Verifiable Auction Mechanisms for Material Reuse in the Built Environment

Stanly Wilson*‡§, Tanapon Suwankesawong*§, Kwabena Adu-Duodu*, Yinhao Li*,
Rajiv Ranjan*, Omer Rana†, Ellis Solaiman*,
*Newcastle University, UK
†Cardiff University, UK
‡St. Vincent Pallotti College of Engineering & Technology, Nagpur, India
§ Authors equally contributed

***Abstract*—Built environments face significant challenges in promoting material reuse due to the lack of trustworthy and transparent trading mechanisms. Existing digital platforms often fail to ensure fairness, bid confidentiality, and auditability. To address this gap, this paper presents the design and implementation of a verifiable auction system for trading reusable construction materials. Built on a Polkadot-based platform, the system supports sealed reverse auctions through a hybrid on-chain/off-chain architecture: encrypted and signed bids are stored in InterPlanetary File System (IPFS), while a *Merkle root* of valid bids is committed on-chain. Zero-knowledge proofs (ZKPs) enable verification of bid correctness without revealing bid values. Stress testing showed moderate latency from proof generation and *IPFS* operations, yet performance remained suitable for auctions lasting minutes or hours. The results demonstrate a scalable, privacy-preserving, and auditable auction mechanism that leverages decentralised technologies to advance circular economy goals.**

***Index Terms*—Circularity, Reuse, Auction, Blockchain**

I. Introduction

The construction industry continues to be the biggest contributor towards material waste [1]. Sustainability and circular economy practices have become a key focus. Enabling effective and trustworthy trading of reusable materials will be vital for managing resource consumption and lowering carbon emissions [2]. However, there is a lack of transparency, unclear material provenance, and limited trust in existing trading systems [3], [4]. Current procurement practices in the construction sector are often centralised, manual, and dependent on intermediaries. This can lead to inefficiencies, lack of transparency and limit product traceability. They do not adequately guarantee fairness or prevent manipulation, leading stakeholders to fear engaging due to unverifiable transactions and potential tampering [2].

Auctions provide an effective mechanism for matching product supply and demand especially in situations where the value of reused material is uncertain and price discovery is required [4]. However, current digital platforms in the construction reuse sector struggle to ensure bid confidentiality, fairness, and auditability simultaneously which are necessary for enabling circularity and sustainability. Conversely, Blockchain technologies support transparency, traceability and auditability. However, existing solutions do not adequately balance privacy and auditability. In such a scenario there is a need for transparent, fair, and privacy-preserving mechanisms, where price competition, procurement scale, and material trustworthiness of material authenticity are important [5], [6]. Hence, this paper integrates auctioning into a blockchain-enabled marketplace, where bids are encrypted and stored in IPFS, while the *Merkle root* summarising valid bids is committed to the blockchain. Our architecture integrates ZKPs into the auction process.

The contributions of this paper are threefold: (i) we design a hybrid on-chain/off-chain auction framework that combines IPFS storage, Merkle-tree commitments, and zero-knowledge proofs to balance privacy with auditability; (ii) we implement the framework on Polkadot with *Groth16*-based ZKPs and evaluate its performance; and (iii) we demonstrate that bid submission latencies remain practical for construction reuse auctions lasting minutes to hours.

The remainder of the paper is structured as follows. Section II covers literature on circularity in construction supply chains and verifiable auction techniques. Section III covers the system architecture and implementation. Section IV details the performance evaluation of the framework. Finally, section V concludes this work and provides future directions.

II. Background and Literature Review

The construction sector generates vast amounts of waste much of which could be recovered and reused to support sustainability objectives. Material reuse is central to the circular economy which aims to extend the lifecycle of products [2]. Various attempts like Material Passport [7], and Madaster [8] have emerged to bring material details under one place to facilitate circularity and exchange of reclaimed products. However, they often depend on manual verification and centralised governance which erodes stakeholder trust. Recent work has explored provenance tracking in construction materials [9].

Auctions have been used in procurement and resource allocation because they provide efficient price discovery and competition [3]. In the current construction scenario, sealed-bid and reverse auctions have been employed for contractor selection, material procurement and service outsourcing. Reverse auctions are relevant in material reuse as they allow the

buyers to set requirements while suppliers compete to offer most favourable terms [4]. However, conventional auction systems in construction face challenges related to fairness and transparency. The lack of independent verifiability forces the participants to perceive the outcomes as biased, leading to reduced engagement and reluctant to engage.

Blockchain technologies have been proposed as a solution to transparency and integrity of transactions, and various auction models have been developed, yet major challenges remain such as storing bids and sensitive information directly on-chain leading issues of transaction cost and privacy concerns. As identified in recent surveys of blockchain-based auctions [3], achieving both transparency and bid confidentiality is a common issue in decentralised auction design. In the context of material reuse markets, suppliers may not wish to disclose their unit costs or inventory strategies to competitors. Without privacy protections, smaller suppliers may be unwilling to participate in the auction, afraid their data will be abused, which makes a verifiable auction mechanism essential to ensure that the winning bid was selected fairly and that no manipulation occurred during or after bidding.

III. Architecture and Implementation

The proposed verifiable auction system is built on top of a marketplace, which is an immutable and decentralized way of recording information and allows independent validation of information by stakeholders. The framework is realised using the *Polkadot* ecosystem, providing scalability and interoperability of *parachains* – and allowing for connection to other blockchains. IPFS is used for decentralised storage, *Groth16* is used for the ZKP generation.

To ensure privacy and confidentiality for bids, the system uses authenticated data structures (ADS), implemented using *Merkle trees* for compact bid inclusion proofs, and ZKPs for providing fast verification and small proof size, making it well-suited for real-time and resource-constrained blockchain environments [10]. The system is designed around a hybrid on-chain/off-chain model that extends existing architectures for auction systems. Bids are encrypted and submitted off-chain to IPFS. Meanwhile, the final *Merkle root* and auction metadata are committed to the blockchain. This design aligns with trends in scalable blockchain applications where only minimal, essential state is stored on-chain [11], [12]. To ensure transparency and trust, the system uses a finalisation function that commits the winner, winning bid value, quantity, and proof on-chain. Figure 1 shows the architecture of the proposed framework.

The core auction metadata is stored on-chain, while bids are first digitally signed by participants to ensure authenticity and are then encrypted and stored off-chain using IPFS. This avoids storing sensitive data on-chain. At the auction finalisation stage, a *Merkle root* representing all valid signed bids is computed and stored on-chain. This allows for efficient and verifiable proof of bid inclusion without revealing the actual bid contents. This hybrid approach achieves a balance among

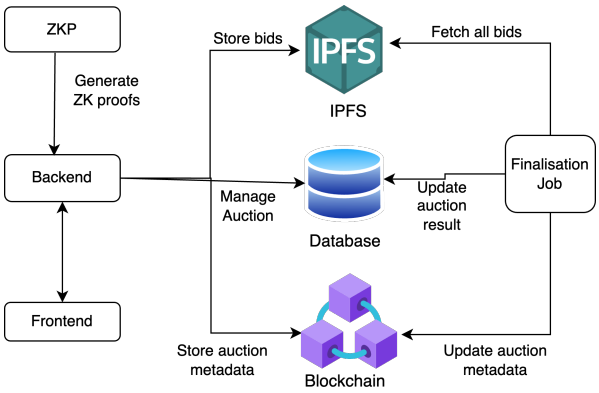

Fig. 1. System Architecture

competing priorities of scalability, privacy, and transparency, which fully on-chain systems often fail to meet.

In addition, another reason for separating on-chain and off-chain functions was to avoid last-second race conditions near auction end. In many blockchain auctions, users compete to submit bids in the final block, risking exclusion due to network congestion, gas bidding, or miner prioritisation. By signing and timestamping pre-bids off-chain and only finalising them post-auction using a *Merkle root*, the system eliminates this bottleneck and ensures deterministic inclusion of all valid bids. Unlike fully off-chain models that sacrifice verifiability, this system commits a *Merkle root* on-chain, enabling public auditability without revealing sensitive bid content.

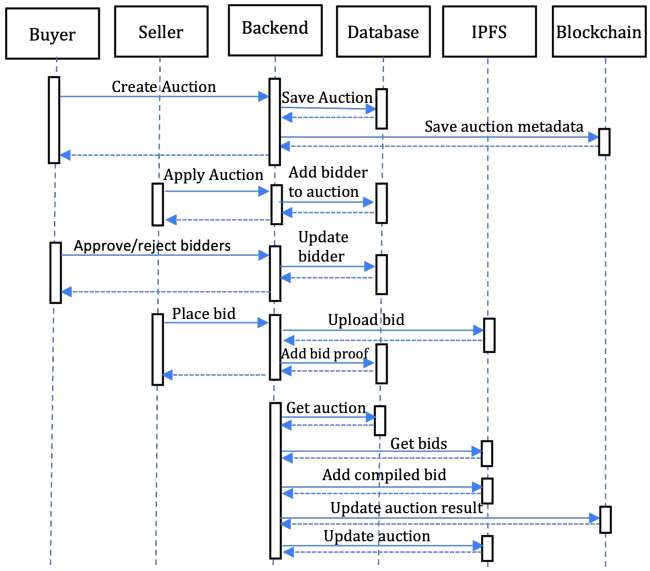

Fig. 2. Auction process

Figure 2 presents the auction process. We adopt a sealed reverse auction. In a reverse auction, buyers make a request for specific products and sellers make offers against each other. A buyer posts a material request, and multiple sellers submit sealed bids. Bids are only revealed and finalised

after the deadline, preserving privacy and price competition. This model is well-suited for bulk procurement of reused or surplus construction materials, where both confidentiality and cost efficiency are essential. Reverse auctions have long been used in procurement to drive price competition [5], and even in recent blockchain-based systems, they remain relevant for matching buyers and sellers [12].

The auction flow is as follows: buyers create an auction request, specifying the required material type, quantity, and an end time for the auction. Sellers who possess relevant materials can apply to the auction by submitting associated material along with their digital product passports (DPP). Buyers then assess the submitted DPP and accept/reject the sellers based on their material needs and the content of the DPP. Once sellers are approved, they can submit sealed bids during the auction window. Each sealed bid specifies a price and the quantity the seller is willing to provide. Each individual bid is uploaded to IPFS and contains the auction ID hash, the bidder's wallet address, the encrypted bid amount, the submission timestamp, and the offered quantity. This process continues until the closing time of the auction.

IV. Performance Evaluation

Submitting a bid involves generating ZKP, digitally signing the bid, encrypting it, and uploading the full pre-bid package to IPFS. In testing, the end-to-end bid submission process typically averaged between 1.7–2.5 seconds per bid, with ZKP generation accounting for the largest share of that time, taking between 1.5 – 2 seconds. To compare off-chain and on-chain bid paths, a controlled stress test with 5 concurrent users was conducted, each executing identical ZKP logic. The evaluation was limited to five concurrent users due to the ZKit toolkit's limited concurrency support and the single-threaded Node.js backend, which led to file I/O collisions during parallel proof generation. Furthermore, tests were run on a consumer-grade machine with limited resources hence results are indicative rather than definitive. Among the successful bids, ZKP generation in the off-chain version consistently took slightly longer (avg. 3.9s) than in the on-chain version (3.2s). Without ZKPs, both methods show similar times (300–400ms); proof generation dominates latency (Table I). A timestamp of each pre-bid off-chain submissions is reacorded for all bids submitted before the deadline. This eliminates risks associated with last-second bidding in blockchain systems. While our stress test involved only five concurrent users, the modular design enables scaling to larger auctions; future work will benchmark performance under higher loads.

TABLE I
Comparative Latency for Bid Submission Paths

Metric	On-chain	Off-chain
Avg Total Submission Time	3.3 – 3.5 sec	4.1 – 4.2 sec
Avg ZKP Generation Time	3.0 – 3.4 sec	3.9 – 4.0 sec
Component Fetch Time	32 – 39 ms	38 – 62 ms
Auction Fetch Time	28 – 46 ms	43 – 179 ms
IPFS Upload Time	N/A	30 – 187 ms
Database Save Time	N/A	25 – 67 ms
Blockchain Tx Time	290 – 870 ms	N/A

V. Conclusion

The paper describes a hybrid on-chain/off-chain design to effectively support verifiable and privacy-preserving reverse auctions, particularly in circular supply chain contexts of built environments. This solution improves scalability by minimising blockchain congestion, while maintaining auditability and verifiable computation. In future work, we aim to support multi-attribute evaluation that can incorporate factors such as material provenance and sustainability scores, optimise cryptographic efficiency for faster ZKP generation, and explore integration with large-scale DPP systems.

Acknowledgments: Supported in part by the Engineering and Physical Sciences Research Council "Digital Economy" programme: EP/V042521/1 and EP/V042017/1

References

[1] H. R. Crawford, "Greenhouse gas emissions of global construction industries," *OP Conference Series: Materials Science and Engineering*, vol. 1218, no. 1, p. 012047, 2022.

[2] L. Harala, L. Alkki, L. Aarikka-Stenroos, A. Al-Najjar, and T. Malmqvist, "Industrial ecosystem renewal towards circularity to achieve the benefits of reuse - learning from circular construction," *Journal of Cleaner Production*, vol. 389, p. 135885, 2023.

[3] X. Liu, L. Liu, Y. Yuan, Y.-H. Long, S.-X. Li, and F.-Y. Wang, "When blockchain meets auction: A comprehensive survey," *IEEE Transactions on Computational Social Systems*, vol. 11, no. 3, pp. 4242–4254, 2024.

[4] R. C. Koirala, K. Dahal, S. Matalonga, and R. Rijal, "A supply chain model with blockchain-enabled reverse auction bidding process for transparency and efficiency," in *2019 13th International Conference on Software, Knowledge, Information Management and Applications (SKIMA)*. IEEE, 2019, pp. 1–6.

[5] S. D. Jap, "Online reverse auctions: Issues, themes, and prospects for the future," *Journal of the Academy of Marketing Science*, vol. 30, no. 4, pp. 506–525, 2002.

[6] I. Amelinckx, S. Muylle, and A. Lievens, "Extending electronic sourcing theory: An exploratory study of electronic reverse auction outcomes," *Electronic Commerce Research and Applications*, vol. 7, no. 1, pp. 119–133, 2008.

[7] T. E. M. Foundation, "Using product passports to improve the recovery and reuse of shipping steel: Maersk line," https://www.ellenmacarthurfoundation.org/circular-examples/using-product-passports-to-improve-the-recovery-and-reuse-of-shipping-steel. Accessed September, 2025.

[8] "The impact of material passports within the property chain - Madaster Global," https://madaster.com/inspiration/the-impact-of-material-passports-within-the-property-chain/, [Online: accessed 05/09/2025].

[9] S. Wilson, K. Adu-Duodu, Y. Li, R. Sham, M. Almubarak, Y. Wang, E. Solaiman, C. Perera, R. Ranjan, and O. Rana, "Blockchain-enabled provenance tracking for sustainable material reuse in construction supply chains," *Future Internet*, vol. 16, no. 4, 2024.

[10] B. Oude Roelink, M. El-Hajj, and D. Sarmah, "Systematic review: Comparing zk-snark, zk-stark, and bulletproof protocols for privacy-preserving authentication," *Security and Privacy*, vol. 7, no. 5, 2024.

[11] X. Wang, H. Li, L. Yi, Z. Ning, X. Tao, S. Guo, and Y. Zhang, "A survey on off-chain networks: Frameworks, technologies, solutions and challenges," *ACM Computing Surveys*, vol. 57, no. 12, 2025.

[12] W. Zhang, W. Yang, C. Chen, N. Li, Z. Bao, and M. Luo, "Toward privacy-preserving blockchain-based electricity auction for v2g networks in the smart grid," *Security and Communication Networks*, vol. 2022, no. 1, p. 6911463, 2022.