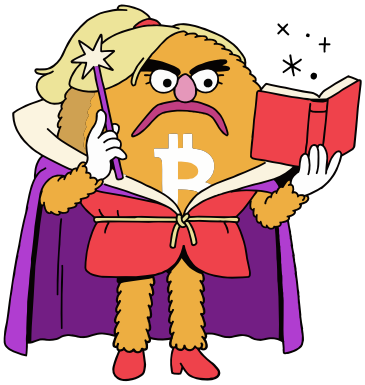
ขอบคุณที่ให้เวลาอ่าน!

นี่เป็นแค่ภาพรวมสั้น ๆ ของแท็พรูท หวังว่าคุณได้อ่านอย่างเพลิดเพลิน พร้อมเรียนรู้เพิ่มเติม ไหม? อยากพิมพ์ซีน (Zine) ฉบับนี้รีเปล่า? ไปดู



https://satsie.dev/zines

สำหรับสาระสำคัญเพิ่มเติม และเนื้อหาไม่ใกล้ไม่ไกลไปจาก สารสาส์นฉบับนี้

แท็พรูท

ภาพรวมกะทัดรัดสำหรับบิทคอยน์อัพเกรด นามว่าแท็พรูท

แท็พรูทอัปเกรดมีองค์ประกอบ 3 ชิ้นส่วน

- BIP-34Ø: กลไกไขรหัสชนอร์
- BIP-341: เมอร์เคิ่ลไลซ์แอ็บแสตร็กท์ ซินแทคส์ทรี (MAST) + แท็พรูท
- BIP-342: แท็พสคริปท์

เมื่อมีการพูดถึงแท็พรูท ในบริบทั่วไป รวมถึงวิธีที่เราได้กล่าวถึงมัน ณ ตอนนี้ โดยปกติแล้วมักจะหมายถึงทั้ง 3 สิ่งนี้โดยรวมกัน

มาดูพวกมันอย่างใกล้ชิดกัน !!

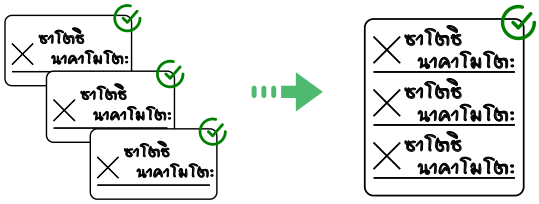
☆ BIP-34Ø: กลไกไขรหัสชนอร์ ☆

บิทคอยน์อิมพรูฟเมนท์โพรโพซอล (BIP) ตัวนี้เป็นการเปิดตัว กลไกไขรหัสที่ชื่อว่าชนอร์ เสริมโครงร่างลายเซ็นตัวใหม่ให้กับระบบ

เมื่อเปรียบเทียบกับโครงร่างลายเซ็นตัวก่อนที่ถูกใช้ภายในเครือข่ายบิทคอยน์ ที่เรียกกันว่า อีซีดีเอสเอ (ECDSA) แล้ว กลไกไขรหัสชนอร์มอบโครงร่างที่ปลอดภัยกว่า ใช้งานง่าย และมีประสิทธิภาพสูงกว่าเล็กน้อยให้กับผู้ใช้

☆ การตรวจสอบลายเซ็นแบบจับกลุ่ม ☆

การตรวจสอบลายเซ็นดิจิทัลโดยปกติจำเป็นต้องใช้การคำนวณซับซ้อนจากสมองกลคอมพิวเตอร์ ปัจจุบันเราสามารถจับกลุ่มลายเซ็นหลากหลาย ผ่านกระบวนการครวจสอบเป็นกลุ่มก้อนเดียวกันได้ แทนที่การตรวจสอบทีละรายการ



☆ สิทธิสันโดษที่ดีขึ้น ☆

บิทคอยน์เปิดทางให้ทุกคนกำหนดหนทางการใช้เหรียญของคุณตามชอบ ก่อนหน้าที่เรามี แท็พรูท ทุกหนทางในการสร้างธุรกรรม จำเป็นต้องเผยข้อมูลที่มาที่ไปสู่สาธารณะ ณ ช่วงเวลาชำระเงิน ก่อให้เสียความเป็นส่วนตัว โดยเฉพาะกับเหรียญ ที่มีข้อกำหนดกฎเกณฑ์รายจ่ายไว้ล่วงหน้า ทำให้ผู้สอดส่องหวังร้าย ขุดคุ้ยธุรกรรมเกี่ยวข้องกับผู้ใช้ได้ง่าย

แท็พรูทอัปเกรดคืออะไรกันแน่ ?

Taproot is a set of improvements that allow ***bitcoin*** to be used in a more scalable and private ways.

Activation date: November 2021
Block height: 709,632.

แท็พรูทเปิดทางฟีเจอร์เชือดเฉือนฉ่ำ ๆ

☆ Key and signature aggregation (MuSig) ☆

If you have public keys A, B and C, they can be combined into one. The same is true for the corresponding signatures.

This means complex multisignature spends can look like ones that only involves 1 key.

☆ BIP-341: สคริปท์แตกกิ่ง + แท็พรูท ☆
บิ๊พตัวนี้สามารถแตกแขนงได้เป็น 2 ปัจจัยะ

1. **สคริปท์แตกกิ่ง:** การจับกลุ่มและเข้ารหัสรวบของโครงร่างข้อมูลดาต้า (data-structures) เป็นเหมือนต้นไม้ เพื่อย่อขนาดตรรกะของหลาย ๆ สคริปท์ ในบิทคอยน์อิมพรูฟเมนท์โพรโพซอลตัวนี้ แต่ละกิ่งไม้ ของต้นไม้ดังกล่าว เป็นเหมือนตรรกะที่ได้จากสคริปท์เดี่ยว และผู้ใช้จ่ายสามารถเลือกผลลัพธ์ ปลายทางได้แค่ทางเดียว ผู้ใช้รับผิดชอบในการแสดงผลของช่องทางตรรกะกิ่งที่เลือก (เราเรียกมันว่า "กิ่งเมอร์เคิ่ล (Merkle branch)")
2. **แท็พรูท:** ทักษะที่ทำให้เราสามารถใช้จ่ายเหรียญด้วยกุญแจไขรหัสเปิดเผย (public key) **หรือ** จากผลลัพธ์เอาท์พุทที่ได้มาจากสคริปท์ แท็พรูทช่วยทุ่นแรงจากสมรรถภาพของเมอร์เคิ่ลไลซ์แอ๊บแสครกท์ ชินแทคส์ทรี (MAST) และกลไกไขรหัสชนอร์ให้เราสร้างธุรกรรมได้อย่าง **ยืดหยุ่น, ลับตา และคล่องประสิทธิภาพ** ด้วยแท็พรูท คุณเองก็สามารถตั้งกฎเกณฑ์ควบคุมรายจ่ายนานา แล้วค่อยเผยแพร่เฉพาะทางที่ใช้เวลาชำระได้

☆ BIP-342: แท็พสคริปท์ ☆
สคริปท์ก็คือ ~~ชื่อตั้งไร้จินตนาการ~~ ชื่อสำหรับภาษาเขียนตรรกะอัจฉริยะ (smart contract) บนเครือข่ายกระจายศูนย์บิทคอยน์ แท็พสคริปท์เป็นเหมือนภาษาที่วิวัฒนาการมาต่อเนื่องจากเดิม และรองรับการใช้งาน กลไกไขรหัสชนอร์บวกกับแท็พรูท

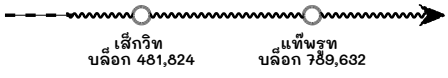
ด้วย Taproot สิ่งเดียวที่จำเป็นต้องเปิดเผยต่อสาธารณะ คือวิธีเฉพาะที่เหรียญถูกใช้ไป ไม่ใช่ความเป็นไปได้อื่น ๆ ทั้งหมด ซึ่งหมายความว่าะ

1. ลดการเปลืองดาต้าบนบล็อก และ
2. ปกป้องสิทธิสันโดษมากกว่าเดิม

ด้วยหลาย ๆ ปัจจัยรวมกัน ทำให้เราเห็นความเด่นชัด และกรณีการใช้งานน่าประทับใจที่สุดของแท็พรูท ซึ่งก็คือการสร้างธุรกรรมอย่างมากความสามารถกว่าเดิม ที่มีรูปลักษณะไม่ต่างจากธุรกรรมสามัญทั่วไป ไม่สำคัญว่าเรากำลังสร้างะุรกรรมเรียบง่ายสมถะ หรือมากสมรรถภาพเชิงเทคนิคซับซ้อนแนบข้อกำหนดใช้งาน ก็ยังดูเหมือนเดิม

แท็พรูทปะทะเส็กวิท

เส็กวิท (SegWit) ก็คืออัปเกรดตัวบิ๊มที่มาก่อนแท็พรูท (Taproot)



มันประกอบไปด้วยหลายอย่าง รวมถึงค่าบ่งบอกเวอร์ชั่น ที่ใช้คู่กับผลลัพธ์เอาทุพุทสคริปท์แต่ละธุรกรรม

สำหรับเส็กวิทแล้ว ค่าตัวนี้ถูกตั้งไว้เป็น "Ø" ("SegWit vØ"). สำหรับแท็พรูท ค่าบ่งบอกคือ "1". จึงเป็นเหตุผลที่บางครั้ง เราเห็นชื่ออ้างอิงแท็พรูทสคริปท์ ว่า "SegWit V1".

ทั้งเส็กวิทและแท็พรูท เป็นการอัปเกรดคนละตัวกันที่ส่งผลแตกต่าง ให้กับผลลัพธ์เอาท์พุทรายธุรกรรมแยกประเภท แท็พรูทได้สร้างต่อยอด บนรากฐานการพัฒนาที่เส็กวิทปูทางเอาไว้

แท็พรูทอัปเกรดที่เกิดขึ้นมันคือซอฟท์ฟอร์ก

ดังนั้นแปลว่าการอัปเกรดที่กล่าวถึง ทำให้กฎฉันทามติ (consensus rules) กระชับยิ่งขึ้น หรือบีบรัดกฎระเบียบภายในเครือข่ายกระจายศูนย์ให้ชัดเจน การผ่านซอฟท์ฟอร์กแต่ละครั้ง จำเป็นต้องใช้แรงตอบรับ เป็นเสียงส่วนมากจากกลุ่มนักขุดเหมือง บิทคอยน์ไมเน่อร์ ในรูปแบบแฮชพาวเวอร์ (hashpower) แต่เป็นทางเลือกเสริมให้กับผู้ใช้ทั่วไป พฤติกรรมวิสามัญก่อนหน้าการเปลี่ยนแปลง ยังคงเป็นโมฆะภายหลังไม่เปลี่ยนจากเดิม และกลุ่มโหนดที่รันบิทคอยน์เวอร์ชั่นก่อน ๆ ยังสื่อสารกับโหนดเวอร์ชั่นใหม่ ๆ ได้ตามเคย