Computer Science and Application 计算机科学与应用, 2025, 15(4), 260-265
Published Online April 2025 in Hans. https://www.hanspub.org/journal/csa
https://doi.org/10.12677/csa.2025.154098

Hans汉斯

面向区块链的保证数据源认证的zk-SNARK方案

司浩然，岳笑含

沈阳工业大学信息科学与工程学院，辽宁 沈阳

收稿日期：2025年3月15日；录用日期：2025年4月14日；发布日期：2025年4月22日

摘　要

现有区块链交易通常使用加密货币作为抵押物并进行链上交易，但由于加密货币的波动性，面临清算风险。本文旨在区块链与链下资产的融合，降低区块链交易风险，并提出一种基于零知识证明的密码学方案，将链下资产绑定到链上交易作为抵押物。该方案在支持区块链交易的同时，确保数据隐私性、数据源认证和低Gas消耗。在性能方面，我们对所提方案进行了功能分析和实验评估，研究了不同实体在各个阶段产生的计算成本。实验结果表明，该方案在功能上可行，并且计算效率较高。综上，该方案为区块链交易提供了一种安全且高效的基于零知识证明的解决方案。

关键词

零知识证明，区块链，Gas

A zk-SNARK Scheme for Ensuring Authentication of Data Source in Blockchain

Haoran Si, Xiaohan Yue

School of Information Science and Engineering, Shenyang University of Technology, Shenyang Liaoning

Received: Mar. 15th, 2025; accepted: Apr. 14th, 2025; published: Apr. 22nd, 2025

Abstract

Existing blockchain transactions typically use cryptocurrencies as collateral for on-chain trading. However, the volatility of cryptocurrencies exposes these transactions to significant liquidation risks. This paper aims to integrate blockchain with off-chain assets to mitigate such risks and proposes a cryptographic scheme based on zero-knowledge proofs that links off-chain assets to on-chain transactions as collateral. The proposed scheme enables secure blockchain transactions

文章引用：司浩然，岳笑含．面向区块链的保证数据源认证的 zk-SNARK 方案[J]．计算机科学与应用，2025，15(4)：260-265. DOI: 10.12677/csa.2025.154098

while ensuring data privacy, authentication of data sources, and low gas cost. From a performance perspective, this paper conducts a functional analysis and experimental evaluation, assessing the computational costs incurred by different entities at various stages. Experimental results demonstrate that the scheme is both functionally viable and computationally efficient. In conclusion, this work presents a secure and efficient zero-knowledge-proof-based solution for blockchain transactions.

Keywords

Zero-Knowledge Proof, Blockchain, Gas

1. 引言

区块链交易[1]为传统的中心化交易提供无中介、透明和开放的替代方案。然而现有区块链交易通常以链上资产进行交易(如加密货币)，易因货币价格波动而发生清算操作，缺乏稳定性[2]。本文旨在实现一种密码学方案，通过链下传统资产进行区块链交易，在增强区块链交易价格稳定的同时，拓展交易资产的范围，增强传统资产的流动性[3]。

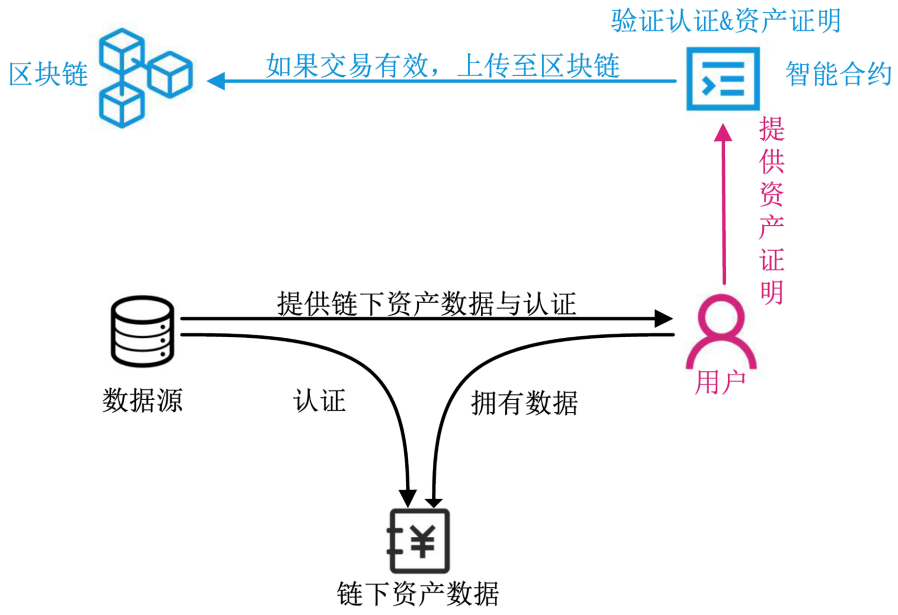

Figure 1. Blockchain transaction scenarios based on off-chain assets
图 1. 基于链下资产的区块链交易场景

在图 1 所示的区块链交易架构中，数据源存储用户的资产数据(如银行存款、房产凭证等)，为参与交易的用户诚实地派发数据认证，同时将认证所需的资产数据发送给用户；用户参与区块链交易，其诉求在不泄露自身资产数据的前提下，向智能合约证明自身资产的有效性，以便交易的有序进行；智能合约旨在验证用户资产与数据认证的有效性，以防止恶意的用户伪造认证或资产数据，对交易造成损失。

综上，基于链下资产的区块链交易场景应当满足如下需求以便交易的公平、安全以及高效进行：数据隐私性，用户不希望自身的资产数据上传至公开透明的区块链中，而是希望通过其它方式，证明自身资产数据的有效性；数据源认证性，恶意的用户会伪造自身的资产数据，继而获得非法利益，因此需要对用户资产数据的来源进行认证；低 Gas 消耗，智能合约会根据处理区块链事务的复杂程度收取一定量的手续费(Gas [4])，继而对用户的交易产生额外的支出，因此在设计方案时，要尽可能缩减用户需要支付的 Gas 费用。

不幸的是，现有技术没有能同时满足上述需求的方案，本文的动机旨在通过密码学技术，实现面向区块链交易的，同时满足数据隐私性、数据源认证性以及低 Gas 消耗的 zk-SNARK 方案。

2. 技术背景

2.1. zk-SNARK

用户通过 zk-SNARK 技术[5]实现自身的资产证明。通过零知识简洁非交互知识论证技术(zero knowledge succinct non-interactive argument of knowledge, zk-SNARK)技术，证明者能够在不泄露自身秘密(witness)的情况下，向验证者证明自身秘密的合法性与知识性。一个安全的 zk-SNARK 应当满足如下性质[6]：

- 稳健性，对于证明者诚实生成的证明，验证者会予以通过；
- 健壮性，对于恶意证明者伪造的证明，验证者通过证明的概率是可忽略的；
- 零知识性，验证者无法从证明以及验证过程中学习到任何有关于证明者秘密的信息；
- 简洁性，验证者的计算代价远小于证明者的计算代价。

2.2. 认证技术

数据源通过认证技术实现对用户资产数据的绑定，以达到防止恶意用户篡改或伪造的目的。值得注意的是，如果采用数字签名技术[7]来确保数据源的认证性则会破坏数据隐私性，这是因为数字签名的验证阶段需要以数据本身作为输入。

为了在不破坏数据隐私性的前提下实现数据源的认证性，本文旨在对 zk-SNARK 的证明进行认证[8]。数据源对证明进行认证，恶意的用户由于 zk-SNARK 的健壮性无法伪造证明，而零知识性则保证了数据隐私性。至此，本文通过此认证实现了用户资产数据、zk-SNARK 证明与认证的绑定，以防止恶意的用户篡改或伪造资产数据。

3. 方案构建

本文方案设计四类参与实体，分别为权威机构、用户、数据源以及智能合约。本文构建方案模型如图 2 所示。各参与实体责任定义如下：

权威机构：权威机构是区块链中去分布交易所的抽象，旨在实现交易的构建与方案的初始化，生成交易明细、部署智能合约以及计算各方所需的公开参数。

用户：用户是区块链交易中的证明方，旨在在不泄露自身资产数据的前提下，通过 zk-SNARK 技术生成自身数据的证明以供智能合约进行验证。

数据源：数据源是用户资产数据的存储方，收到用户的认证请求后，诚实地为用户的资产数据生成认证，并将认证与资产数据发送给对应用户。

智能合约：智能合约是交易的验证方，通过权威机构部署的代码，依次验证用户资产数据源的有效性以及用户的证明的有效性。当且仅当二者验证均有效时才会验证通过，继而进行交易的下一步，最后上传交易事务至区块链。

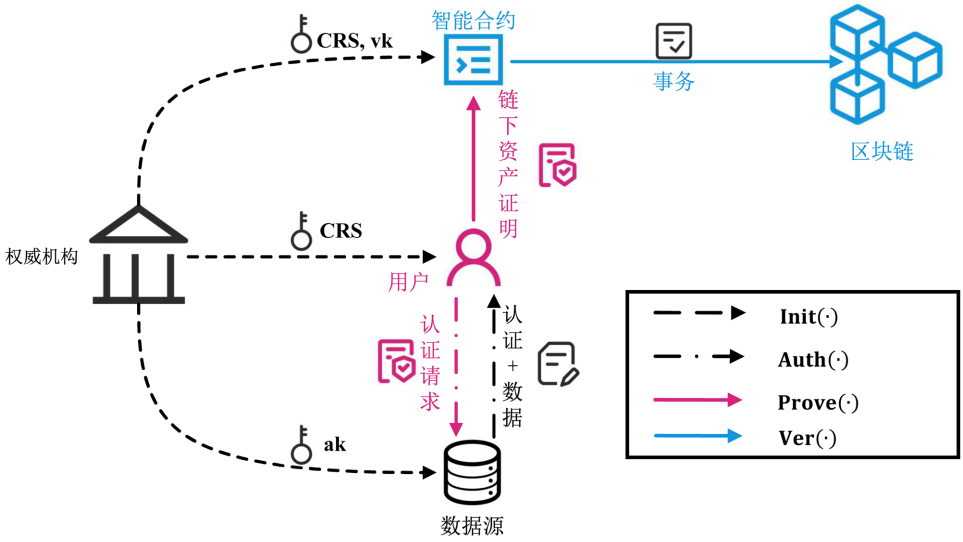

Figure 2. System model
图 2. 系统模型

3.1. 方案形式化描述

1) **初始化阶段**

$\mathrm{Init}(\lambda) \to (pp, \mathcal{R}, CRS, (ak, vk))$：

权威机构生成方案中各参与实体所需的参数，并将其分发给对应实体。权威机构以安全参数 λ 为输入，输出公开参数 pp 和 zk-SNARK 关系 $\mathcal{R}$，继而依次运行如下子算法：

$\mathrm{ProofKeyGen}(\mathcal{R}, pp) \to CRS$：权威机构通过 pp 和 $\mathcal{R}$ 生成 zk-SNARK 所需的公共参考串 CRS，其中包含证明密钥 PK 和验证密钥 VK。

$\mathrm{AuthKeyGen}(pp) \to (ak, vk)$：权威机构为数据源生成对应的“认证–验证”密钥对 (ak, vk)。

2) **认证阶段**

$\mathrm{Auth}(pp, \mathcal{R}, ak, \eth) \to \sigma$：

用户向数据源发送认证请求，以获得对应的认证。数据源继而通过如下算法为用户生成认证。数据源通过认证技术，以认证密钥 ak 和用户的数据 $\eth$ 生成认证 σ。最后，数据源将认证与数据发送给用户。

3) **证明阶段**

$\mathrm{Prove}(pp, \mathcal{R}, CRS, (耩\ \bar{}), \sigma) \to \pi$：

用户通过权威机构定义的估值多项式，计算自身的链下资产数据是否满足交易需求。如果满足，则通过 zk-SNARK 技术生成链下资产证明。具体的，用户收到数据源发送的链下资产数据及对应认证 σ 后，用户以 CRS 中的证明密钥 PK、链下资产数据 $\eth$、估值多项式的计算中间值 $\tilde{n}$ 为输入，计算自身链下资产证明的 π(包含认证 σ)。最后，用户将证明 π 与中间值 $\tilde{n}$ 发送至智能合约。

4) **验证阶段**

$\mathrm{Ver}(pp, CRS, vk, \tilde{n}, \pi) \to 1\ or\ 0$：

智能合约收到用户发送的中间值 $\tilde{n}$、证明 π，首先通过认证 σ 和认证的验证密钥 ak 来验证用户的链下资产的数据源的认证性，如果验证通过，则证明用户没有伪造自身的链下资产数据。继而智能合约通过证明的验证密钥 VK、估值多项式的计算中间值 $\tilde{n}$ 和证明 π 验证用户的估值多项式结果的有效性。如果

认证和证明的验证都通过，则输出 1，代表此次验证有效，继而运行交易的后续操作，并将事务上传至区块链；否则输出 0，代表验证不通过并拒绝提供服务。

3.2. 安全需求

完整性：对于用户诚实生成的认证与资格证明，智能合约验证通过的概率为 1。

健壮性：对于恶意的用户通过伪造的资产数据生成的证明，智能合约验证通过的概率是可忽略的。

数据隐私性：敌手不能从用户的认证与资格证明中获得任何有关于链下资产数据的信息。

数据源认证性：对于恶意的用户伪造的认证，智能合约验证通过的概率是可忽略的。

4. 性能分析

本节进行了仿真实验来测试实际性能。使用的测试平台参数如下：3.4GHz 的 i5 8250uCPU，8GB 内存，windows10 操作系统，Rust 编程语言与 arkwork 密码学库[9]。令 m 为约束数量、l 为陈述数量、d 为多项式的阶、M 为一次标量乘法操作、E 为一次指数乘法操作，以及 P 为一次双线性配对操作，本方案与现有方案 AD-SNARK [10]的复杂度比较如表 1 所示。

Table 1. Comparison of scheme complexity
表 1. 方案复杂度对比

数量	AD-SNARK	本方案
Init	$m(7E+M)+4E$	$(3n+d+m+1)E$
Auth	$2(m-l)(E+M)$	$7E+(3m+6-l)M$
Prove	$7(m-l)E$	$(7m-2l)E$
Verify	$(m-l+1)E+17P$	$(6E+4M)3P$

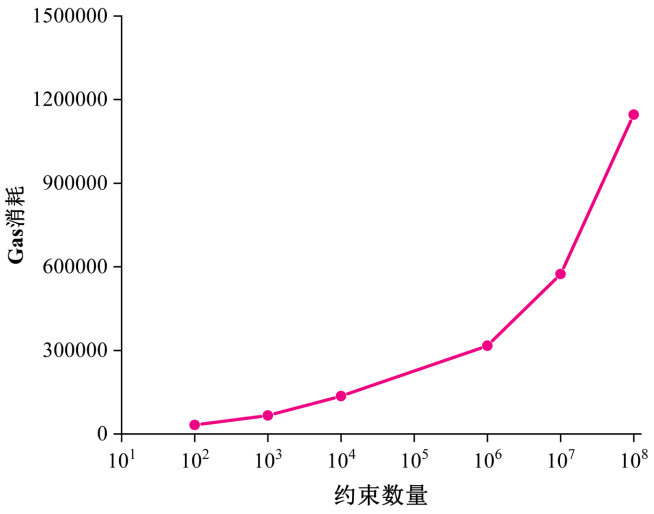

Figure 3. Gas consumption for smart contracts running algorithm Ver
图 3. 智能合约运行 Ver 算法的 Gas 花销

根据本文所模拟的实体环境，本文给出了不同资格约束数量时智能合约运行验证算法 Ver 的 Gas 花销，如图 3 所示。假设所有资格证明都验证通过，由图 3 可知，约束为10^7 (一般情况)时，本方案的 Gas 消耗为 61,394。

5. 结论

本文提出了一种面向区块链的保证数据源认证的 zk-SNARK 方案，通过密码学技术，同时满足区块链交易场景中所需的数据隐私性、数据源认证性与低 Gas 消耗。从性能角度出发，根据不同阶段理论时间代价与模拟智能合约 Gas 消耗代价可以看出，本方案的各阶段均在各实体的计算范围内。

致　谢

感谢全部参与本文章撰写工作的作者。

参考文献

[1] Jensen, J., Von Wachter, V. and Ross, O. (2021) An Introduction to Decentralized Finance (Defi). *Complex Systems Informatics and Modeling Quarterly*, No. 26, 46-54. https://doi.org/10.7250/csimq.2021-26.03

[2] Schueffel, P. (2021) Defi: Decentralized Finance—An Introduction and Overview. *Journal of Innovation Management*, **9**, 1-11. https://doi.org/10.24840/2183-0606_009.003_0001

[3] Gupta, A., Rathod, J., Patel, D., Bothra, J., Shanbhag, S. and Bhalerao, T. (2020) Tokenization of Real Estate Using Blockchain Technology. *Applied Cryptography and Network Security Workshops*, Rome, 19-22 October 2020, 77-90. https://doi.org/10.1007/978-3-030-61638-0_5

[4] Masla, N., Vyas, V., Gautam, J., Shaw, R.N. and Ghosh, A. (2021) Reduction in Gas Cost for Blockchain Enabled Smart Contract. 2021 *IEEE 4th International Conference on Computing*, *Power and Communication Technologies* (*GUCON*), Kuala Lumpur, 24-26 September 2021, 1-6. https://doi.org/10.1109/gucon50781.2021.9573701

[5] Groth, J. (2016) On the Size of Pairing-Based Non-Interactive Arguments. *Advances in Cryptology-EUROCRYPT* 2016: 35*th Annual International Conference on the Theory and Applications of Cryptographic Techniques*, Vienna, 8-12 May 2016, 305-326. https://doi.org/10.1007/978-3-662-49896-5_11

[6] Parno, B., Howell, J., Gentry, C. and Raykova, M. (2016) Pinocchio: Nearly Practical Verifiable Computation. *Communications of the ACM*, **59**, 103-112. https://doi.org/10.1145/2856449

[7] Miller, P.S. and Smart, T.G. (2010) Binding, Activation and Modulation of Cys-Loop Receptors. *Trends in Pharmacological Sciences*, **31**, 161-174. https://doi.org/10.1016/j.tips.2009.12.005

[8] Boneh, D. and Boyen, X. (2004) Short Signatures without Random Oracles. In: *International Conference on the Theory and Applications of Cryptographic Techniques*, Springer, 56-73. https://doi.org/10.1007/978-3-540-24676-3_4

[9] GitHub (2024) Ackworks. https://github.com/arkworks-rs

[10] Backes, M., Barbosa, M., Fiore, D. and Reischuk, R.M. (2015) ADSNARK: Nearly Practical and Privacy-Preserving Proofs on Authenticated Data. 2015 *IEEE Symposium on Security and Privacy*, San Jose, 17-21 May 2015, 271-286. https://doi.org/10.1109/sp.2015.24