The Wyvern Protocol

Project Wyvern Developers

Working Draft

Abstract

The Wyvern 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 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 intrinsically ill-suited to automation. Smart contracts provide 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

N.B. "Digital asset" 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 asset exchange is both wide and deep. A class of purely digital assets already exists: virtual gear in video games, 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. On-chain settlement enables easy, cheap, and fast transfer, comprehensive auditing, and incontrovertible proof of ownership.

Existing marketplaces for the trade of digital assets (and digital promises to ship physical assets) 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], 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

[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/).
[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/).

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 because Amazon has all the buyers. 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 much 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 occasional startup to refuse acquisition stands virtually no chance against an incumbent who 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 assets, a protocol run by smart contracts can implement support for new kinds of automated commerce and secondary markets far more quickly than the existing marketplaces. 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 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 (the combination of on-chain contracts and off-chain infrastructure) will be responsible for the full exchange process and all associated state.

The protocol should:

- Allow parties to list specific assets they own for sale
- Allow parties to register intent to purchase assets with specific properties
- Match buyer and seller intent as efficiently as possible
- Settle the asset transfer once a buyer and seller have agreed to terms
- Provide a comprehensive on-chain audit trail of all transactions for future use

3.2 Practical Decentralized Governance

The present developers will bootstrap protocol development, implement the first frontend, 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 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 exchange protocol should not be restricted to a particular *kind* of digital asset. Rather, the protocol should support any asset with a digitally settleable ownership representation: a record on a ledger representing ownership of an asset transferable with a call to a smart contract. 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 same 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 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 as the peer-to-peer digital cash originally envisioned in the Bitcoin whitepaper[6].

This is a complex goal. Even if the protocol itself is stable, the requirements for incentive alignment will change as the market conditions evolve. Originally, Bitcoin's incentives were much more aligned, as without functional use cases driving demand the network would likely not have achieved speculative velocity, but once speculative velocity was achieved speculation quickly took precedence as a use case due to far stronger network effects. The initial token structure ties expected token value to future exchange protocol throughput 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:

[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).

- Protocol governance: WYV tokenholders will have voting rights in the Wyvern DAO proportional to their token holdings.
- Protocol fees: The Wyvern Exchange and future frontends will charge fees (probably fractions of a percent, set by the frontend) for order settlement. This will need to be abstracted away from end-users to prevent unnecessary mental transaction costs.

4.1.2 Supply

Capped at 2 million. A bit over five percent of supply is initially allocated to the Wyvern DAO, and the remaining ninety-odd 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 consensus, 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 Wyvern 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 delegator 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 their previously chosen delegate.

One additional tweak is put in place to prevent proposal spam: a small stake requirement 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

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.

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 Protocol 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 Design

Let us suppose two agents interacting with a distributed ledger have utility functions preferencing certain states of that ledger over others. Aiming to maximize their utility, these agents may construct with their utility functions

[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/).

along with the present ledger state a mapping of state transitions (transactions) to marginal utilities. Any composite state transition with positive marginal utility for both agents and enactable by the combined permissions of both agents is a possible and mutually desirable trade, and the trustless code execution provided by a distributed ledger renders the requisite atomicity trivial.

Relative to this model, the present Exchange instantation makes two concessions to practicality:

- State transition preferences are not matched directly but are instead intermediated by a standard of tokenized value agreed upon by the participants of a trade.
- A small fee is charged in WYV tokens, specified by the frontend which hosts the orderbook, to support the real-world infrastructure necessary to match intent.

4.3.2 Protocol

4.3.2.1 Synopsis

The Wyvern Protocol is an Ethereum framework for the exchange of nonfungible digital assets. Protocol users - human-operated Ethereum accounts or other Ethereum smart contracts - place orders expressing the intent to sell or buy a particular asset or any asset with certain characteristics. The protocol's job is to match buyer and seller intent on-chain such that the asset transfer and payment happen atomically. The protocol functions solely as a settlement layer - orderbook storage and matching algorithms are left to off-chain infrastructure.

The protocol is representation-agnostic: it supports any asset that can be represented on the Ethereum chain (i.e., transferred in an Ethereum transaction or in a sequence of transactions). Users will be able to buy and sell anything from CryptoKitties to ENS names to smart contracts themselves. The protocol "knows nothing" about asset representations - instead, buyer and seller intents are specified as functions over the space of Ethereum transactions, as follows:

- Buy-side and sell-side orders each provide calldata (bytes) - for a sell-side order, the state transition for sale, for a buy-side order, the state transition to be bought. Along with the calldata, orders provide `replacementPattern`: a bytemask indicating which bytes of the calldata can be changed (e.g. NFT destination address). When a buy-side and sell-side order are matched, the desired calldatas, masked with the bytemasks, are unified and checked for agreement. This alone is enough to implement common simple state transitions, such as "transfer my CryptoKitty to any address" or "buy any of this kind of nonfungible token".
- Orders of either side can optionally specify a static (no state modification) callback function, which receives configurable data along with the actual calldata as a parameter. This allows for arbitrary transaction validation

functions. For example, a buy-side order could express the intent to buy any CryptoKitty with a particular set of characteristics (checked in the static call), or a sell-side order could express the intent to sell any of three ENS names, but not two others. Use of the EVM's STATICCALL opcode, added in Ethereum Metropolis, allows the static calldata to be safely specified separately and thus this kind of matching to happen correctly - that is to say, wherever the two validation callbacks mapping Ethereum transactions to booleans intersect.

4.3.2.2 Asset Specification

The Wyvern Protocol simply proxies transaction execution. Exchange users must grant control of whatever assets they wish to sell to an individual proxy smart contract and then sign approval of particular transactions when they wish to buy or sell an asset through the Exchange, granting the Exchange the right to execute the necessary transaction through the proxy contract. The user can transfer their assets back to themselves at any time.

The proxy contract exposes the following interface:

```
function proxy(address dest, HowToCall howToCall, bytes calldata)
  public returns (bool result)
```

After ensuring that the user has authorized the sender to execute the provided transaction, the proxy contract simply executes:

```
dest.call(calldata)
```

This enables a very wide set of potential use-cases, such as a paying an automated bug bounty when an invariant is violated or paying anyone who can solve a hard computational problem (e.g. paying directly for Bitcoin block solutions with a smart contract), and has the added benefit of substantially reducing the attack surface of the Exchange protocol as a whole, since the Exchange contract need only be provided the requisite permissions to execute particular trades and is not required to hold assets directly.

4.3.2.3 Sale Specification

An order must specify the method of sale: an algorithm used to determine under what conditions an asset can be bid on, under what conditions an asset can be purchased, and the final asset purchase price (this abstracts over many common kinds of sale / auction). The method of sale must implement the following abstract interface:

```
enum Side { Buy, Sell }

enum SaleKind { FixedPrice, DutchAuction }
```

```
function validateParameters(SaleKind saleKind,
  uint expirationTime) pure internal returns (bool)
function canSettleOrder(uint listingTime,
  uint expirationTime) view internal returns (bool)
function calculateFinalPrice(Side side,
  SaleKind saleKind, uint basePrice, uint extra,
  uint listingTime, uint expirationTime)
  view internal returns (uint finalPrice);
```

Initially, the Exchange will implement fixed-price sales and standard Dutch auctions. Future pricing algorithms should be added in accordance with market demand. Note that pricing algorithms which require asset escrow (e.g. English auction) will require additional protocol alterations.

4.3.2.4 Payment Tokens

The Exchange supports any ERC20-compatible token as a payment method for assets, chosen by the seller at time of listing. Frontends may choose to allow only orders with particular payment tokens on their orderbooks. Frontends may allow users to pay with whichever token they wish and convert it to the seller's desired token seamlessly through protocols such as 0x[10].

4.3.2.5 Fee Structure

The Exchange will charge a fee in WYV to settle orders, split by maker/taker. This fee is configurable by the Exchange frontend. Fees are paid immediately when an order is settled.

Fees are paid to an Ethereum address, which can be an account or a contract supporting more complex functionality. For example, frontends may elect to support affiliate links and pass part of the fee on to users who refer sales.

4.3.2.6 Upgradability

The primary exchange contract holds no assets or tokens and can simply be swapped out for a new version whenever a change is desired. Users will need to reauthorize the new contract via ERC20 `approve`. Proxy contracts to hold assets are managed by a registry controlled by the Wyvern DAO, which can authorize a new protocol version after a mandatory 2-week delay (to provide users time to withdraw assets in case of a malicious DAO).

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

4.3.3 Initial Web Frontend

The initial frontend will provide a generic interface for listing, browsing, and purchasing assets. Mass-market usability will come later - this is 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. The initial frontend will also implement a split-fee affiliate link system and provide a standard asset registry.

5 Risks

5.1 Execution Risk

Putting control of the exchange protocol 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.

Ethereum, although the most widely used smart contract platform at the moment, has yet to surmount several critical technical hurdles, primarily in the area of network scaling. Many potential Ethereum alternatives exist: NEO[12], Tezos[13],

[11] 'Buy/Sell Digital Currency - Coinbase' (https://www.coinbase.com/).
[12] 'NEO Smart Economy' (https://neo.org).
[13] 'Tezos Crowdfunding' (https://www.tezos.com/).

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.

[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).