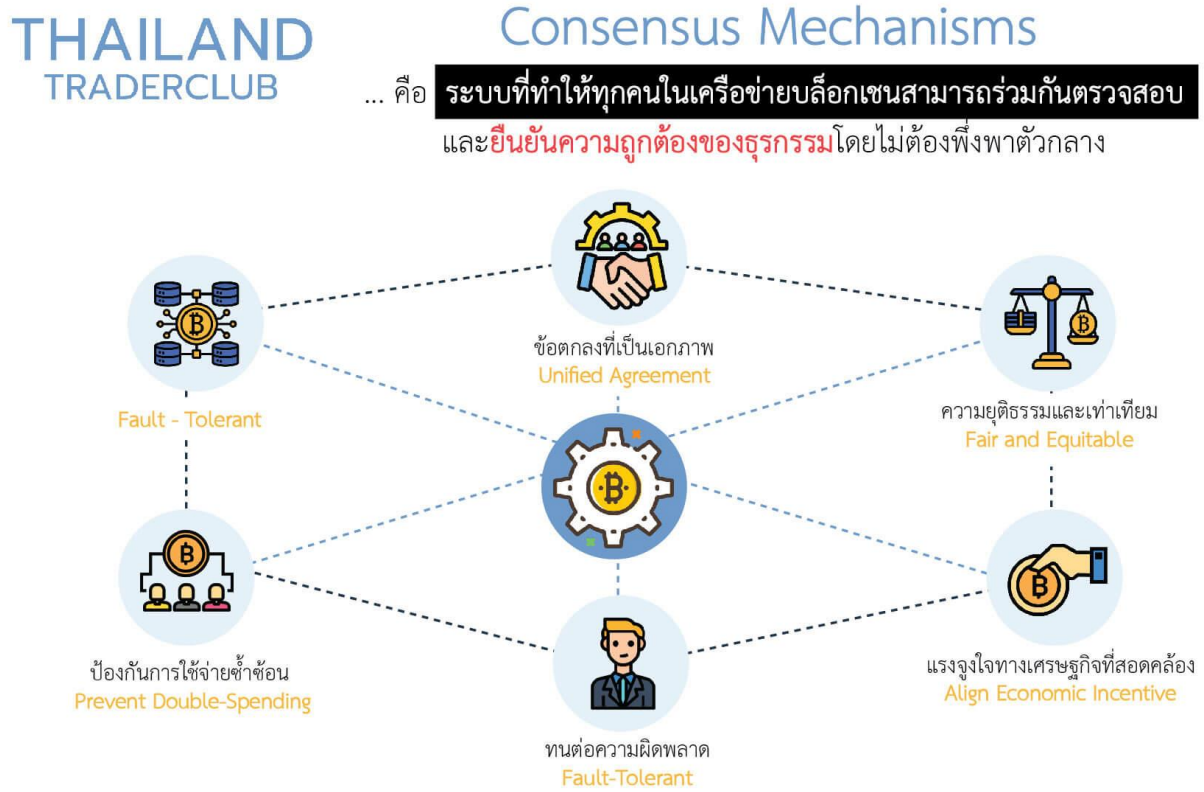
Consensus Mechanism: กลไกการตกลงในเครือข่าย

เทคโนโลยีบล็อกเชนได้เปลี่ยนแปลงวิธีที่เราจัดการและบันทึกข้อมูลในโลกดิจิทัล โดยเฉพาะอย่างยิ่งผ่านระบบการกระจายอำนาจที่ไม่ต้องพึ่งพาตัวกลาง แต่การที่จะทำให้ระบบแบบกระจายศูนย์นี้ทำงานได้อย่างมีประสิทธิภาพ จำเป็นต้องมีกลไกพิเศษที่เรียกว่า **"Consensus Mechanism"** หรือ **"ระบบฉันทามติ"**



ทำความเข้าใจ Consensus Mechanism

Consensus Mechanism เปรียบเสมือนกฎเกณฑ์ที่ทุกคนในเครือข่ายต้องปฏิบัติตาม เพื่อให้การบันทึกข้อมูลในบล็อกเชนเป็นไปอย่างถูกต้องและน่าเชื่อถือ ในระบบดั้งเดิมเช่นธนาคาร เรามีหน่วยงานกลางที่ทำหน้าที่ตรวจสอบและยืนยันความถูกต้องของธุรกรรม แต่ในโลกของบล็อกเชน ที่ไม่มีตัวกลาง ระบบฉันทามติจะเข้ามาทำหน้าที่นี้แทน

ระบบฉันทามติทำงานผ่านเครือข่ายคอมพิวเตอร์แบบ Peer-to-Peer ที่กระจายตัวอยู่ทั่วโลก เมื่อมีการทำธุรกรรมใดๆ ข้อมูลจะถูกรวบรวมเป็น 'บล็อก' จากนั้นคอมพิวเตอร์ในเครือข่ายจะร่วมกันตรวจสอบความถูกต้องตามกฎที่กำหนด เมื่อทุกฝ่ายยืนยันว่าข้อมูลถูกต้อง บล็อกนั้นจึงจะถูกเพิ่มเข้าไปในเชน

Consensus Mechanism คืออะไร

- **Consensus Mechanism คือ ระบบที่ใช้ในการตรวจสอบและยืนยันธุรกรรมในเครือข่ายบล็อกเชน โดยทุกโหนดในเครือข่ายจะต้องเห็นพ้องต้องกัน**
- เป็นกลไกสำคัญที่ทำให้เครือข่ายบล็อกเชนสามารถดำเนินงานได้โดยไม่ต้องมีตัวกลาง
- ช่วยป้องกันการโกงและสร้างความน่าเชื่อถือให้กับระบบ
- ระบบนี้ทำให้เรา***ไม่จำเป็นต้องมีตัวกลาง*** เช่น ธนาคาร มาคอยตรวจสอบธุรกรรม เพราะทุกคนในเครือข่ายช่วยกันทำหน้าที่นี้ และการที่ต้องได้รับการยืนยันจากหลายๆ โหนดก็ทำให้ยากที่จะโกงระบบ เพราะต้องควบคุมโหนดส่วนใหญ่ในเครือข่ายให้ได้ก่อน

เราจะรู้ได้อย่างไรว่า ข้อมูลที่จะบันทึกลงไปนั้นถูกต้อง?

เราสามารถรู้ได้ว่าข้อมูลที่จะบันทึกลงในบล็อกเชนนั้นถูกต้องผ่านกระบวนการตรวจสอบแบบกระจายศูนย์ของ Consensus Mechanism โดยทำงานดังนี้:

- **เมื่อมีการทำธุรกรรมเกิดขึ้น** ข้อมูลจะถูกส่งไปยังคอมพิวเตอร์หรือโหนดทุกเครื่องในเครือข่าย แต่ละโหนดจะทำการตรวจสอบความถูกต้องโดยใช้กฎเกณฑ์เดียวกัน
- เช่น **ในกรณีการโอนเงินคริปโต** โหนดจะตรวจสอบว่าผู้ส่งมีเงินเพียงพอหรือไม่ ลายเซ็นดิจิทัลถูกต้องหรือไม่ และธุรกรรมนี้ไม่ได้ถูกใช้ไปแล้วหรือไม่ (ป้องกันการใช้เงินซ้ำ)
- เมื่อโหนดส่วนใหญ่ในเครือข่าย (มากกว่า 51%) ยืนยันว่าธุรกรรมถูกต้องตามกฎเกณฑ์ ข้อมูลนั้นจึงจะถูกบันทึกลงในบล็อกเชน
- วิธีนี้ทำให้เราไม่ต้องเชื่อใจตัวกลางใดๆ เพราะความถูกต้องของข้อมูลถูกรับรองโดยเครือข่ายทั้งหมด และการจะโกงระบบนั้นแทบเป็นไปไม่ได้ เพราะต้องควบคุมโหนดส่วนใหญ่ในเครือข่ายพร้อมกัน
- กล่าวง่ายๆ คือ **แทนที่จะให้ธนาคารเพียงแห่งเดียวเป็นผู้ตรวจสอบ เรามีคอมพิวเตอร์นับพันนับหมื่นเครื่องที่ช่วยกันตรวจสอบและยืนยันความถูกต้องของข้อมูล** ทำให้ระบบมีความน่าเชื่อถือและปลอดภัยมากกว่าการพึ่งพาตัวกลางเพียงรายเดียว

ความสำคัญของระบบฉันทามติในบล็อกเชน

ระบบฉันทามติมีความสำคัญต่อการทำงานของบล็อกเชนใน 2 ด้านหลัก ได้แก่ การรักษาความปลอดภัยของข้อมูล และการสร้างระบบที่ไม่ต้องพึ่งพาตัวกลาง

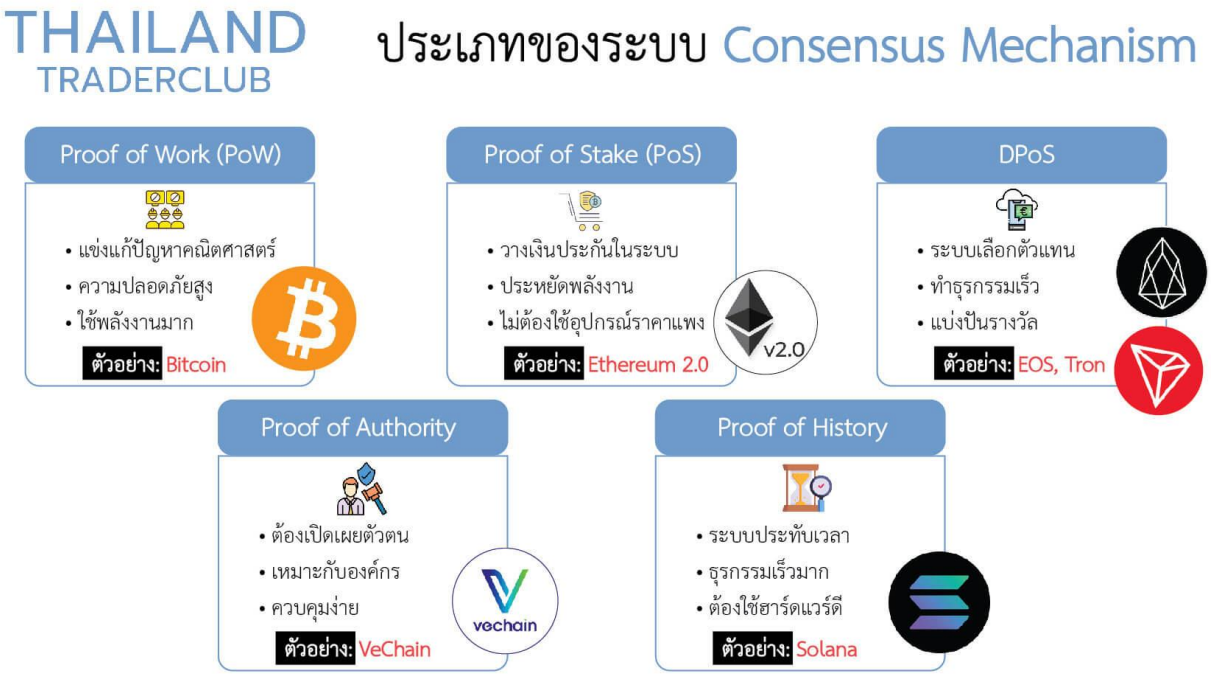
1.การป้องกันข้อผิดพลาดและธุรกรรมที่เป็นอันตราย

- ในการจัดการกับข้อมูลสำคัญอย่างยอดเงินคงเหลือของผู้ใช้ ความถูกต้องแม่นยำเป็นสิ่งที่ขาดไม่ได้
- ระบบฉันทามติช่วยให้มั่นใจได้ว่าข้อมูลที่ถูกบันทึกลงในบล็อกเชนนั้นถูกต้องและปลอดภัย
- เปรียบเสมือนการมีผู้ตรวจสอบหลายคนที่ต้องเห็นพ้องต้องกันว่าข้อมูลนั้นถูกต้องก่อนที่จะอนุญาตให้บันทึก
- หากมีใครพยายามบันทึกข้อมูลที่ผิดพลาดหรือเป็นอันตราย โหนดส่วนใหญ่ในเครือข่ายจะตรวจจับและปฏิเสธข้อมูลนั้น ทำให้การโจมตีหรือปลอมแปลงข้อมูลเป็นไปได้ยากมาก

2.การสร้างระบบที่กระจายอำนาจและปลอดภัย

- ระบบฉันทามติทำให้เครือข่ายบล็อกเชนสามารถทำงานได้โดยไม่ต้องพึ่งพาองค์กรกลางใดๆ เพราะทุกโหนดในเครือข่ายสามารถร่วมกันตรวจสอบและยืนยันความถูกต้องของข้อมูลได้
- ยิ่งมีผู้เข้าร่วมเครือข่ายมากเท่าไร การจะควบคุมหรือปลอมแปลงข้อมูลก็ยิ่งทำได้ยากขึ้นเท่านั้น เพราะต้องได้รับการยอมรับจากโหนดส่วนใหญ่ในเครือข่าย
- ระบบนี้จึงทำให้บล็อกเชนมีความปลอดภัยสูง และสามารถรับประกันได้ว่าข้อมูลที่ถูกบันทึกนั้นผ่านการตรวจสอบอย่างรอบคอบแล้ว

5 รูปแบบหลักของ Consensus Mechanism ที่ควรรู้จัก



Proof of Work (PoW)

- ระบบฉันทามติแบบดั้งเดิมที่ใช้ในบิทคอยน์
- นักขุด (Miners) แข่งกันแก้ปัญหาทางคณิตศาสตร์ที่ซับซ้อน
- ผู้ชนะจะได้สิทธิ์ตรวจสอบธุรกรรมและรับรางวัลเป็นเหรียญคริปโต
- ข้อดี: มีความปลอดภัยสูง
- ข้อเสีย: ใช้พลังงานมาก

Proof of Stake (PoS)

- ผู้ตรวจสอบต้องวางเงินประกัน (Stake) ในระบบ
- โอกาสได้เป็นผู้ตรวจสอบขึ้นอยู่กับจำนวนเงินที่วาง
- ใช้ในเครือข่าย Ethereum, Cardano, Tezos
- ข้อดี: ประหยัดพลังงาน ไม่ต้องใช้อุปกรณ์ราคาแพง
- ข้อเสีย: อาจกระจุกตัวในกลุ่มผู้ถือเหรียญรายใหญ่

Delegated Proof of Stake (DPoS)

- ผู้ถือเหรียญเลือกตัวแทน (Delegate) ให้ทำหน้าที่ตรวจสอบ
- ตัวแทนจะแบ่งรางวัลให้ผู้ที่เลือกตน
- ใช้ในเครือข่าย EOS, Tron, Ark
- ข้อดี: ทำธุรกรรมได้เร็ว ประหยัดพลังงาน
- ข้อเสีย: อาจมีการรวมกลุ่มของตัวแทน

Proof of Authority (PoA)

- ผู้ตรวจสอบต้องเปิดเผยตัวตนและมีชื่อเสียงที่ดี
- เหมาะกับเครือข่ายส่วนตัวหรือองค์กร
- ใช้ใน VeChain, JP Morgan
- ข้อดี: ธุรกรรมเร็ว ควบคุมง่าย
- ข้อเสีย: มีการรวมศูนย์สูง

Proof of History (PoH)

- ใช้ระบบประทับเวลาในการตรวจสอบธุรกรรม
- ไม่ต้องรอการยืนยันจากโหนดจำนวนมาก
- ใช้ในเครือข่าย Solana
- ข้อดี: ทำธุรกรรมได้เร็วมาก
- ข้อเสีย: ต้องพึ่งพาฮาร์ดแวร์ที่มีประสิทธิภาพสูง

แต่ละระบบมีจุดเด่นและข้อจำกัดที่แตกต่างกัน การเลือกใช้ขึ้นอยู่กับวัตถุประสงค์ของแต่ละโครงการ เช่น ต้องการความปลอดภัยสูง ความเร็วในการทำธุรกรรม หรือการประหยัดพลังงาน

กลไกการทำงานของ Consensus Mechanism

ระบบฉันทามติในบล็อกเชนทำงานผ่านองค์ประกอบสำคัญ 3 ส่วนที่ทำงานประสานกัน เปรียบเสมือนระบบประชาธิปไตยในโลกดิจิทัล ที่ทุกฝ่ายต้องเห็นพ้องต้องกันก่อนจะตัดสินใจใดๆ มาดูแต่ละส่วนอย่างละเอียด

ประกอบด้วย 3 ส่วนหลัก คือ

- **โหนดในเครือข่าย (Nodes)**
- **กฎการตกลง (Rules)**
- **การตรวจสอบและยืนยัน (Verification)**

1. โหนดในเครือข่าย (Nodes)

โหนด คือ คอมพิวเตอร์แต่ละเครื่องที่เชื่อมต่อกันในเครือข่ายบล็อกเชน เปรียบเสมือนสมาชิกสภาที่มีสิทธิ์ออกเสียงในการตัดสินใจ *โดยโหนดแต่ละตัวจะมีหน้าที่*

- เก็บสำเนาของบล็อกเชนทั้งหมด
- รับและส่งต่อข้อมูลธุรกรรมใหม่ๆ
- ตรวจสอบความถูกต้องของธุรกรรมตามกฎที่กำหนด
- มีส่วนร่วมในการยืนยันและบันทึกข้อมูลลงในบล็อกเชน

2. กฎการตกลง (Rules)

กฎคือมาตรฐานที่ทุกโหนดต้องใช้ในการตรวจสอบธุรกรรม เปรียบเสมือนรัฐธรรมนูญที่ทุกคนต้องยึดถือ *ตัวอย่างของกฎที่สำคัญ*

- การตรวจสอบความถูกต้องของลายเซ็นดิจิทัล
- การยืนยันว่าผู้ส่งมีเงินเพียงพอสำหรับการทำธุรกรรม
- การป้องกันการใช้เงินซ้ำ (double-spending)
- การกำหนดรูปแบบและขนาดของบล็อกข้อมูล

3. การตรวจสอบและยืนยัน (Verification)

เป็นขั้นตอนที่โหนดทั้งหมดร่วมกันตรวจสอบและยืนยันความถูกต้องของธุรกรรม *โดยมีกระบวนการดังนี้*

- เมื่อมีธุรกรรมใหม่เกิดขึ้น จะถูกส่งไปยังโหนดทั้งหมดในเครือข่าย

- แต่ละโหนดจะตรวจสอบธุรกรรมตามกฎที่กำหนด
- หากโหนดส่วนใหญ่ (มากกว่า 51%) ยืนยันว่าธุรกรรมถูกต้อง
- ธุรกรรมจะถูกรวมเข้าเป็นบล็อกและเชื่อมต่อกับบล็อกเชน

ทั้งสามส่วนนี้ทำงานร่วมกันเพื่อสร้างระบบที่โปร่งใส ปลอดภัย และไม่ต้องพึ่งพาตัวกลาง ทำให้ทุกคนสามารถเชื่อมั่นได้ว่าข้อมูลที่ถูกบันทึกในบล็อกเชนนั้นผ่านการตรวจสอบอย่างรอบคอบและเชื่อถือได้