ขอบคุณที่สละเวลาอ่าน !!

และเราขอขอบคุณอย่างยิ่งต่อแหล่งข้อมูลดังต่อไปนี้:

ซีโร่ซิงค์
https://zerosync.org

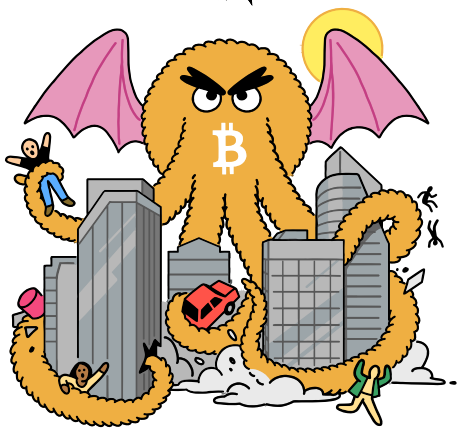
บิทคอยน์ อ๊อพเทค
https://bitcoinops.org

ซิลเด็ด ไคลเอนท์ไซด์วาลิเดชั่น
กิทฮับ: ShieldedCSV/ShieldedCSV

Awesome บิทวีเอ็ม
กิทฮับ: Rsync25/awesome-bitvm

บทนำคุณไทเลอร์ วิทเท้ิล
กิทฮับ: twhit223/bitvm_primer

การมาถึงของยุคใหม่ของสมาร์ทคอนแทรคบิทคอยน์



ไขปริศนาเทคโนโลยีขั้นสูง

เข้าถึงยากของบิทคอยน์
ที่ทุกคนควรรู้จัก

ฉุดไม่อยู่แล้ว ยานลำนี้

"บิทวีเอ็มปลดกลไกไขสมรรถภาพประมวลผลให้กับ **บิทคอยน์** อย่างไม่ก้าวก่ายฉันทามติ เพียงแต่เพิ่มเกต NAND และปริศนาท้าพิสูจน์"

"อย่าดันข้อมูลขยะมาให้โหนดผมนะ..."

ไม่ใช่การประมวลผลขนาดใหญ่เลย ที่เกิดขึ้นบนเครือข่าย **บิทคอยน์** หากแต่เป็น **บทพิสูจน์ประมวลผล** , คล้ายคลึงกับการทำงาน อ๊อพติมิสติกโรลอั๊พ (optimistic rollup)

เลี่ยงไม่ให้เพื่อนบ้านคอมพิ้วท์นานเกินรอ

สคริปท์ของ **บิทคอยน์** อนุญาตเพียงแค่ ร้อยกว่าอ๊อพโค้ด เอง บีบรัดการออกแบบสัญญาอัจฉริยะเชิงซับซ้อนเกินเบอร์มาถึงปัจจุบัน หากใครทะเยอทะยาน สร้างธุรกรรมเขียนโปรแกรมขนาดมหึมา สามารถสตั๊นเน็ตเวิร์กให้ชะงักได้ทุกโหนดไป แล้วส่งผลกระทบให้กับความกระจายศูนย์ของเครือข่าย **บิทคอยน์**

โรลอั๊พมอบคุณสมบัติควบสองโลกให้กับเรา บิทคอยเน่อร์สามารถ ประมวลผลพึงประสงค์ โดยแนบโปรแกรมไม่เล็กก็ใหญ่ไว้ในแอดเดรสแท็พรูท (Taproot) ที่มีขนาด มินิม่อลกะทัดรัด ไม่สร้างความก่อกวนมากมายให้กับระบบ

ก่อนอื่นทำความรู้จัก **โคฟเวอแนนท์** กัน

โคเวอแนนท์คือแขนงข้อนำเสนอการปรับปรุง ฉันทามติโปรโตคอลของ **บิทคอยน์** เพื่อให้สคริปท์สามารถกันธุรกรรมไม่ให้เกิดขึ้นได้ แม้จากผู้มีสิทธิ์ถึงไปทางสคริปท์อื่น ๆ ที่ระบุ

เรายังไม่มีหรอกนะ โคฟเวอแนนท์บน **บิทคอยน์** หน่ะ แต่ว่าเราสามารถ emulate หรือสังเคราะห์กลไกคล้ายเคียงได้ การเอ็มมูเลทโคฟเวอแนนท์ใน BitVM 2 เป็นการทำงานอ้อม ๆ เพื่อให้เรากำหนด กรรมการเซ็นข้อพิสูจน์ล่วงหน้าสำหรับการเลียนแบบการใช้จ่ายเชิงซับซ้อน ที่ยังไม่สามารถพิสูจน์บนเครือข่าย **บิทคอยน์** ได้โดยตรง เกิด trust assumption ไว้วางใจคนใน ก้อนเล็ก ๆ ขึ้นมา

*บิทวีเอ็มคือสะพานเชื่อมระหว่าง **บิทคอยน์** กับระบบนิเวศน์เสริมข้างเคียง*

โดยทั่วไป สะพานเชื่อมจะได้รับการรักษาความปลอดภัยโดยใช้ระบบมัลติซิกแบบสหพันธ์ (federated multisig) ซึ่งการถอนเงินไม่สามารถทำได้ฝ่ายเดียว แต่ต้องได้รับการอนุมัติจากเสียงข้างมาก

BitVM เหมือนเพื่อนซะที่ไหน !!

มันคือโมเดลความเชื่อถือแบบ 1 ใน N ซึ่งตราบใดที่มีผู้ดำเนินการที่ซื่อสัตย์เพียงหนึ่งคนที่ยังทำงานอยู่ คุณก็สามารถถอนมูลค่าบนเชนออกมาได้ ผู้ใช้สามารถเดิมพัน ที่ผู้ดำเนินการซื่อสัตย์คนเดียวแทนที่จะต้องอาศัยเสียงส่วนใหญ่ของผู้เข้าร่วมในสหพันธ์

ทำไมต้องพูดถึง Covenants เมื่อหัวข้อหลักเป็น BitVM ?

เพราะ **บิทคอยน์** เป็นผู้ตรวจสอบแบบกระจายอำนาจเพียงหนึ่งเดียวในโลก เครือข่ายทำการตรวจสอบความถูกต้องของหลักฐาน ลายเซ็น และธุรกรรมอย่างเท่าเทียม

> การตัดสินใจในการออกแบบภายใต้ **บิทคอยน์** รวมถึงความไม่สมบูรณ์ตามการประมวลผลทัวริ่ว (Turing completeness) ในภาษาสคริปต์ ทำให้โหนดทุกตัวสามารถตรวจสอบสคริปต์ได้อย่างมีประสิทธิภาพ ด้วยองค์ประกอบสแตก 1,000 ตัว และ 201 opcode โดยไม่ต้องเชื่อใจใคร

ทั้ง Covenants และ BitVM ท้าทายขีดจำกัดนี้ แต่ BitVM ทำได้โดยไม่ต้องมีการเปลี่ยนแปลงโปรโตคอล **บิทคอยน์** (ยังไม่ใช่ตอนนี้) แต่ด้วยการเปลี่ยนแปลงแนวคิดครั้งใหญ่

ตอนนี้ชาวบิทคอยน์สามารถทำอะไรได้บ้าง ที่เคยทำไม่ได้ก่อนหน้านี้?

แทนที่จะปล่อยให้ซอฟต์แวร์ที่ไม่จำเป็นเพิ่มภาระบนเชนหลักเมนเน็ต BitVM กลับเป็นการเปิดทางให้ผลงานสำคัญบางอย่าง ในโลกไซเฟอร์พังค์ได้ปรากฏในวงการค้นคว้าวิจัยแล้วโต้เถียงพัฒนา **บิทคอยน์**

ทีมอิสระเร่งสร้างตัวตรวจสอบพิสูจน์ความรู้เป็นศูนย์ (Zero-Knowledge Proof Verifier) บน **บิทคอยน์** สคริปต์และแทปสคริปต์อีกครั้งด้วยวิธีแก้ไขที่นำเสนอโดยการวิจัย BitVM

อัตราการเติบโตของนวัตกรรม

โปรโตคอล	**ระยะเวลาดำเนินผล**	**ขนาดธุรกรรม**	**รอบธุรกรรม**
บิมวีเอ็ม (ลอจิกเกต)	หลายสัปดาห์	เทร่าไบต์	~ 50
บิทวีเอ็ม	หลายวัน	กิกาไบต์	~ 38
BitVM2	หลายนาที	เมกาไบต์	1

แล้วมันโอเพ่นซอร์สด้วย !!

ในเดือนมีนาคม 2025 ZeroSync ได้ทำการทดสอบแนวคิดเบื้องต้นของ zkCoins เสร็จสมบูรณ์ และพันธมิตร BitVM อัลลิแอ็นซ์ได้ดำเนินการพัฒนาสะพานเชื่อม BitVM ภายใต้ใบอนุญาต MIT แล้ว

มาดูการอัปเกรดที่ใช้งานง่ายสำหรับผู้ใช้กันเถอะ !!

ไคลเอนต์ไซด์วาลิเดชั่นคุมเกราะ (Shielded Client-Side Validation)

ประวัติการทำธุรกรรมเป็นแหล่งข้อมูลที่สำคัญสำหรับเชื่อมโยงธุรกรรม และเปิดเผยตัวตนของผู้ใช้ โปรโตคอลการตรวจสอบฝั่งไคลเอนต์ (Client-Side Validation) ที่หลักฐานของเหรียญ เผยประวัติการทำธุรกรรมของเหรียญนั้น ให้ข้อได้เปรียบเรื่องความเป็นส่วนตัวมากกว่าธุรกรรมบนบล็อกเชน แบบโปร่งใส ผู้ส่งจะกระจายตัวบ่งชี้ (nullifiers) ไปยังผู้รับซึ่งประกอบด้วยประวัติเต็มของเหรียญ

โมเดล CSV ที่เป็นที่รู้จักในปัจจุบัน

- โปรโตคอล RGB
- Taproot Assets ของ Lightning Labs

ด้วยแนวคิด Shielded CSV บน BitVM รอยเท้าตัวบ่งชี้ (nullifier) สามารถจำกัดขนาดให้อยู่ที่ 64 ไบต์ และประกอบด้วยเฉพาะหลักฐานความถูกต้องโดยไม่เปิดเผยข้อมูลที่ทำให้สูญเสียความเป็นนิรนาม