TECHNICAL PAPER · VERSION 1.0 · NOVEMBER 2026

ACTUARUS

Programmable escrow: exchanging valuable goods between strangers, with no one holding the funds

> *"Blockchain only matters if it solves a concrete problem."*
>
> ACTUARUS

Etan Fouquet · Business development and distribution
Arthur Veneau · Technical lead
Wilfrid Dubreuil · Core developer

CONTENTS

Summary
1 · Prologue: 2008
2 · The wager on trust
3 · What current solutions do not solve
4 · Genesis: a barn, three friends
5 · Programmable contracts
6 · The ACTUARUS principle
7 · Technical architecture
8 · Dispute resolution
9 · Security
10 · Business model
11 · Legal framework
12 · Roadmap
13 · Conclusion
References

SUMMARY

Buying a valuable item from a stranger is still a gamble. A buyer who pays upfront risks receiving nothing; a seller who ships first risks never being paid. Existing solutions — bank or notarial escrow, documentary credit, secure payment platforms — reduce that risk at the cost of delays of several days and high fees, and by entrusting the funds to an intermediary.

ACTUARUS offers a **non-custodial on-chain escrow**. The buyer's funds are locked in a public smart contract on the Solana blockchain, and can only leave it with the agreement of two of the three signatories to the transaction: the buyer, the seller and the arbitrator. ACTUARUS orchestrates the contract, the proof and the timestamping, without ever taking possession of the funds or being able to move them alone. Settlement takes a few minutes, in approved stablecoins, and every step leaves a trace that anyone can verify.

This document explains where ACTUARUS comes from, the problem it solves, and how it works technically, as written in the program's public code.

What this document is not

This technical paper is neither a public offering of crypto-assets nor a solicitation of investment. ACTUARUS issues no token and promises no return.

CHAPTER 1

PROLOGUE: 2008

Proof instead of trust

On October 31, 2008, in the middle of the financial crisis, an author signing as Satoshi Nakamoto published a nine-page paper: *Bitcoin: A Peer-to-Peer Electronic Cash System* [1]. The observation is simple: online commerce relies almost entirely on financial institutions acting as trusted third parties. These intermediaries arbitrate disputes, which makes payments reversible and costly, and forces every merchant to distrust their customers.

> *"What is needed is an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party."*
>
> Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, 2008 [1]

Bitcoin solved the first problem: sending value to a stranger, without a bank and without the possibility of double-spending. But from its very introduction, Nakamoto pointed to a limit. An irreversible payment protects the seller; it leaves the buyer without recourse. His answer fits in one sentence: routine escrow mechanisms could easily be implemented to protect buyers.

Eighteen years later, that "routine" escrow has still not entered everyday use. Exchanging a real asset — a vehicle, a machine, a digital asset — for a payment, between two people who do not know each other, remains as risky as ever. This is the missing link ACTUARUS wants to build.

CHAPTER 2

THE WAGER ON TRUST

Why an exchange between strangers fails

In 1970, the economist George Akerlof described the “market for lemons” [2]. In the used market, the seller knows the true condition of the item; the buyer does not. Unable to tell a good vehicle from a bad one, the buyer distrusts everyone, offers an average price, and the good sellers end up leaving the market. Information asymmetry does not merely create victims: it destroys exchanges that would have benefited both parties.

A direct transaction concentrates two risks, symmetrical and impossible to eliminate through good faith alone:

- **The buyer's risk**: paying for an item that does not exist, never arrives, or does not match what was promised.
- **The seller's risk**: delivering an item and never being paid, or having a payment reversed after delivery.

The scale of the problem is measurable. In 2024 alone, the FBI's Internet Crime Complaint Center recorded **49,572 complaints** of non-payment or non-delivery, for **more than $785 million** in reported losses in the United States [3]. These figures only count victims who filed a complaint, and do not measure the transactions that never took place for lack of trust.

Added to these two risks is the opacity of the asset itself: its history, its successive owners and its actual condition at the time of each sale remain unverifiable.

CHAPTER 3

WHAT CURRENT SOLUTIONS DO NOT SOLVE

Securing has always meant entrusting

Tools exist to secure an exchange. All rest on the same principle: temporarily entrusting the funds to a third party. That principle has a price.

Solution	How it works	Limits
Bank or notarial escrow	A bank or a public officer holds the funds until the conditions are met.	Several days of delay, significant fees, business hours only, reserved for large amounts.
Documentary credit	The buyer's bank undertakes to pay the seller upon presentation of compliant documents, under the International Chamber of Commerce's UCP 600 rules [4].	Heavy procedure, banking costs, several weeks; the bank checks documents, not the goods.
Secure payment platforms	An intermediary collects the payment and passes it on to the seller after confirmation.	Funds are held by the platform: the user depends on its solvency and its decisions.
Direct payment	Bank transfer or cash, no intermediary.	No protection: one of the two parties takes all the risk.

None of these solutions offers speed, a predictable cost, proof verifiable by everyone, and the assurance that no one can dispose of the funds alone, all at once. This fourfold objective guided the design of ACTUARUS.

CHAPTER 4

GENESIS: A BARN, THREE FRIENDS

How ACTUARUS was born

It all begins with a childhood friendship. Etan and Arthur grew up together, then life drew them apart. Years later, chance brought them face to face again. Each had followed their own path, and their skills no longer had anything in common.

Etan trades goods. He buys and resells, most often from one individual to another, and he knows intimately the problem Akerlof describes: none of his transactions is truly secure, and sometimes the products delivered do not live up to what was promised. Every purchase is a gamble.

Arthur, for his part, has been working in blockchain since 2021. He knows what a smart contract can guarantee where trust is lacking. Together, they decide to look for a solution. But the conclusion is quickly drawn: Arthur masters blockchain without the coding experience such a project requires, and Etan has neither.

It is Etan who knows the missing piece: Wilfrid, a computing veteran. Years spent serving large French companies, notably in insurance, and a role in the creation of the Carte Vitale. The kind of profile that knows what it means to build a system that millions of people must be able to rely on.

The two friends go to find him, their idea in mind. One day, the three of them meet in a barn in the countryside. They talk, compare what they know, try to understand what each sees of the problem. As the conversation unfolds, the idea takes shape: an escrow where code replaces the trusted third party, and where no one can dispose of other people's money alone.

ACTUARUS was born there: from a rediscovered friendship that became a trio, from a lived problem, and from a barn.

CHAPTER 5

PROGRAMMABLE CONTRACTS

From the coffee machine to the smart contract

In 1997, the computer scientist and jurist Nick Szabo formalized the notion of *smart contract* [5]: a protocol that executes the clauses of a contract by itself, so that no party can evade them. His founding example is the vending machine: the machine only hands over the product once the coin is received, with no need to trust the merchant.

It took until 2014 and Vitalik Buterin's Ethereum white paper [6] for such contracts to become programmable on a public blockchain. Then, in 2017, Anatoly Yakovenko introduced Solana [7], an architecture designed to process a very large number of transactions at very low cost.

Why Solana

- **Cost**: network fees on Solana amount to a fraction of a cent per operation, which allows ACTUARUS to bear them entirely. On Ethereum, those fees would have weighed directly on the price paid by users.
- **Speed**: a transaction is confirmed within seconds, which makes locking and releasing funds almost instantaneous.
- **Ecosystem**: EURC and USDC, Circle's stablecoins, and the Squads multisig, which secures ACTUARUS's accounts, are natively available on Solana.

CHAPTER 6

THE ACTUARUS PRINCIPLE

Code holds the funds, ACTUARUS orchestrates the proof

An ACTUARUS transaction follows four steps. The rules are set before the deposit and can no longer be modified unilaterally once the funds are locked.

1 **Agreement**
The parties set the price, the condition of the item, the delivery conditions and the compliance criteria. These terms form an electronic contract signed by both parties, via Firma, with two-factor authentication by email.

2 **Locking**
The buyer deposits the funds into the smart contract, in EURC, USDC or SOL. They are locked by the code, in a vault specific to the transaction.

3 **Verification**
The seller delivers and submits supporting documents; the buyer inspects the item and confirms its compliance. A warranty period opens, during which the buyer can dispute.

4 **Release**
The smart contract releases the funds to the seller. The transaction is closed, timestamped, and recorded in the item's tamper-proof history.

Party	Role	What it cannot do
Buyer	Deposits the funds, confirms compliance, may open a dispute.	Recover the funds without the seller's or the arbitrator's agreement.
Seller	Delivers the item, submits supporting documents, receives the payment.	Collect without the buyer's or the arbitrator's agreement, or before the warranty period ends.
Smart contract	Holds the funds and executes the decided outcome.	Execute anything other than what the parties signed.
ACTUARUS	Drafts the contract, timestamps, pays the network fees, arbitrates disputes.	Move the funds alone, or impose a split.

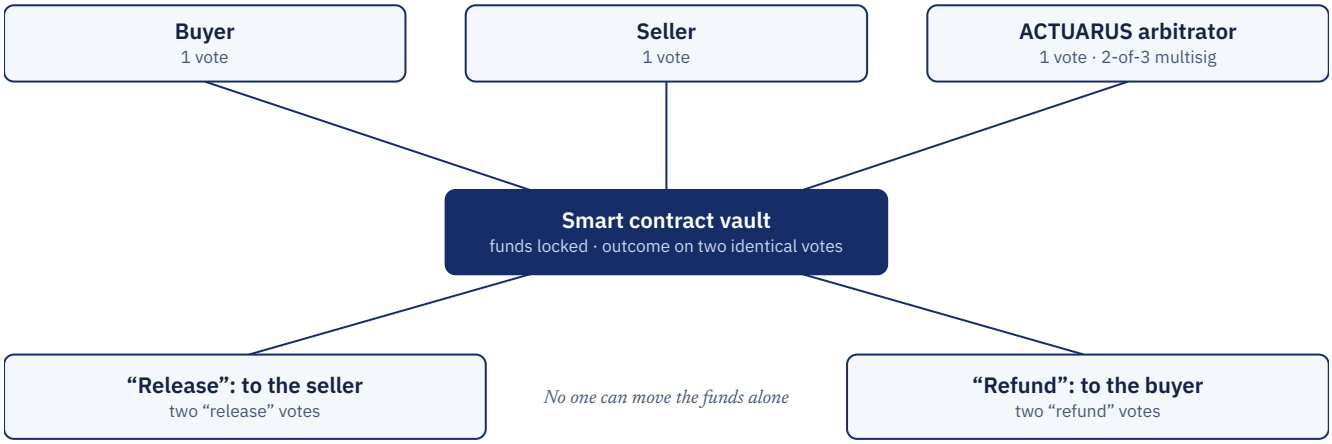
CHAPTER 7

TECHNICAL ARCHITECTURE

What the code guarantees

The ACTUARUS escrow program is deployed on Solana at address **DNwHyasEkHQYfswjPAxvnudCgN1gdZuHA2y2TSp8GVXE**. It is built with the Anchor framework and its source code is published under the Apache 2.0 license [8].

A 2-of-3 multisignature escrow. Each deposit brings together three distinct signatories: the buyer, the seller and the arbitrator. Each votes only once, “release” or “refund”, and their vote is final. At the second identical vote, the funds are paid out: to the seller for “release”, to the buyer for “refund”. The program checks that the three accounts are different, so that no signatory holds two votes.



A warranty period. Once the seller's supporting documents are submitted, a warranty period opens, lasting at least 24 hours and at most one year. When it ends, if no “refund” vote has been cast and no dispute has suspended it, anyone can trigger the payment to the seller. The funds therefore never remain locked for lack of a second vote, and the buyer always has at least a full day to dispute.

Partial refund. The seller can offer to give back part of the amount; if the buyer accepts that exact amount, the proposed share goes to the buyer and the rest to the seller, in the same transaction. The arbitrator cannot impose a split.

Network fees covered. A platform account, separate from the arbitrator, pays the network fees and the storage reserve of each account. The parties receive exactly the amounts set at deposit. This account is neither an arbitrator nor a recipient of commissions.

Item	Detail
Accepted assets	SOL, USDC and EURC — for tokens, only official Circle issuances, verified by the program.
Commission	Set and collected at the time of deposit; it cannot be modified during a transaction.
Arbitrator	Squads multisig vault: each of its votes requires the approval of two of three signatories.
Closing	Once the deposit is settled, the transaction's accounts are closed; the history remains recorded on the blockchain.

Item	Detail
Proof	Contract signed via Firma, fingerprint and timestamp of each step, viewable in the item's history.

CHAPTER 8

DISPUTE RESOLUTION

A human decision, informed by an AI jury

An escrow is only as good as the way it handles disagreements. When a dispute is opened, the warranty period is suspended and the funds stay locked.

1 **Opening**
One of the parties opens the dispute. Each submits its evidence: photos, messages, documents.

2 **Jury**
Five artificial intelligence agents are drawn at random from one hundred, according to the nature of the transaction. Neither party chooses its jurors.

3 **Analysis**
Each agent examines the signed contract, the evidence and the legal sources, then issues a reasoned opinion.

4 **Decision**
A member of the ACTUARUS team reviews the file and the jury's opinions, and decides within five days on a refund to the buyer or a payment to the seller.

The decision is expressed on the blockchain through the arbitrator's vote. That vote is never enough on its own: it must join that of one of the two parties to reach the majority of two votes. No funds are refunded or released by an artificial intelligence alone, and none can be by ACTUARUS alone.

Other projects have explored fully decentralized arbitration, entrusting the decision to anonymous jurors paid in tokens [9]. ACTUARUS made a different choice: that of an identifiable, accountable human decision, supported by the systematic analysis of an AI jury.

CHAPTER 9

SECURITY

Verifiable by everyone, not only by us

Guarantee	Implementation
Audit	Smart contract audited by AMJI-CONCEPT; version 1.3.0, audit of November 6, 2026. The fixes resulting from the audit are referenced in the code.
Public code	Source published on GitHub (Actuarus/escrow-program), under the Apache 2.0 license.
Verifiable build	The program recompiles reproducibly: anyone can verify that the published code is the code deployed on Solana.
Controlled upgrades	The upgrade authority is a 2-of-3 Squads multisig, with a 48-hour delay before any change.
Immutability	The contract becomes immutable at the end of a three-month corrective maintenance period following its launch.
Key separation	The account that pays the fees, the arbitrator and the upgrade authority are three distinct accounts. The test key cannot be compiled for the main network.
Reporting	Security contact published: contact@actuarus.com.

CHAPTER 10

BUSINESS MODEL

A price known before you commit

ACTUARUS earns revenue through a tiered (marginal) commission, calculated by bracket: each rate only applies to the part of the price within its bracket. Network fees, the electronic contract, on-chain proof and dispute handling are included. There are no sign-up fees and no subscription, and the parties choose who pays the commission.

Price bracket	Rate on the bracket
Up to €10,000	5.5%
€10,000 to €50,000	5%
€50,000 to €100,000	3.8%
€100,000 to €500,000	2.5%
€500,000 to €1,000,000	2%
Above €1,000,000	1%

For example, a €15,000 transaction costs €800, or 5.33%; a €100,000 transaction costs €4,450, or 4.45%. The minimum amount is €5 per transaction. A custom quote is offered for large volumes and marketplaces.

The referral program. Anyone can recommend ACTUARUS. When the seller was referred, the referrer receives 20% of ACTUARUS's commission on each of their sales, with no cap. The referral program does not change the price paid by the parties.

CHAPTER 11

LEGAL FRAMEWORK

An architecture designed for European law

The ACTUARUS solution falls **outside the scope of the European MiCA regulation** [10]. ACTUARUS is neither a payment institution nor a custodian: it does not hold, exchange or transfer crypto-assets on behalf of its users, and cannot move any escrowed funds alone. The conversion between euros and stablecoins is carried out with authorized providers, chosen by the users.

Settlement in approved stablecoins. EURC and USDC are e-money tokens issued by an institution authorized in the European Union, backed one for one and redeemable at face value.

The electronic signature. Contracts are signed via Firma, as an electronic signature within the meaning of the eIDAS regulation [11], reinforced by two-factor authentication. The signed contract, its timestamp and the on-chain trace together constitute the proof of the transaction.

Personal data. No identity data is recorded in clear on the blockchain. The obligations specific to users are detailed in the compliance notes published by ACTUARUS.

CHAPTER 12

ROADMAP

What is done, what is next

Milestone	Status
Escrow program deployed on Solana, source code published	Completed
Smart contract audit by AMJI-CONCEPT, version 1.3.0	Completed · November 2026
Firma electronic contract, AI jury and human decision	Completed
Referral program	Completed
End of corrective maintenance: contract permanently immutable	Three months after launch
Dedicated offer for marketplaces, integrated into their flow	Upcoming
Opening to other networks, including Ethereum, when costs allow	Horizon

CHAPTER 13

CONCLUSION

The contract, and nothing but the contract

In 2008, Nakamoto imagined “routine” escrow to protect buyers. ACTUARUS offers a concrete realization: a contract signed by two free parties, executed by code that anyone can read, and whose funds no party — not even ACTUARUS — can divert alone.

This idea is older than the blockchain. In the nineteenth century, the American jurist Lysander Spooner already argued that the authority of a commitment rests only on the consent of those who bind themselves to it [12]:

> *“The Constitution has no inherent authority or obligation. It has no authority or obligation at all, unless as a contract between man and man.”*
>
> Lysander Spooner (1808–1887), *No Treason*, No. VI, 1870 [12]

ACTUARUS applies this principle to exchange: the only rule that matters is the one the parties signed. And because blockchain only matters if it solves a concrete problem, we chose to solve one that everyone has already encountered: trusting a stranger.

REFERENCES

[1] Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. bitcoin.org/bitcoin.pdf

[2] Akerlof, G. A. (1970). The Market for “Lemons”: Quality Uncertainty and the Market Mechanism. *The Quarterly Journal of Economics*, 84(3), 488-500.

[3] Federal Bureau of Investigation (2025). *Internet Crime Report 2024*. Internet Crime Complaint Center (IC3).

[4] International Chamber of Commerce (2007). *Uniform Customs and Practice for Documentary Credits*, ICC Publication No. 600 (UCP 600).

[5] Szabo, N. (1997). Formalizing and Securing Relationships on Public Networks. *First Monday*, 2(9).

[6] Buterin, V. (2014). *Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform*.

[7] Yakovenko, A. (2017). *Solana: A new architecture for a high performance blockchain*.

[8] ACTUARUS (2026). Escrow program, version 1.3.0. github.com/Actuarus/escrow-program

[9] Lesaege, C., Ast, F. and George, W. (2019). *Kleros*, short paper.

[10] Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets (MiCA).

[11] Regulation (EU) No 910/2014 of 23 July 2014 (eIDAS), as amended by Regulation (EU) 2024/1183.

[12] Spooner, L. (1870). *No Treason, No. VI: The Constitution of No Authority*. Boston.

This technical paper describes how ACTUARUS works as of the date of its publication. It is neither a public offering of crypto-assets, nor investment advice, nor legal or tax advice. ACTUARUS issues no token. Contact: contact@actuarus.com