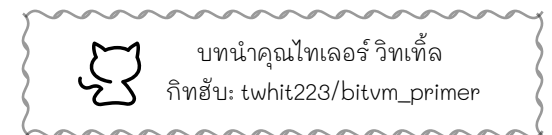
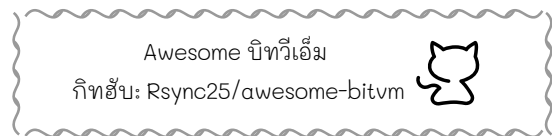
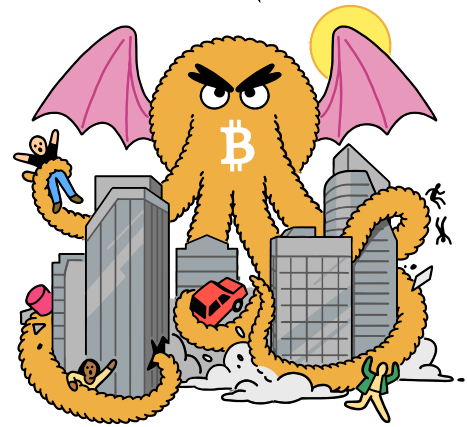


> **ขอบคุณที่สละเวลาอ่าน !!** <

และเราขอขอบคุณอย่างยิ่งต่อแหล่งข้อมูลดังต่อไปนี้:



วารสารวิชาการเชิงปฏิบัติฉบับพิเศษ **บิตวีเอ็ม** ฉบับพิเศษฉบับทดลอง



ไซปรีศนาเทคโนโลยีขั้นสูง

เข้าถึงยากของบิตคอยน์
ที่ทุกคนควรรู้จัก

จุดไม่อยู่แล้ว ยานลำนี้

"บิตวีเอ็มปลดกลไกไฮสมรรถภาพประมวลผลให้กับ **บิตคอยน์** อย่างไม่ก้าวร้าวแน่นอนตามตีเพียงแต่เพิ่มเกต NAND และปริศนาท้าทาย"



"อย่าดันข้อมูลขยะมาให้โหนดผมนะ..."



ไม่ใช่การประมวลผลขนาดใหญ่เลย ที่เกิดขึ้นบนเครือข่าย **บิตคอยน์** หากแต่เป็น **บทพิสูจน์ประมวลผล**, คล้ายคลึงกับการทำงาน อ็อปติมิสติกโรลอัพ (optimistic rollup)

เลี้ยงไม่ให้เป็นบ้านคอมพิวเตอร์นานเกินรอ

สคริปต์ของ **บิตคอยน์** อนุญาตเพียงแค่ว่า ร้อยกว่าอ็อปโค้ดเอง บัณฑิตการออกแบบสัญญาอัจฉริยะเชิงซับซ้อนเกินเบอร์มาถึงปัจจุบัน หากใครทะเยอทะยาน สร้างธุรกรรมเขียนโปรแกรมขนาดมหึมา สามารถสแต็คเนตเวิร์กให้ชะงักได้ทุกโหนดไปแล้วส่งผลกระทบให้กับความกระจายศูนย์ของเครือข่าย **บิตคอยน์**

โรลอัพมอบคุณสมบัติควบสองโลกให้กับเรา บิตคอยน์เนอร์สามารถ ประมวลผลฟังก์ชันฟังก์ชัน โดยแบบโปรแกรมไม่เล็กก็ใหญ่ไว้ในแอตเดรสแทปรูท (Taproot) ที่มีขนาด มินิมอลกะทัดรัด ไม่สร้างความก่อกวนมากมายให้กับระบบ

> **ก่อนอื่นทำความรู้จัก โคฟเวอแนนท์** กัน <

โคฟเวอแนนท์คือแขนงข้อนำเสนองการปรับปรุง นันทามติโปรโตคอลของ **บิตคอยน์** เพื่อให้สคริปต์สามารถกันธุรกรรมไม่ให้เกิดขึ้นได้ แม้จากผู้มีสิทธิ์ถึงไปทางสคริปต์อื่น ๆ ที่ระบุ



เรายังไม่มีหอรกนะ โคฟเวอแนนท์บน **บิตคอยน์** นะ แต่ว่าเราสามารถ emulate หรือสังเคราะห์กลไกคล้ายเคียงได้ การเฝ้าดูแลโคฟเวอแนนท์ใน BitVM 2 เป็นการทำงานอ้อม ๆ เพื่อให้เรากำหนด กรรมาการเซ็นข้อพิสูจน์ล่วงหน้าสำหรับการเลียนแบบการใช้จ่ายเชิงซับซ้อน ที่ยังไม่สามารถพิสูจน์บนเครือข่าย **บิตคอยน์** ได้โดยตรง เกิด trust assumption ไว้วางใจคนใน ก้อนเล็ก ๆ ขึ้นมา



โดยทั่วไป สะพานเชื่อมจะได้รับการรักษาความปลอดภัย
โดยใช้ระบบมัลติซิกแบบสหพันธ์ (federated multisig) ซึ่ง
การถอนเงินไม่สามารถทำได้ฝ่ายเดียว แต่ต้องได้รับการ
อนุมัติจากเสียงข้างมาก

> **BitVM เหมือนเพื่อนซี้ที่ไหน !!** <

มันเป็นโมเดลความเชื่อถือแบบ 1 ใน N ซึ่งตราบใดที่มีผู้ดำเนินการ
การที่ซื่อสัตย์เพียงหนึ่งคนที่ยังทำงานอยู่ คุณก็สามารถถอน
มูลค่าบนเชนออกมาได้ ผู้ใช้สามารถเดิมพัน ที่ผู้ดำเนินการ
ซื่อสัตย์คนเดียวแทนที่จะต้องอาศัยเสียงส่วนใหญ่ของผู้เข้า
ร่วมในสหพันธ์

แทนที่จะปล่อยให้ซอฟต์แวร์ที่ไม่จำเป็นเพิ่มภาระบนเชน
หลักเมนเน็ต BitVM กลับเป็นการเปิดทางให้ผลงานสำคัญ
บางอย่าง ในโลกไซเฟอร์ฟังก์ได้ปรากฏในวงการค้นคว้า
วิจัยแล้วโต้เถียงพัฒนา **บิทคอยน์**

ทีมอิสระเร่งสร้างตัวตรวจสอบพิสูจน์ความรู้เป็นศูนย์
(Zero-Knowledge Proof Verifier) บน **บิทคอยน์** ๗คริปต์
และแทปสคริปต์อีกครั้งด้วยวิธีแก้ไขที่นำเสนอโดยการวิจัย
BitVM

อัตราการใช้ของนวัตกรรม

โปรโตคอล	ระยะเวลาดำเนินการ	ขนาดธุรกรรม	รอบธุรกรรม
บิทวีเอ็ม (ลอจิกเกต)	หลายสัปดาห์	เทราไบต์	~ 50
บิทวีเอ็ม BitVM2	หลายวัน	กิกาไบต์	~ 38
	หลายนาที	เมกาไบต์	1

> แล้วมันโอเพ่นซอร์สด้วย !! <

ในเดือนมีนาคม 2025 ZeroSync ได้ทำการทดสอบแนวคิด
เบื้องต้นของ zkCoins เสร็จสมบูรณ์ และพันธมิตร BitVM
อัลลิแอนด์ได้ดำเนินการพัฒนาสะพานเชื่อม BitVM ภายใต้
ใบอนุญาต MIT แล้ว