

MEV (Miner Extractable Value): มูลค่าที่ขุดได้จากการจัดเรียงธุรกรรม

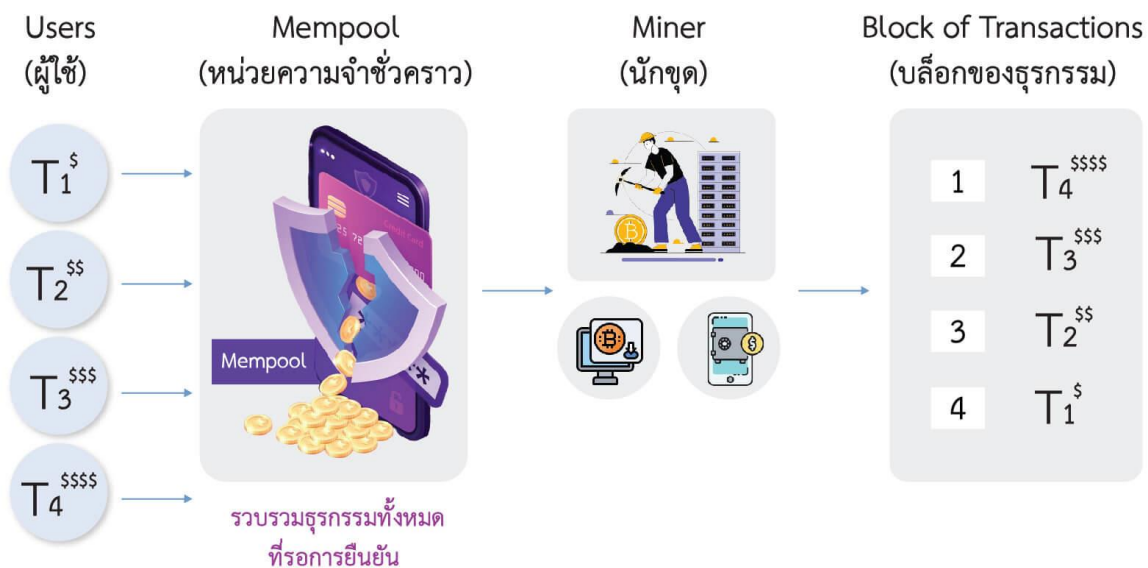
ทุกครั้งที่คุณซื้อขายคริปโตบนบล็อกเชน มีใครบางคนอาจกำลังแอบหยิบเงินจากกระเป๋าของคุณโดยที่คุณไม่รู้ตัว **MEV คือ กลไกที่ทำให้นักขุดและบอทพิเศษสามารถรีดเงินจากธุรกรรมของผู้ใช้ทั่วไป** ด้วยอำนาจในการจัดเรียงลำดับการซื้อขาย พวกเขา กำลังทำอะไรหลายพันล้านดอลลาร์ ทำไมเรื่องนี้ถึงสำคัญและเราจะปกป้องตัวเองได้อย่างไร? ลองไปติดตามกัน ดังนี้ค่ะ

MEV (Miner-Extractable Value) คืออะไร?

- **MEV หรือ Miner-Extractable Value** คือ มูลค่าที่นักขุด (miners) หรือผู้ตรวจสอบความถูกต้องของการทำธุรกรรมบนบล็อกเชนสามารถดึงออกมาได้
- โดยการจําลัดบธุรกรรมตามใจชอบ ภายในบล็อกที่พวกเขาสร้าง ซึ่งทำให้พวกเขาสามารถทำกำไรจากผู้ใช้งานทั่วไปโดยที่ผู้ใช้งานไม่รู้ตัว

THAILAND
TRADERCLUB

กระบวนการทำธุรกรรมบนบล็อกเชน



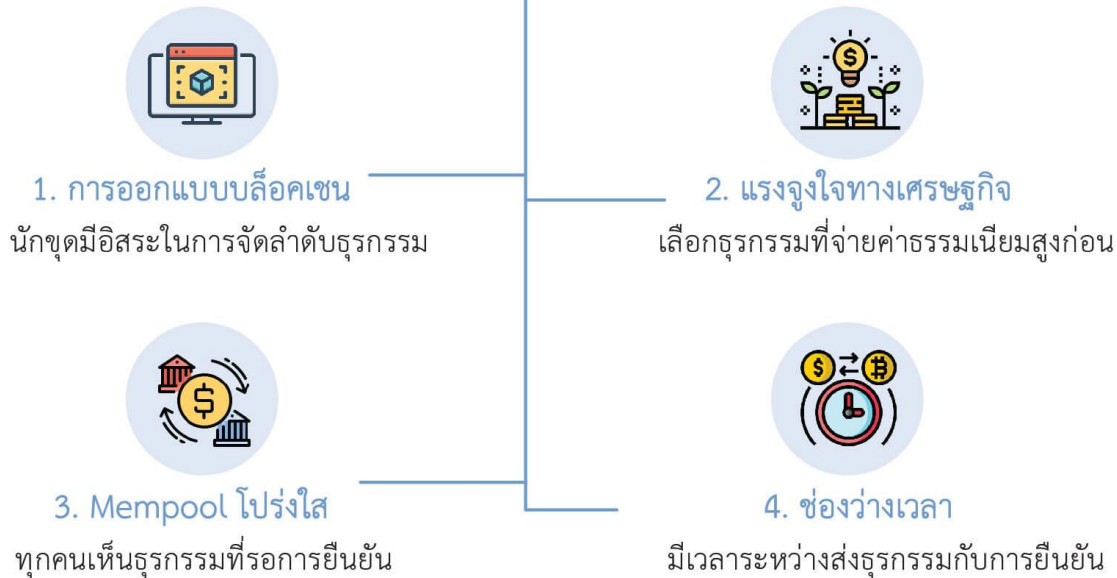
ภาพนี้ แสดงการทำงานของบล็อกเชน โดยนักขุดเลือกธุรกรรมตามค่าธรรมเนียม ไม่ใช่ตามลำดับเวลา ช่องโหว่นี้ทำให้เกิด MEV

เหตุใดจึงเกิด MEV?

สาเหตุหลักที่ทำให้เกิด MEV มาจากลักษณะการออกแบบของเครือข่ายบล็อกเชนที่ให้อิสระแก่นักขุด (miners) หรือผู้ตรวจสอบ (validators) ในการจัดการธุรกรรม

THAILAND
TRADERCLUB

สาเหตุที่ทำให้เกิด MEV



ลองขยายความเพิ่มเติมเพื่อให้เข้าใจมากขึ้น ดังนี้ค่ะ

- **การออกแบบของบล็อกเชน:** โดยพื้นฐานแล้ว บล็อกเชนถูกออกแบบให้นักขุดหรือผู้ตรวจสอบทำหน้าที่รวบรวมและตรวจสอบความถูกต้องของธุรกรรม แต่ไม่ได้กำหนดกฎเกณฑ์ตายตัวว่าต้องจัดลำดับธุรกรรมอย่างไร
- **ระบบแรงจูงใจทางเศรษฐกิจ:** เครือข่ายบล็อกเชนส่วนใหญ่ให้แรงจูงใจแก่นักขุดในการเลือกธุรกรรมที่มีค่าธรรมเนียมสูง เพราะพวกเขาได้รับค่าธรรมเนียมเหล่านั้น ทำให้ธุรกรรมที่จ่ายมากกว่ามักได้รับการประมวลผลก่อน
- **ความโปร่งใสของ mempool:** ทุกธุรกรรมที่รอการยืนยันสามารถถูกมองเห็นได้โดยทุกคนในเครือข่าย ซึ่งเป็นการเปิดเผยความตั้งใจทางการเงินของผู้ใช้ก่อนที่ธุรกรรมจะถูกบันทึกลงบล็อกเชน
- **ช่องว่างทางเวลา:** มีช่วงเวลาระหว่างการส่งธุรกรรมกับการยืนยันธุรกรรม ในช่วงเวลานี้เองที่ MEV searchers สามารถวิเคราะห์และสร้างธุรกรรมของตนเองเพื่อฉกฉวยโอกาส

เครือข่ายบล็อกเชนถูกออกแบบให้รับประกันความถูกต้องของธุรกรรม (ไม่มีการใช้จ่ายซ้ำซ้อน) และความต่อเนื่องของการสร้างบล็อก แต่ไม่ได้ให้การรับประกันเกี่ยวกับลำดับการประมวลผลธุรกรรม นี่คือช่องว่างที่ทำให้เกิด MEV ขึ้น

ทั้งหมดนี้ เรียกได้ว่า เป็นสาเหตุพื้นฐานที่ทำให้เกิดปรากฏการณ์ MEV ซึ่งตอนนี้ได้กลายเป็นปัญหาสำคัญในระบบนิเวศ DeFi ที่ต้องการการแก้ไขอย่างเร่งด่วน

รูปแบบของ MEV ที่พบบ่อย

การแลกเปลี่ยนแบบ Arbitrage

- บอทของบุคคลที่สามทำการซื้อขายระหว่าง DEX (Decentralized Exchanges) ตั้งแต่สองแห่งขึ้นไป
- **ทำกำไรจากส่วนต่างราคา** โดยซื้อจากแพลตฟอร์มที่ราคาต่ำกว่าและขายในแพลตฟอร์มที่ราคาสูงกว่า
- เกิดการแข่งขันแบบ "สงครามการเสนอราคาก้าว" ระหว่างบอท arbitrage ที่แข่งกันจ่ายค่าธรรมเนียมสูงขึ้นเรื่อย ๆ
- **ผลกระทบ:** ค่าธรรมเนียมเครือข่ายสูงขึ้นสำหรับทุกคน แม้ว่าจะช่วยปรับสมดุลราคาในตลาดก็ตาม

การซื้อขายแบบตัดหน้า (Frontrunning)

- บอทสามารถเห็นธุรกรรมที่กำลังจะเกิดขึ้นใน mempool
- **คัดลอกธุรกรรมและจ่ายค่าแก๊สสูงกว่า** เพื่อให้ธุรกรรมของตนถูกประมวลผลก่อน
- เปลี่ยนราคาตลาดของสินทรัพย์และได้กำไรจากธุรกรรมของผู้ใช้ทั่วไป
- **ผลกระทบ:** ผู้ใช้ได้รับโทเคนน้อยกว่าที่คาดไว้ (เกิด slippage) และเสียเงินโดยไม่รู้ตัว เหมือนจ่าย "ค่าธรรมเนียมที่มองไม่เห็น"

ผลกระทบของ MEV

ผลกระทบต่อผู้ใช้

- ค่าธรรมเนียมเครือข่ายสูงขึ้นสำหรับทุกคน
- การซื้อขายเกิด slippage มากขึ้น (ได้ราคาแย่กว่าที่คาดหวัง)
- เสียเงินให้กับบอทและนักขุดโดยไม่รู้ตัว

ผลกระทบต่อเครือข่าย

- แบนด์วิดท์ของเครือข่ายถูกใช้ไปกับการแข่งขันระหว่างบอท
- อาจนำไปสู่ปัญหาด้านความมั่นคงของ consensus ในกรณีที่รุนแรง

การแก้ไขปัญหา MEV: Chainlink Fair Sequencing Services (FSS)

แนวคิดหลักของ Chainlink FSS

Chainlink FSS เป็นโซลูชันที่แก้ปัญหา MEV โดย:

- แยกการจัดลำดับธุรกรรมจากการสร้างบล็อก - นักขุดยังคงสร้างบล็อก แต่ไม่มีอำนาจในการจัดลำดับธุรกรรมอีกต่อไป
- มอบหน้าที่จัดลำดับให้เครือข่าย oracle - เครือข่าย oracle แบบกระจายอำนาจของ Chainlink ทำหน้าที่ตัดสินลำดับอย่างเป็นกลาง

วิธีการทำงานของ FSS

- ผู้ใช้ส่งธุรกรรม - ไปยังเครือข่าย oracle หรือลงใน mempool ตามปกติ (รองรับวิธีการเดิม)
- Oracle จัดลำดับธุรกรรม - ตามนโยบายที่กำหนดไว้ล่วงหน้า เช่น "เรียงตามเวลาที่มาถึง"
- Oracle ลงนามรับรองลำดับ - เครือข่าย oracle ลงความเห็นพ้องและรับรองลำดับของธุรกรรม
- Smart contract ประมวลผลตามลำดับที่รับรอง - ธุรกรรมจะถูกประมวลผลตามลำดับที่ oracle กำหนด

นโยบายการจัดลำดับที่รองรับ

- เรียงตามเวลาที่มาถึง (FIFO) - ธุรกรรมที่มาก่อนได้รับการประมวลผลก่อน
- การเรียงลำดับแบบเข้ารหัส - ธุรกรรมถูกเข้ารหัสก่อน จัดลำดับ แล้วจึงถอดรหัส ป้องกันการเห็นล่วงหน้า
- กฎที่กำหนดเอง - แอปพลิเคชันสามารถกำหนดนโยบายเฉพาะได้ตามความต้องการ

ประโยชน์หลักของ FSS

- ลดค่าธรรมเนียมเครือข่าย - ขจัดสงครามการประมูลราคาซื้อขายระหว่าง MEV searchers
- ปกป้องผู้ใช้ - ป้องกันการถูกตัดหน้า (frontrunning) และการโจมตีแบบแซนด์วิช
- สร้างความเท่าเทียม - ทุกผู้ใช้ได้รับการปฏิบัติเหมือนกัน ไม่ว่าจะมีทุนมากหรือน้อย
- เพิ่มความมั่นคงของเครือข่าย - ลดความเสี่ยงจากการปรับโครงสร้างบล็อก (block reorg)

ข้อดีทางเทคนิค

- ทำงานกับบล็อกเชนที่มีอยู่แล้ว - ไม่ต้องทำการเปลี่ยนแปลงบล็อกเชนหลัก
- รองรับแอปพลิเคชันหลากหลาย - เหมาะกับ DEX, lending protocols และแอปพลิเคชัน DeFi อื่นๆ
- ขยายขอบเขตได้ - รองรับบล็อกเชนหลายแพลตฟอร์มและ layer-2 โซลูชัน

Chainlink FSS จึงเป็นแนวทางที่ครอบคลุมในการสร้างระบบบล็อกเชนที่ยุติธรรมกว่า โปร่งใสกว่า และมีประสิทธิภาพมากกว่า ช่วยให้ DeFi สามารถเติบโตอย่างยั่งยืนโดยที่ผู้ใช้ไม่ถูกเอาเปรียบจากกลไก MEV

ประโยชน์ของ Chainlink FSS

- **สร้างความยุติธรรม:** ธุรกรรมถูกจัดลำดับตามกฎที่กำหนดไว้ล่วงหน้า ไม่ใช่ตามผู้ที่จ่ายเงินมากที่สุด
- **ลดค่าธรรมเนียม:** ช่วยลดสงครามการประมูลค่าก๊าซ
- **ปรับปรุงประสบการณ์ผู้ใช้:** ทำให้การทำธุรกรรมบน DeFi มีความเป็นธรรมมากขึ้น
- **ปกป้องผู้ใช้:** ป้องกันการถูกตัดหน้า (frontrunning) และวิธีการอื่นๆ ที่ดึงมูลค่าจากผู้ซื้อ
- **เพิ่มความแม่นยำในการคาดการณ์ผลลัพธ์:** ผู้ใช้สามารถคาดการณ์ผลลัพธ์ของธุรกรรมได้แม่นยำมากขึ้น เนื่องจากไม่มีการแทรกแซงจากบอทหรือนักขุดที่จะเปลี่ยนแปลงราคาหรือลำดับการทำธุรกรรม
- **สร้างสภาพแวดล้อมที่เหมาะสมต่อผู้ขายรายย่อย:** ผู้ใช้ทั่วไปที่มีเงินทุนจำกัดสามารถเข้าถึงและใช้ประโยชน์จาก DeFi ได้อย่างเท่าเทียม โดยไม่เสียเปรียบผู้เล่นรายใหญ่หรือผู้ที่มีเทคโนโลยีขั้นสูง
- **เพิ่มความโปร่งใสของตลาด:** ทำให้ตลาด DeFi มีความโปร่งใสมากขึ้น โดยขจัดกลยุทธ์การทำกำไรที่ไม่เป็นธรรมและไม่โปร่งใส ช่วยสร้างความเชื่อมั่นให้แก่นักลงทุนและผู้ซื้อ
- **ลดความเสี่ยงจากการสูญเสียเงินโดยไม่รู้ตัว:** ขจัด "ค่าธรรมเนียมที่มองไม่เห็น" ที่ผู้ใช้สูญเสียจากการตัดหน้า และการโจมตีแบบแซนด์วิช ซึ่งอาจมีมูลค่าสูงถึง 10-30% ในบางกรณี
- **เพิ่มประสิทธิภาพการใช้ทรัพยากรเครือข่าย:** ลดการใช้แบนด์วิดท์และพื้นที่บล็อกไปกับธุรกรรมที่ไม่จำเป็นจากการแข่งขัน MEV ทำให้เครือข่ายสามารถรองรับธุรกรรมที่มีประโยชน์ได้มากขึ้น
- **เสริมสร้างความมั่นคงของระบบนิเวศ DeFi:** ช่วยให้โปรโตคอล DeFi มีเสถียรภาพมากขึ้น โดยลดความผันผวนของราคาที่เกิดจากการตัดหน้าและกลยุทธ์ MEV อื่นๆ
- **สนับสนุนนวัตกรรมในแอปพลิเคชัน DeFi:** เปิดโอกาสให้นักพัฒนาสร้างแอปพลิเคชันที่ไม่ต้องกังวลเกี่ยวกับปัญหา MEV หรือการออกแบบเพื่อป้องกันการถูกเอาเปรียบ
- **สนับสนุนมาตรฐานทางจริยธรรมในบล็อกเชน:** ส่งเสริมระบบที่ยึดมั่นในหลักการกระจายอำนาจและเป็นธรรมอย่างแท้จริง สอดคล้องกับวิสัยทัศน์ดั้งเดิมของเทคโนโลยีบล็อกเชน
- **ป้องกันการผูกขาดอำนาจ:** ลดการกระจุกตัวของอำนาจที่เกิดจากการที่ผู้เล่นรายใหญ่ที่มีเทคโนโลยีขั้นสูงสามารถควบคุมตลาด MEV ได้มากกว่า
- **รองรับการทำงานข้ามเชน:** ออกแบบให้สามารถทำงานได้กับหลายบล็อกเชนและ layer-2 โซลูชัน ช่วยให้เกิดมาตรฐานการจัดลำดับธุรกรรมที่เป็นธรรมทั่วทั้งระบบนิเวศ

สรุป: ทำไม MEV ถึงสำคัญกับเรา?

MEV หรือ Miner-Extractable Value เป็นปัญหาที่ส่งผลกระทบต่อทุกคนที่ใช้บล็อกเชนและ DeFi แม้คุณอาจไม่เคยได้ยินชื่อนี้มาก่อน แต่คุณอาจเคยเป็นผู้ได้รับผลกระทบโดยไม่รู้ตัว ลองคิดถึงสถานการณ์เหล่านี้:

MEV ส่งผลกระทบต่อทุกคนในชีวิตประจำวัน

- **เปรียบเทียบเหมือนคนแข่งคิว:** ลองนึกภาพว่าคุณกำลังยืนต่อแถวซื้อตั๋วคอนเสิร์ตที่คุณรอมานานทั้งปี แต่มีคนกลุ่มหนึ่งสามารถจ่ายเงินให้พนักงานเพื่อแซงคิวคุณได้ ทำให้คุณไม่ได้ตั๋วที่ต้องการ หรือต้องจ่ายแพงขึ้น นี่คือนั่นที่เกิดขึ้นใน DeFi ทุกวัน
- **เปรียบเทียบเหมือนคนเห็นการ์ดของคุณ:** เหมือนคุณกำลังเล่นไพ่ แต่คู่แข่งสามารถเห็นไพ่ในมือคุณได้ก่อนที่คุณจะเปิดมัน แล้วพวกเขาใช้ข้อมูลนี้เอาเปรียบคุณ ธุรกรรมใน mempool ก็เหมือนไพ่ที่ยังไม่ได้เปิด และ MEV searcher คือคนที่แอบมองไพ่ของคุณ

ผลกระทบที่เกิดขึ้นในโลกจริง

เมื่อคุณทำธุรกรรมบนบล็อกเชน คุณอาจประสบกับปัญหาเหล่านี้:

- **คุณจ่ายค่าธรรมเนียมที่สูงเกินไป:** การแข่งขันระหว่างบอท MEV ทำให้ค่าธรรมเนียมทั้งเครือข่ายสูงขึ้น ทุกคนต้องจ่ายแพงขึ้นแม้ไม่ได้เกี่ยวข้องกับ MEV โดยตรง เหมือนเวลาที่ราคาอาหารในร้านสูงขึ้นเพราะต้องจ่ายค่าเช่าที่แพงขึ้น
- **คุณได้รับราคาที่แย่กว่าที่คาดหวัง:** คุณคิดว่าจะซื้อโทเคนในราคา X แต่เมื่อธุรกรรมของคุณเสร็จสิ้น คุณกลับได้โทเคนน้อยกว่าที่คาดหวัง ทำไม? เพราะมีบอท frontrunning ไปซื้อก่อนคุณและดันราคาขึ้น
- **คุณสูญเสียโอกาสในการทำกำไร:** ถ้าคุณเห็นโอกาสในการทำ arbitrage หรือโอกาสดีๆ ในตลาด แต่คุณไม่มีบอทหรือเทคโนโลยีขั้นสูง คุณแทบไม่มีโอกาสเลยที่จะฉกฉวยโอกาสนั้นก่อนคนอื่น
- **การใช้งาน DeFi ที่ไม่แน่นอน:** คุณไม่สามารถคาดการณ์ผลลัพธ์ของธุรกรรมได้อย่างแม่นยำ ทำให้การวางแผนและการลงทุนยากขึ้น ราวกับคุณพยายามเล่นเกมที่กฎเปลี่ยนไปเรื่อยๆ