

ขอบคุณที่ให้เวลาอ่าน!

นี่เป็นแค่ภาพรวมสั้น ๆ ของแท็พรูท หวังว่าคุณได้อ่านอย่างเพลิดเพลิน พร้อมเรียนรู้เพิ่มเติมไหม? อยากพิมพ์ขึ้น (Zine) ฉบับนี้รึเปล่า? ไปดู



<https://satsie.dev/zines>

สำหรับสาระสำคัญเพิ่มเติม และเนื้อหาไม่ไกลไม่ไกลไปจาก สารสาส์นฉบับนี้

สารสาส์นลับของเชตตี้



แท็พรูท

ภาพรวมกะทัดรัดสำหรับบิตคอยน์ออฟเกรด
นามว่าแท็พรูท

8

แท็พรูทอัปเดตมืองค์ประกอบ 3 ชิ้นส่วน

- BIP-340: กลไกไฮรอสซอร์
- BIP-341: เมอร์เคิลไลซ์แอสสตรีก์
ซินแทกซ์ (MAST) + แท็พรูท
- BIP-342: แท็พสคริปต์

เมื่อมีการพูดถึงแท็พรูท ในบริบททั่วไป รวมถึงวิธีที่เราได้กล่าวถึงมัน ณ ตอนนี้อยู่ โดยปกติแล้วมันจะหมายถึงทั้ง 3 สิ่งนี้โดยรวมกัน

มาดูพวกมันอย่างใกล้ชิดกัน !!

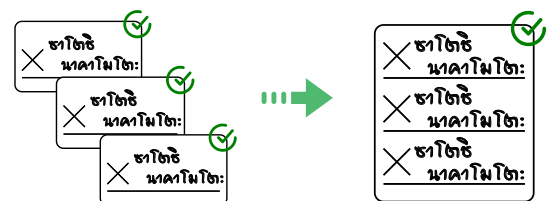
☆ BIP-340: กลไกไฮรอสซอร์ ☆

บิตคอยน์อิมพรูฟเมนต์โพรโทคอล (BIP) ตัวนี้เป็นกาเปิดตัว กลไกไฮรอสซอร์ที่ชื่อว่าซอร์เสริมโครงร่างลายเซ็นตัวใหม่ให้กับระบบ

เมื่อเปรียบเทียบกับโครงร่างลายเซ็นตัวก่อนที่ถูกใช้ภายในเครือข่ายบิตคอยน์ ที่เรียกกันว่า อีซีดีเอสเอ (ECDSA) แล้ว กลไกไฮรอสซอร์มีโครงร่างที่ปลอดภัยกว่า ใช้งานง่าย และมีประสิทธิภาพสูงกว่าเล็กน้อยให้กับผู้ใช้

☆ การตรวจสอบลายเซ็นแบบจับกลุ่ม ☆

การตรวจสอบลายเซ็นดิจิทัลโดยปกติจำเป็นต้องใช้การคำนวณซับซ้อนจากสมการคอมพิวเตอร์ ปัจจุบันเราสามารถจับกลุ่มลายเซ็นหลากหลาย ผ่านกระบวนการตรวจสอบเป็นกลุ่มก่อนเดียวกันได้ แทนที่การตรวจสอบทีละรายการ



☆ สิทธิสันโดษที่แข็งแกร่งกว่าเดิม ☆

บิตคอยน์เปิดทางให้ทุกคนกำหนดหนทางการใช้เหรียญของคุณตามชอบ ก่อนหน้าที่เรามี แท็พรูท ทุกหนทางในการสร้างธุรกรรม จำเป็นต้องเผยแพร่ข้อมูลที่ไปที่สาธารณะ ณ ช่วงเวลาชำระเงิน ก่อให้เกิดความเสี่ยงส่วนตัว โดยเฉพาะกับเหรียญ ที่มีข้อกำหนดกฎเกณฑ์รายจ่ายไว้ล่วงหน้า ทำให้ผู้ส่ดส่่งหวังร้าย ขุดคุ้ยธุรกรรมเกี่ยวข้องกับผู้ใช้ได้ง่าย

6

3

แท็พรูทอัปเกรดคืออะไรกันแน่ ?

แท็พรูทคือชุดการปรับปรุงที่ช่วยให้บิตคอยน์สามารถถูกใช้งานได้อย่างมีประสิทธิภาพในการขยายสมรรถภาพเสถียรยิ่งกว่าเดิม และรักษาความเป็นส่วนตัวได้ดีขึ้น

วันที่เปิดใช้งาน: พฤศจิกายน 2021
หมายเลขบล็อก: 709,632.

แท็พรูทเปิดทางฟิเจอร์เชิดเนื่อนน้ำ ๆ

☆ การรวมกุญแจสาธารณะและลายเซ็นดิจิทัล (MuSig) ☆

หากคุณมีกุญแจสาธารณะ (public key) ก, ข และ ค พวกมันสามารถใช้ร่วมกันเป็นกุญแจเดียวได้ สิ่งเดียวกันนี้ใช้กับลายเซ็นดิจิทัลที่สอดคล้องกันด้วย



นี่หมายความว่า การใช้หลายลายเซ็นที่ซับซ้อน สามารถพรางตาเหมือนกับการใช้กุญแจเดียวที่เกี่ยวข้องกับเพียงกุญแจเดียวเท่านั้น

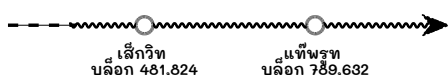
ด้วย Taproot สิ่งเดียวที่จำเป็นต้องเปิดเผยต่อสาธารณะ คือวิธีเฉพาะที่เหรียญถูกใช้ไป ไม่ใช่ความเป็นไปได้อื่น ๆ ทั้งหมด ซึ่งหมายความว่า:

1. ลดการเปลืองดาต้าบนบล็อก และ
2. ปกป้องสิทธิสันโดษมากกว่าเดิม

ด้วยหลาย ๆ ปัจจัยรวมกัน ทำให้เราเห็นความเด่นชัด และกรณีการใช้งานน่าประทับใจที่สุดของแท็พรูท ซึ่งก็คือการสร้างธุรกรรมอย่างมีความสามารถกว่าเดิม ที่มีรูปลักษณะไม่ต่างจากธุรกรรมสามัญทั่วไป ไม่สำคัญว่าเรากำลังสร้างธุรกรรมเรียบง่ายสมถะ หรือมากสมรรถภาพเชิงเทคนิคซับซ้อนแบบข้อกำหนดใช้งาน ก็ยังคงเหมือนเดิม

แท็พรูทปะทะเล็กวิท

เล็กวิท (SegWit) ก็คืออัปเกรดตัวบีมที่มาก่อนแท็พรูท (Taproot)



☆ BIP-341: สคริปต์แตกกิ่ง + แท็พรูท ☆

บีมตัวนี้สามารถแตกแขนงได้เป็น 2 ปัจจัย:

1. **สคริปต์แตกกิ่ง:** การจับกลุ่มและเข้ารหัสของโครงสร้างข้อมูลดาต้า (data-structures) เป็นเหมือนต้นไม้ เพื่อย่อขนาดตรรกะของหลาย ๆ สคริปต์ ในบิตคอยน์เดิมพุ่มเมทโพธิ์พอลตัวนี้ แต่ละกิ่งไม้ ของต้นไม้ดังกล่าว เป็นเหมือนตรรกะที่ได้จากสคริปต์เดียว และผู้ใช้จ่ายสามารถเลือกผลลัพธ์ปลายทางได้แค่ทางเดียว ผู้ใช้จ่ายขอในการแสดงผลของช่องทางตรรกะกิ่งที่เลือก (เราเรียกมันว่า "กิ่งเมอร์เคิล (Merkle branch)")
2. **แท็พรูท:** ทักษะที่ทำให้เราสามารถใช้จ่ายเหรียญด้วยกุญแจสาธารณะเปิดเผย (public key) หรือ จากผลลัพธ์อาทพุทที่ได้มาจากสคริปต์ แท็พรูทช่วยทุนแรงจากสมรรถภาพของเมอร์เคิลไลซ์แอ็บสแตรกท์ ซินแทคส์ทรี (MAST) และกลไกไซรส์ชันอร์ให้เราสร้างธุรกรรมได้อย่าง **ยืดหยุ่น, ลับตา และคล่องประสิทธิภาพ** ด้วยแท็พรูท คุณเองก็สามารถตั้งกฎเกณฑ์ควบคุมรายจ่ายนานา แล้วค่อยเผยแพร่เฉพาะทางที่ใช้เวลาชำระได้

☆ BIP-342: แท็พสคริปต์ ☆

สคริปต์ก็คือ **ชื่อตั้งไรจินตนาการ** ชื่อสำหรับภาษาเขียนตรรกะอัจฉริยะ (smart contract) บนเครือข่ายกระจายศูนย์บิตคอยน์ แท็พสคริปต์เป็นเหมือนภาษาที่วิวัฒนาการมาต่อเนื่องจากเดิม และรองรับการใช้งาน กลไกไซรส์ชันอร์บวกกับแท็พรูท

มันประกอบไปด้วยหลายอย่าง รวมถึงค่าบงบอกเวอร์ชัน ที่ใช้คู่กับผลลัพธ์อาทพุทสคริปต์แต่ละธุรกรรม

สำหรับเล็กวิทแล้ว ค่าตัวนี้ถูกตั้งไว้เป็น "0" ("SegWit v0"). สำหรับแท็พรูท ค่าบงบอกคือ "1". จึงเป็นเหตุผลที่บางครั้ง เราเห็นชื่ออ้างอิงแท็พรูทสคริปต์ ว่า "SegWit V1".

ทั้งเล็กวิทและแท็พรูท เป็นการอัปเกรดคนละตัวกันที่ส่งผลแตกต่าง ให้กับผลลัพธ์อาทพุทรายธุรกรรมแยกประเภท แท็พรูทได้สร้างต่อยอด บนรากฐานการพัฒนาที่เล็กวิทปูทางเอาไว้

แท็พรูทอัปเกรดที่เกิดขึ้นมันคือซอฟต์แวร์ฟอร์ก

ดังนั้นแปลว่าการอัปเกรดที่กล่าวถึง ทำให้กฎฉันทามติ (consensus rules) กระชับยิ่งขึ้น หรือบีบรัดกฎระเบียบภายในเครือข่ายกระจายศูนย์ให้ชัดเจน การผ่านซอฟต์แวร์ฟอร์กแต่ละครั้ง จำเป็นต้องใช้แรงตอบรับ เป็นเสียงส่วนมากจากกลุ่มนักขุดเหมือง บิตคอยน์ไมเนอร์ ในรูปแบบแฮชพาวเวอร์ (hashpower) แต่เป็นทางเลือกเสริมให้กับผู้ใช้ทั่วไป พฤติกรรมวิสามัญก่อนหน้าการเปลี่ยนแปลง ยังคงเป็นโมฆะภายหลังไม่เปลี่ยนจากเดิม และกลุ่มโหนดที่รันบิตคอยน์เวอร์ชันก่อน ๆ ยังสื่อสารกับโหนดเวอร์ชันใหม่ ๆ ได้ตามเคย