Prepared by

Group 9

9 December 2023

DeTrust: Redefining Trust in Every Contract

Abstract

In this white paper, we present an overview of the DeTrust platform, outlining its core components and key features. We'll delve into the creation of customisable smart contracts, the community-driven dispute resolution mechanism, the utility of the DTR token, user reputation systems, and our unwavering commitment to privacy and security.

Join us on this journey as we navigate the intricate landscape of digital contracts, forging a path toward a future where trust is at the heart of every digital interaction. DeTrust is poised to revolutionise the way we transact, offering a safer, more secure, and community-driven alternative for financial and service-based agreements.

Welcome to DeTrust: Redefining Trust in Every Contract.

1. Introduction

1.1 Building Trust in a Digital World

In an increasingly digital world, where transactions and agreements span across borders and boundaries, trust is paramount. Traditional methods of establishing trust through intermediaries and centralised systems are no longer sufficient to meet the needs of today's global, decentralised economy. It is within this landscape that DeTrust emerges—a groundbreaking solution designed to restore trust in digital contracts and transactions.

1.2 The Trust Challenge

Digital contracts, which underpin a vast array of financial, commercial, and service interactions, have revolutionised the way we engage with the world. However, as their adoption grows, so too does the challenge of ensuring the security, transparency, and fairness of these agreements. Trust issues, disputes, and uncertainties often plague these digital interactions, leaving users exposed to risks and vulnerabilities.

1.3 Introducing DeTrust

DeTrust is a visionary blockchain-based platform that reimagines the way we create, execute, and enforce digital contracts. Rooted in the principles of decentralisation, transparency, and community consensus, DeTrust empowers users to interact with

confidence, assured that their agreements are backed by a robust and impartial framework.

1.4 Our Vision

At DeTrust, we envision a world where trust is inherent in every digital interaction. Our platform leverages the transformative potential of blockchain technology to provide users with a secure, transparent, and community-driven approach to contract creation and resolution. By removing the need for intermediaries and placing trust decisions in the hands of the community, we aim to redefine the way we engage in transactions and service agreements.

2. Why Blockchain?

2.1 Trust in a Trustless Environment

Blockchain and decentralised consensus empower users to engage in digital contracts in a trustless environment. This means that parties can collaborate and transact securely without necessarily trusting each other. The use of self-fulfilling smart contracts means that trust is instead established through code and community consensus, reducing the risk of contractual disputes. Additionally, the inherent immutability of blockchain ensures that once contract details are recorded, they cannot be altered or tampered with. This feature enhances trust and security in digital contracts, a level of assurance that traditional forms of storage may lack.

2.2 Sense of Ownership and Responsibility

Decentralisation extends to the governance of the DeTrust platform itself. Decisions regarding dispute resolution, protocol upgrades and rule changes are made collectively by the community of token holders. The transparency of blockchain technology allows all participants to independently verify governance decisions and ensures that each participant's influence is proportionate to their ownership of tokens. This decentralised governance model is more inclusive and transparent compared to traditional decision-making structures. This democratic approach ensures that the platform evolves in a manner that aligns with the interests and values of its users. It also fosters a sense of ownership and responsibility among participants.

2.3 Increasing Efficiency by Reducing Intermediaries

Traditional contract enforcement often involves intermediaries such as banks and legal entities. These intermediaries add complexity, cost, and potential delays to transactions.

DeTrust removes the need for a central authority to oversee transactions, streamlining the contract process, making it more efficient and cost-effective for users. Making use of the blockchain's decentralised nature, DeTrust ensures that transactions are executed directly between parties, enhancing efficiency and lowering barriers to entry.

2.4 Summary

The utilisation of blockchain and decentralised distributed ledger technology lies at the core of DeTrust's mission to build trust in digital contracts. By harnessing the transparency, security, and community-driven governance of these technologies, DeTrust offers a superior alternative to centralised systems, enhancing the trust and security of digital agreements across various domains.

3. Use Cases and Applications

DeTrust opens the door to a wide array of use cases and applications, revolutionising the way digital contracts are created and executed. Below are some key scenarios where DeTrust can make a significant impact.

3.1 Financial Contracts

3.1.1 Lending and Borrowing

DeTrust provides a secure platform for individuals and businesses to create customised lending agreements. Borrowers can access funds with confidence, while lenders can ensure repayment terms are met with transparency and dispute resolution as a safeguard.

3.1.2 Investment Agreements

DeTrust can be used for creating investment contracts, enabling individuals and entities to pool their resources in ventures with defined terms and transparent profit-sharing mechanisms.

3.2 Service Agreements

3.2.1 Freelancer Contracts

Freelancers and clients can establish service contracts with clear deliverables, milestones, and payment terms. Smart contracts on DeTrust ensure that funds are held in escrow until services are satisfactorily delivered.

3.2.2 Subscription Services

Subscribers can create and automate subscription payment agreements with service providers. DeTrust's dispute resolution system can intervene in cases of service disruptions or disputes over subscription terms.

3.3 E-commerce and Trade

3.3.1 Purchase Agreements

Buyers and sellers in e-commerce can create digital purchase agreements that automatically release funds upon successful delivery or receipt of goods. Dispute resolution is available in case of delivery issues.

3.4 Intellectual Property

3.4.1 Content Licensing

Content creators and licensors can use DeTrust to create digital contracts for licensing their intellectual property. Royalties and compensation are automatically distributed based on predefined terms.

3.5 Employment Contracts

3.5.1 Employment Agreements

Employers and employees can establish employment contracts with clear terms, including compensation, benefits, and termination clauses. Smart contracts can automate payroll and benefit disbursements.

3.6 Summary

These are just a few examples of the diverse use cases and applications that DeTrust empowers. The platform's customisable smart contracts, decentralised dispute resolution, and trust-enhancing features make it a versatile tool for individuals and businesses across various industries, bringing newfound trust and security to digital interactions.

4. Key Value Proposition

DeTrust is designed to address the following key challenges in the digital contract ecosystem.

4.1 Security and Trust

Digital contracts often lack transparency and can be vulnerable to manipulation or disputes. DeTrust provides a secure and transparent environment for creating and executing contracts, enhancing trust among users.

4.2 Customisation

Every user's needs are unique, and generic contract templates may not suffice. DeTrust allows users to create customizable smart contracts using the Solidity programming language. This customization empowers users to tailor contracts to their specific requirements.

4.3 Fair Dispute Resolution

Disputes can arise in any contractual relationship. DeTrust introduces a community-driven dispute resolution mechanism. If a dispute occurs, the community reviews chat logs and transaction data to vote on a resolution. This ensures fairness and reduces the reliance on costly and time-consuming legal processes.

5. Technical Architecture

DeTrust's technical architecture is designed to provide a secure, transparent, and user-centric environment for creating, executing, and resolving digital contracts. Our platform leverages cutting-edge blockchain technology and decentralised systems to provide a robust foundation for users to confidently engage in digital contracts while redefining trust in every interaction.

5.1 Blockchain Infrastructure

DeTrust operates on a permissionless blockchain infrastructure, ensuring open and inclusive participation. The blockchain serves as the foundational ledger for recording all transactions and smart contracts. It employs a hybrid consensus mechanism combining elements of Proof of Stake (PoS) and Proof of Authority (PoA) to ensure transaction validation and network security.

5.2 Smart Contracts

At the heart of DeTrust are smart contracts, coded in Solidity. These smart contracts enable users to define and customise the terms, conditions, and actions of their digital agreements. To ensure the reliability of these contracts, each contract needs to be verified by other users. The number of verifications needed is proportional to the tier of the user. Once deployed on the blockchain, smart contracts are self-executing, eliminating the need for intermediaries.

5.3 Decentralised Dispute Resolution

DeTrust's innovative decentralised dispute resolution system is a key component of the platform. When disputes arise, community members can anonymously review evidence and vote on resolutions. In cases where a consensus is not reached, randomly selected community members act as moderators to make the final decision. This system ensures fairness and impartiality in dispute resolution.

5.4 Trust Score System

The trust score of a user, defined by Trust, is a decimal value between 1 and 5 to DeTrust users. Each user will begin with a neutral score of 2.5, and will be segmented according to trust score tiers:

Tier	Trust Score	Description
A	4.5 - 5.0	Highly trusted
B	3.0 - 4.49	Trusted
C	2.0 - 2.99	Neutral
D	0 - 1.99	Unreliable

5.4.1 Earning and Losing Trust

These are the following ways in which users of DeTrust will earn or lose Trust.

1. When users successfully complete a contract with no security issues or disputes, the Trust of both parties increases.
2. If a contract is found to be fraudulent, the Trust of the contract parties will be decreased. Should any users falsely verify these fraudulent contracts, the Trust of these users will be decreased as well.

3. Users will stake Trust when voting in a dispute. The user's Trust will increase if he chooses the majority vote, and decrease if he chooses the minority vote.
4. During a dispute mediation, should the mediator deem that a contract party is committing fraudulent acts, they can propose a reduction in Trust of the user.

5.5 Consensus Mechanism

Our hybrid consensus mechanism combines the efficiency of PoS with the security of PoA. Validators are selected based on their stake in the network and their authority status. This approach ensures fast transaction processing while maintaining network integrity and security.

5.6 Decentralised Storage

To safeguard contract data and minimise single points of failure, DeTrust employs decentralised storage solutions. Contract-related information is distributed across the network, ensuring redundancy and resilience.

5.7 Privacy Measures

While maintaining transparency, DeTrust prioritises user privacy. Advanced encryption techniques and zero-knowledge proofs protect sensitive contract data and transaction details, ensuring confidentiality where needed.

5.8 Scalability

DeTrust addresses scalability challenges through layer 2 scaling solutions and off-chain processing. This approach enables the platform to handle increased transaction volumes efficiently as it grows. DeTrust is actively exploring the possible integration with MetaMask, a widely used Ethereum wallet and gateway to the decentralised web. This integration will allow users to seamlessly interact with the DeTrust platform using their MetaMask wallets, simplifying the onboarding process and providing a familiar interface for managing digital contracts.

5.9 Summary of System Design

The costs, rewards and penalties for contract creation and completion can be summarised as follows:

Tier	**Contract Creation Cost (DTR)**	**Contract Completion Reward (Trust Score)**	**Contract Verification Reward**	**Penalty for False Verification**
A	20 (2 users)	+ 1		Parties: - 2 Trust,

B	40 (4 users)	+ 5	+ 10	DTR burned to 500 Verifiers: - 1 Trust, DTR - 100
C	80 (8 users)	+ 10		
D	100 (10 users)	+ 15		

Table 1: Contract Creation Costs, Rewards and Penalties

5.10 In-depth Details of the System Design and Token Economy

Please refer to the DeTrust System Design Document for more in-depth details of DeTrusts technical architecture and token economy.

6. Token Economy

6.1 What is DTR for?

DTR is an in-app currency for users to use to pay for transactions. DTR does not have any value in the real world and will not have a market cap.

When users first join the DeTrust platform, they will receive 500 DTR. To create smart contracts, both the Initiator and Respondent are required to pay a fee corresponding to their respective trust score tiers for contract creation as shown in Table 1. Should the user have insufficient DTR they will be unable to create more smart contracts until more DTR is obtained. There are a total of four ways to obtain DTR.

6.2 How to obtain DTR?

1. Issue tokens weekly to all users based on their tiers.
    - Tier A: 200 DTR
    - Tier B: 100 DTR
    - Tier C: 50 DTR
    - Tier D: 0 DTR

2. Users can purchase DTR using ETH.

3. Users can obtain DTR by participating in disputes as a voter on the majority side, or as a mediator.

4. Users, in Tier C and above, can obtain DTR by verifying contracts other users have created.

7. Governance Mechanism

One of the core pillars of DeTrust's governance mechanism is its decentralised dispute resolution system. Designed to ensure fairness and impartiality in resolving contract disputes, this system leverages community consensus and blockchain technology. The following is an in-depth look at how it operates.

7.1 Dispute Submission

When a dispute arises between parties involved in a DeTrust contract, any affected party can submit the dispute to the platform. This submission initiates the dispute resolution process.

7.2 Community Review

Upon dispute submission, the community, consisting of DTR token holders, has the opportunity to review the dispute. This review process is essential in ensuring a diversity of perspectives and impartial judgement.

7.3 Access to Evidence

To make informed decisions, the community members have access to all relevant evidence, including chat logs and transaction data associated with the disputed contract. This transparency ensures a comprehensive understanding of the dispute.

7.4 Anonymous Voting

Community members cast anonymous votes to determine the outcome of the dispute. Anonymity ensures that votes are based solely on the merits of the case, without bias or external influence.

7.5 Majority Decision

The dispute resolution outcome is determined by a majority vote within the community. If one resolution option garners more votes than the other, it becomes the final decision.

7.6 Random Moderators (Fallback Mechanism)

In cases where the community vote results in a tie or an inconclusive outcome, a fallback mechanism comes into play. Randomly selected users from the community are designated as moderators to make the final decision. This ensures that disputes are ultimately resolved, even in scenarios of voting deadlock.

7.7 Transparency and Accountability

Every step of the dispute resolution process is recorded on the blockchain, providing transparency and accountability. Users can verify the fairness and legitimacy of the resolution.

7.8 Incentivising Participation

To encourage active participation in the dispute resolution process, community members who engage in reviewing disputes and align their votes with the majority receive DTR token rewards. This incentive ensures an engaged and vigilant community.

7.9 Evolving Dispute Resolution

As the DeTrust platform grows, the dispute resolution mechanism may evolve. Community feedback and governance decisions will guide improvements, making the process more efficient and effective.

7.10 Summary

The decentralised dispute resolution mechanism is a testament to DeTrust's commitment to impartiality, transparency, and community empowerment. It ensures that contract disputes are resolved fairly, with the collective wisdom of the community driving the outcomes. As DeTrust's governance evolves, so too will the dispute resolution process, keeping it aligned with the values and needs of its users.

8. Stakeholder Incentives

8.1 Users

8.1.1 Secure and Customisable Contracts

Users benefit from secure smart contracts that are customisable to their specific needs, reducing the risk of misunderstandings or disputes.

8.1.2 Trust Scores

Users who consistently fulfil contracts without disputes or with favourable dispute outcomes earn higher trust scores. A higher trust score enhances their reputation within the DeTrust community, making them more attractive partners for future contracts. Additionally, earning a higher trust score will increase a user's likelihood of being chosen as a moderator, potentially resulting in rewards for their participation.

8.1.3 DTR Rewards

Successful contract fulfilment and participation in dispute resolution can earn users DTR tokens. These tokens can be used for creating more contracts.

8.2 Moderators

8.2.1 DTR Rewards

Moderators play a critical role in dispute resolution. They are rewarded with DTR tokens for their active involvement in ensuring fair outcomes. This incentive encourages knowledgeable and impartial community members to act as moderators.

8.3 Summary

DeTrust's stakeholder incentives are aligned with the platform's objectives: to create a secure, transparent, and community-driven environment for digital contract creation and resolution. Users are rewarded for their trustworthiness, and moderators for their impartiality—all of which contribute to building a strong and thriving DeTrust ecosystem.

9. Possible Improvements

- Include future plans for enhancements and expansions.

In this section, we outline our future plans for enhancing and expanding the DeTrust platform. Our commitment to continuous improvement aims to elevate the quality of trust within the DeTrust community and provide a more versatile and user-centric experience.

9.1 Outcome variation

To enhance the flexibility and inclusivity of DeTrust, we envision introducing a feature that allows the community to suggest alternative outcomes for contract resolutions. Recognising that outcomes suggested by the involved parties might be too extreme, this improvement would enable users to propose additional outcomes. Subsequently, community members can choose from a range of suggested outcomes, or through a democratic voting process, select the most fitting resolution. This approach ensures that the contract resolution process is not confined to binary options but reflects the diverse perspectives and preferences within the DeTrust community.

9.2 Service Delivery Evaluation

Acknowledging the nuanced nature of service delivery, DeTrust plans to refine its contract resolution system to consider the varying degrees of success or failure. Contracts often exist in a spectrum, and by incorporating this variability into our resolution mechanism, users can assess the quality of service on a more granular level. This enhancement aims to capture the subtleties of contract outcomes, providing a more comprehensive and nuanced evaluation that better aligns with the real-world complexities of service delivery.

9.3 Economic Incentives for Responsible Voting

To mitigate the potential for biassed voting, we recognise the importance of introducing economic incentives that promote responsible decision-making within the DeTrust ecosystem. While users may have social connections with the involved parties, implementing a cost for making poor votes can encourage more thoughtful and impartial judgments. This approach ensures that users are motivated to vote based on the merit of the contract rather than personal relationships.

By incorporating these improvements, DeTrust aims to evolve into a platform that not only addresses the challenges of trust in digital contracts but also adapts to the dynamic needs and expectations of its diverse user base.

10. Conclusion

DeTrust is not just a platform; it is a vision of trust redefined.

We have harnessed blockchain technology and decentralised governance to create a space where trust is tangible and disputes are fairly resolved. With DeTrust, every digital contract is backed by a community that values transparency, security, and fairness. Our commitment to continuous improvement ensures a more secure, efficient, and user-centric platform.

Join us in shaping the future where trust in every contract is a reality.

Welcome to DeTrust, where we will redefine trust in your contracts.