Unicrow Whitepaper

Unstoppable escrow

> *„Imagine if gold turned to lead when stolen. If the thief gives it back, it turns to gold again."*
>
> *–Satoshi Nakamoto, 11. Aug. 2010*

1 Summary

Unicrow is an Arbitrum-based, censorship-resistant payment and escrow protocol that enables two parties to trade in the physical world without the need to place their trust in the counterparty or any third party. Honest trading behavior is incentivized through smart contracts, an immutable reputation system using trade parties' on-chain identities and E2E encrypted messaging.

While Unicrow's novel use-case lies in its trust-minimization, users can also opt to use a model that includes a trusted third party arbitrator. Where third parties are available, Unicrow helps to reduce operational overhead, security risks, and regulatory exposure associated with traditional (incl. crypto-multisig) escrow services.

Unicrow's developer-friendly toolkit makes it easy to integrate into any marketplace platform.

Note: This whitepaper is slightly out of date since our understanding of implications and applications of this concept based on the market feedback has evolved and expanded. We will bring it up to date in the next couple of weeks and also expand some these thoughts at our upcoming blog.

2 Problem

2.1 Trust

The existing escrow infrastructure is based on trust and therefore censorable and vulnerable to attacks - an assessment which is valid for both legacy/fiat and for cryptocurrency payments.

In a world with omnipresent barriers to trade, economic freedom is constantly under threat by state actors, corporate media and the oligopoly of platform providers. In the absence of a truly unstoppable payment and escrow platform like Unicrow, many market segments operate in adversarial environments of volatility.

Cryptocurrencies were designed to provide permissionless payment means. However, there are limits to the use of crypto payments for real world physical exchange of goods. How can a seller of watches be sure that they will receive payment when the goods are delivered?

Introducing an escrow to a real world physical exchange between two parties requires a trusted third party which is often costly, subject to onerous regulations, and may be fraudulent. Furthermore, there is often an asymmetry between the exchange value and trust when parties are operating in adversarial environments. Reputational mechanisms are key to balancing this asymmetry but currently are maintained solely on centralized, trusted information sources and marketplaces.

2.2 Costs

It is also operationally burdensome and heavily regulated and at times, prohibitively expensive for SMEs or marketplaces operating with tight margins.

2.1 Existing escrow alternatives

2.1.1 Fiat payments

All existing forms of escrow when it comes to fiat payments is that they come with the necessary preconditions and issues involved in dealing with legacy finance system:

- KYC/AML checks slow the processes down and expose users' data to breaches
- They are restrictive and censorable, leaving many market participants out based on their location, political affiliation, or personal preferences

Traditional finance escrow

Banks and regulated financial institutions provide professional escrow services or letters of credit for various use-cases.

High value physical goods exchange

In the market for high-value secured transactions such as real estate, cars, or art, professional escrow services are well-established and highly reputable. However, these age-old markets are also full of inefficiencies. Many players are unsatisfied with typically expensive offerings, or are left out of such markets altogether.

Trade finance and factoring

In trade finance and factoring, banks typically provide letters of credit and involve trusted third parties to mediate disputes if they arise. Besides issues already mentioned in the summary of this section, they can be prohibitively expensive for SMEs that trade or produce with distant parties whom they haven't built the necessary trust with.

Equities financing

In financing e.g. PIPE for SPACs, banks typically provide escrow for fiat payments made into the facility. This is highly expensive for the SPAC sponsors, and unsuited for potential crypto-investments into the SPACs.

Payment processors

Card payment processors offer escrow-like services (e.g. *manual payouts* in Stripe) that allow to hold the payment for a period or until the payment is released manually.

2.1.2 Cryptocurrency payments

Some of the most obvious use-cases where escrow for cryptocurrency payments are required and used include:

- Marketplaces and platforms connecting buyers and sellers that accept cryptocurrency payments;
- Crypto OTC platforms and brokers. Special concern are those in jurisdictions where they - and by proxy their users - are at risk of attack by state actors;
- Tokenization of assets where the cryptocurrency is paid upfront, but needs to be locked in order for processes to take place in the meatspace.

Centralized marketplace escrow

Some marketplaces, or platforms facilitating trades between their users choose fully centralized and custodial escrow that they operate unilaterally. It goes without saying that such a setup is the most prone to attacks and fraud.

Third party custodial escrow

Professional crypto-custodians offer escrow services in a similar manner to banks and financial institutions in the fiat payment system. While professionally run and arguably very safe, their risk and regulatory exposure means they are even more costly than the banking escrow services.

Multisig and MPC

Centralized marketplaces, OTC platforms, or third party crypto-escrow services often rely on multisig or multi-party computation to require consensus between two of the three parties (buyer, seller, and the marketplace or an arbitrator).

This is certainly superior to a simply centralized crypto-escrow, but it faces collective action problems. For the seller to receive the funds, it requires an active engagement of either a buyer or the marketplace to sign 2/3 transactions. That creates not only operational overhead, but also a risk of the funds being locked in case both seller and arbitrator stop communicating. Regulations pertaining to such setups depend on the jurisdiction, but in general holding even a subset of keys to a balance inevitably leads to regulatory exposure.

3. Unicrow's solution

Note: throughout the following pages, some details are omitted for brevity purposes. In those cases, details are provided in the online documentation and linked from here.

3.1 High-level design

Unicrow uses SDK-integrated contracts that allow a buyer to deposit an agreed upon amount of tokens for a selected seller directly or via a third party marketplace/platform. In a successful transaction, the seller or the marketplace can claim the balance to the addresses as defined.

In disputed transactions however, an unsatisfied buyer can challenge the purchase for a pre-defined time period. If the payment is challenged, a new challenge period starts and the payout is reversed towards the buyer to claim. The seller can re-challenge during the extended challenge period. This will make the seller a payee again and extend the challenge period to give the buyer an opportunity to re-challenge. The payment will be stuck in this loop until one of the parties gives up and lets the payment be released, until they agree on a settlement, or until they agree on an arbitrator to step in.

Additionally the platform will provide support for end-to-end encrypted communication and transferrable reputation scoring for all ethereum identities involved in the trades.

3.2 Payment flow

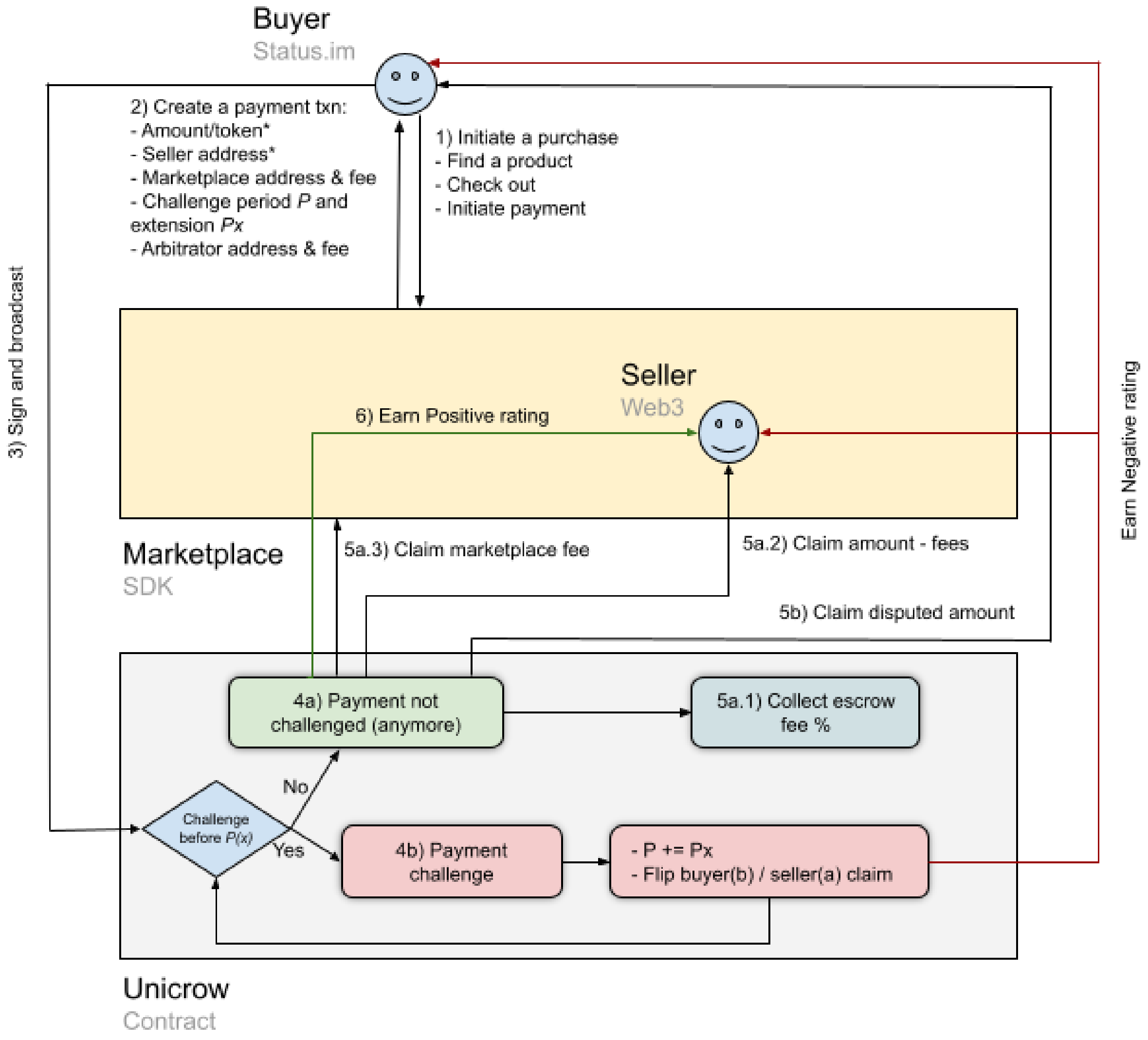

Fig 1: Payment flow

Initiate (1,2)

It is assumed that a Web3 marketplace takes care of the user interaction, including serializing the payment transaction for the user to sign.

For this purpose, Unicrow provides an easy-to-use, well-documented developer toolkit. The toolkit allows developers to embed the experience into their UI or to use Unicrow's UI components in order to save their implementation time but also to provide consistent user experience and assurance of security for users who will learn to trust Unicrow.

Deposit (3)

The contract will be able to receive a payment in a transaction with the following parameters:

- Seller's address
- Payment amount and token address
- Marketplace's address (0x00..00 for no marketplace)
- Marketplace's fee (can be 0)
- Challenge period *P* (in seconds)
- Challenge period extension *Px* (defaults to *P* if 0)
- Arbitrator's address (0x00..00 for no arbitrator)
- Arbitrator's fee (can be 0)

The contract generates and returns a unique incremental escrow ID, which is used to reference the payment in all future interactions.

When the payment is received, the amount is locked in the escrow until the challenge period expires, or until the buyer releases the payment manually[1]

Release and claim

When the challenge period expires (4a), the seller or the marketplace[2] can call a claim function which withdraws their shares of the payment to their respective addresses (5a.2) after a deduction of the escrow fee (5a.1).

Note: In the actual implementation, calling a claim of any share will claim all shares at once to save everyone's gas costs. This way, marketplace can even pro-actively run a claiming service on behalf of its users

The buyer can manually release the payment before the challenge period expires, which will improve their reputation score.

Challenge

If the buyer is not happy with the delivery, they can challenge the payment within the period *P* by sending a challenge transaction to the contract (4b). The challenge sets a new challenge period and also sets the buyer as the payee of the escrow. The new challenge period starts at the end of the current challenge period and lasts the predefined *Px*. If *P+Px* expires without a seller's challenge, the buyer can claim the amount and have the money returned (5b).

[1] Leaving arbitration and settlement aside for the moment

[2] Or technically anyone

The seller, if they accept the challenge, can speed up the release of the funds to the buyer (to decrease a hit to their reputation score), or challenge the claim back, delaying (potentially indefinitely) the ultimate payment of the deposit to the seller or the buyer. Thus the "*gold turns to lead*" in Satoshi's conception.

The challenges will reflect negatively on both seller's and buyer's reputation.

While the dispute continues, both the buyer and the seller can seek other (incl. traditional legal) measures to convince the other party to remedy the situation.

The buyer and the seller can also settle the dispute manually by arbitrarily splitting the amount between themselves (e.g. seller could offer a discount to the buyer for damaged goods). Both parties have to confirm the same settlement ratio on-chain.

Finally, both parties can agree on calling an external arbitrator if it hasn't been defined before. In this case too the arbitrator (and their fee) needs to be confirmed on-chain by both parties. The arbitrator may step in at any time and either release the payment to the seller, refund it to the buyer, or split it between the buyer and the seller arbitrarily.

Refund

To prevent reputation damage, the seller may refund the payment to the buyer before any challenge is made. In this case, no fees are charged and the transaction is refunded to the buyer in full.

Reputation (6)

Any transaction that is concluded without challenge reflects positively on the seller's reputation. A buyer can earn a positive reputation by releasing the payment before the challenge period expires.

The ratings/reputation, rather than issued and written will be simply populated from the historical transaction data. This way, there will be no additional costs of reputation, and the model can be fine-tuned based on observations of the real-world trade data.

Settlement

The settlement takes the form of percentage shares between the parties (e.g. the seller may offer the buyer a 20% discount in order for them to release the payment).

The settlement must be confirmed by both parties on-chain. The contract will check if both proposals match and if yes, it will execute the settlement.

In such a case, all fees are discounted proportionally and paid out of the seller's share.

E.g. if a 100 DAI payment with the protocol fee of 1% and the marketplace fee of 10% is settled 80/20 between the buyer and the seller (i.e. buyer is given a 20% discount):

- 20 DAI goes back to the buyer
- 0.8 DAI of the total is deducted for the protocol fee
- 8 DAI is the marketplace
- 71.2 DAI is claimed to the seller

If an arbitrator (see below) fee was defined, this fee will also be discounted and deducted accordingly.

Arbitration

If the arbitrator has been defined in the original payment, or if - when the dispute starts - both parties agree on chain on an arbitrator[3], the arbitrator can step in and decide the payment in one of the three ways:

a) Release the payment to the seller
b) Refund the payment in full to the buyer
c) Settle the payment arbitrarily between the two parties

As with settlement, platform and marketplace fees are charged proportionally to and deducted from the seller's share.

However, in this case and to neutralize arbitrator’s incentives, the arbitration fee will be charged in full and deducted proportionally from buyer’s and seller’s share.

E.g. if arbitrator’s fee was set upfront to 5%, and 20% discount to the buyer was decided by the arbitrator:

- 1% of the total amount will be deducted from the buyer’s share
- 4% of the total amount will be deducted from the sellers share

In another example, if the arbitrator refunds the payment to the buyer, 5% will be deducted from the original amount that the buyer receives.

3.3 Fees

Protocol fee

The contract would charge a fee for processing payments and for the escrow service. The fee is defined as a percentage[4] of the transaction amount in ETH or ERC20.

[3] Technically, another ethereum identity
[4] Technically, bps

The fee can be changed by a governance vote, but is hard-capped in the contract to 1% (100 bps).

The fee is sent to the treasury at the time when the payment is claimed. For this purpose, the treasury address is stored in the *UnicrowClaim* contract and governable.

Marketplace fees

Because the payments on Unicrow will be made directly between buyers and sellers, it is necessary to create a mechanism for marketplaces to receive a fee for their service of connecting their users.

The marketplace fee (in bps) and the receiving address will be set as transaction parameters. The buyer doesn't need to be aware of this (unless they look at the transaction), they simply care about how much tokens they are paying.

4. Platform

4.1 Toolkit

Unicrow is primarily aimed at marketplaces, and other platforms connecting real-world trade parties. These platforms - being experts at their particular domains - know best how to reach out to and communicate with customers, how to segment and display sellers, buyers, and listings, and how to facilitate logistics, legal processes, etc.

Unicrow provides a developer-friendly payment, escrow, dispute resolution, and arbitration toolkit for the platform developers to easily integrate the contracts.

The platform will also provide a simple UI toolkit for the marketplace to integrate during the payment process in order to maintain a consistent user experience across the platforms.

The platform will further provide an interface to check buyers' and sellers' rating (which will almost without exception be done by the marketplaces, but this is to provide it independently and to make the ratings transferable across marketplaces).

4.2 Indexer

In order to remove any dependence on centralized architecture, Unicrow doesn't rely on a subgraph, but rather provides an open-source custom indexer that the developers will be able to easily deploy to their architecture. The indexer allows administrators to easily filter incoming events relevant for the marketplace by simply providing one or multiple marketplace addresses in the configuration.

The indexer can connect to any node of the administrator’s choosing.

4.3 Web3 App

While the platform will rely primarily on marketplaces to drive adoption, usage, and growth, a simple app will be provided for the following purposes:

- For users to be able to test the platform
- p2p trades where no marketplace needs to be involved
- As a fallback mechanism for buyers and sellers to access their funds populated in the contract in case their preferred marketplace ceases to exist.
- For developer to re-use the app’s code in their own marketplaces (the app will be open-sourced for this purpose)
- Independent verification of the user and marketplace reputation

4.4 Summary

In summary, the products delivered as a part of the platform are:

- Contracts
- SDK
- Indexer
- Web3 app

All of these will be released as open source (incl. the web3 app, which should provide best practice and templates for integrating the SDK).

5 Governance and immutability

In order for the platform to be truly unstoppable, the deployed contracts must be immutable, i.e.:

- The contracts cannot be stopped or "upgraded" (AKA replaced)
- The escrow rules must be immutable - no one can interfere in the payment and dispute flow beyond how it is defined, not even *Unicrow* governance
- No white- or black-lists of addresses that can use the escrow or tokens that can be used in the escrow will be built
    - *That also means users need to be cautious about which tokens they use in the escrow as Unicrow cannot block malicious behavior in the tokens used in the escrows*
- The protocol fee will be hard-capped, even governance must not be able to set it above a certain uncompetitive level.

The ultimate goal is for the platform to be governed directly by DAO. That, however requires favorable market conditions for token launch. In the meantime, the platform will be governed by Gnosis multisig contract.

The important thing is, that neither current, nor future DAO governance can interfere with the immutable escrow rules. The governance body can change only the following parameters:

- Protocol Fee (hard-capped at 1%)
- Address where the protocol fee is sent
- Addresses of *crowRewards* and *protocolFeeRewards* contracts
    - More details on what these addresses will be revealed later, but for now what matters is that changing these parameters cannot change the immutable rules of the escrow
- Governance contract address - for the future transition to DAO governance