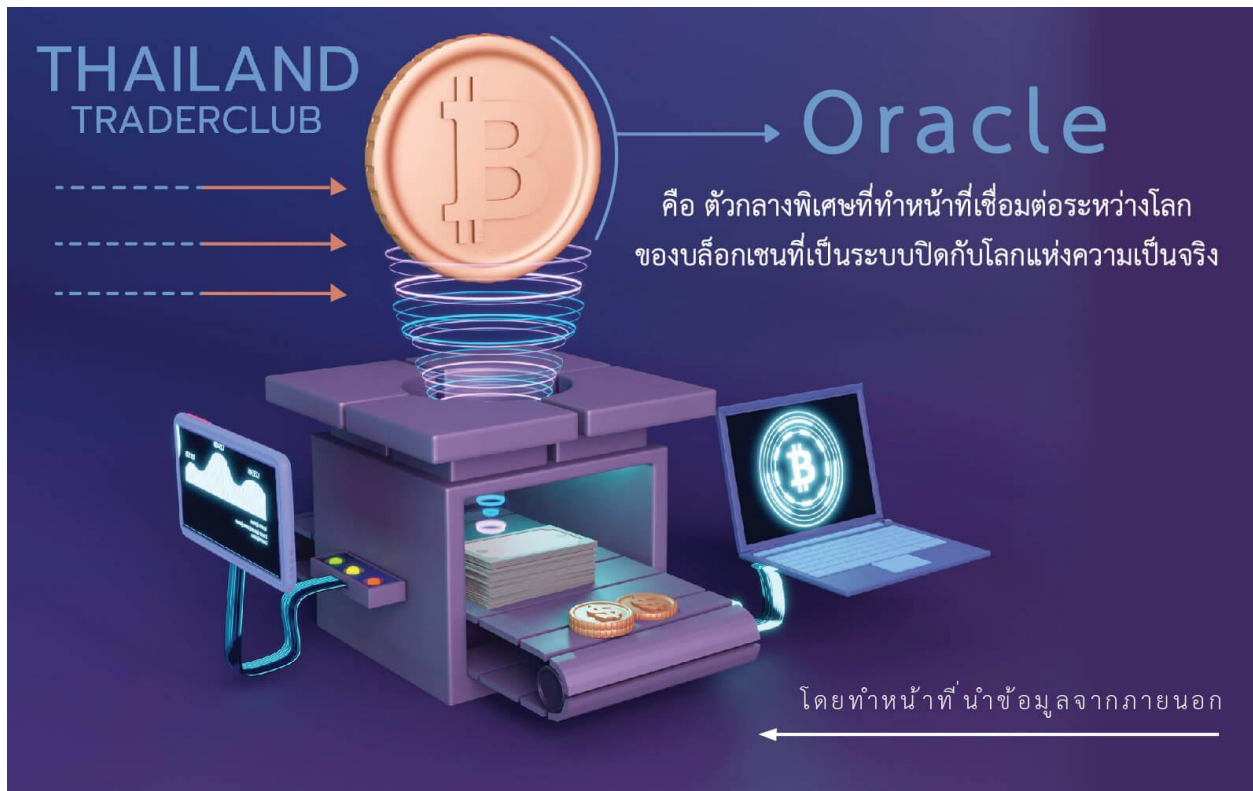


Oracle: ตัวเชื่อมโลกจริงกับบล็อกเชน

ในยุคที่เทคโนโลยีบล็อกเชนกำลังเติบโตอย่างรวดเร็ว การเชื่อมต่อระหว่างโลกดิจิทัลและโลกแห่งความเป็นจริงกลายเป็นความท้าทายสำคัญ เพราะโดยธรรมชาติแล้ว บล็อกเชนถูกออกแบบให้เป็นระบบปิดที่ไม่สามารถรับข้อมูลจากภายนอกได้โดยตรง Oracle จึงถูกพัฒนาขึ้นมาเพื่อทำหน้าที่เป็นสะพานเชื่อมระหว่างสองโลกนี้

โดยทำหน้าที่นำข้อมูลจากโลกภายนอก เช่น ราคาสินทรัพย์ ผลการแข่งขันกีฬา หรือข้อมูลสภาพอากาศ เข้าสู่ Smart Contract บนบล็อกเชนได้อย่างปลอดภัยและน่าเชื่อถือ การมีอยู่ของ Oracle จึงเป็นปัจจัยสำคัญที่ทำให้เทคโนโลยีบล็อกเชนสามารถนำไปประยุกต์ใช้ในชีวิตจริงได้อย่างกว้างขวางมากขึ้น โดยเฉพาะในยุคที่ DeFi และ Web3 กำลังเฟื่องฟู ทำให้การใช้งานบล็อกเชนไม่ได้จำกัดอยู่แค่ในโลกดิจิทัลอีกต่อไป



Oracle คืออะไร?

Oracle คือ ตัวกลางพิเศษที่ทำหน้าที่เชื่อมต่อระหว่างสองโลก - โลกของ Blockchain กับโลกแห่งความเป็นจริงของเรา เราลองนึกภาพว่า Blockchain เป็นเหมือนห้องที่ปิดสนิท ไม่สามารถรับรู้ข้อมูลจากภายนอกได้โดยตรง Oracle จึงเปรียบเสมือน "ตัวแทนพิเศษ" ที่สามารถนำข้อมูลจากภายนอกเข้ามาในห้องนี้ได้ อย่างปลอดภัยและน่าเชื่อถือ

ทำไมเราถึงต้องมี Oracle? เพราะ Smart Contract ที่ทำงานบน Blockchain ไม่สามารถเข้าถึงข้อมูลภายนอกได้โดยตรง แต่ในความเป็นจริง Smart Contract จำเป็นต้องใช้ข้อมูลจากโลกภายนอกในการทำงานและตัดสินใจ เช่น

- ถ้าเรามี Smart Contract ที่จ่ายเงินประกันเมื่อฝนตก มันจำเป็นต้องรู้ว่าวันนี้ฝนตกจริงหรือไม่
- ถ้าเรามีการเดิมพันผลฟุตบอล Smart Contract ต้องรู้ผลการแข่งขันที่เกิดขึ้นจริง
- ถ้าเราต้องการแลกเปลี่ยนเงินดิจิทัลเป็นเงินดอลลาร์ Smart Contract ต้องรู้อัตราแลกเปลี่ยนปัจจุบัน

Oracle ทำงานอย่างไร?

1. **รวบรวมข้อมูล:** Oracle จะรวบรวมข้อมูลจากแหล่งที่เชื่อถือได้ในโลกจริง เช่น เว็บไซต์ทางการ เซนเซอร์ วัตถุประสงค์ หรือฐานข้อมูลที่น่าเชื่อถือ
2. **ตรวจสอบความถูกต้อง:** ข้อมูลจะผ่านการตรวจสอบความถูกต้องและความน่าเชื่อถือ เพื่อให้แน่ใจว่าข้อมูลที่จะส่งเข้า Blockchain นั้นถูกต้องและไม่ถูกปลอมแปลง
3. **แปลงข้อมูล:** Oracle จะแปลงข้อมูลให้อยู่ในรูปแบบที่ Smart Contract สามารถเข้าใจและนำไปใช้งานได้
4. **ส่งข้อมูลเข้า Blockchain:** ข้อมูลที่ผ่านการตรวจสอบและแปลงแล้วจะถูกส่งเข้าสู่ Smart Contract บน Blockchain อย่างปลอดภัย

ยกตัวอย่างการใช้งานจริง

สมมติว่าเรามี Smart Contract ที่ทำหน้าที่จ่ายเงินประกันภัยพิบัติเมื่อเกิดภัยแล้ง Oracle จะทำงานดังนี้:

- รวบรวมข้อมูลปริมาณน้ำฝนจากสถานีตรวจอากาศในพื้นที่
- ตรวจสอบความถูกต้องของข้อมูลโดยเปรียบเทียบกับแหล่งข้อมูลหลายแหล่ง
- แปลงข้อมูลปริมาณน้ำฝนให้อยู่ในรูปแบบที่ Smart Contract เข้าใจได้
- ส่งข้อมูลเข้าสู่ Smart Contract เพื่อใช้ตัดสินใจว่าควรจ่ายเงินประกันหรือไม่

ความสำคัญของ Oracle: Oracle ทำให้ Blockchain และ Smart Contract สามารถทำงานได้อย่างมีประสิทธิภาพมากขึ้น โดยช่วยให้

- Smart Contract สามารถตัดสินใจได้โดยใช้ข้อมูลจริงจากโลกภายนอก
- เพิ่มความยืดหยุ่นในการสร้างแอปพลิเคชันบน Blockchain
- ทำให้ Blockchain สามารถตอบสนองต่อเหตุการณ์ในโลกจริงได้

Oracle จึงเป็นเหมือนสะพานเชื่อมที่สำคัญระหว่างเทคโนโลยี Blockchain กับโลกแห่งความเป็นจริง ช่วยให้ Smart Contract สามารถทำงานได้อย่างชาญฉลาดและมีประสิทธิภาพมากขึ้น โดยใช้ข้อมูลจริงในการตัดสินใจ

ความเป็นมาและความสำคัญของ Oracle ตัวเชื่อมโลกจริงกับบล็อกเชน

- เทคโนโลยีบล็อกเชนถูกออกแบบให้เป็นระบบปิดที่มีความปลอดภัยสูง แต่มีข้อจำกัดคือไม่สามารถรับข้อมูลจากโลกภายนอกได้โดยตรง ทำให้ Smart Contract ไม่สามารถทำงานได้อย่างมีประสิทธิภาพ
- Oracle จึงถูกพัฒนาขึ้นมาเพื่อทำหน้าที่เป็นสะพานเชื่อมระหว่างบล็อกเชนกับโลกแห่งความเป็นจริง ช่วยให้ Smart Contract สามารถใช้ข้อมูลจากภายนอกในการทำงานได้
- รูปแบบแรกของ Oracle เป็นแบบ Centralized ที่ใช้แหล่งข้อมูลเพียงแหล่งเดียว แต่พบว่าสร้างความเสี่ยงและขาดความน่าเชื่อถือ เพราะขัดกับหลักการของบล็อกเชนที่ต้องการหลีกเลี่ยงการพึ่งพาตัวกลาง
- จึงมีการพัฒนาต่อมาเป็น Decentralized Oracle ที่ใช้แหล่งข้อมูลหลายแหล่งและมีการตรวจสอบความถูกต้องร่วมกัน ทำให้ระบบมีความน่าเชื่อถือมากขึ้น
- ในยุคที่ DeFi กำลังเติบโต Oracle มีความสำคัญมากขึ้น เพราะการทำธุรกรรมทางการเงินต้องใช้ข้อมูลจากโลกภายนอก เช่น ราคาสินทรัพย์และอัตราแลกเปลี่ยน
- โครงการสำคัญอย่าง Chainlink, Band Protocol และ MakerDAO ได้พัฒนาระบบ Oracle ที่มีความน่าเชื่อถือสูง เพื่อรองรับการเติบโตของระบบนิเวศบล็อกเชน
- ปัจจุบัน Oracle ได้กลายเป็นโครงสร้างพื้นฐานสำคัญของระบบบล็อกเชน และยังคงพัฒนาต่อไปเพื่อเพิ่มความปลอดภัย ความน่าเชื่อถือ และประสิทธิภาพในการทำงาน
- เป้าหมายสำคัญของการพัฒนา Oracle คือการรองรับการใช้งานที่หลากหลายและซับซ้อนมากขึ้นในอนาคต เพื่อให้เทคโนโลยีบล็อกเชนสามารถทำงานร่วมกับระบบต่างๆ ในโลกจริงได้อย่างมีประสิทธิภาพ



ประเภทของ Oracle

การเลือกใช้ Oracle แต่ละประเภทขึ้นอยู่กับความต้องการของแต่ละ Smart Contract เช่น ถ้าต้องการข้อมูลที่รวดเร็วและไม่ซับซ้อนอาจเลือกใช้ Centralized Oracle แต่ถ้าเป็นธุรกรรมที่มีมูลค่าสูงควรใช้ Decentralized Oracle เพื่อความปลอดภัยและความน่าเชื่อถือที่มากขึ้น

Oracle แบ่งออกเป็น 3 กลุ่มหลักตามลักษณะการทำงาน ได้แก่:

กลุ่มที่ 1: แบ่งตามแหล่งที่มาของข้อมูล - Software และ Hardware Oracle

- **Software Oracle** คือ ตัวกลางที่ดึงข้อมูลจากแหล่งข้อมูลดิจิทัลบนอินเทอร์เน็ต เปรียบเสมือนเจ้าหน้าที่ที่คอยติดตามและรวบรวมข้อมูลจากโลกออนไลน์ เช่น เมื่อเราต้องการทราบราคา Bitcoin ปัจจุบัน Software Oracle จะทำหน้าที่ดึงข้อมูลราคาจากแหล่งที่น่าเชื่อถือต่างๆ เช่น Binance หรือ Coinbase แล้วส่งเข้าสู่ Smart Contract
- **Hardware Oracle** ทำงานคล้ายกับนักวิทยาศาสตร์ที่ใช้เครื่องมือวัดค่าต่างๆ ในโลกจริง โดยจะรับข้อมูลจากอุปกรณ์ตรวจวัดทางกายภาพ เช่น ถ้าเรามี Smart Contract ที่จ่ายเงินประกันเมื่ออุณหภูมิสูงเกิน 35 องศา Hardware Oracle จะอ่านค่าจากเครื่องวัดอุณหภูมิจริงแล้วส่งข้อมูลเข้าสู่ Smart Contract

กลุ่มที่ 2: แบ่งตามทิศทางการไหลของข้อมูล - Inbound และ Outbound Oracle

- Inbound Oracle ทำหน้าที่เหมือนพนักงานรับเอกสาร ที่นำข้อมูลจากโลกภายนอก (Off-chain) เข้าสู่ Smart Contract บน Blockchain เช่น การนำข้อมูลผลการแข่งขันฟุตบอลเข้าสู่ Smart Contract เพื่อจ่ายเงินรางวัลการเดิมพัน
- Outbound Oracle ทำงานในทิศทางตรงข้าม คือ ส่งข้อมูลจาก Smart Contract ออกสู่โลกภายนอก เปรียบเสมือนพนักงานส่งจดหมาย เช่น เมื่อมีการชำระเงินค่าเช่าบ้านผ่าน Smart Contract เรียบร้อยแล้ว Outbound Oracle จะส่งสัญญาณไปปลดล็อคประตูบ้านโดยอัตโนมัติ

กลุ่มที่ 3: แบ่งตามรูปแบบการจัดการข้อมูล - Centralized และ Decentralized Oracle

- Centralized Oracle มีศูนย์กลางในการจัดการข้อมูลเพียงแห่งเดียว เหมือนกับการมีคนคนเดียวที่เป็นผู้ให้ข้อมูล ข้อดีคือการทำงานรวดเร็ว แต่มีความเสี่ยงหากแหล่งข้อมูลนั้นมีปัญหาหรือถูกโจมตี
- Decentralized Oracle ใช้แหล่งข้อมูลหลายแหล่งและมีการตรวจสอบความถูกต้องร่วมกัน เหมือนการมีคณะกรรมการหลายคนช่วยกันยืนยันข้อมูล ทำให้ข้อมูลมีความน่าเชื่อถือสูงและลดความเสี่ยงจากการพึ่งพาแหล่งข้อมูลเดียว

บทบาทสำคัญของ Oracle

บทบาทสำคัญของ Oracle คือ การเป็นตัวกลางที่เชื่อมต่อระหว่างโลกของบล็อกเชนกับโลกแห่งความเป็นจริง โดยทำหน้าที่หลายด้านที่สำคัญ

ประการที่ 1

- Oracle ทำหน้าที่เป็นผู้รวบรวมและตรวจสอบข้อมูล เปรียบเสมือนนักข่าวที่ต้องตรวจสอบความถูกต้องของข้อมูลก่อนนำเสนอ Oracle จะรวบรวมข้อมูลจากแหล่งต่างๆ
- ไม่ว่าจะเป็นเว็บไซต์ ฐานข้อมูล หรือเซนเซอร์ แล้วทำการตรวจสอบความถูกต้องก่อนส่งต่อไปยัง Smart Contract

ประการที่ 2

- Oracle ทำหน้าที่แปลงข้อมูลให้อยู่ในรูปแบบที่ Smart Contract เข้าใจได้
- เสมือนล่ามที่แปลภาษาระหว่างสองฝ่าย เพราะข้อมูลจากโลกภายนอกอาจอยู่ในรูปแบบที่แตกต่างกัน
- Oracle จะทำการแปลงข้อมูลเหล่านี้ให้อยู่ในรูปแบบที่เหมาะสมสำหรับการใช้งานบนบล็อกเชน

ประการที่ 3

- Oracle ทำหน้าที่รับประกันความน่าเชื่อถือของข้อมูล

- เหมือนผู้ตรวจสอบบัญชีที่ต้องรับรองความถูกต้องของงบการเงิน
- โดยเฉพาะในกรณีของ Decentralized Oracle ที่ใช้แหล่งข้อมูลหลายแหล่งและมีการตรวจสอบร่วมกัน ทำให้ข้อมูลที่ได้มีความน่าเชื่อถือสูง

ประการที่ 4

- Oracle ช่วยให้ Smart Contract สามารถทำงานได้อย่างชาญฉลาด เพราะสามารถตัดสินใจบนพื้นฐานของข้อมูลจริงจากโลกภายนอก
- เช่น การจ่ายเงินประกันเมื่อเกิดภัยพิบัติ หรือการชำระเงินตามอัตราแลกเปลี่ยนปัจจุบัน

ประการที่ 5

- Oracle มีบทบาทสำคัญในการขยายขอบเขตการใช้งานของบล็อกเชน ทำให้เทคโนโลยีนี้สามารถนำไปประยุกต์ใช้ได้กว้างขวางขึ้น ไม่ว่าจะเป็นในด้านการเงิน การประกันภัย หรือการซื้อขายสินทรัพย์ต่างๆ

การทำงานของ Oracle จึงเปรียบเสมือนสะพานที่ทำให้เทคโนโลยีบล็อกเชนสามารถก้าวข้ามข้อจำกัดของระบบปิด และเชื่อมต่อกับโลกแห่งความเป็นจริงได้อย่างมีประสิทธิภาพ ทำให้การใช้งานบล็อกเชนมีความหมายและตอบโจทย์การใช้งานจริงมากขึ้น

ความเสี่ยงของการใช้งาน Oracle

ความเสี่ยงของการใช้งาน Oracle สามารถเปรียบเทียบได้กับการสร้างบ้านบนฐานรากที่ไม่มั่นคง แม้ตัวบ้านจะแข็งแรงเพียงใด แต่หากฐานรากมีปัญหา ทั้งหลังก็อาจพังทลายได้ ในทำนองเดียวกัน Oracle ก็เปรียบเสมือนฐานรากของข้อมูลที่ Smart Contract ใช้ในการตัดสินใจ

ความเสี่ยงด้านความถูกต้องของข้อมูล

- Oracle เป็นแหล่งข้อมูลสำคัญที่ Smart Contract ใช้ในการตัดสินใจ
- การตัดสินใจในแต่ละครั้งอาจเกี่ยวข้องกับมูลค่ามหาศาลหลายล้านดอลลาร์
- หากข้อมูลที่ได้รับไม่ถูกต้อง จะส่งผลให้การตัดสินใจผิดพลาดทั้งหมด (garbage in, garbage out)

ความเสี่ยงจากการเป็นจุดล้มเหลวเดียว (Single Point of Failure)

- การพึ่งพา Oracle ที่ขาดความน่าเชื่อถือเป็นความเสี่ยงร้ายแรง
- ข้อมูลอาจไม่ถูกต้องตั้งแต่ต้นทาง หรือถูกแก้ไขโดยเจ้าของ Oracle
- เมื่อ Oracle ล้มเหลว ระบบทั้งหมดที่พึ่งพาข้อมูลนั้นก็ล้มเหลวตามไปด้วย

ความเสี่ยงที่ไม่สามารถย้อนกลับได้

- ธรรมชาติของ Blockchain คือการไม่สามารถแก้ไขหรือย้อนกลับรายการได้

- ความผิดพลาดเพียงครั้งเดียวอาจนำไปสู่ความเสียหายถาวร
- อาจส่งผลให้ Protocol ทั้งระบบล้มเหลวโดยไม่สามารถกู้คืนได้

ด้วยเหตุนี้ การเลือกใช้ Oracle ที่มีความน่าเชื่อถือและมีระบบการตรวจสอบที่รัดกุมจึงเป็นสิ่งสำคัญอย่างยิ่ง เพื่อป้องกันความเสียหายที่อาจเกิดขึ้นและไม่สามารถแก้ไขได้ในภายหลัง

สรุปเรื่อง Oracle ในมุมมองที่เข้าใจง่าย

ลองนึกภาพว่าบล็อกเชนเป็นเหมือนห้องประชุมที่ปิดสนิท มีระบบรักษาความปลอดภัยแน่นหนา แต่ไม่มีหน้าต่างหรือประตูที่จะรับข้อมูลจากโลกภายนอก ซึ่งทำให้การประชุมหรือตัดสินใจเรื่องสำคัญๆ เป็นไปได้ยาก เพราะขาดข้อมูลจากภายนอก Oracle จึงเปรียบเสมือนเจ้าหน้าที่พิเศษที่ได้รับความไว้วางใจให้เป็นผู้นำข้อมูลจากภายนอกเข้ามาในห้องประชุมนี้

ในชีวิตจริง เราต้องการข้อมูลมากมายในการตัดสินใจ เช่น ถ้าเราจะซื้อบ้าน เราต้องรู้ราคาตลาด ถ้าจะเดินทาง เราต้องรู้สภาพอากาศ หรือถ้าจะลงทุน เราต้องรู้ราคาหุ้น Smart Contract บนบล็อกเชนก็เช่นกัน - มันต้องการข้อมูลจากโลกภายนอกเพื่อทำงานได้อย่างมีประสิทธิภาพ Oracle จึงทำหน้าที่เป็นผู้ช่วยที่คอยนำข้อมูลเหล่านี้เข้ามาให้

แต่เหมือนกับการเลือกผู้ช่วยในชีวิตจริง เราต้องเลือกคนที่ไว้วางใจได้ เพราะข้อมูลผิดๆ เพียงครั้งเดียวอาจนำไปสู่การตัดสินใจที่ผิดพลาดร้ายแรง โดยเฉพาะในโลกของบล็อกเชนที่เมื่อตัดสินใจไปแล้ว ไม่สามารถย้อนกลับมาแก้ไขได้ เหมือนกับการเซ็นสัญญาด้วยหมึกถาวรที่ลบไม่ได้

ปัจจุบัน Oracle ได้พัฒนาจากการพึ่งพาแหล่งข้อมูลเดียว มาเป็นการใช้หลายแหล่งข้อมูลที่คอยตรวจสอบซึ่งกันและกัน เหมือนการมีคณะกรรมการหลายคนที่จะช่วยกันตรวจสอบความถูกต้อง แทนที่จะเชื่อคนเพียงคนเดียว ทำให้ระบบมีความน่าเชื่อถือมากขึ้น

Oracle จึงเป็นเหมือนสะพานสำคัญที่ทำให้เทคโนโลยีบล็อกเชนสามารถนำมาใช้ในชีวิตจริงได้อย่างมีความหมาย ไม่ใช่แค่เป็นระบบปิดที่แยกตัวออกจากโลกภายนอก แต่เป็นเทคโนโลยีที่สามารถตอบสนองและปรับตัวตามสถานการณ์จริงได้ ทำให้การใช้งานบล็อกเชนมีประโยชน์และใกล้ตัวเรามากขึ้นในชีวิตประจำวัน