ขอบคุณที่ให้เวลาอ่าน!

นี่เป็นแค่ภาพรวมสั้น ๆ ของแท็พรูท หวังว่าคุณได้อ่านอย่างเพลิดเพลิน พร้อมเรียนรู้เพิ่มเติมไหม ? อยากปรินท์นิตยสารกะทัดรัดฉบับนี้รีเปล่า ? ไปดู

https://satsie.dev/zines

เพื่อทรัพยากรเสริม และเนื้อหาไม่ใกล้ไม่ไกล ไปจาก สารสาส์นฉบับนี้

แท็พรูท

ภาพรวมกะทัดรัดสำหรับบิทคอยน์อัพเกรด นามว่าแท็พรูท

แท็พรูทอัปเกรดมีองค์ประกอบ 3 ชิ้นส่วน

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

เมื่อมีการพูดถึงแท็พรูท ในบริบทท่วไป รวมถึงวิธีที่เราได้กล่าวถึงมัน ณ ตอนนี้ โดยปกติแล้วมักจะหมายถึงทั้ง 3 สิ่งนี้โดยรวมกัน

มาดูพวกมันอย่างใกล้ชิดกัน !!

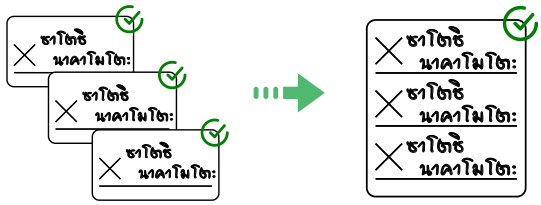
☆ BIP-34Ø: กลไกไขรหัสชนอร์ ☆

บิทคอยน์อิมพรูฟเมนท์โพรโพซอล (BIP) ตัวนี้เป็นการเปิดตัว กลไกไขรหัสที่ชื่อว่าชนอร์ เสริมโครงร่างลายเซ็นตัวใหม่ให้กับระบบ

เมื่อเปรียบเทียบกับโครงร่างลายเซ็นตัวก่อนที่ถูกใช้ภายในเครือข่ายบิทคอยน์ ที่เรียกกันว่า อีซีดีเอสเอ (ECDSA) แล้ว กลไกไขรหัสชนอร์มอบโครงร่างที่ปลอดภัยกว่า ใช้งานง่าย และมีประสิทธิภาพสูงกว่าเล็กน้อยให้กับผู้ใช้

☆ การตรวจสอบลายเซ็นแบบจับกลุ่ม ☆

การตรวจสอบลายเซ็นดิจิทัลโดยปกติจำเป็นต้องใช้การคำนวณซับซ้อนจากสมองกลคอมพิวเตอร์ ปัจจุบันเราสามารถจับกลุ่มลายเซ็นหลากหลาย ผ่านกระบวนการครวจสอบเป็นกลุ่มก้อนเดียวกันได้ แทนที่การตรวจสอบทีละรายการ



☆ Better privacy while spending ☆

bitcoin allows you to specify multiple ways to spend a coin. Prior to Taproot, all these ways had to be made public when the coin was spent. This is bad for privacy, especially for coins with unique spending rules, making them easy to identify.

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: Script Trees + Taproot ☆
This BIP is made of 2 thigs:

1. **Script trees:** Tree-like data structures used to compactly encode multiple scripts. In this BIP, each leaf represents a single script and only one leaf may be chosen by the spender. The spender is responsible for showing the path of the leaf (AKA the "Merkle branch").
2. **Taproot:** A technique that allows a coin to be spent by public key OR by script. Taproot leverages the power of MAST and Schnorr to make transactions more **flexible, private and efficient.** With Taproot, you can set up many different spending constraints, but only reveal the one that is used!

☆ BIP-342: Tapscript ☆
Script is the ~~terribly uncreative~~ name for ***bitcoin***'s smart contract language. Tapscript is an upgraded scripting language that supports Schnorr and Taproot.

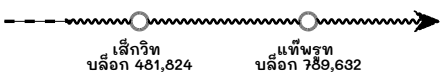
With Taproot, the only thing that needs to be public is the specific way in which a coin was spent, not all other possibilities. This means:

1. ลดการเปลืองดาต้าบนบล็อก และ
2. ปกป้องสิทธิสันโดษมากกว่าเดิม

Together, many features contribute to what is perhaps Taproot's most impressive use case: making many different ways of spending *bitcoin* indistinguishable from one another. It doesn't matter how simple or complex the spending rules are.

แท็พรูทปะทะเส็กวิท

เส็กวิท (SegWit) ก็คืออัปเกรดตัวบึ้มที่มาก่อนแท็พรูท (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