PayrLink

Whitepaper v1.0.1

Secure Blockchain-Powered Escrow Service with Private Transactions and Decentralized Arbitration

March 2021

Abstract

PayrLink is a smart contract-powered protocol that offers a trustless escrow service with default private transactions and decentralized arbitration. Users benefit from fast, private transactions in their agreements. In the case of disputes, a fair, cost-efficient, and impartial arbitration is provided regardless of the value of the contract.

1. Introduction

It is hard to trust anyone these days, especially in a world where everything takes place online. The days of making deals based on a handshake alone are long gone. Regardless of whether a deal is online or offline, involved parties need to feel that the transaction is (1) safe, (2) fair, and (3) private.

Unfortunately, by design, transactions and balances on the blockchain are fully public. Every single transaction can be viewed on block explorers (e.g. Etherscan). Once a link between the real-world owner and the wallet address has been established, that person's entire transaction history is entirely on display. Anyone with that information can easily view your payment history, trace the source of your funds, and analyze your on-chain activity.

What if you could rely on a trustless system guaranteed to leverage the power of decentralization to make sure both sides receive justice?

What if you did not want your history and balances to be publicly viewed by everyone? What if, when it came to your transactions, you wanted anonymity and privacy?

These challenges are what PayrLink has emerged to solve. In this document, we put forward a novel smart contract-powered system to disrupt conventional escrow services by adding trustlessness, privacy by default, and decentralized arbitration - all for a fraction of their traditional costs.

2. Decentralized Escrow Service

“Whoever controls the courts controls the state”. Aristotle.

- What is a decentralized escrow service?

In traditional finance, an escrow service facilitates all aspects of the transaction: receiving the money from the buyer, confirming the buyer has received their items or services, and releasing the funds to the seller. Traditional escrow services can take a lot of time to settle payments, are vulnerable to scams, and fail to address the risk of a dispute between the parties of the agreement.

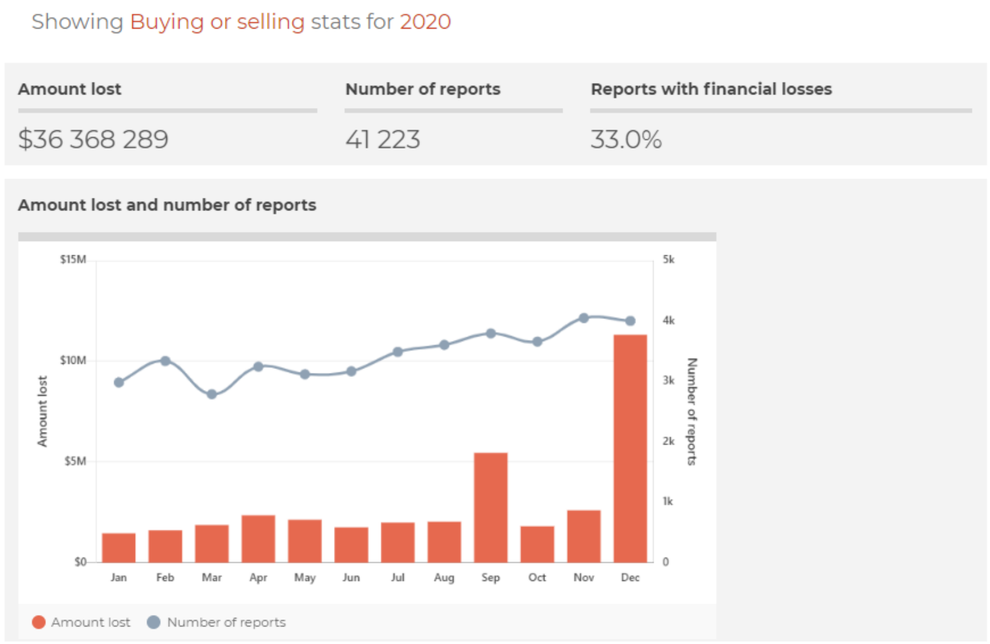
Blockchain, in general, and smart contracts, in particular, have afforded a unique opportunity to solve the shortcomings of traditional escrows. By putting a smart contract at the center of the agreement, escrow transactions become exponentially quicker, significantly more secure, and significantly cheaper. A smart contract is trustless and only executes based on its programming. There is no room for corruption, and officials cannot be bought.

For example: Using conventional escrow services, a simple domain transfer can take days for the seller to receive their money. However, in a decentralized smart contract-powered escrow service, that process could be settled in a matter of minutes/hours.

- Industry Statistics

In recent years, there has been an influx of online transactions between buyers and sellers. Unfortunately, this has coincided with a steady increase in fraud in such transactions.

The chart below shows the increase of “buying and selling” related fraud transactions recorded in Australia during 2020 alone.



Showing Buying or selling stats for 2020

Amount lost	Number of reports	Reports with financial losses
$36 368 289	41 223	33.0%

Amount lost and number of reports

Source: https://www.scamwatch.gov.au/scam-statistics?date=2020&scamid=15

This fraud could have been avoided if a secure and trusted escrow service had been used to facilitate the transactions. PayrLink prides itself in providing a secure service to prevent the losses consumers otherwise would have faced due to fraud.

At the time of establishing the agreement, smart contracts have to designate PayrLink as their arbitrator. When they opt-in, contract creators choose how many jurors and which sub-court will rule their contract in case of a dispute. The idea is that they will select a type of court specialized in the topic of the contract/agreement. For instance, a software development contract will choose a software development arbitration court; an insurance contract will select an insurance arbitration court, and so on.

- Juror votes

During the arbitration process, jurors assess the presented evidence and commit their vote to one of the parties. Jurors selected to any given sub-court will have staked their PAYR tokens for a minimum of one month prior. This condition is to ensure that the jurors will not be immediately related to the agreement/dispute. At the time of voting, jurors submit a hash (vote, address) originating from their address. This is required to make the commitment of each juror different, thus preventing a juror from blindly copying another. When the voting is complete, the individual votes are revealed, and the PayrLink smart contract verifies that it matches the commitment. Jurors failing to reveal their vote are penalized. Jurors who voted incorrectly have to forfeit a portion of their staked PAYR tokens.

After a juror has made a commitment, their vote cannot be changed. But it is still not visible to other jurors or to the parties. This prevents the vote of a single juror from influencing the votes of the others. Jurors can still declare that they voted in a certain way, but it is challenging for them to prove that to other jurors. This is an important feature for the 'focal point' to arise. In game theory, the focal point is the solution that participants would choose in the absence of communication. If jurors knew the votes of the other Jurors, they could be tempted to vote along similar lines instead of the Focal Point.

As these two step processes of committing and then revealing one's vote requires additional user interactions, in some low stakes subcourts, one might want votes to be issued publicly to simplify the user experience.

- Arbitration Fee

Arbitration fees are charged whenever a formal dispute is raised. These fees help ensure that spam arbitration requests are penalized, and jurors are compensated for their work. Each juror in concordance with the final ruling will be paid a fee determined by the sub-court where the dispute is resolved. The smart contract will determine which party will bear the arbitration fee. The rules can be simple. For instance, the party raising the dispute or the party appealing is obligated to pay the fee.

Dispute arbitration fees will be distributed to jurors who take part in the subcourt.

- Common Transaction Fee

PayrLink receives a fraction of the total amount as a common transaction fee. Common transaction fees will be distributed to all jurors who have staked PAYR tokens on the protocol.

3. A Use Case of Arbitrated Contracts

Alice is an entrepreneur based in the United States. She hires Bob, a programmer from Mexico, on a P2P freelancing platform to build a new website for her company. After they agree on a price and the terms and conditions of the agreement, Bob gets to work. A couple of weeks later, he delivers the product. However, Alice is not satisfied with the end result. She argues that the quality of Bob's work is considerably lower than expected. Bob replies that he did exactly what was in the agreement. Alice is frustrated. She can't hire a lawyer for a claim of just a couple hundred dollars with someone halfway around the world.

What if the contract had a clause stating that, should a dispute arise, it would be settled by PayrLink decentralized arbitration? After Bob stops replying to her messages, Alice taps a button that says "Appeal to PayrLink" and fills a simple form explaining her claim.

Thousands of miles away, Chief is a software developer in China, receives a notification. In his "spare time" on the bus commuting to his job, he checks the PayrLink Court Platform to find some arbitration works. He earns a few extra thousand dollars per year by serving as a juror in software development disputes between freelancers and their clients. He usually rules cases in the Website Quality Sub-court. This court requires skills in HTML, JavaScript, and web design to solve disputes between freelancers and their customers. Chief has been staking his 20000 PAYR tokens for over a month. PayrLink uses the Proof-of-Stake approach to set up the sub-courts that will resolve the raised disputes. Jurors with larger stakes will have a greater likelihood of being selected for the arbitration sub-courts and thereby earn the arbitration fees.

Similarly, James, a programmer from England, and Momir, from Serbia, also staked their respective PAYR tokens and were selected as arbitrators, alongside Chief, for the Website Quality Sub-court. They will never know each other, but they will collaborate to settle the dispute between Alice and Bob. On the bus ride back home, Chief analyzes the evidence presented to them and votes for the party he believes is right.

Two days later, after all three Jurors have voted, Alice and Bob receive an email: “The jury has ruled in favor of Alice. The website was not delivered in accordance to the terms and conditions agreed upon by the parties. The smart contract has transferred the funds to Alice”. Jurors are rewarded for their work, and the case is closed.

4. Private Solution with Zero-Knowledge Proof

Over the years, there have been many attempts at creating private transactions on Ethereum. Some workarounds trying to obscure value flows, like using a centralized mixing service, introduce a high degree of counterparty and surveillance risk. PayrLink uses various cryptographic methods, including implementations of ZKP (Zero-Knowledge Proof) to achieve its privacy functionality.

In cryptography, a zero-knowledge proof or zero-knowledge protocol is a method by which one party (the prover) can prove to another party (the verifier) that they know a value, x, without conveying any information apart from the fact that they know the value x. The essence of zero-knowledge proofs is that it is trivial to prove that one possesses knowledge of certain information by simply revealing it; the challenge is to prove such possession without revealing the information itself or any additional information.

If proving a statement requires that the prover possesses some secret information, then the verifier will not be able to demonstrate the statement to anyone else without possessing the secret information. The statement being proved must include the assertion that the prover has such knowledge, but not the knowledge itself. Otherwise, the statement would not be proven in a zero-knowledge fashion because it provides the verifier with additional information about the statement. A zero-knowledge proof of knowledge is a special case when the statement consists only of whether the prover possesses the secret information.

Interactive zero-knowledge proofs require interaction between the individual (or computer system) proving their knowledge and the individual validating the proof.

A zero-knowledge proof approach must satisfy three properties:

- Completeness: if the statement is true, the honest verifier (that is, one following the protocol properly) will be convinced of this fact by an honest prover.
- Soundness: if the statement is false, no cheating prover can convince the honest verifier that it is true, apart from rare instances.
- Zero-knowledge: if the statement is true, no verifier learns anything other than the fact that the statement is true.

PayrLink improves transaction privacy by breaking the on-chain link between the recipient and the assets received with Zero-Knowledge Proof approaches. It uses a smart contract that accepts deposits that a different address can withdraw.

To make a deposit, the user inputs the destination address and sends its hash (called a commitment) along with the deposited amount to the PayrLink smart contract. The contract accepts the deposit and adds the commitment to its list of deposits.

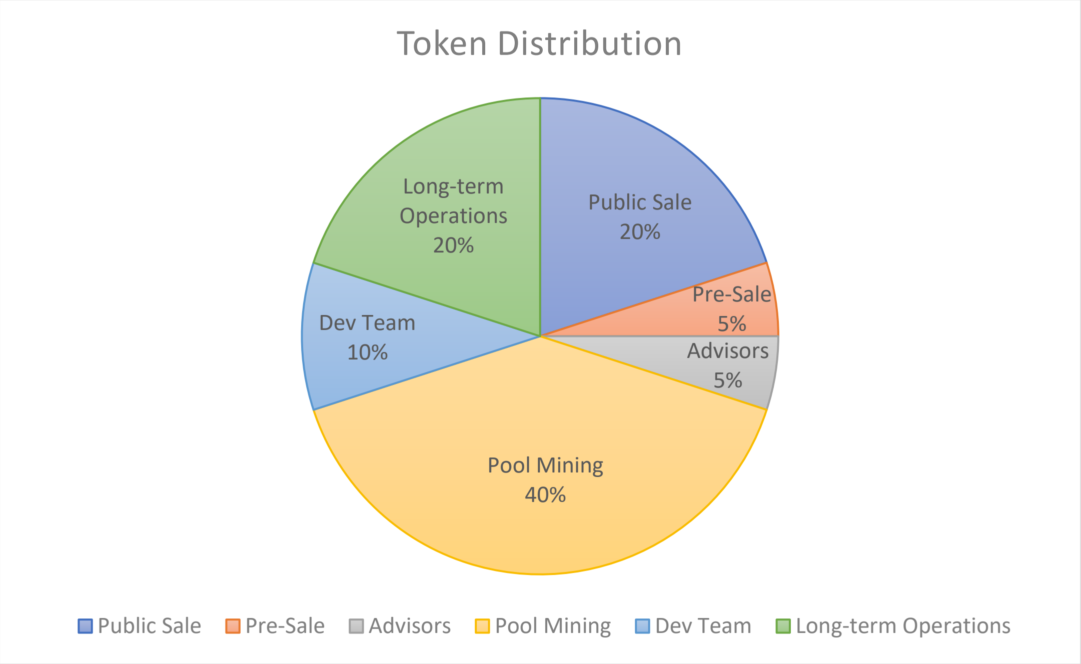
Later, the user decides to release the funds to the destination address. In order to do that, the receiver should provide proof that he or she possesses an address to a commitment from the smart contract's list of deposits.

Once the receiver provides the proof, the funds become the deposit of the receiver, meaning that they can be sent to another address in a private manner.

5. Incentive Advantages

	PayrLink	NAT	Escrow	MangoPay	ShieldPay
Use of Crypto	Yes	Yes	No	No	No
Transaction Fee	0.8%	1~3%	1~6%	1.8%	1.5~3%
Dispute Arbitration Fee	1.2%	1.2%	1~2%	1~2%	1~2%
Decentralized Voting Arbitration	Yes	Yes	No	No	No

6. Tokenomics



A total supply of 200,000,000 PAYR will be minted, of which 50,000,000 PAYR will be made available during the initial token sales.

There will be no soft cap, meaning the project will launch irrespective of the funds raised. The token distribution policy's core focus will be to maximize dispersion while mitigating the risk of centralization.

10% of the total PAYR supply is dedicated to the founding team of PayrLink, while 5% of the supply has been allocated for our advisors.

7. Conclusion

The rise of the digital economy created labor, capital, and product markets that operate in real-time across national boundaries. Cryptocurrencies provide members of this new digital economy a means of engaging in quick transactions in a secure fashion. PayrLink offers smart contract-powered escrow services with private transactions by default and decentralized arbitration. Blockchain users can now access private, trustless services and can rest assured knowing that any dispute will see justice in an efficient and decentralized manner.