

Hydro Raindrop
การรับรองความถูกต้องสาธารณะใน Blockchain

มกราคม 2018

สารบัญ

[นามธรรม](#)

[อาคาร Blockchain &
Ethereum บน Ethereum](#)

[Merkle Trees](#)

[สัญญาสมาร์ท](#)

[Ethereum เครื่องเสมือน](#)

[บัญชีแยกประเภททั่วไป](#)

[บัญชีแยกประเภททั่วไปสำหรับการวางแผนระบบภาคเอกชน
เพื่อการยอมรับ](#)

[Raindrop](#)

[รู้ความมั่นคงทางการเงิน](#)

[Equifax ช่องโหว่](#)

[การเพิ่มเลเยอร์ Blockchain](#)

[Hydro Raindrop](#)

[การดูโดยละเอียด](#)

[เปิดตัว Raindrop ต่อสาธารณชน](#)

[กรณีศึกษา - Raindrop กับ OAuth 2.0](#)

[ความเสี่ยง](#)

ข้อสรุป

นามธรรม

HYDRO: นิรุกติศาสตร์ - จากสมัยโบราณ Greek ὑδρο- (*hudro-*), จาก ὑδωρ (*húdōr*, “น้ำ”)

ไฮโดรช่วยให้ระบบภาคเอกชนใหม่ๆและระบบที่มีอยู่สามารถรวมและใช้ประโยชน์จากพลวัตที่เปลี่ยนแปลงไปอย่างไม่เปลี่ยนแปลงและต่อเนื่องของสาธารณชนblockchainเพื่อเพิ่มแอปพลิเคชันและความปลอดภัยของเอกสารการจัดการข้อมูลประจำตัวการทำธุรกรรมและปัญญาประดิษฐ์.

ในบทความนี้จะมีการจัดทำกรณีที่ระบบภาคเอกชนเช่นAPIsใช้ไฮโดรบล็อกสาธารณะเพื่อเพิ่มความปลอดภัยผ่านการตรวจสอบความถูกต้องของสาธารณะ.

เทคโนโลยีที่เรียกว่า"Raindrop"ธุรกรรมที่ดำเนินการผ่านสัญญาสมาร์ทที่ตรวจสอบสิทธิ์การเข้าถึงระบบภาครัฐแบบสาธารณะและสามารถเติมเต็มวิธีการพิสูจน์ตัวตนแบบส่วนตัวที่มีอยู่ได้เทคโนโลยีมีจุดมุ่งหมายเพื่อให้การรักษาความปลอดภัยเพิ่มเติมสำหรับข้อมูลทางการเงินที่ละเอียดอ่อนซึ่งมีความเสี่ยงมากขึ้นจากการแฮ็กและการละเมิด.

การใช้งานHydroRaindropครั้งแรกจะดำเนินการบนแพลตฟอร์มAPIไฮโดรเจนชุดAPIแบบโมดูลาร์นี้มิให้บริการแก่องค์กรและนักพัฒนาซอฟต์แวร์ทั่วโลกเพื่อสร้างต้นแบบสร้างทดสอบและปรับใช้แพลตฟอร์มเทคโนโลยีทางการเงินและผลิตภัณฑ์ที่มีความซับซ้อน.

Hydro Raindrop จะพร้อมให้ชุมชนนักพัฒนาซอฟต์แวร์ระดับโลกในฐานะซอฟต์แวร์โอเพนซอร์สเพื่อให้ นักพัฒนาสามารถรวมไฮโดรเข้ากับ REST API ได้.

BlockchainและEthereum

ไฮโดรถูกนำมาใช้งานบนเครือข่าย Ethereum ก่อนที่จะให้รายละเอียดเพิ่มเติมเกี่ยวกับโครงการคุณ ควรทำความเข้าใจกับแนวคิดพื้นฐาน เกี่ยวกับ blockchainและEthereum .

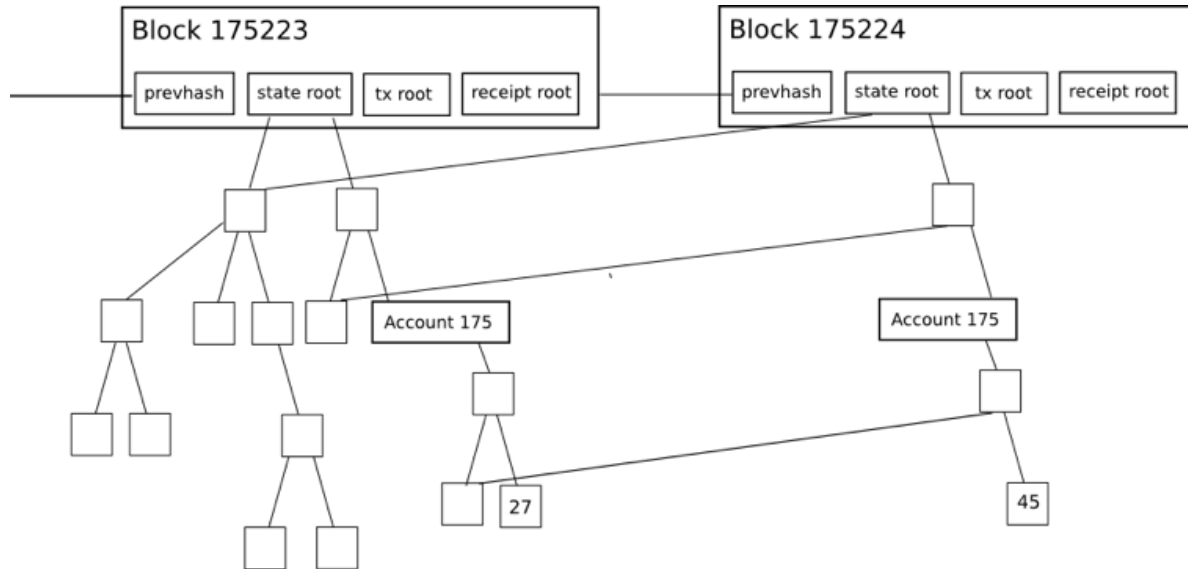
สร้างบน Ethereum

มากเป็นแพลตฟอร์มเช่น Snapchat ถูกสร้างขึ้นด้วย Swift และเครื่องมืออื่น ๆ ที่นำเสนอบนแพลตฟอร์ม Apple iOS ดังนั้นก็สามารถป้องกันการใช้งานจะสร้างขึ้นด้านบนของ Ethereum Snap Inc. ไม่จำเป็นต้องสร้าง iOS จึงใช้เป็นโครงสร้างพื้นฐานเพื่อเปิดตัวแอปพลิเคชันสื่อ สังคมออนไลน์ที่เปลี่ยนแปลง เกม

ไฮโดรโครงการคล้าย ๆ กัน มันขึ้นอยู่กับนักพัฒนานับพันทั่วโลกที่กำลังทำงานเพื่อให้เทคโนโลยี blockchainต้นแบบมีความรวดเร็วแข็งแกร่งและมีประสิทธิภาพมากขึ้นไฮโดรยกระดับโครงสร้างพื้นฐานด้านการพัฒนาอย่างต่อเนื่องโดย การพัฒนาปฏิสัมพันธ์ที่มุ่งเน้นผลิตภัณฑ์ไปสู่เทคโนโลยี blockchain ซึ่งสามารถนำเสนอผลประโยชน์ที่เป็นรูปธรรมต่อการใช้งานด้านบริการทางการเงิน .

Merkle Trees

Merkle Trees ใช้ในระบบกระจายเพื่อการตรวจสอบข้อมูลที่มีประสิทธิภาพพวกเขามีประสิทธิภาพเพราะใช้แฮชแทนไฟล์เต็มแ ฮชเป็นวิธีการเข้ารหัสไฟล์ที่มีขนาดเล็กกว่าไฟล์จริงๆส่วนหัวของบล็อกทั้งหมดใน Ethereum มีสาม Merkle Trees สำหรับธุรกรรมใบเสร็จรับเงินและรัฐ :



แหล่ง: [Merkling in Ethereum](#); Vitalik Buterin, Ethereum ผู้สร้าง

วิธีนี้ทำให้ลูกค้าที่มีน้ำหนักเบาได้รับคำตอบที่สามารถตรวจสอบได้สำหรับคำถามเช่น:

- บัญชีนี้มีอยู่หรือไม่?
- อะไรคือยอดเงินปัจจุบัน?
- มีรายการนี้ถูกรวมอยู่ในกลุ่มใดกลุ่มหนึ่งหรือไม่ • มีเหตุการณ์พิเศษเกิดขึ้นในที่อยู่นี้ในวันนี้?

สัญญาสมาร์ท

แนวคิดหลักที่เปิดใช้งานโดย Ethereum และเครือข่าย blockchain อื่น ๆ คือสัญญาที่ชาญฉลาด เหล่านี้เป็นบล็อกที่ดำเนินการด้วยตนเองของโค้ดที่หลายฝ่ายสามารถโต้ตอบกับการตัดสินใจจำเป็นในการเป็นพ่อค้าคนกลางที่เชื่อถือได้ รหัสในสัญญาแบบสมาร์ทสามารถมองเห็นได้เช่นเดียวกับข้อกำหนดตามกฎหมายในสัญญากระดาษแบบดั้งเดิม แต่ยังสามารถบรรลุการทำงานที่กว้างขวางมากขึ้น สัญญาสามารถมีเงื่อนไขการลงโทษสำหรับการไม่ปฏิบัติตามข้อกำหนดหรือสามารถเริ่มต้นกระบวนการอื่น ๆ ได้ เมื่อถูกเรียกใช้สัญญาดำเนินการตามที่ระบุไว้ในช่วงเวลาของการใช้งานในห่วงโซ่สาธารณะที่น่าเสนอองค์ประกอบในตัวของความไม่เปลี่ยนแปลงและการกระจายอำนาจ.

สัญญาสมาร์ทเป็นเครื่องมือสำคัญในการสร้างโครงสร้างพื้นฐานของ Ethereum การทำงานหลักของเลเยอร์ไฮโดรคัสเตอร์สามารถทำได้ผ่านทางสัญญาที่กำหนดเองตามที่กล่าวไว้ในบทความนี้.

Ethereum เครื่องเสมือน

Ethereum Virtual Machine (EVM) เป็นสภาพแวดล้อมรันไทม์สำหรับสัญญาสมาร์ทเมื่อ Ethereum EVM ช่วยป้องกันการโจมตีแบบ Denial of Service (DoS) ทำให้มั่นใจได้ว่าโปรแกรมยังคงไร้ข้อผิดพลาด

และช่วยให้การสื่อสารไม่สามารถขัดจังหวะได้ การดำเนินการเกี่ยวกับ EVM มีค่าใช้จ่ายที่เกี่ยวข้องกับพวกเขา ซึ่งเรียกว่าก๊าซซึ่งขึ้นอยู่กับทรัพยากรด้านการคำนวณที่จำเป็น ทุกรายการมีปริมาณก๊าซสูงสุดที่กำหนดให้เรียกว่าขีด จำกัด g ถ้าก๊าซที่บริโภคโดยการทำธุรกรรมถึงขีด จำกัด จะหยุดดำเนินการต่อไป.

ปัญหาแยกประเภททั่วไป

ปัญหาแยกประเภททั่วไปสำหรับระบบเอกชน

ระบบที่ใช้แพลตฟอร์มบริการทางการเงินเว็บไซต์และแอปพลิเคชันสามารถอธิบายได้บ่อยๆว่าเป็นสื่อในการรับส่งข้อมูลซึ่งจะส่งเรียกค้นเก็บอัปเดตและประมวลผลข้อมูลสำหรับหน่วยงานที่ตนติดต่อด้วยเนื่องจากลักษณะของข้อมูลนี้และบริการทางการเงินโดยทั่วไป ระบบเหล่านี้มักอาศัย การดำเนินงานที่ซับซ้อนในลักษณะส่วนตัว และแบบรวมศูนย์การพึ่งพาโครงสร้างของเอกชนจะช่วยเปิดประตูสู่ความหลากหลายของความปลอดภัยความโปร่งใสและประสิทธิภาพที่จะเกิดขึ้นได้โดยการนำเอาองค์การภายนอกที่เกินขอบเขตของระบบภายใน .

เป็นเช่นนั้นด้วย Hydrogen's API เวกี. Hydro มีจุดมุ่งหมายที่จะใช้ประโยชน์ดังกล่าวข้างต้นโดยการอนุญาต Hydrogen ผู้ใช้สามารถเชื่อมต่อกับ blockchain ในรูปแบบที่รวมเข้ากับความเป็นส่วนตัวได้อย่างลงตัว Hydrogen ระบบนิเวศ.

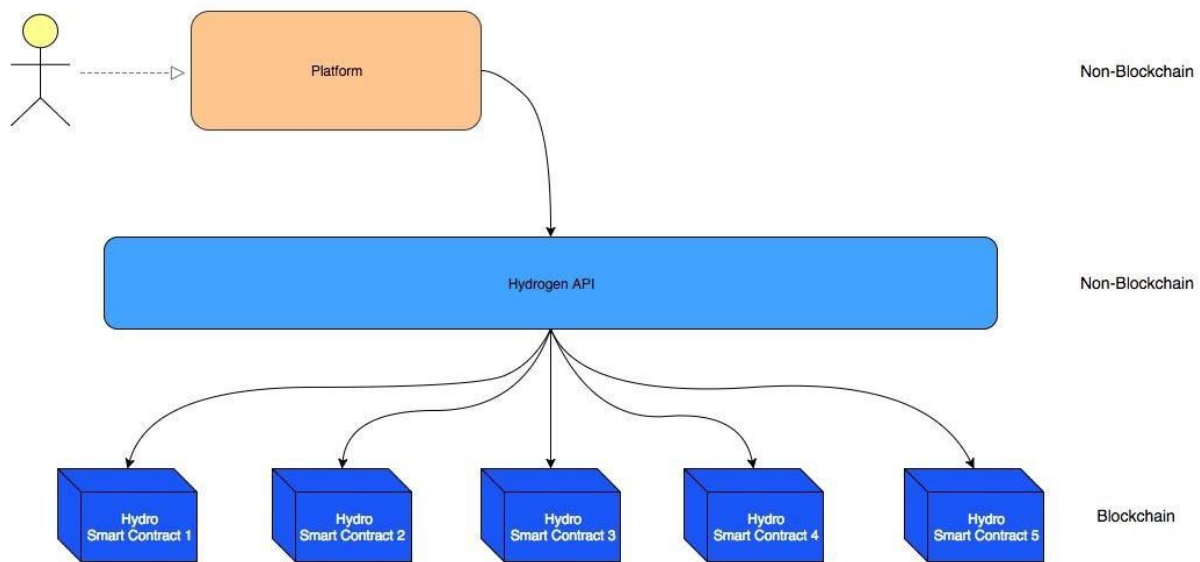


การดำเนินการที่ใช้ blockchain สาธารณะอาจเกิดขึ้นก่อนระหว่างหรือหลังการดำเนินงานส่วนตัว การมีปฏิสัมพันธ์ระหว่างองค์กรประกอบส่วนตัวและองค์กรประกอบสาธารณะสามารถช่วยในการตรวจสอบ, ประทับตราบันทึกหรือปรับปรุงกระบวนการภายในระบบนิเวศ

รื้อของโมเดลนี้ทำให้กระบวนการต่างๆมีประสิทธิภาพมากขึ้นโดยการตะประโยชน์ของเทคโนโลยี blockchain โดยเฉพาะซึ่ง จะทำให้ได้ผลดีที่สุด สุดแม้ว่ากรอบงานลูกผสมนี้อาจใช้ไม่ได้กับทุกแพลตฟอร์ม, Hydro มุ่งเน้นไปที่การให้ค่าสำหรับกรณีที่เป็น .

สถาปนิกเพื่อการยอมรับ

Hydro แตกต่างจากการริเริ่ม blockchain ที่มีอยู่มากมายเนื่องจากสามารถอยู่ได้อย่างอิสระและสร้างเลเยอร์ใหม่ ๆ หรือระบบเดิมโดยไม่ด้ ้องมีการเปลี่ยนแปลงระบบ แทนที่จะแทนที่, Hydro มีจุดมุ่งหมายเพื่อเพิ่มพูนขึ้น แพลตฟอร์มและสถาบันที่เชื่อมต่อกับ Hydrogen APIs สามารถเข้าถึงได้โดยอัตโนมัติ blockchain .



ขอบเขตของแพลตฟอร์มบริการทางการเงินที่สามารถใช้ประโยชน์ได้ Hydrogen กว้าง ๆ. แพลตฟอร์มเหล่านี้สามารถใช้พลังงานได้เกือบทุก ก่ออย่างไม่ ว่าจะเป็นที่บ้านบริกร รด้านข้อมูลที่เป็นกรรมสิทธิ์ใด ๆ ดำเนินการ ข้อมูลส่วนตัวและใช้งานได้ในทุกสภาพแวดล้อม เปิดใช้งานโดย Hydrogen'sโครงสร้างและเป็นกับไฮโดร ทำท หน้าที่เป็นโป รแกรมควบคุมเสริมของการนำไปใช้.

Raindrop

สร้างขึ้นที่ด้านบนของบัญชีแยกประเภทสาธารณะ Hydro นี้เป็นบริการตรวจสอบสิทธิ์แบบ blockchain ซึ่งเรียกว่า "Raindrop" ซึ่งมีความปลอดภัยด้านการรักษาความปลอดภัยที่สามารถมองเห็นได้ทั่วโลกซึ่งสามารถตรวจสอบค่าขอเข้าถึงได้จากแหล่งข้อมูลที่ได้รับอนุญาต

โปรโตคอลการตรวจสอบสิทธิ์ส่วนตัวเช่น OAuth 2.0 มีระดับความทนทานและประโยชน์ที่แตกต่างกันสำหรับสเปกตรัมของกรณีการใช้งานที่มีอยู่ มีความจำเป็นที่จะต้องแข่งขันกับหรือพยายามแทนที่โปรโตคอลเหล่านี้ – ไฮโดรเสนอแนวทางในการเพิ่มประสิทธิภาพโดยการรวมหลักการของบล็อกเชนเป็นส่วนประกอบของขั้นตอนการตรวจสอบสิทธิ์ นี้สามารถเพิ่มชั้นที่มีประโยชน์ของการรักษาความปลอดภัย เพื่อช่วยป้องกันการละเมิดระบบและการประนีประนอมข้อมูล.

ก่อนที่จะตรวจสอบด้านเทคนิคของ Raindrop ลองมาดูปัญหาที่กำลังพยายามแก้.

รู้ความมั่นคงทางการเงิน

การเพิ่มขึ้นของยุคข้อมูลได้เพิ่มความเสี่ยงและนี่เป็นสิ่งสำคัญอย่างยิ่งสำหรับการให้บริการทางการเงิน แพลตฟอร์มการเงินมักเป็นเกตเวย์ไปยังข้อมูลที่มีความสำคัญและเป็นส่วนตัวจำนวนมากเช่นหมายเลขประจำตัวประชาชนข้อมูลรับรองบัญชีและประวัติการทำธุรกรรม เนื่องจากข้อมูลเหล่านี้มีความสำคัญอย่างยิ่งการเข้าถึงโดยไม่ได้รับอนุญาตจึงมักเกิดผลร้ายแรง

บริษัท วิจัยอุตสาหกรรมของ บริษัท เทรนด์ไมโครเปิดเผยรายงานที่พบว่ารายการสินค้าข้อมูลที่สามารถระบุตัวตนได้ถูกขโมยได้ถูกขายบน Deep Web สำหรับราคาเพียง 1 เหรียญการสแกนเอกสารเช่นหนังสือเดินทางมีเพียง \$ 10 และเอกสารรับรองการเข้าสู่ระบบของธนาคาร สำหรับน้อย \$ 200 ทำให้การแจกจ่ายข้อมูลที่ถูกขโมยมีการแยกส่วนและไม่สามารถเข้าถึงได้มากขึ้น

น่าเสียดายที่ระบบการเงินที่มีอยู่จะไม่มียุติที่ชัดเจนในเรื่องของการป้องกันการฉ้อโกงและการสื่อสารข้อมูลกับผู้มีส่วนได้เสีย.

- จากการศึกษาเมื่อเร็ว ๆ นี้โดย Javelin Strategy & Research - การศึกษาการทุจริตในปี 2017 - 16 พันล้าน ดอลลาร์ถูกขโมยไปจาก 15,4 ล้าน ผู้บริโภคสหรัฐในปี 2016 เนื่องจากความล้มเหลวของระบบการเงินเพื่อปกป้อง Personally Identifiable Information (PII) .
- ในเดือนเมษายน 2017, ไชแมนเทคโนโลยีเผยแพร่รายงานภัยคุกคามด้านความปลอดภัยทางอินเทอร์เน็ตซึ่งมีมูลค่าประมาณ 1.1 พันล้านชิ้นของ PII ที่ถูกบุกรุกด้วยกำลังการผลิตที่หลากหลายในช่วง 2016.
- การละเมิดข้อมูลในปีงบประมาณ 2016 โดยการรักษาความปลอดภัยตามความเสี่ยงพบว่าการละเมิดข้อมูลจำนวน 4,149 รายเกิดขึ้นในธุรกิจทั่วโลกในปีพ. ศ. 2560 ซึ่งมีการเปิดเผยข้อมูลมากกว่า 4.2 พันล้านรายการ.
- รายงานการคุกคามภัยคุกคามข้อมูล Thales ฉบับปี พ.ศ. 2017 (Thales Data Threat Report - Financial Services Edition) ซึ่งเป็นการสำรวจผู้เชี่ยวชาญด้านไอทีทั่วโลกในการให้บริการ

ระดับมืออาชีพพบว่า 49% ขององค์กรที่ให้บริการทางการเงินได้รับความเดือดร้อนจากการรักษาความปลอดภัยในอดีต 78% ใช้จ่ายเงินเพื่อปกป้องตัวเองมาก ขึ้น แต่ 73% กำลังเปิดตัวโครงการใหม่เกี่ยวกับเทคโนโลยี AI, IoT และระบบคลาวด์ก่อนที่จะเตรียมโซลูชันด้านความปลอดภัยที่เหมาะสม.

Equifax ช่องโหว่

เมื่อวันที่ 29 กรกฎาคม 2017 บริษัท Equifax ซึ่งเป็นหน่วยงานรายงานเครดิตแห่งสหรัฐอเมริกาอายุ 118 ปี ถูกแฮ็ก ผู้บริโภค 143 ล้านรายได้รับข้อมูล PII รวมทั้งหมายเลขประกันสังคม ลูกค้า 209,000 รายมีข้อมูลบัตรเครดิตที่ถูกบุกรุก

อะไรคือสาเหตุของการฝ่าฝืนนี้?

เริ่มต้นด้วยเทคโนโลยีแบ็กเอนด์ที่ใช้โดย Equifax Struts เป็นเฟรมเวิร์กโอเพนซอร์สสำหรับการพัฒนาเว็บแอปพลิเคชันในภาษาการเขียนโปรแกรม Java ซึ่งสร้างขึ้นโดย Apache Software Foundation CVE-2017-9805 เป็นช่องโหว่ใน Apache Struts ที่เกี่ยวข้องกับการใช้ปลั๊กอิน Struts REST กับตัวจัดการ XStream เพื่อจัดการกับโหนด XML หากใช้ประโยชน์จะช่วยให้ผู้บุกรุกที่ไม่ได้รับการรับรองความถูกต้องจากระยะไกลสามารถเรียกใช้โค้ดที่เป็นอันตรายบนเซิร์ฟเวอร์แอปพลิเคชันเพื่อรับเครื่องหรือเริ่มโจมตีเพิ่มเติมได้ นี้ถูก patched โดย Apache สองเดือนก่อนที่จะละเมิด Equifax

Apache Struts มีข้อบกพร่องในปลั๊กอิน REST XStream ที่เรียกใช้งานเนื่องจากโปรแกรมไม่ผ่านการรับรองความถูกต้อง de-serializes ข้อมูลป้อนผู้ใช้ในคำขอ XML โดยเฉพาะอย่างยิ่งปัญหาเกิดขึ้นในวิธีการ toObject () ของ XStreamHandler ซึ่งไม่ได้กำหนดข้อ จำกัด ใด ๆ เกี่ยวกับค่าขาเข้าเมื่อใช้ deserialization XStream ลงในออบเจกต์ส่งผลให้ช่องโหว่ในการประมวลผลโค้ดโดยพลการ

แม้ว่าปลั๊กอิน REST นี้จะมีการบุกรุกควรมีความสำคัญหรือไม่? มีวิธีการใช้เทคโนโลยี blockchain เพื่อรักษาความปลอดภัยข้อมูลทางการเงินของลูกค้าจำนวน 143 ล้านคนเหล่านี้ในขณะที่ยังคงใช้ REST API และระบบ Java ที่ใช้อยู่หรือไม่?

การเพิ่มเลเยอร์ Blockchain

เป็นที่ชัดเจนว่าสามารถปรับปรุงเกตเวย์ข้อมูลทางการเงินได้อย่างสมบูรณ์ ลองมาดูกันว่าไฮโดรเจนเป็นอย่างไร

กลไกพื้นฐานที่เป็นเอกลักษณ์ของเครือข่าย Ethereum ช่วยให้มั่นใจได้ถึงการทำธุรกรรมเนื่องจากผู้เข้าร่วมทำธุรกรรมที่ได้รับการลงนามอย่างถูกต้อง ความเป็นจริงนี้นำไปสู่การกระจายอำนาจและความไม่เปลี่ยนแปลง แต่ที่สำคัญกว่านั้นก็คือเวกเตอร์สำหรับการลดการเข้าถึงเกตเวย์ที่ไม่ได้รับอนุญาตที่จัดการกับข้อมูลที่ละเอียดอ่อน

ด้วยไฮโดรการพิสูจน์ตัวตนสามารถบ่งบอกถึงการดำเนินการทำธุรกรรมบน blockchain ตัวอย่างเช่น API สามารถเลือกตรวจสอบผู้พัฒนาและแอปพลิเคชันได้โดยกำหนดให้พวกเขาเริ่มทำธุรกรรมโดยเฉพาะโดยมี payload ข้อมูลเฉพาะเจาะจงระหว่างที่อยู่เฉพาะใน blockchain เป็นเงื่อนไขเบื้องต้นที่จะเริ่มต้นโปรโตคอลการรับรองความถูกต้องมาตรฐาน.

Hydro Raindrop

ฝนตกมีแพ็คเก็ตน้ำฝนตั้งแต่ 0.0001 ถึง 0.005 เซนติเมตร ในพายุฝนฟ้าคะนองทั่วไปมีแพ็คเก็ตเหล่านี้บนพื้นดินขนาดสุมควา มเร็วและรูปร่างแต่ละแบบ ด้วยเหตุนี้คุณจึงไม่สามารถคาดเดาลักษณะที่แน่นอนของฝนได้ ในทำนองเดียวกันทุกการทำธุรกรรม การตรวจสอบความถูกต้องของไฮโดรเจนมีความเป็นเอกลักษณ์และแทบจะเป็นไปไม่ได้ที่จะเกิดขึ้นโดยบังเอิญนั่นคือเหตุผลที่เราเรียกพวกเขาว่า aindrops

แพลตฟอร์มบริการทางการเงินมักใช้การยืนยัน micro-deposit เพื่อตรวจสอบบัญชีลูกค้า แนวคิดนี้ง่ายมาก: แพลตฟอร์มทำให้มีการฝากเงินจำนวนน้อย ๆ ไว้ในบัญชีธนาคารที่ผู้ใช้อ้างสิทธิ์ เพื่อที่จะพิสูจน์ว่าผู้ใช้เป็นเจ้าของบัญชีดังกล่าวจริงๆเขาหรือเธอต้องส่งเงินมัดจำกลับไปแพลตฟอร์มซึ่งจะได้รับการตรวจสอบแล้ว วิธีเดียวที่ผู้ใช้สามารถทราบจำนวนเงินที่ถูกต้อง (นอกเหนือจากการคาดเดา) คือการเข้าถึงบัญชีธนาคารที่เป็นปัญหา

การตรวจสอบด้วย Raindrop กับไฮโดรเป็นแบบเดียวกัน แทนที่จะส่งผู้ใช้งานหนึ่งและส่งต่อไปเราจะกำหนดธุรกรรมและผู้ใช้จะต้องดำเนินการจากกระเป๋าเงินที่รู้จัก วิธีเดียวที่ผู้ใช้สามารถทำธุรกรรมที่ถูกต้องคือการเข้าถึงกระเป๋าเงินที่ต้องการ

การใช้ Raindrops ทั้งระบบและ accessor สามารถตรวจสอบความถูกต้องของการอนุมัติในบัญชีแยกประเภทสาธารณะที่ไม่เปลี่ยนแปลงได้ การทำธุรกรรมแบบ blockchain นี้แยกจากการดำเนินงานของระบบพื้น

ฐานที่เกิดขึ้นบนเครือข่ายแบบกระจายและขึ้นอยู่กับความ เป็นเจ้าของคีย์ส่วนตัว ดังนั้นจึงทำหน้าที่เป็นเวกเตอร์ การตรวจสอบที่มีประโยชน์.

การดูโดยละเอียด

มีสี่หน่วยงานที่เกี่ยวข้องในกระบวนการตรวจสอบไฮโดร:

1. **Accessor** - บุคคลที่พยายามเข้าถึงระบบ ในกรณีของ Hydrogen, accessor คือสถาบันการเงิน หรือแอปที่ใช้ Hydrogen APIs สำหรับโครงสร้างพื้นฐานระบบดิจิทัลหลัก.
2. **System** - ระบบหรือเกตเวย์ที่เข้าถึงโดย Accessor สำหรับ Hydrogen, ระบบคือ Hydrogen API ตัวเอง.
3. **Hydro** - โมดูลที่ใช้โดยระบบเพื่อสื่อสารและเชื่อมต่อกับ blockchain.
4. **Blockchain** - บัญชีแยกประเภทสาธารณะที่ประมวลผลรายการ HYDRO และมีสัญญาไฮโดรสมาร์ ทซึ่งข้อมูลอาจถูกผลักดัน หรือดำเนินการอื่นๆ.

Raindrop แต่ละอย่างครบถ้วนเป็นชุดของพารามิเตอร์การทำธุรกรรมหารายการ:

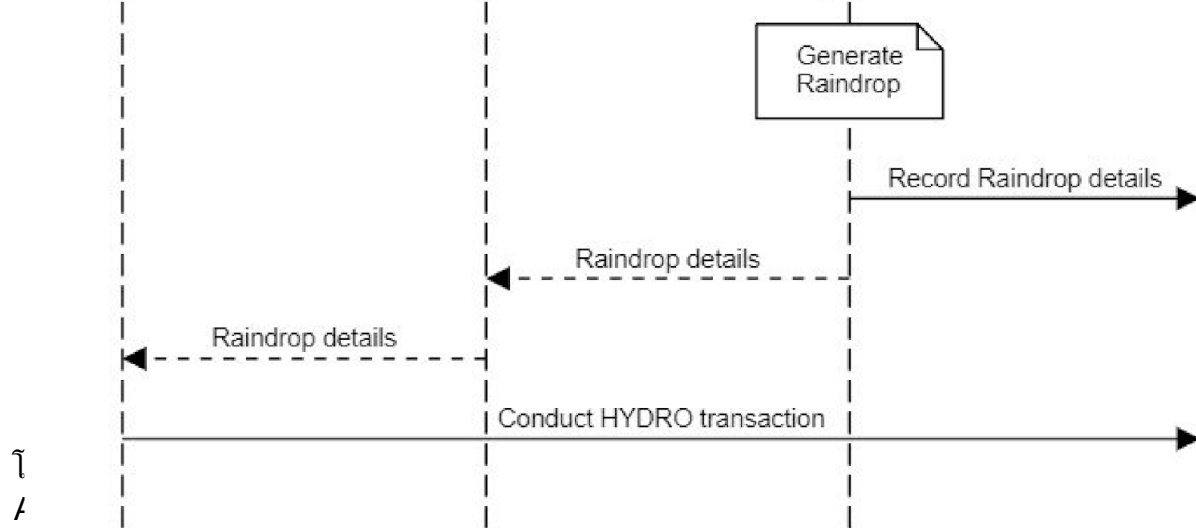
1. **Sender-** ที่อยู่ที่ต้องทำธุรกรรม.
2. **ผู้รับ -** ปลายทางของการทำธุรกรรม ซึ่งสอดคล้องกับการเรียกวิธีการในสัญญาไฮโดรสมาร์ท.
3. **ID -** ตัวระบุที่เชื่อมโยงกับระบบ.
4. **จำนวน -** จำนวนที่แน่นอนของ **HYDRO** ที่จะส่ง.
5. **ทำหาย...** - สตริงตัวเลขและตัวอักษรที่สร้างขึ้นโดยอัตโนมัติ.

ด้านล่างเป็นโครงร่างของกระบวนการตรวจสอบสิทธิ์ซึ่งสามารถแบ่งออกได้เป็น 3 ขั้นตอนโดยทั่วไป:

1. การเริ่มต้น
2. Raindrop
3. การตรวจสอบ

การเริ่มต้นจะเริ่มต้นด้วยระบบ (เช่น Hydrogen) ที่ลงทะเบียนเพื่อใช้ Hydro และได้รับข้อมูลประจำตัวทำให้ระบบสามารถสื่อสารกับ blockchain ผ่านโมดูลไฮโดรได้ ระบบจะเชื่อมต่อ Accessor (เช่นสถาบันการเงิน) ที่ลงทะเบียนที่อยู่สาธารณะจากนั้นส่งที่อยู่จดทะเบียนไปยัง Hydro ที่อยู่นี้ถูกเขียนขึ้นมาอย่างไม่น่าเชื่อบน blockchain ในรายการที่อนุญาตพิเศษที่เก็บไว้ในสัญญา ไฮโดรสมาร์ท ระบบได้รับการยืนยันว่าที่อยู่นั้นได้รับอนุญาตพิเศษซึ่งสามารถยืนยันได้ว่าเป็นงานที่สามารถดูได้แบบสาธารณะ การลงทะเบียนระบบจะต้องเกิดขึ้นเพียงครั้งเดียวเท่านั้นในขณะที่รายการที่อนุญาตพิเศษของ Accessor จะต้องเกิดขึ้นเพียงครั้งเดียวต่อ Accessor.

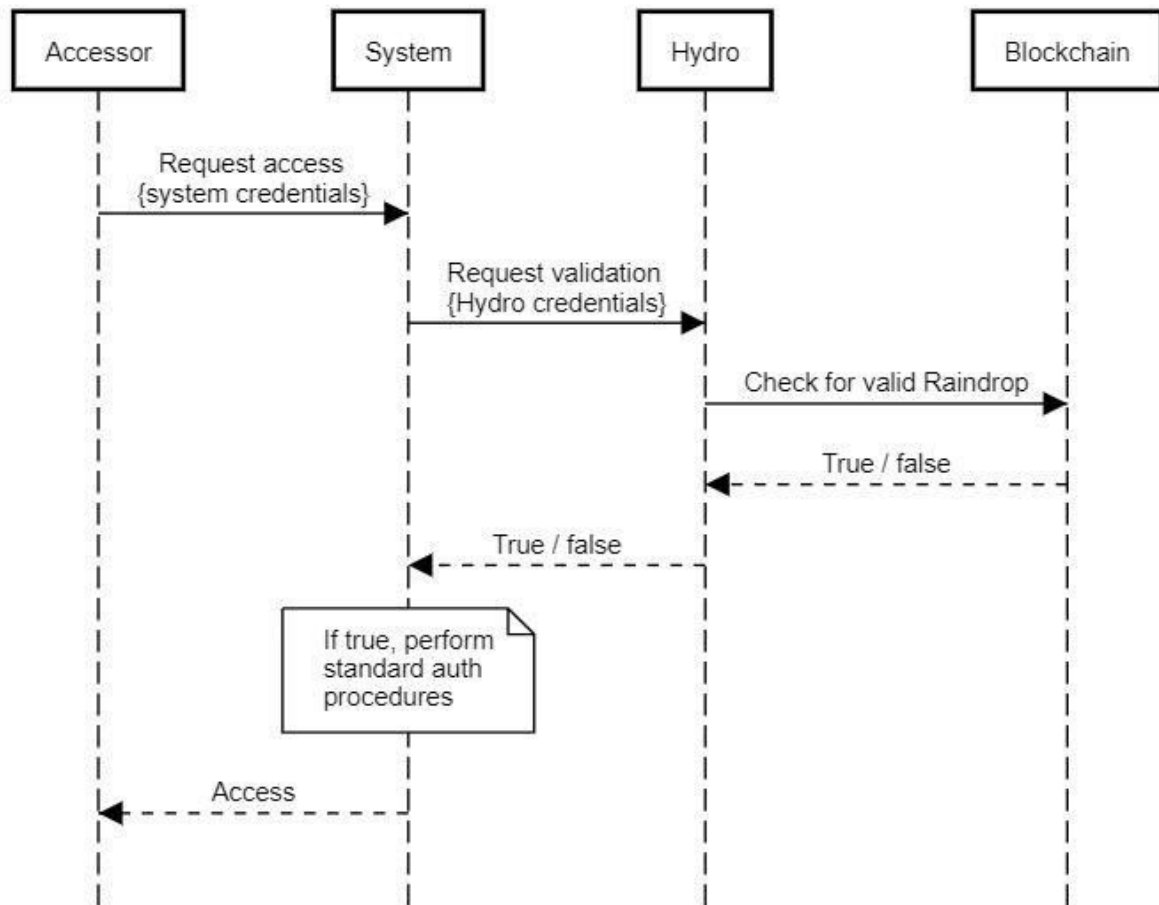
หลังจากการเริ่มต้นเสร็จสมบูรณ์หลักของกระบวนการตรวจสอบความถูกต้องของไฮโดรสามารถเริ่มต้นได้ Accessor ที่ต้องทำธุรกรรม Raindrop จะเริ่มกระบวนการนี้โดยการร้องขอรายละเอียด Raindrop จากระบบและระบบจะส่งคำขอไปยัง Hydro ไฮโดรสร้าง Raindrop ใหม่จัดเก็บรายละเอียดบางอย่างอย่างไม่อัน



ขั้นตอนสุดท้ายของกระบวนการคือการตรวจสอบ ในขั้นตอนนี้ **Accessor** จะร้องขอการเข้าถึงระบบผ่านทางกลไกที่กำหนดไว้ของ **System** ก่อนที่จะมีการใช้โปรโตคอลการพิสูจน์ตัวตนมาตรฐานใด ๆ ระบบจะถาม **Hydro** ว่า **Accessor** สามารถทำธุรกรรม **Raindrop** ได้หรือไม่ ไฮโดรเชื่อมต่อกับสัญญาสามารถตรวจสอบความถูกต้องและตอบสนองด้วยการกำหนดจริง / เท็จ ระบบสามารถทำได้

เพื่อตัดสินใจว่าควรดำเนินการอย่างไรโดยใช้ข้อนี้ – ถ้าเป็นเท็จระบบสามารถปฏิเสธการเข้าถึงได้และหากเป็นความจริงระบบ จะให้สิทธิ์การเข้าถึง.

Authentication with Hydro: Validation



ถ้าเราพิจารณาข้อมูลประจำตัวของระบบฐานหรือโพรโทคอลระบบใด ๆ ที่มีอยู่ซึ่งเป็นปัจจัยหนึ่งในการตรวจสอบสิทธิ์สิ่งสำคัญคือเลเยอร์ไฮโดรจะเป็นตัวกลางที่มีประโยชน์ เมื่อตรวจสอบพาหะนำโรคทั้งสองแบบเราสามารถยืนยันประโยชน์ได้อย่างง่ายดาย:

- Vector 1 - ผู้บุกรุกขโมยข้อมูลรับรองระบบฐานของ Accessor
 - 1 ผู้โจมตีจะพยายามเข้าถึงระบบที่มีข้อมูลประจำตัวของระบบที่ต้องการ
 - ระบบจะตรวจสอบกับ Hydro เพื่อตรวจสอบว่ามีการทำรายการธุรกรรมที่ต้องการใน blockchain หรือไม่
- Hydro ส่งกลับเท็จและระบบปฏิเสธการเข้าถึง
- Vector 2 - ผู้โจมตีจะขโมยกุญแจส่วนตัวไปที่กระเป๋าสตางค์ของ Accessor
 - 1 ผู้โจมตีจะพยายามทำธุรกรรมไฮโดรจากที่อยู่ที่อยู่ลงทะเบียนโดยไม่จำเป็นต้องมีรายละเอียด Raindrop
- ผู้โจมตีไม่สามารถทำธุรกรรม blockchain ที่ต้องการ

- ผู้โจมตียังไม่สามารถร้องขอการเข้าถึงระบบได้โดยไม่ต้องมีข้อมูลประจำตัวของระบบที่เหมาะสม

เห็นได้ชัดว่าผู้โจมตีต้องขโมยข้อมูลประจำตัวของระบบฐานและกฎแจกจ่ายสแตคของ Accessor เพื่อเข้าถึงระบบ ในเรื่องนี้ไฮโดรได้เพิ่มปัจจัยการพิสูจน์ตัวตนเพิ่มเติมแล้ว.

เปิดแผนสู่สาธารณะ

แม้ว่าบริการรับรองความถูกต้องแบบ blockchain นี้ได้รับการออกแบบมาเพื่อช่วยรักษาความปลอดภัยของระบบนิเวศของไฮโดรเจน API แต่ก็สามารถใช้งานได้กับแพลตฟอร์มและระบบที่แตกต่างกัน เนื่องจากเรารู้สึกว่าคนอื่นอาจได้ รับประโยชน์จากเลเยอร์การยืนยันนี้ เราจึงเปิดให้ใช้งาน

เช่นเดียวกับไฮโดรเจนจะรวมไว้เป็นเงื่อนไขเบื้องต้นสำหรับการเข้าถึงระบบนิเวศ API ดังนั้นระบบใด ๆ จึงสามารถเพิ่มระบบและโพรโทคอลที่มีอยู่ได้ แพลตฟอร์มใด ๆ ไม่ว่าจะเป็น API แอปพลิเคชันซอฟต์แวร์สำหรับองค์กรแพลตฟอร์มเกม ฯลฯ สามารถใช้ประโยชน์ไฮโดรเพื่อวัตถุประสงค์ในการตรวจสอบสิทธิ์ได้ เอกสารที่เป็นทางการจะมีอยู่ใน GitHub สำหรับผู้ที่ต้องการรวมเลเยอร์ blockchain นี้ไว้ในกรอบการรับรองความถูกต้องหรือ REST API.

กรณีศึกษา - ผันตกด้วย OAuth 2.0

มีหลายสิบวิธีที่ Raindrop release สามารถใช้โดยองค์กรเอกชนได้ APIs ฐานข้อมูลและเครือข่ายส่วนตัวได้สร้างระบบที่ซับซ้อนของโทเค็นคีย์แอปและโพรโตคอลในช่วงทศวรรษที่ผ่านมาเพื่อพยายามรักษาความปลอดภัยข้อมูลที่สำคัญ ตัวอย่างเช่น Google กลายเป็นหนึ่งในผู้ให้บริการผลิตภัณฑ์ยอดนิยมในตลาดที่มีแอป Google Authenticator ดังที่ได้กล่าวไว้ก่อนหน้านี้ไม่มีเหตุผลที่จะแข่งขันหรือแทนที่โพรโตคอลที่มีอยู่เหล่านี้ได้

ในฐานะกรณีศึกษาที่อธิบายคร่าวๆเกี่ยวกับวิธีการใช้ไฮโดรเจนในการรับรองความถูกต้องของไฮโดรเจนเป็นเลเยอร์ความปลอดภัยในกรอบความปลอดภัยโดยรวมของ API:

1. พาร์ทเนอร์ของ Hydrogen API จะต้องอยู่ที่ IP ของสภาพแวดล้อมต่างๆที่อนุญาตพิเศษ.
2. พาร์ทเนอร์ต้องขอให้อยู่ที่ Hydro สาธารณะ.
3. การโทรไปยัง API ของ Hydrogen และการถ่ายโอนข้อมูลจะถูกเข้ารหัสและส่งผ่านโพรโตคอล HTTPS.
4. พาร์ทเนอร์ต้องทำรายการน้ำฝนที่ถูกต้องจากที่อยู่ Hydro ที่จดทะเบียน.
5. พาร์ทเนอร์ต้องใช้การตรวจสอบ OAuth 2.0 OAuth (Open Authorization) เป็นมาตรฐานแบบเปิดสำหรับการตรวจสอบสิทธิ์และการให้สิทธิ์ที่ใช้โทเค็น Hydrogen สนับสนุน "ข้อมูลรับรองสิทธิ์

ของเจ้าของทรัพยากร" และ "ลูกค้า"ข้อมูลประจำตัว "และผู้ใช้ API แต่ละรายจะต้องให้ข้อมูลประจำตัวสำหรับคำขอการตรวจสอบสิทธิ์.

6. หากไม่มีองค์ประกอบใด ๆ ทั้ง 5 องค์ประกอบข้างต้นถูกละเมิดคู่ค้าของ Hydrogen จะได้รับโทเค็นที่ไม่ซ้ำกันซึ่งจะได้รับการตรวจสอบและยืนยันด้วยการเรียก API แต่ละครั้ง.
7. โทเค็นใช้ได้ภายใน 24 ชั่วโมงหลังจากนั้นคู่ค้าต้องตรวจสอบตัวเองอีกครั้ง.

หากมีการละเมิดขั้นตอนใด ๆ ผู้ใช้จะถูกบล็อกจากการเข้าถึง API ทั้งนี้ แอ็กเกอร์ไม่สามารถหลีกเลี่ยงปัจจัยด้านความปลอดภัยเหล่านี้ได้โดยการคาดเดาแบบสุ่มเนื่องจากมีชุดค่าผสมที่เป็นเอกลักษณ์หลายล้านชุด

การตรวจสอบความถูกต้องของไฮโดรไซต์ blockchain เป็นองค์ประกอบที่สำคัญของโปรโตคอลความปลอดภัยไฮโดรเจน ทีมไฮโดรเจนสนับสนุนให้คู่ค้าตั้งค่ากระเปาะสแตงค์หลายลายเซ็นและจัดเก็บคีย์ส่วนตัวในสถานที่ที่มีความปลอดภัยหลายแห่งแยกต่างหากจากข้อมูลรับรองอื่น ๆ ดังนั้นจึงไม่ใช่จุดล้มเหลวเพียงจุดเดียว กระเปาะสแตงค์หลายลายเซ็นที่มีความถูกต้องเหมาะสมไม่เพียง แต่เป็นเรื่องยากที่จะขโมย แต่ลักษณะสาธารณะของ blockchain ยังช่วยให้สามารถรับรู้ถึงการโจรกรรมได้อย่างรวดเร็วเนื่องจากเกี่ยวข้องกับความปลอดภัยของ API ทุกคนสามารถดูความพยายามในการตรวจสอบสิทธิ์ในสัญญาไฮโดรอัจฉริยะซึ่งหมายความว่าวันที่แพลตฟอร์มถูกบุกรุกเป็นเวลาหลายเดือนนับจากนี้ไปอาจเป็นสิ่งที่ผ่านมา ขณะนี้แอ็กเกอร์ API สามารถขัดขวางการทำงานที่รวดเร็วขึ้นเนื่องจากความสามารถในการตรวจหาการอนุมัติที่ไม่คาดคิดในแบบเรียลไทม์จากทุกที่ในโลก.

ความเสี่ยง

เช่นเดียวกับเทคโนโลยีที่เพิ่งเริ่มต้นอื่น ๆ เช่นวันเริ่มต้นของโซเชี่ยลมีเดียอีเมลและสตรีมมิ่งแอปพลิเคชัน (ซึ่งพึ่งพาการเชื่อมต่อแบบ dial-up) เป็นสิ่งสำคัญที่ทีมพัฒนาหลักจะติดตามการพัฒนาใหม่ ๆ ในความเร็วและปริมาณธุรกรรมของ Ethereum คุณสามารถจินตนาการได้ว่า YouTube กำลังพยายามเปิดตัวในปีพ. ศ. 2538 หรือไม่? หรือ Instagram ถูกเสนอครั้งแรกบน Blackberry?

นักพัฒนาหลัก Ethereum เช่น Vitalik Buterin และ Joseph Poon ได้เสนอ Plasma: Scalable Autonomous Smart Contracts อัปเดตเป็น Ethereum protocol:

พลาสมาเป็นกรอบที่เสนอสำหรับการดำเนินการตามสัญญาสมรรถนะที่กระตุ้นและบังคับใช้ซึ่งสามารถปรับขนาดได้เป็นจำนวนมากต่อการอัปเดตสถานะต่อวินาที (ซึ่งอาจเป็นพันล้าน) ซึ่งทำให้ blockchain สามารถเป็นตัวแทนของแอปพลิเคชันทางการเงินแบบกระจายอำนาจได้ทั่วโลก สัญญาสมรรถนะเหล่านี้มีการมุ่งใจให้ดำเนินการต่อโดยอัตโนมัติผ่านค่าธรรมเนียมการทำธุรกรรมเครือข่ายซึ่งจะขึ้นอยู่กับ blockchain ต้นแบบ (เช่น Ethereum) เพื่อบังคับให้เกิดการเปลี่ยนสถานะของทรานแซคชัน.

อื่น ๆ เช่น The Raiden Network ได้เสนอโซลูชันการปรับขนาดแบบไม่ใช้สายโซ่ที่ออกแบบมาเพื่อใช้งานการทำธุรกรรมที่รวดเร็วขึ้นและลดค่าธรรมเนียม ในขณะนี้ Raindrop จะทำให้ความเครียดน้อยที่สุดในกรอบ Ethereum ทำให้ความสามารถในการปรับขยายเป็นความเสี่ยงที่น้อยมากต่อความสำเร็จของเทคโนโลยี.

ข้อสรุป

ความไม่เปลี่ยนแปลงของ blockchain สาธารณะมีวิธีการใหม่ ๆ เพื่อเพิ่มความปลอดภัยให้กับระบบภาคเอกชนเช่น APIs

บทความนี้แสดงให้เห็นถึงสิ่งสำคัญสามประการ:

1. Blockchains สาธารณะสามารถเพิ่มมูลค่าในบริการทางการเงิน.
2. Raindrop ของ HYDRO สามารถเพิ่มความปลอดภัยให้กับระบบภาคเอกชน.
3. มีการประยุกต์ใช้ HYDRO Raindrop ในแพลตฟอร์มไฮโดรเจน API ทันที.

ทีมงานของ HYDRO เชื่อว่ากรอบที่กำหนดไว้จะเป็นโครงสร้างพื้นฐานด้านความปลอดภัยมาตรฐานสำหรับระบบไฮบริดเอกชน และระบบไฮบริดใหม่ซึ่งจะเป็นประโยชน์ต่อผู้มีส่วนได้เสียทั้งหมดในอุตสาหกรรมบริการทางการเงินและอื่น ๆ.

Sources:

Ethereum; [Merkling in Ethereum](#)

Trend Micro; [What Do Hackers Do With Your Stolen Identity?](#)

Javelin Strategy & Research; [The 2017 Identity Fraud Study](#)

Symantec; [Internet Security Threat Report](#)

Risk Based Security; [2016 Data Breach Trends - Year in Review](#)

Thales; [2017 Thales Data Threat Report - Financial Services Edition](#)

Apache.org; [Apache Struts 2 Documentation - S2-052](#)

Joseph Poon and Vitalik Buterin; [Plasma: Scalable Autonomous Smart Contracts](#)