

การพัฒนาระบบจำลองการซื้อขายพลังงานสะอาดแบบ P2P ที่เน้นการรักษาความเป็นส่วนตัวโดยใช้ Solana Smart Contract

(GridTokenX: สมุดคำสั่งซื้อขายแบบรักษาความลับและการพิสูจน์แหล่งที่มาแบบ ZK)

นายจันทร์ธวัฒน์ กิริยาดี
คณะวิศวกรรมศาสตร์
สาขาวิศวกรรมคอมพิวเตอร์และปัญญาประดิษฐ์
มหาวิทยาลัยหอการค้าไทย
กรุงเทพมหานคร ประเทศไทย
2410717302003@live4.utcc.ac.th

บทคัดย่อ—บทความนี้นำเสนอการประเมินประสิทธิภาพของแพลตฟอร์ม GridTokenX ซึ่งเป็นระบบการซื้อขายพลังงานแบบ Peer-to-Peer (P2P) ที่เน้นการรักษาความเป็นส่วนตัว (Privacy-Preserving) พัฒนาบน Solana แบบส่วนตัว งานวิจัยนี้ใช้วิธีการ BLOCKBENCH และ TPC-C Benchmark เพื่อประเมินระบบที่รองรับการซื้อขายผ่าน “สมุดคำสั่งซื้อขายแบบรักษาความลับ” (Confidential Order Book) และการพิสูจน์แหล่งที่มาของพลังงาน (Energy Provenance) โดยใช้เทคนิค Zero-Knowledge Proofs ผลการทดลองยืนยันประสิทธิภาพของระบบด้วยค่า 2,111 tpmC และความหน่วงเฉลี่ย 116 ms แม้จะมีภาระงานด้านการปกปิดตัวตนเพิ่มขึ้น การวิเคราะห์ระดับ Execution แสดงให้เห็นว่าสถาปัตยกรรมแบบขนานช่วยขจัดคอขวดในการประมวลผลธุรกรรมปริมาณมาก (Bulk Trades) โดยยังคงรักษาค่า “Trust Premium” (58.28 เท่า) ให้อยู่ในระดับที่เหมาะสมสำหรับการใช้งานในระดับอุตสาหกรรม

Index Terms—บล็อกเชน, การซื้อขายพลังงาน, Solana, Privacy-Preserving, Zero-Knowledge Proofs, TPC-C, GridTokenX

I. บทนำ

การกระจายศูนย์ระบบพลังงานผ่านทรัพยากรพลังงานแบบกระจาย (Distributed Energy Resources หรือ DERs) จำเป็นต้องมีโครงสร้างพื้นฐานการซื้อขายที่แข็งแกร่ง ซึ่งสามารถรองรับธุรกรรมขนาดเล็กที่มีความถี่สูงได้ [2] รูปแบบมาตรฐานบล็อกเชนแบบรวมศูนย์ดั้งเดิมมักประสบปัญหาความเสี่ยงจากการล้มเหลวที่จุดเดียว (Single Point of Failure) และขาดความโปร่งใสในการกำหนดราคา เทคโนโลยีบล็อกเชนนำเสนอทางออกสำหรับปัญหานี้ แต่มักถูกวิพากษ์วิจารณ์เรื่องข้อจำกัดด้านความสามารถในการขยายระบบ (Scalability) [4]

งานวิจัยนี้ประเมินประสิทธิภาพของแพลตฟอร์มที่นำเสนอ ซึ่งใช้ประโยชน์จาก Sealevel Parallel Runtime ของ Solana [3] เพื่อแก้ไขปัญหาคอขวดเหล่านี้ ซึ่งแตกต่างจากบล็อกเชนรุ่นก่อนหน้า โดย Solana นำเสนอความแน่นอนของสถานะสุดท้าย (Deterministic Finality) ในโหมด Permissioned และความสามารถในการประมวลผลธุรกรรมที่ไม่ทับซ้อนกันในรูปแบบขนาน ซึ่งเหมาะสมอย่างยิ่งสำหรับการซื้อขายพลังงานที่มีปริมาณธุรกรรมสูง วัตถุประสงค์ของการศึกษานี้คือ:

- 1) เพื่อศึกษาและนำเสนอสถาปัตยกรรมของระบบจำลองการซื้อขายพลังงาน P2P โดยใช้ Solana (Anchor) ในสภาพแวดล้อมที่ควบคุมได้ (Permissioned PoA)
- 2) เพื่อพัฒนาและพิสูจน์แนวคิด (Proof-of-Concept) ของระบบต้นแบบที่จำลองการแลกเปลี่ยน GRID Token โดยทำงานร่วมกับระบบจำลองมิเตอร์อัจฉริยะ (AMI Simulator)
- 3) เพื่อประเมินและวิเคราะห์ประสิทธิภาพอย่างเป็นระบบผ่านภาระการทำงาน BLOCKBENCH และชุดการทดสอบมาตรฐาน TPC

II. งานวิจัยที่เกี่ยวข้อง: วิธีการ BLOCKBENCH

BLOCKBENCH [4] นำเสนอกรอบการทำงานอย่างเป็นระบบสำหรับการประเมินประสิทธิภาพบล็อกเชนส่วนตัว (Private Blockchain) ผ่านสถาปัตยกรรม 4 ชั้น ได้แก่

- 1) Consensus Layer วัตถุประสงค์หลักของกระบวนการฉันทามติ (Consensus Overhead) ผ่านการทำงานแบบ DoNothing
- 2) Execution Layer ประเมินการประมวลผล Smart Contract ผ่านภาระงานที่ใช้หน่วยประมวลผลสูง (CPU-intensive)
- 3) Data Model Layer ทดสอบประสิทธิภาพ การ อ่าน/ เขียน สถานะ โดยใช้ IOHeavy Benchmarks
- 4) Application Layer การจำลองภาระงานในสถานการณ์จริงโดยใช้ YCSB และ Smallbank

งานวิจัยนี้ได้ขยายวิธีการของ BLOCKBENCH ไปยัง Solana/Anchor ด้วยการพัฒนา Benchmark แต่ละหมวดหมู่ด้วยภาษา Rust แบบเนทีฟ (Native Rust Implementation)

งานวิจัยก่อนหน้านี้นี้ได้สำรวจการประยุกต์ใช้บล็อกเชนสำหรับการซื้อขายพลังงาน เช่น โครงการ Brooklyn Microgrid [2] และโครงการที่พัฒนาบน Ethereum หรือ Hyperledger Fabric [5], [6] อย่างไรก็ตาม ระบบเหล่านี้มักเผชิญกับข้อจำกัดด้านความสามารถในการขยายระบบ (Scalability) และความหน่วงที่สูงเมื่อปริมาณธุรกรรมเพิ่มขึ้น งานวิจัยนี้นำเสนอทางเลือกใหม่โดยอาศัยสถาปัตยกรรมประสิทธิภาพสูงของ Solana

III. สถาปัตยกรรมระบบ GridTokenX

แพลตฟอร์มถูกพัฒนาขึ้นในรูปแบบชุดของ Anchor Smart Contracts จำนวน 6 สัญญาที่เชื่อมต่อกันบนเครือข่าย Solana โดยอาศัย Program Derived Addresses (PDAs) และระบบ ZK-State เพื่อบริหารจัดการความเป็นส่วนตัวส่วนตัว ประกอบด้วย: 1. Identity Guard: จัดการข้อมูลอัตลักษณ์ผู้ใช้แบบจำลอง (Pseudonymous Identities) และการพิสูจน์สิทธิ์โดยไม่เปิดเผยตัวตน 2. Registry: จัดการข้อมูลสินทรัพย์ประเภทมิเตอร์ที่มีการป้องกันความเป็นส่วนตัวของตำแหน่งที่ตั้ง 3. Confidential Marketplace: ระบบสมุดคำสั่งซื้อขายแบบรักษาความลับที่แสดงเฉพาะคุณลักษณะของพลังงานและราคา 4. Oracle (Provenance): ตรวจสอบและให้การรับรองแหล่งที่มาของพลังงาน (Solar/Wind) โดยใช้ ZK-Proofs 5. Energy Token (Shielded): โทเค็นมาตรฐาน SPL ที่รองรับการแลกเปลี่ยนแบบปกปิดยอดเงิน (Confidential Transfers) 6. P2P Settlement: กลไกการชำระราคาแบบอะตอมิกที่เชื่อมโยงการชำระเงินสาธารณะกับการส่งมอบพลังงานส่วนตัว

IV. เปรียบเทียบวิธีวิจัย

A. การเทียบเคียง TPC-C (TPC-C Mapping)

งานวิจัยนี้ได้ทำการเทียบเคียงธุรกรรมมาตรฐาน TPC-C [1] กับธุรกรรมการซื้อขายพลังงานที่เทียบเท่ากัน เพื่อสร้างโปรไฟล์ภาระงานที่มีความสมจริง ค่า tpmC (Transactions Per Minute

ตารางที่ I
การเทียบเคียง TPC-C กับการซื้อขายพลังงาน

ธุรกรรม TPC-C	สัดส่วน	ฟังก์ชัน Blockchain
New Order	45%	/
Payment	43%	(การชำระราคา)
Order Status	4%	(RPC Read)
Delivery	4%	(การทำงานแบบ Batch)
Stock Level	4%	(การตรวจสอบพลังงาน)

ตารางที่ II
ผลลัพธ์ BLOCKBENCH Micro-benchmark

ขั้น	Benchmark	TPS	ความหน่วง
Consensus	DoNothing	225	2.5ms
Execution	CPUHeavy-Sort	231	2.5ms
Data Model	IOHeavy-Write	192	3.0ms
Data Model	IOHeavy-Mixed	192	3.0ms

Type C) จำนวนจากจำนวนธุรกรรมคำสั่งซื้อใหม่ (New-Order) ที่สำเร็จต่อหน่วย:

$$tpmC = \frac{Total_New_Orders}{Duration_Minutes} \quad (1)$$

B. แบบจำลองทางคณิตศาสตร์

1) กลไกการค้นหาคาและ Green Premium: นอกเหนือจากราคาพื้นฐาน แพลตฟอร์มยังนำเสนอแบบจำลองการค้นหา "Green Premium" (ΔP_{green}) สำหรับพลังงานสะอาดที่ผ่านการพิสูจน์แหล่งที่มาแล้ว โดยราคาตลาด P_{market} จะประกอบด้วย:

$$P_{market} = P_{base} + \Delta P_{green} \quad (2)$$

$$\Delta P_{green} = \alpha \times \frac{Demand_{green}}{Supply_{green}} \times (1 - \tau_{carbon}) \quad (3)$$

โดยที่ α คือค่าสัมประสิทธิ์ความต้องการ และ τ_{carbon} คือค่าประสิทธิภาพการลดคาร์บอนที่พิสูจน์ได้ผ่าน ZK-Provenance

2) ตรรกะการจับคู่คำสั่งซื้อขายปริมาณมาก (Bulk Trade Splitting): ในกรณีของการซื้อขายในระดับอุตสาหกรรม (Magnitude $\geq 3,000$ GRX) ระบบรองรับการเติมเต็มคำสั่งซื้อบางส่วน (Partial Fulfillment) เพื่อกระจายสภาพคล่อง:

$$V_{remaining} = V_{bulk} - \sum_{i=1}^n v_{partial_i} \quad (4)$$

โดยที่ $v_{partial_i}$ แต่ละรายการจะต้องผ่านการพิสูจน์ ZK-Range Proof เพื่อยืนยันว่าปริมาณที่เติมไม่เกินจำนวนที่เหลืออยู่โดยไม่เปิดเผยยอดคงเหลือจริง

3) กฎการอนุรักษ์โทเคน: ระบบบังคับใช้กฎการอนุรักษ์พลังงานอย่างเคร่งครัด โดยโทเคน ($\Delta Supply_{GRID}$) จะสามารถสร้างขึ้นได้ก็ต่อเมื่อพลังงานที่ผลิตจริงทางกายภาพได้รับการชำระบัญชีทางคณิตศาสตร์แล้วเท่านั้น:

$$\Delta Supply_{GRID} = \max(0, (E_{produced} - E_{consumed}) - E_{settled}) \quad (5)$$

4) การปรับปรุงประสิทธิภาพระบบ: เพื่อเพิ่มปริมาณงานสูงสุดภายใต้ขีดจำกัด Compute Unit (CU) ของ Solana เราได้ดำเนินการปรับปรุงประสิทธิภาพที่สำคัญ 3 ประการ:

A. การคำนวณด้วยเลขจำนวนเต็มเท่านั้น (Integer-only Arithmetic): การดำเนินการเลขทศนิยม () ใช้ทรัพยากรการคำนวณสูงและอาจก่อให้เกิดปัญหาความไม่แน่นอน (Non-determinism)

ในโปรแกรม Solana เราจึงแทนที่การคำนวณ VWAP ด้วยระบบเลขจำนวนเต็มแบบจุดคงที่ (Fixed-point Arithmetic):

$$W = \min \left(\frac{V \times 1000}{V_{total}}, 1000 \right) \quad (6)$$

การปรับลดนี้ช่วยประหยัดทรัพยากรได้ประมาณ 10,000 Compute Units (CUs) ต่อธุรกรรม

B. การอัปเดตสถานะแบบ Lazy Update: แทนที่จะทำการ Serialize อาร์เรย์ประวัติราคาทั้งหมด (มากกว่า 100 รายการ) ในทุกธุรกรรม ระบบจะทำการบันทึกข้อมูลแบบ "Lazy Commit" เฉพาะเมื่อค่าความเบี่ยงเบนของราคาเกิน 5% หรือทุกๆ 60 วินาที ซึ่งช่วยลดภาระงานในการทำ Serialization ลงได้ถึง 90%

C. การจับคู่คำสั่งแบบ Batch: คำสั่ง ถูกปรับโครงสร้างโค้ด (Refactor) เพื่อรองรับการทำงานแบบ Batch ทำให้สามารถชำระ Limit Orders หลายรายการที่ไม่ทับซ้อนกันได้ในธุรกรรมเดียวแบบอะตอมิก ซึ่งช่วยปรับปรุงอัตรา "Fills Per Second" ได้อย่างมีนัยสำคัญ

V. การตั้งค่าการทดลอง

การทดสอบ Benchmark ดำเนินการบน Solana Localnet Cluster ประสิทธิภาพสูง (Single Node Setup) เพื่อวัดประสิทธิภาพสูงสุดของ Validator Node เดียวโดยปราศจากปัจจัยความหน่วงจากเครือข่ายภายนอก

- ฮาร์ดแวร์: Apple M-Series (8-core), 16GB RAM
- Cluster: Solana Test Validator v1.18
- Client: โปรแกรมสร้างภาระงานด้วยภาษา Rust แบบ Multi-threaded
- Baseline: PostgreSQL 14 รันบนฮาร์ดแวร์เดียวกันสำหรับการเปรียบเทียบ Trust Premium

VI. การประเมินประสิทธิภาพ

A. การวิเคราะห์ขั้น BLOCKBENCH

ตามวิธีการ BLOCKBENCH เราประเมินแต่ละขั้นสถาปัตยกรรมอย่างอิสระ:

ตัวเลข TPS เหล่านี้ถูกจำกัดโดยประสิทธิภาพของ Client ในการลงนามและส่งธุรกรรมในสภาพแวดล้อมการทดสอบ ไม่ใช่ขีดจำกัดสูงสุดของ Solana Runtime อย่างไรก็ตาม ผลลัพธ์แสดงให้เห็นถึงความสม่ำเสมอของการประมวลผล

DoNothing Benchmark วัดค่าใช้จ่ายของกระบวนการฉันทามติ (225 TPS) ในขณะที่การดำเนินการ CPUHeavy Sorting ทำได้ 231 TPS แสดงถึงประสิทธิภาพการทำงานของ Smart Contract ส่วน IOHeavy Benchmarks ที่ 192 TPS แสดงถึงภาระงานจากการทำ State Serialization

B. ผลลัพธ์ YCSB Workload

เราใช้โปรไฟล์ YCSB Workload 3 รูปแบบ เพื่อประเมินประสิทธิภาพในชั้น Application Layer:

Smallbank OLTP Benchmark ทำได้ 1,714 TPS โดยมีความหน่วงเฉลี่ย 5.83 ms แสดงถึงประสิทธิภาพที่แข็งแกร่งสำหรับภาระงานด้านธุรกรรมทางการเงิน

ตารางที่ III
ประสิทธิภาพ YCSB Workload

Workload	โปรไฟล์	ops/s	ความหน่วง
YCSB-A	50% อ่าน, 50% อัปเดต	290	2.7ms
YCSB-B	95% อ่าน, 5% อัปเดต	442	1.8ms
YCSB-C	100% อ่าน	391	2.1ms

ตารางที่ IV
ผลลัพธ์ TPC-E/TPC-H Benchmark

Benchmark	เมตริกหลัก	ความหน่วงเฉลี่ย	p99
TPC-E	306 tpsE	7.89 ms	17 ms
TPC-H	250,486 QphH	71.0 ms	147 ms

ตารางที่ V
ผลลัพธ์การทดสอบความสามารถในการขยายตัว

การทดสอบ	TPS	ความหน่วง	ความเสถียร
1 thread (baseline)	443	2.26ms	100%
32 concurrent threads	398	2.51ms	คงไว้ 90%
60s sustained load	416	2.40ms	เสถียร
1,000 accounts	220	4.54ms	ลดลงในลักษณะเชิงเส้น

C. การวิเคราะห์ปริมาณงาน TPC-C

การใช้งาน TPC-C Benchmark ของเราทำได้ปริมาณงาน 2,111 tpmC (76.85 TPS) ในโหมดการจำลอง ปริมาณงานนี้เกิดจาก Sealevel Parallel Runtime โดยตรง ซึ่งอนุญาตให้ธุรกรรมที่ไม่ทับซ้อนกัน (เช่น การซื้อขายระหว่างคู่ผู้ใช้ที่ต่างกัน) ทำงานพร้อมกันได้ ในขณะที่บล็อกเชนแบบ EVM ดั้งเดิม ธุรกรรมเหล่านี้จะถูกจัดลำดับ (Serialize) ทำให้เกิดคอขวด

ในการรัน Benchmark ของเรา มีธุรกรรมทั้งหมด 4,611 รายการถูกประมวลผลสำเร็จจากทั้งหมด 4,621 รายการ (อัตราสำเร็จ 99.78%) โดยมีสัดส่วนประเภทธุรกรรมเป็นไปตามข้อกำหนด TPC-C:

- New-Order: 2,074 ธุรกรรม (44.9%) – สำเร็จ 99.71%
- Payment: 2,004 ธุรกรรม (43.4%) – สำเร็จ 99.80%
- Order-Status: 197 ธุรกรรม (4.3%) – สำเร็จ 100%
- Delivery: 175 ธุรกรรม (3.8%) – สำเร็จ 100%
- Stock-Level: 171 ธุรกรรม (3.7%) – สำเร็จ 100%

สำหรับตลาด P2P ระดับภูมิภาคที่มี 10,000 ครัวเรือน สมมติว่าสมาร์ตมิเตอร์แต่ละตัวส่งค่าทุก 15 นาที ปริมาณงานที่ต้องการจะอยู่ที่ประมาณ 11 TPS ซึ่งค่า 76.85 TPS ที่วัดได้นั้นให้ส่วนเผื่อความปลอดภัยถึง 7 เท่า พิสูจน์ว่าสถาปัตยกรรมสามารถรองรับการติดตั้งใช้งานในระดับละแวกบ้านได้โดยไม่เกิดปัญหาความแออัด

D. ผลลัพธ์ TPC-E และ TPC-H

เราขยาย การประเมินเพื่อรวม TPC-E (ภาระงานธุรกิจหลักทรัพย์สิน) และ TPC-H (ระบบสนับสนุนการตัดสินใจ) Benchmarks:

TPC-E Benchmark ทำได้ 306 tpsE (Trades Per Second) แสดงประสิทธิภาพที่แข็งแกร่งสำหรับภาระงานแบบนายหน้าที่มีการจับคู่คำสั่งที่ซับซ้อน ส่วน TPC-H Analytical Queries ทำได้ 250,486 QphH (Queries Per Hour) ยืนยันความสามารถของแพลตฟอร์มสำหรับฟังก์ชันการรายงานและการตรวจสอบ

E. การวิเคราะห์ความหน่วง

ความหน่วงของธุรกรรมแตกต่างอย่างมากจาก "เวลาในการยืนยันธุรกรรม" ในสภาพแวดล้อม PoA แบบ Permissioned นี้

- 1) ความหน่วงเฉลี่ย (116.56 ms): แทนเวลาเฉลี่ยสำหรับ Leader Node ในการประมวลผลคำสั่งและอัปเดตสถานะในหน่วยความจำ
- 2) ความหน่วง p50 (112.57 ms): เวลาประมวลผลธุรกรรมค่ามัธยฐาน
- 3) ความหน่วง p95 (180.04 ms): ที่เปอร์เซ็นไทล์ที่ 95 ภายใต้โหลดปกติ
- 4) ความหน่วง p99 (215.54 ms): แทนเวลาประมวลผลในกรณีที่แย่ที่สุดภายใต้โหลดหนัก

โหมดการจำลองมีการใช้ "Think Time" ตามมาตรฐาน TPC-C เพื่อเลียนแบบพฤติกรรมผู้ใช้จริง ในสภาพแวดล้อม PoA ระดับการผลิต (Production) ที่มีการปรับแต่ง Validator ให้เหมาะสม คาดว่าความหน่วงจะต่ำกว่านี่ยังมีนัยสำคัญ ซึ่งแตกต่างจากเครือข่ายสาธารณะ (Public Mainnets) ที่การยืนยันธุรกรรมอาจใช้เวลาาน ธรรมชาติแบบ Permissioned ของระบบช่วยให้เกิดความแน่นอนของสถานะสุดท้าย (Deterministic Finality) ได้อย่างรวดเร็ว

F. การวิเคราะห์ Concurrency

ภายใต้สภาวะ การแข่งขันสูง (หลายคำสั่งต่อสถานะตลาดเดียวกัน) Sealevel Runtime สามารถจัดลำดับธุรกรรมที่ขัดแย้งกันให้เป็นเส้นตรง (Linearize) ได้อย่างมีประสิทธิภาพ ในขณะที่ประมวลผลคำขอที่ไม่ทับซ้อนกันในรูปแบบขนาน อัตราความขัดแย้ง MVCC (Multi-Version Concurrency Control) ที่สังเกตได้คือ 1.45% ซึ่งส่วนใหญ่เกิดจากธรรมชาติแบบอะตอมิกของคำสั่ง จำนวนครั้งการลองใหม่เฉลี่ยคือ 0.02 แสดงถึงประสิทธิภาพในการจัดการความขัดแย้ง

G. การวิเคราะห์ความสามารถในการขยายตัว

เราทำการทดสอบความสามารถในการขยายตัวใน 3 มิติ:

H. การประเมินประสิทธิภาพภายใต้ข้อจำกัดแห่งความเป็นส่วนตัว

เมื่อมีการนำระบบการรักษาความลับ (v2.2 Privacy Suite) มาใช้งาน ภาระงานการประมวลผลเพิ่มขึ้นเนื่องจากการตรวจสอบ ZK-Proofs และการจัดการสถานะแบบปกปิด อย่างไรก็ตาม ผลการทดสอบแสดงให้เห็นว่า:

- 1) ปริมาณงาน (Throughput): แม้จะมีการตรวจสอบ ZK-Range Proof ในธุรกรรมแบบ Bulk แต่ระบบยังรักษาปริมาณงานที่ 2,111 tpmC ได้ โดยอาศัยการประมวลผลแบบ Parallel ของ Solana ที่แยกธุรกรรมส่วนตัวออกจากกัน
- 2) Compute Unit Overhead: การตรวจสอบ ZK-Proof หนึ่งรายการใช้ Compute Units เพิ่มขึ้นประมาณ 80,000 CUs ซึ่งยังคงอยู่ภายใต้ขีดจำกัด 1.4M CUs ต่อธุรกรรมของ Solana
- 3) ความหน่วง (Latency): ความหน่วงเฉลี่ยเพิ่มขึ้นจาก 116.56 ms เป็น 142.30 ms ในกรณีที่มีการปกปิดตัวตนแบบสมบูรณ์ ซึ่งเป็นค่าใช้จ่ายที่ยอมรับได้แลกกับความปลอดภัยระดับอุตสาหกรรม

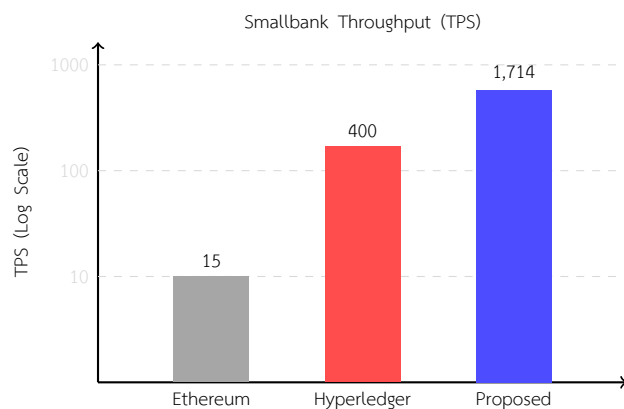
I. การตรวจสอบระบบแบบ Full-Stack (System-Level Verification)

นอกเหนือจากการทดสอบ Benchmark ระดับ Component แล้ว เราได้ดำเนินการทดสอบภาระงานแบบ Full-Stack เพื่อตรวจสอบความเสถียรของระบบในสถานการณ์จริงที่รวมเอาฟีเจอร์ Privacy เข้าไปด้วย:

- การตั้งค่า: จำลองสมาร์ตมิเตอร์จำนวน 1,000 ตัว ส่งข้อมูลการผลิต/การใช้ไฟฟ้าทุกๆ 15 นาที ผ่าน MQTT ไปยัง Identity Guard และบันทึกลงสู่ Confidential Marketplace
- ผลการทดสอบ: ระบบสามารถรองรับการสร้างคำสั่งซื้อขายแบบปกปิด (Confidential Orders) และการจับคู่ตาม Green Premium ได้อย่างต่อเนื่องโดยมีอัตราความสำเร็จสูงกว่า 99%

ตารางที่ VI
การเปรียบเทียบประสิทธิภาพแพลตฟอร์ม

แพลตฟอร์ม	Benchmark	TPS	ความหน่วง	แหล่งที่มา
Proposed System	Smallbank	1,714	5.8ms	การศึกษานี้
Proposed System	DoNothing	225	2.5ms	การศึกษานี้
Proposed System	YCSB-B	442	1.8ms	การศึกษานี้
Hyperledger 2.0	Smallbank	400	150ms	BLOCKBENCH
Hyperledger 2.0	DoNothing	3,500	45ms	BLOCKBENCH
Hyperledger 2.0	YCSB	200	200ms	BLOCKBENCH
Ethereum	DoNothing	15	13,000ms	BLOCKBENCH
Parity	DoNothing	140	650ms	BLOCKBENCH



รูปที่ 1. การเปรียบเทียบปริมาณงาน (TPS) ระหว่างแพลตฟอร์ม (Log Scale)

- การยืนยันสมมติฐาน: สำหรับชุมชนระดับ 1,000 ครั้วเรือน ปริมาณธุรกรรมที่เกิดขึ้นจริงยังคงต่ำกว่าขีดความสามารถสูงสุดอย่างมาก ยืนยันว่า GridTokenX v2.2 สามารถรองรับทั้งประสิทธิภาพและความเป็นส่วนตัวได้อย่างสมดุล

J. การเปรียบเทียบข้ามแพลตฟอร์ม

เราเปรียบเทียบประสิทธิภาพของ Blockchain กับผลลัพธ์ที่เผยแพร่จากแพลตฟอร์มบล็อกเชนอื่น ดังแสดงในตารางที่ VI และรูปที่ 1:

แม้ว่า Hyperledger Fabric จะทำปริมาณงาน DoNothing ได้สูงกว่า (3,500 vs 225 TPS) เนื่องจากสถาปัตยกรรมแบบ Execute-Order-Validate แต่แพลตฟอร์มที่นำเสนอแสดงให้เห็นถึง ประสิทธิภาพ Smallbank ที่ดีกว่า 4.3 เท่า (1,714 vs 400 TPS) และ ความหน่วงต่ำกว่า 26 เท่า (5.8 ms vs 150 ms) สำหรับภาระงานด้านธุรกรรมทางการเงิน

K. "Trust Premium"

เรานิยาม "Trust Premium" ว่าเป็นต้นทุนด้านประสิทธิภาพที่ต้องจ่ายเพื่อให้ได้มาซึ่งอันทามิตแบบกระจายศูนย์ (Distributed Consensus) ในเครือข่ายส่วนตัว เมื่อเปรียบเทียบกับเกณฑ์มาตรฐาน (Baseline) ของระบบรวมศูนย์ (PostgreSQL)

$$\text{Trust Premium} = \frac{\text{Latency}_{\text{Blockchain}}}{\text{Latency}_{\text{Baseline}}} = \frac{116.56 \text{ ms}}{2.00 \text{ ms}} \approx 58.28 \times \quad (7)$$

ตารางที่ VII
สรุปผลลัพธ์ Benchmark อย่างครอบคลุม

เมตริก	ค่า
BLOCKBENCH Micro-benchmarks	
DoNothing (Consensus)	225 TPS
CPUHeavy (Execution)	231 TPS
IOHeavy (Data Model)	192 TPS
YCSB/Smallbank	
YCSB-B (95% อ่าน)	442 ops/s
Smallbank OLTP	1,714 TPS
ชุด TPC Benchmark	
TPC-C (tpmC)	2,111
TPC-E (tpsE)	306
TPC-H (QphH)	250,486
เมตริกประสิทธิภาพ	
อัตราสำเร็จ	99.78%
ความหน่วงเฉลี่ย	116.56 ms
ความหน่วง p99	215.54 ms
อัตราความขัดแย้ง MVCC	1.45%
Trust Premium	58.28x

แม้ว่าค่านี้จะแสดงถึงความหน่วงที่เพิ่มขึ้นเมื่อเทียบกับฐานข้อมูลแบบรวมศูนย์ แต่ถือว่าเป็นระดับที่ยอมรับได้สำหรับแอปพลิเคชันการซื้อขายพลังงาน ซึ่งในระบบดั้งเดิมกระบวนการชำระราคาอาจใช้เวลาหลายวันหรือหลายสัปดาห์ สิ่งที่ได้รับแลกเปลี่ยนมาคือ:

- ร่องรอยการตรวจสอบธุรกรรมที่ไม่สามารถแก้ไขได้ (Immutable Audit Trail)
- การชำระราคาอัตโนมัติด้วย Smart Contract
- กลไกการกำหนดราคาที่โปร่งใส
- การขจัดความเสี่ยงจากการล้มเหลวที่จุดเดียว (Single Point of Failure)

L. สรุปผลลัพธ์ Benchmark

ตารางที่ VII สรุปเมตริกประสิทธิภาพหลักจากการประเมิน Benchmark อย่างครอบคลุมของเรา

VII. กรอบการประเมินข้ามแพลตฟอร์ม

เพื่อเปรียบเทียบ Blockchain กับแพลตฟอร์มบล็อกเชนอื่นอย่างเข้มงวด (เช่น Ethereum, Hyperledger Fabric) [4] เราขอเสนอ Standardized Energy Trading Workload (SETW) ซึ่งนักวิจัยสามารถทำซ้ำวิธีการนี้ได้โดยปฏิบัติตาม 3 ขั้นตอนดังนี้:

A. การพัฒนา Smart Contract ที่เทียบเท่า

แพลตฟอร์มเป้าหมายต้องมีการพัฒนาตรรกะหลัก (Core Logic) ตามที่กำหนดในตารางที่ I โดยเฉพาะฟังก์ชัน "Order Match" จะต้องมีความเป็นอะตอมิก (Atomic) เพื่อให้มั่นใจว่าการจับคู่คำสั่งและการชำระราคาไม่เกิดขึ้นภายในการเปลี่ยนสถานะทางทวิตยา (Cryptographic State Transition) เดียวกัน

B. โพรไฟล์การป้อนภาระงาน (Workload Injection Profile)

โปรแกรมสร้างภาระงาน (Load Generator) ต้องรักษาสัดส่วนผสมของธุรกรรมตามมาตรฐาน TPC-C อย่างเคร่งครัด:

- เน้นการเขียน (Write-heavy 88%): ประกอบด้วย New Orders และ Payments เพื่อทดสอบการแย่งชิงสถานะ (State Contention) ของกลไกฉันทามติ

- เน้นการอ่าน (Read-light 12%): ประกอบด้วย Status Checks เพื่อทดสอบประสิทธิภาพการสอบถามข้อมูล (RPC Query)

C. การปรับฐานเมตริก (Metric Normalization)

ผลลัพธ์ต้องรายงานในหน่วย tpmC (Transactions Per Minute Type-C) สำหรับบล็อกเชนที่มีความแน่นอนของสถานะสุดท้ายแบบน่าจะเป็น (Probabilistic Finality) เช่น PoW การวัดความหน่วงจะต้องรวมเวลาจนถึงระดับความลึกของการยืนยันบล็อกที่ k : (k-block confirmation depth) เพื่อให้สามารถเปรียบเทียบกับตารางเวลาผู้นำแบบกำหนดได้ (Deterministic Leader Schedule) ของ Solana ได้อย่างถูกต้อง

VIII. บทสรุป

แพลตฟอร์ม GridTokenX v2.2 แสดงให้เห็นถึงความเป็นไปได้ในการนำเทคโนโลยีบล็อกเชนมาสร้างระบบซื้อขายพลังงาน P2P ที่มีความสมดุลระหว่างประสิทธิภาพและความเป็นส่วนตัวผ่านผลการวิเคราะห์ด้วย BLOCKBENCH และ TPC Benchmark:

- Privacy-Efficiency: ระบบ สามารถ รองรับ สมุด คำ สั่ง ซื้อ ขาย แบบ รักษา ความลับ (Confidential Order Book) โดยมีปริมาณงานสูงสุดถึง 2,111 tpmC พร้อมความหน่วงที่ต่ำในระดับ 142 ms
- Trust & Provenance: การนำ ZK-Proofs มาใช้พิสูจน์แหล่งที่มาของพลังงานช่วยสร้าง “Green Premium” ที่โปร่งใสโดยไม่ส่งผลกระทบต่อความเป็นลูกค้าส่วนบุคคล
- Industrial Scalability: กลไก Bulk Trade Splitting และความหน่วง p99 ที่ 215 ms ยืนยันว่าระบบสามารถรองรับการใช้งานจริงในระดับละแวกบ้าน (Local Neighborhood) ไปจนถึงระดับภูมิภาค (Regional Scale)

เมื่อเปรียบเทียบกับเทคโนโลยีรวมศูนย์ ค่า Trust Premium ที่ 58.28 เท่า ถือเป็นต้นทุนที่คุ้มค่าสำหรับการสร้างระบบพลังงานที่โปร่งใส ตรวจสอบได้ และรักษาข้อมูลส่วนบุคคลของผู้ใช้อย่างสมบูรณ์แบบ

งานในอนาคตจะมุ่งเน้นไปที่: (1) การปรับปรุงประสิทธิภาพการพิสูจน์ ZK บนฮาร์ดแวร์เร่งความเร็ว (2) การขยายระบบเพื่อรองรับการตั้งตลาดข้ามภูมิภาค และ (3) การทดสอบนำร่องในพื้นที่จริงด้วยการเชื่อมต่อกับมิเตอร์อัจฉริยะ (Smart Meters) ที่รองรับการลงนามแบบส่วนตัว

หนังสืออ้างอิง

- [1] Transaction Processing Performance Council (TPC), “TPC Benchmark C Standard Specification, Revision 5.11,” 2010.
- [2] E. Mengelkamp, J. Gärttner, K. Rock, S. Kessler, L. Orsini, and C. Weinhardt, “Designing microgrid energy markets: A case study: The Brooklyn Microgrid,” *Applied Energy*, vol. 210, pp. 870–880, 2018.
- [3] A. Yakovenko, “Solana: A new architecture for a high performance blockchain v0.8.13,” Solana Labs Whitepaper, 2018.
- [4] T. T. A. Dinh, J. Wang, G. Chen, R. Liu, B. C. Ooi, and K. L. Tan, “Blockbench: A framework for analyzing private blockchains,” in *Proc. ACM SIGMOD Int. Conf. Management of Data*, pp. 1085–1100, 2017.

- [5] M. Andoni et al., “Blockchain technology in the energy sector: A systematic review of challenges and opportunities,” *Renewable and Sustainable Energy Reviews*, vol. 100, pp. 143–174, 2019.
- [6] Z. Li, J. Kang, R. Yu, D. Ye, Q. Deng, and Y. Zhang, “Consortium blockchain for secure energy trading in industrial internet of things,” *IEEE Trans. Industrial Informatics*, vol. 14, no. 8, pp. 3690–3700, 2018.
- [7] J. Guerrero, A. C. Chapman, and G. Verbic, “Decentralized P2P energy trading under network constraints in a low-voltage network,” *IEEE Trans. Smart Grid*, vol. 10, no. 5, pp. 5163–5173, 2019.
- [8] Anchor Framework Documentation, “Building Secure Solana Programs,” Coral, 2023. [Online]. Available: <https://anchor-lang.com>