Project Definition Document

October 30, 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:

1 Proposal

1.1 Problem to be Solved

Mainstream consumer marketplaces either use *open*, incrementally visible bidding or no auctions at all, which undermines sealed-bid privacy and fairness. For example, eBay's auction model exposes live bid progression (via proxy bidding), and the highest bidder at close wins (eBay Help 2025). Facebook Marketplace, by contrast, is a listing-based peer-to-peer venue with messaging and checkout links rather than a formal auction protocol (Meta/Facebook Help Center 2025); reports highlight elevated scam risk and weak buyer protections in such ad-hoc workflows (Korn et al. 2024).

Public blockchains add strong auditability but are susceptible to transaction ordering attacks (*front-running*/MEV), which can leak or distort bids during submission and reveal phases (Daian et al. 2020). In sealed-bid contexts, cryptographic auction protocols exist to hide non-winning bids entirely (Sako 2000), but deploying them without a trusted auctioneer requires secure multiparty computation (MPC). MPC has been shown to work in production for real markets (e.g., the Danish sugar-beet auction), where parties jointly compute winner and clearing price without revealing individual bids (Bogetoft et al. 2009). Mature MPC frameworks (e.g., MP-SPDZ built on SPDZ-family protocols) demonstrate practical performance across secret-sharing, HE, and garbled-circuit backends (Keller 2020; Damgård et al. 2012; Evans et al. 2018).

This project addresses the absence of a **peer-to-peer sealed-bid marketplace** that (1) preserves bidder privacy by default, (2) mitigates front-running risk during submission, and (3) operates without a central auctioneer. It combines MPC for bid evaluation with a decentralized transport substrate (Veilid) for identity, routing, and availability.

My main objective for this project is to create a tech demo of an application running on top of the Veilid network, allowing users to list and sell items using Monero as the primary vehicle for transactions, executed at the completion of bid on the stagenet network (where the framework is identical to mainnet, but the tokens are valueless). My hope is that one day this tech demo can evolve into a fully fledged marketplace that protects the privacy of its users.

1.2 Project Objectives

- The primary objective is to have an application (full frontend) running on top of the Veilid network that has listing and purchase capabilities, with text being unlocked

upon successful win of bid.
- Integrate MPC algorithm for sealed-bid capabilities, resulting bid victory allows for hash to unlock content of file, else file remains encrypted.
- Objective 3

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

- Author, A. (Year). *Title of the paper.* Journal/Source.
- Author, B. (Year). *Title of another reference.*

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.