the DAO can change it), so executing this strategy shouldn't require a large amount of capital.

[7] 'Ethlance - hire or work for Ether cryptocurrency' (https://ethlance.com).
[8] 'The Bounties Network' (https://bounties.network/).
[9] 'Push Open Source Repos Forward | Gitcoin' (https://gitcoin.co/).

4.2.4 Upgradability

Beyond the ability to change its own voting rules, the DAO is not directly self-upgrading. However, were the DAO shareholders to wish to alter some form of the DAO's functionality, they could execute a series of motions which would create a new DAO contract, with the desired alterations, transfer to it all assets belonging to the first DAO (including control of the Wyvern Exchange contract), and modify frontend interfaces to point to the new contract — effectively swapping out the old DAO (still existent as a contract, but useless without assets) for the new one. We think this mechanism would be reasonably practical and is preferable to more complex self-update provisions in the initial contract code.

4.3 The Wyvern Exchange — exchange.projectwyvern.com

4.3.1 Protocol

4.3.1.1 Item Specification

Pair of IPFS metadata, {{ Ownable smart contract || ERC721 || Nothing }}.

Can we abstract over ownable better than this? e.g. another smart contract interface, various implementations for Ownable / ERC721 / etc.

4.3.1.2 Sale Specification

Kinds of auction.

4.3.1.3 Payment Tokens

The Wyvern Exchange supports any ERC20-compatible token as a payment method for items, chosen by the seller at time of listing. A whitelist managed by the DAO is used to avoid malicious / scam tokens. Frontends may allow users to pay with whichever token they wish (regardless of which token the item is listed for) seamlessly through protocols such as 0x[10]. The DAO controls a whitelist of token addresses (to prevent scam tokens with similar ticker symbols).

4.3.1.4 Escrow & Dispute Resolution

EscrowProvider interface, whitelist for implementations.

Example escrow providers: no escrow, mutually trusted third party (e.g. Wyvern DAO) who can charge fee.

4.3.1.5 Frontend Interface

[10] '0x: The Protocol for Trading Tokens' (https://0xproject.com/).

4.3.1.6 Fee Structure

Frontends will provide an address to receive split fees on each transaction (can later withdraw).

Wyvern Exchange affiliate links?

Automatic split fee to charity? - https://www.ethereum.org/donate

Anti-spam: listing, bidding, purchase settlement (is this necessary?). Percentage: 0.1% of purchase price in whichever token back to the DAO. Frontend incentivization: split fees?

4.3.1.7 Upgradability

Swappable interface / implementation smart contracts by DAO (optional to user). Frontend will have to abstract some of this, common SDKs will be provided (first for Javascript).

4.3.2 Initial Frontend

The initial frontend provides a generic interface item listing, browsing, purchase, and dispute resolution, intended as a functional proof-of-concept to be utilized by early adopters and markets particularly well-served by the capabilities of the exchange protocol.

Affiliate links instead of frontend fee.

5 Risks

5.1 Execution Risk

Putting control of the exchange protocol and profit from the exchange's operation directly in the hands of a DAO poses certain risks. The decentralized application ecosystem is very young, and it remains to be seen whether essential functions such as hiring and promotion will be executable by a DAO (which can do no more than issue transactions to other smart contracts on the Ethereum chain). An open protocol and distributed shareholder base mitigates this risk somewhat, as parties other than the DAO may contribute development and marketing efforts back to the protocol in which they hold stake, but the particulars are far from certain.

5.2 Platform Risk

The current market capitalization of cryptocurrencies is primarily driven by speculation (whether justified or not), not application throughput. The most end-user-accessible product right now, Coinbase[11], is built primarily on a centralized technology stack and gives up most of the fundamental guarantees a distributed ledger provides (e.g., a disgruntled fiat power can analyze or seize your Coinbase account). Real-world broad-base consumer usability will require substantial improvements in both underlying distributed ledger technology and higher-level user experience abstractions and is probably years out. End user desktop and mobile applications interfacing to the exchange protocol will require such advances to feasibly compete with established centralized marketplaces.

Although the most widely used smart contract platform at the moment, Ethereum has yet to surmount several critical technical hurdles, primarily in the area of network scaling. Many potential Ethereum alternatives exist: NEO[12], Tezos[13], Cardano[14], and Zen Protocol[15], to name just a few, all promise some form of smart contract support, and existing cryptocurrencies such as Zcash[16] may implement programmability on top of their current systems[17]. At the present early technical and economic stage, the future capabilities and market shares of particular smart contract platforms are difficult to predict. The Wyvern DAO should actively research potentially superior platforms, and, should the cost-benefit make sense, transfer or duplicate the exchange implementation as the overall ecosystem evolves and future trajectories become clearer.

6 Future Directions

6.1 Automation

6.2 Interfaces

(Virtual Reality)

6.3 Derivatives

(futures on individual Beanie Babies)

[11] 'Buy/Sell Digital Currency - Coinbase' (https://www.coinbase.com/).
[12] 'NEO Smart Economy' (https://neo.org).
[13] 'Tezos Crowdfunding' (https://www.tezos.com/).
[14] 'Cardano Hub - Home of the Ada cryptocurrency and technological platform' (https://www.cardanohub.org/en/home/).
[15] 'Zen Protocol - A Financial Engine' (https://www.zenprotocol.com/).
[16] 'Zcash - All coins are created equal.' (https://z.cash/).
[17] 'zooko on Twitter: "Okay, I think this will turn out to be the..."' (https://twitter.com/zooko/status/937101934057492480).

References

‘0x: The Protocol for Trading Tokens’ (https://0xproject.com/).

‘Amazon.com: Online Shopping for Electronics, Apparel, Computers, Books, DVDs and more’ (https://www.amazon.com/).

‘Bitcoin: A Peer-to-Peer Electronic Cash System’ (https://bitcoin.org/bitcoin.pdf).

‘Buy and Sell Online: PC Games, Software, Gift Cards and More at G2A.COM’ (https://www.g2a.com/).

‘Buy/Sell Digital Currency - Coinbase’ (https://www.coinbase.com/).

‘Cardano Hub - Home of the Ada cryptocurrency and technological platform’ (https://www.cardanohub.org/en/home/).

‘Electronics, Cars, Fashion, Collectibles, Coupons and More | eBay’ (https://www.ebay.com/).

‘Ethlance - hire or work for Ether cryptocurrency’ (https://ethlance.com).

‘NEO Smart Economy’ (https://neo.org).

‘Push Open Source Repos Forward | Gitcoin’ (https://gitcoin.co/).

‘Send Money, Pay Online or Set Up a Merchant Account - PayPal’ (https://www.paypal.com/us/home).

‘Tezos Crowdfunding’ (https://www.tezos.com/).

‘The Bounties Network’ (https://bounties.network/).

‘XBT-Cboe Bitcoin Futures’ (http://cfe.cboe.com/cfe-products/xbt-cboe-bitcoin-futures).

‘Zcash - All coins are created equal.’ (https://z.cash/).

‘Zen Protocol - A Financial Engine’ (https://www.zenprotocol.com/).

‘zooko on Twitter: "Okay, I think this will turn out to be the..."’ (https://twitter.com/zooko/status/937101934057492480).