Project Definition Document

November 1, 2025

Project Title: Decentralized Peer-to-Peer SMPC Sealed-bid auction app over the Veilid framework

Degree Programme: BSc (Hons) Computer Science

Project Consultant: Martin Nyx Brain

By: Anker Rasmussen

anker.rasmussen@city.ac.uk

Category: Academic Client Project

Subcategory: Application Development

Word count:779

Proprietary Interests: None

1 Proposal

1.1 Problem to be Solved

Popular online consumer marketplaces either use *open, incrementally visible bidding* or *no auctions at all*, which undermines sealed-bid privacy and fairness. eBay's proxy-bidding model reveals live bid progression and awards the item to the highest bid at close [1]. Facebook Marketplace, by contrast, is a listing-plus-messaging workflow rather than a formal auction protocol, with weak buyer protections [2]. Public blockchains add strong auditability but invite transaction ordering attacks (front-running/MEV) that can leak or distort bids during submission and reveal phases [3]. Cryptographic sealed-bid auctions can hide non-winning bids entirely; deploying them without a trusted auctioneer requires secure multiparty computation (MPC). MPC has been demonstrated in production (e.g., the Danish sugar-beet auction) and modern frameworks such as MP-SPDZ show practical performance across secret-sharing, HE, and garbled-circuit backends [4, 5, 6, 7, 8].

What is Veilid?

Veilid is a privacy-first, open-source, peer-to-peer application framework. Each app embeds a node into a global overlay where peers are equal (no privileged relays), connections are end-to-end encrypted, and private routing obscures network locations. After a brief bootstrap, apps communicate directly over transports such as UDP/TCP/QUIC/Web and exchange data via a secure DHT designed for mobile and desktop [9]. In short: an application overlay providing addressable, encrypted endpoints (public-key identities) and metadata-minimizing communication, independent of any blockchain.

Why Veilid for this marketplace?

The marketplace requires private identities, censorship-resistant transport, and NAT-friendly reachability without a trusted coordinator. Veilid offers: (i) addressable, encrypted endpoints keyed by public keys (not IPs), (ii) a secure DHT for publishing listings and locating MPC parties, and (iii) obfuscated routing that reduces metadata leakage during bid submission and MPC setup [9]. Because Veilid is blockchain-agnostic, settlement can occur off-overlay (Monero stagenet) while *coordination* and *communication* remain private and decentralized—aligning with the goals of sealed-bid privacy, front-running resistance, and auctioneerless operation [10].

Project Goal

Build a **peer-to-peer sealed-bid marketplace** that (1) preserves bidder privacy by default, (2) mitigates front-running risk during bid submission, and (3) operates *without a central auctioneer*. The prototype combines MPC for winner/price computation with *Veilid* for identity, routing, and availability [9]. Payments clear on *Monero stagenet* after the MPC outcome is published—exercising the full flow without handling real funds—while inheriting the confidential-transaction model and unlinkability properties from the CryptoNote design [10].

1.2 Project Objectives

- **Main objective.** This project shall deliver a working peer-to-peer marketplace application on the Veilid network that exclusively supports sealed-bid listings and private content unlock for the winning bidder.
- **Testable objectives.**
  - *Listings and purchases.* Implement end-to-end flows: create listing → submit bid → determine winner → complete purchase. **Test:** demo run and automated integration tests covering success/edge cases (invalid bid, tie, timeout).
  - *Sealed-bid via MPC.* Integrate a multi-party computation protocol to select the highest valid bid without revealing non-winning bids. **Test:** unit tests with mocked parties; property tests showing loser-bid privacy; reproducible benchmark for N bidders.
  - *Encrypted content unlock.* Ensure listing content remains encrypted; only the winner obtains the decryption key/hash after settlement. **Test:** verify ciphertext remains inaccessible to non-winners; successful decrypt by winner; tamper tests.
  - *Settlement on Monero Stagenet.* Simulate network init, funded wallets, and programmatic "real" transactions for deposits/escrow/release. **Test:** scripted stagenet transactions with confirmations; failure/reorg handling.

1.3 Project Beneficiaries

Identify who benefits from this project (users, researchers, organizations, etc.) and how they benefit.

1.4 Project Plan

Provide a high-level timeline of the project. You can use a list or table if preferred.

- Placeholder0
- Placeholder1
- Placeholder2
- Placeholder3

1.5 Risks Affecting the Project

Outline any technical, logistical, or ethical risks that may affect project success, and how you plan to mitigate them.

1.6 Legal, Social, Ethical and Professional Considerations

Discuss any relevant ethical or legal implications of your project (e.g., data privacy, bias, intellectual property, accessibility).

1.7 References

References

[1] eBay Help, *How bidding works*, Accessed 29 Oct 2025, 2025. [Online]. Available: `https://www.ebay.co.uk/help/buying/bidding/bidding?id=4003`.

[2] Meta/Facebook Help Center, *Marketplace help center: Using marketplace to buy and sell*, Accessed 29 Oct 2025, 2025. [Online]. Available: `https://www.facebook.com/help/1713241952104830`.

[3] P. Daian, S. Goldfeder, T. Kell, Y. Li, X. Zhao, I. Bentov, L. Breidenbach and A. Juels, *Flash boys 2.0: Frontrunning, transaction reordering, and consensus instability in decentralized exchanges*, 2019. DOI: `10.1109/SP40000.2020.00040`. arXiv: `1904.05234 [cs.CR]`. [Online]. Available: `https://arxiv.org/abs/1904.05234`.

[4] P. Bogetoft, D. L. Christensen, I. Damgård, M. Geisler, T. Jakobsen, M. Krøigaard, J. D. Nielsen, J. B. Nielsen, K. Nielsen, J. Pagter, M. Schwartzbach and T. Toft, “Secure multiparty computation goes live,” in *Financial Cryptography and Data Security*, R. Dingledine and P. Golle, Eds., Berlin, Heidelberg: Springer Berlin Heidelberg, 2009, pp. 325–343, ISBN: 978-3-642-03549-4. DOI: `10.1007/978-3-642-03549-4_20`. [Online]. Available: `https://link.springer.com/chapter/10.1007/978-3-642-03549-4_20`.

[5] M. Keller, “Mp-spdz: A versatile framework for multi-party computation,” in *Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security*, ser. CCS ’20, Virtual Event, USA: Association for Computing Machinery, 2020, pp. 1575–1590, ISBN: 9781450370899. DOI: `10.1145/3372297.3417872`. [Online]. Available: `https://doi.org/10.1145/3372297.3417872`.

[6] I. Damgård, V. Pastro, N. Smart and S. Zakarias, “Multiparty computation from somewhat homomorphic encryption,” in *Advances in Cryptology – CRYPTO 2012*, R. Safavi-Naini and R. Canetti, Eds., Berlin, Heidelberg: Springer Berlin Heidelberg, 2012, pp. 643–662, ISBN: 978-3-642-32009-5.

[7] D. Evans, V. Kolesnikov and M. Rosulek, “A pragmatic introduction to secure multi-party computation,” *Found. Trends Priv. Secur.*, vol. 2, no. 2–3, pp. 70–246, Dec. 2018, ISSN: 2474-1558. DOI: `10.1561/3300000019`. [Online]. Available: `https://doi.org/10.1561/3300000019`.

[8] K. Sako, “An auction protocol which hides bids of losers,” in *Public Key Cryptography*, H. Imai and Y. Zheng, Eds., Berlin, Heidelberg: Springer Berlin Heidelberg, 2000, pp. 422–432, ISBN: 978-3-540-46588-1. DOI: `10.1007/978-3-540-46588-1_28`. [Online]. Available: `https://link.springer.com/chapter/10.1007/978-3-540-46588-1_28`.

[9] Veilid Project. “Veilid developer book.” Official developer documentation for the Veilid framework, Accessed: Oct. 31, 2025. [Online]. Available: `https://veilid.gitlab.io/developer-book/`.

[10] N. van Saberhagen, “Cryptonote v 2.0,” Original CryptoNote whitepaper; commonly cited in Monero literature, Oct. 17, 2013. Accessed: Oct. 31, 2025. [Online]. Available: `https://decred.org/research/saberhagen2013.pdf`.

2 Research Ethics Checklist

Summarize any ethical considerations and indicate whether formal ethics approval is needed. If applicable, reference consent forms or procedures.

3 Client Information Sheet (External Client Projects Only)

Provide details about the client organization, contact person, and nature of collaboration.

4 Appendix: Use of Generative AI (if applicable)

If AI tools (e.g., ChatGPT, Copilot) were used in preparing this document or project materials, describe exactly how and to what extent they were used.

5 Appendix: Legal, Social, Ethical, and Professional Issues (LSEPI)

For Category 3 projects, provide a more detailed analysis of relevant LSEPI topics.