# **Project Proposal**

### 

## A. Thông Tin Chung

* **Môn học:** Công nghệ Blockchain
* **Tên đề tài:** Voting/DAO mini app cho lớp học
* **Giảng viên hướng dẫn**: Trần Hưng Nghiệp, [nghiepth@uit.edu.vn](mailto:nghiepth@uit.edu.vn)
* **Thời gian thực hiện:** tháng 9/2025 - tháng 12/2025
* **Nhóm**: <STT: 7 - CryptoGuard>
* **Thành viên:**

1. Nguyễn Duy Khánh, 240104009, [khanhnd.19@grad.uit.edu.vn](mailto:khanhnd.19@grad.uit.edu.vn), 0908844732
2. Huỳnh Quốc Bữu, 240104026, [buuhq.19@grad.uit.edu.vn](mailto:buuhq.19@grad.uit.edu.vn), 0979387803
3. Nguyễn Đức Linh, 240104039, [linhnd.19@grad.uit.edu.vn](mailto:linhnd.19@grad.uit.edu.vn), 0965002228
4. Nguyễn Duy Nghĩa, 240104045, [nghiand.19@grad.uit.edu.vn](mailto:nghiand.19@grad.uit.edu.vn), 0383213327
5. Trần Võ Bảo Thiên, 240104052, [thientvb.19@grad.uit.edu.vn](mailto:thientvb.19@grad.uit.edu.vn), , 0866989279

### 

## B. Nội Dung Thuyết Minh

### **1. Abstract (Tóm tắt)**

Trong các môi trường học tập truyền thống, việc tổ chức các cuộc bỏ phiếu nội bộ như bầu lớp trưởng, chọn phương án học tập hay đánh giá phản hồi thường thực hiện thủ công hoặc qua các biểu mẫu tập trung. Các phương pháp này tuy thuận tiện nhưng dễ phát sinh vấn đề về tính xác thực, minh bạch và khả năng kiểm chứng kết quả. Công nghệ blockchain mở ra một hướng tiếp cận mới khi cho phép lưu trữ dữ liệu bất biến, phân tán và công khai.

Đề tài này tập trung phát triển một **Voting/DAO mini app** chạy trên testnet Ethereum, sử dụng smart contract viết bằng Solidity kết hợp MetaMask và giao diện web thân thiện. Ứng dụng cho phép người tổ chức tạo đề xuất, sinh viên tham gia bỏ phiếu, hệ thống tự động khóa phiếu khi hết hạn, và kết quả được ghi nhận trực tiếp trên blockchain. Mục tiêu là xây dựng một nguyên mẫu dễ triển khai trong thực tế, đáp ứng ba tiêu chí chính: **minh bạch**, **chống gian lận** và **khả năng kiểm chứng độc lập**.

### **2. Introduction (Mục tiêu & Bối cảnh)**

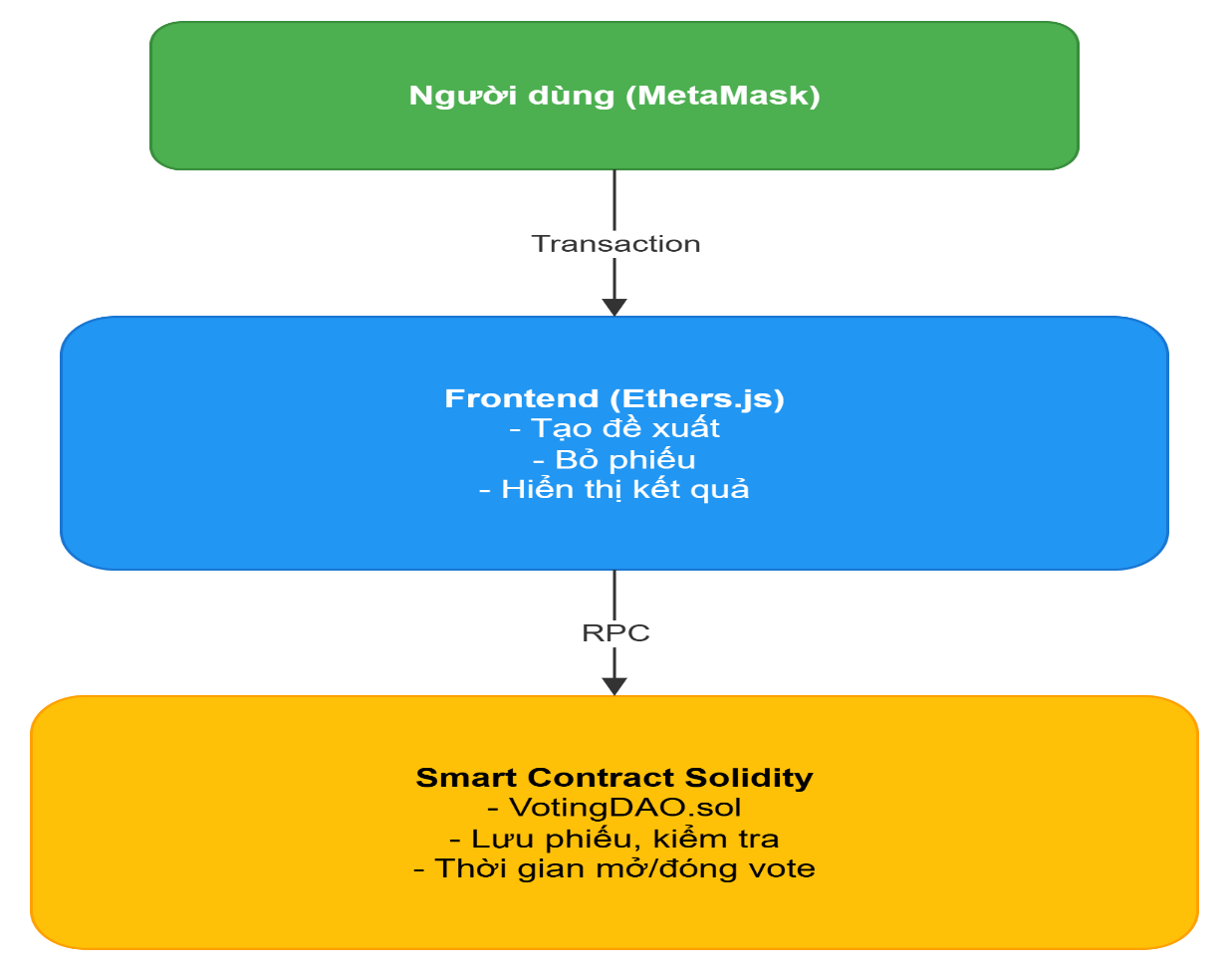
* **Bối cảnh**: Trong bối cảnh chuyển đổi số trong giáo dục, nhu cầu tổ chức các hoạt động lấy ý kiến, bình chọn, bầu chọn một cách minh bạch ngày càng tăng. Tuy nhiên, các công cụ phổ biến hiện nay như Google Form, Excel hoặc phiếu giấy thường thiếu tính xác thực: người tổ chức có thể sửa kết quả, dữ liệu có thể bị thay đổi hoặc không có cơ chế xác minh độc lập. Blockchain — với các đặc tính bất biến (immutability), phân tán (decentralization) và công khai (transparency) — là một công nghệ phù hợp để giải quyết các hạn chế trên.
* **Mục tiêu tổng thể:**
* Xây dựng một ứng dụng bỏ phiếu phi tập trung đơn giản, hoạt động trên testnet Ethereum.
* Áp dụng mô hình DAO cơ bản để minh bạch hóa quá trình bỏ phiếu trong môi trường lớp học.
* Thử nghiệm các kỹ thuật smart contract để kiểm soát quyền bỏ phiếu, kiểm chứng kết quả.
* **Câu hỏi/bài toán cụ thể**: vài mục tiêu / câu hỏi / vấn đề cụ thể rõ ràng mà nhóm đã xác định và sẽ trả lời.
* Làm thế nào để đảm bảo mỗi người chỉ được bỏ phiếu một lần mà không cần đăng ký phức tạp?
* Làm thế nào để đảm bảo kết quả không bị sửa đổi?
* Làm thế nào để triển khai được một ứng dụng đơn giản nhưng có tính thực thi và trình diễn rõ ràng?

### **3. Related Work (Khảo sát liên quan & Phạm vi)**

* **Các công trình / ứng dụng / papers liên quan** (có thể liệt kê 2-3 công trình chính, kèm 1-2 câu mô tả).
* M. Al-Riyami et al., *“Blockchain-Based E-Voting Mechanisms: A Survey and a Proposal”*, MDPI Electronics, 2024. — Khảo sát các cơ chế bỏ phiếu blockchain và so sánh các kỹ thuật mã hóa.
* N. Al-Khalil et al., *“FASTEN: Fair and Secure Distributed Voting Using Smart Contracts”*, arXiv, 2021. — Đề xuất giao thức voting minh bạch và chống gian lận.
* H. Wang et al., *“DAO voting mechanism resistant to whale and collusion”*, Frontiers in Blockchain, 2024. — Phân tích các mô hình bỏ phiếu DAO chống thao túng.
* **Điểm mới hoặc khác biệt**: xác định vị trí tương đối của đề tài so với các công trình hiện có. Nhóm sẽ bổ sung cái gì?
* Đề tài này không nhằm phát minh cơ chế mới mà tập trung vào **ứng dụng mô hình voting DAO trong môi trường giáo dục nhỏ** — quy mô lớp học, dễ cài đặt và minh bạch.
* Giao diện được đơn giản hóa để sinh viên dễ tham gia, không yêu cầu kỹ năng blockchain nâng cao.
* **Phạm vi**: nêu rõ cái nào làm, cái nào không làm (để tránh ôm đồm).
* Xây dựng smart contract cơ bản, kết nối MetaMask.
* Giao diện frontend đơn giản (HTML/JS).
* Triển khai và demo trên testnet Sepolia.
* Không triển khai cơ chế ẩn danh nâng cao (ring signatures, ZKP).
* Không xử lý vấn đề collusion phức tạp hay voting có trọng số.

### **4. Methodology (Phương pháp dự kiến)**

* **Hướng tiếp cận**: ứng dụng / phân tích / nghiên cứu dùng các phương pháp nào, kỹ thuật nào, cách đánh giá nào, độ đo nào…
* **Thiết kế kiến trúc hệ thống** dựa trên mô hình 3 lớp: người dùng – frontend – blockchain.
* **Phát triển và triển khai smart contract** sử dụng Solidity, kiểm soát chặt chẽ logic bỏ phiếu (hasVoted, thời gian mở/đóng).
* **Tích hợp giao diện người dùng** bằng Ethers.js để kết nối MetaMask, giúp sinh viên có thể bỏ phiếu dễ dàng mà không cần thao tác kỹ thuật phức tạp.
* **Công cụ**: ngôn ngữ lập trình, frameworks, platforms, libraries…
* **~~Ngôn ngữ:~~** ~~Solidity (smart contract), JavaScript (frontend)~~
* **Smart contract language:** Solidity
* **Development framework:** Hardhat (deploy + test)
* **Blockchain platform:** Ethereum testnet (Sepolia)
* **Ví người dùng:** MetaMask
* **RPC Provider:** Alchemy / Infura API
* **Frontend Language ~~Giao diện:~~** Javascript (HTML/CSS + Ethers.js)
* **Thiết kế sơ bộ**: 1 hình minh họa / sơ đồ đơn giản (nếu có).



* **Phương pháp đánh giá**
* Kiểm tra tính đúng đắn: số phiếu hợp lệ, không cho phép double-vote.
* Kiểm tra tính toàn vẹn: so sánh log on-chain và giao diện.
* Đo lường kỹ thuật: thời gian giao dịch, gas fee trung bình, số người tham gia tối đa.
* Kiểm thử trên testnet với một nhóm sinh viên thực tế.

### **5. Planning (Kế hoạch công việc)**

* **Timeline**: theo tuần (VD: tuần 1-2: khảo sát, tuần 3-6: phát triển, tuần 7-8: thử nghiệm, tuần 9-10: viết báo cáo + trình bày / demo).

| **Giai đoạn** | **Tuần** | **Nội dung công việc chính** | **Đầu ra** |
| --- | --- | --- | --- |
| Giai đoạn 1: Khảo sát & thiết kế | Tuần 1–2 | - Nghiên cứu tài liệu học thuật về e-voting & DAO. - Xác định kiến trúc hệ thống, logic bỏ phiếu, ràng buộc bảo mật. - Thiết kế sơ đồ quy trình. | - Bản phân tích yêu cầu kỹ thuật. - Thiết kế kiến trúc. |
| Giai đoạn 2: Phát triển Smart Contract | Tuần 3–4 | - Viết và kiểm thử VotingDAO.sol. - Thiết lập môi trường Hardhat, testnet Sepolia. - ~~Viết unit test.~~ | - Smart contract hoàn chỉnh. ~~- Unit test pass 100%.~~ |
| Giai đoạn 3: Phát triển giao diện | Tuần 5–6 | - Xây dựng frontend (HTML/CSS/JS + Ethers.js). - Tích hợp MetaMask và các chức năng voting. - Hoàn thiện UI ~~UX~~ cơ bản. | - Ứng dụng web hoạt động với ví thật trên testnet. |
| Giai đoạn 4: Kiểm thử và đo lường | Tuần 7–8 | - Thử nghiệm nhóm nhỏ sinh viên. - Đo thời gian xử lý, số phiếu hợp lệ, gas fee. - Ghi nhận sự cố, tối ưu. | - Bảng kết quả thử nghiệm. - Log on-chain kiểm chứng. |
| Giai đoạn 5: Báo cáo & trình bày | Tuần 9–10 | - Viết báo cáo kỹ thuật. - Hoàn thiện slide trình bày. - Demo hệ thống thực tế. | - Báo cáo hoàn chỉnh. - Slide bảo vệ. - Ứng dụng demo. |

* **Phân công dự kiến**: mỗi thành viên phụ trách rõ ràng (dev, đọc paper, thu thập data, viết báo cáo, trình bày). Phân công thực tế sẽ nộp sau khi hoàn thành.

| **STT** | **Họ và tên** | **Mã số SV** | **Vai trò chính** | **Nhiệm vụ dự kiến** |
| --- | --- | --- | --- | --- |
| 1 | Nguyễn Duy Khánh | 240104009 | Backend & Smart Contract Dev | - Thiết kế kiến trúc hệ thống. - Viết & kiểm thử smart contract VotingDAO.sol. - Deploy lên testnet. |
| 2 | Huỳnh Quốc Bữu | 240104026 | Frontend Developer | - Xây dựng giao diện web (HTML/CSS/JS + Ethers.js). - Kết nối MetaMask. - Kiểm thử tính năng người dùng. |
| 3 | Nguyễn Đức Linh | 240104039 | Nghiên cứu & Viết báo cáo | - Khảo sát paper, phân tích tài liệu liên quan. - Viết phần *Related Work* & *Introduction*. - Hỗ trợ viết báo cáo tổng hợp. |
| 4 | Nguyễn Duy Nghĩa | 240104045 | Phân tích dữ liệu & đánh giá | - Thu thập dữ liệu thực nghiệm (vote, gas, thời gian). - Phân tích kết quả. - Viết phần *Expected Results*. |
| 5 | Trần Võ Bảo Thiên | 240104052 | Trình bày & kiểm thử hệ thống | - Chuẩn bị slide & demo. - Thực hiện trình bày trước hội đồng. - Tham gia kiểm thử cuối cùng. |

### **6. Expected Results (Kết quả dự kiến)**

Nêu rõ những kết quả / sản phẩm dự kiến sẽ đạt được. VD: các ứng dụng, tính năng, kết quả phân tích đánh giá, …

(**Lưu ý:** Sản phẩm đề tài gồm code demo, technical report, thuyết trình. Tiêu chí: prototype chạy được, hoặc kết quả phân tích rõ ràng, hoặc câu hỏi nghiên cứu có trả lời cơ bản.)

* **Sản phẩm kỹ thuật**:
* Smart contract VotingDAO.sol hỗ trợ tạo đề xuất, bỏ phiếu Yes/No, khóa phiếu tự động và lưu kết quả on-chain.
* Giao diện web kết nối MetaMask, cho phép sinh viên bỏ phiếu và xem kết quả trực tiếp.
* **Kết quả thử nghiệm**:
* Thời gian xử lý trung bình ≤ 15s/phiếu.
* Tỷ lệ phiếu hợp lệ ≥ 95%.
* Kết quả minh bạch, kiểm chứng độc lập trên blockchain.
* **Sản phẩm báo cáo**:
* Báo cáo kỹ thuật (technical report), slide thuyết trình, demo thực tế.
* Phân tích ngắn gọn ưu điểm – hạn chế và khả năng ứng dụng thực tế.

### **7. References (Tài liệu tham khảo)**

[1] Al-Riyami, M. et al., “Blockchain-Based E-Voting Mechanisms: A Survey and a Proposal”, *Electronics (MDPI)*, 2024.  
[2] Al-Khalil, N. et al., “FASTEN: Fair and Secure Distributed Voting Using Smart Contracts”, *arXiv preprint arXiv:2102.10594*, 2021.  
[3] Wang, H. et al., “DAO voting mechanism resistant to whale and collusion”, *Frontiers in Blockchain*, 2024.  
[4] Nakamoto, S., “Bitcoin: A Peer-to-Peer Electronic Cash System”, 2008.  
[5] Vitalik Buterin, “DAOs, DACs, DAs and More: An Incomplete Terminology Guide”, Ethereum Foundation Blog, 2014.