비트코인 볼트(Bitcoin Vault): 고차원의 보안성을 지닌 디지털 골드

Eyal Avramovich
github.com/bitcoinvault

초록. 비트코인에 대한 나카모토 사토시(Satoshi Nakamoto)의 비전은 개인 간(P2P) 거래 가능한 디지털 화폐를 만드는 것이었습니다. 이 프로토콜을 성공리에 구현한 여러 포크의 대다수는 이 비전을 개선해서 더욱 확장 가능하고 효율적인 결제 시스템을 제공하려고 노력했습니다. 우리는 비트코인이 내놓은 가장 중요한 약속은 교환 매체가 아니라 가치 저장 수단의 역할이라고 봅니다. 현금이 아니라 더욱 나은 금인 셈입니다. 우리는 궁극적인 디지털 가치 저장소를 만들어 이 약속을 이행하기 위하여 원래의 프로토콜을 바탕으로 일련의 수정 작업을 거친 버전을 제안합니다. 비트코인의 유효 트랜잭션 확인 시간을 10분에서 24시간으로 늘림으로써 금의 대용물인 비트코인이 지닌 가장 큰 결함을 해결할 수 있습니다. 그 결함은 바로 도난에 취약하다는 점입니다. 이 시스템은 커피값 결제보다는 노후 대비 평생 저축을 마음 편하게 보유하는 데 맞추어져 있습니다. 모든 트랜잭션에 대하여 체인에서 144개 블록에 걸쳐서 경고해주고 긴급시에는 이전에는 사용하지 않았던 응급 복구 키로 취소할 수 있기 때문에 취약점이 없는 시스템입니다. 이 시스템의 부트스트랩은 하드포크를 통하지 않고 보다 공정하고 신속한 채굴 메커니즘을 통하기 때문에 짧은 기간 내에 이 시스템이 비트코인을 따라잡을 수 있게 됩니다. 우리는 도난 방지 디지털 금의 비전을 수립한 비트코인 로얄(Bitcoin Royale) 백서[1]의 제작자에게 모든 공을 돌리고 싶습니다. 우리 팀은 그 아이디어를 바탕으로 진행해서 아래에서 언급하게 될 중요한 기능을 모두 구현해 나가고 6.2절에서 설명할 추가 기능인 세 번째 개인 키 솔루션으로 더욱 발전시킬 예정입니다.

1. 소개

비트코인[2]은 2009년에 시작된 혁신적인 분산형 결제 시스템으로, 신뢰할 수 있는 금융 기관을 거치지 않고서 당사자들끼리 직접 트랜잭션 할 수 있습니다. 이 시스템은 신뢰할 수 있는 운영자 없이 분산 원장(distributed ledger)을 유지하기 위해 작업 증명에 의존합니다. 이 시스템은 정직한 노드가 협력하는 공격자 노드 그룹보다 많은 CPU 전원을 제어하는 한 안전합니다. 비트코인의 창시자인 나카모토 사토시(Satoshi Nakamoto)는 비트코인을 "디지털 화폐 시스템"이라고 설명했습니다.

비트코인 코드 베이스의 포크 형태로 원래 프로토콜을 성공적으로 수정한 버전 여러 가지가 여러 해에 걸쳐 출시되었습니다. 여기에는 트랜잭션 확인 시간을 줄이고 GPU와 같은 소비자급 하드웨어를 선호하도록 작업 증명 알고리즘을 변경하여 2011년에 출시된 라이트코인(Litecoin)[3], 블록 크기를 늘려 원래 프로토콜의 트랜잭션 처리량을 확장하여 2017년에 출시된 비트코인 캐시(Bitcoin Cash)[4]. 그리고 해싱 알고리즘을 변경하여 특수 채굴 장비를 폐기하면서 2017년에 출시된 비트코인 골드(Bitcoin Gold)[5] 등이 포함됩니다.

원래 비전에 충실하게도, 이러한 포크 및 기타 포크의 주요 초점은 비트코인을 더 나은 결제 시스템으로 만드는 데 맞춰져 있습니다. 높은 트랜잭션 수수료, 10분의 확인 시간, 초당 약 4개에 불과한 트랜잭션 처리량 등 원래 프로토콜의 한계로 인해 오늘날 비트코인은 중앙 집중식 온라인 결제 시스템과 경쟁할 수 없습니다.

2. 디지털 화폐 또는 디지털 골드

비트코인은 디지털 화폐로는 소비자의 선택을 별로 받지 못했지만, 디지털 금 형태로는 큰 성공을 거두었습니다. 업계에서는 비트코인이 트랜잭션 수단으로서 가치가 있는지 또는 실제로 가치 저장 수단으로서 우수한지에 대한 오랜 논쟁이 있었습니다. 금은 일상 용품과 서비스에 대한 효과적인 결제 수단이 아닙니다. 소비자는 주로 금에 투자해서 인플레이션에 대비하고 향후 구매력을 유지합니다. 국가 통화와는 다르게 비트코인은 고정 통화 정책과 제한된 공급량으로 인해 특히 매력적입니다.

역사를 살펴보면 어떤 시스템을 동시에 여러 가지 목표를 달성하도록 설계하는 것은 거의 불가능하다는 사실이 드러납니다. 비트코인을 교환 수단으로 최적화하면 가치 저장 수단으로의 잠재력이 줄어듭니다. 또한 디지털 화폐에 필요한 유용성을 추가로 희생하면 디지털 금으로의 유용성을 크게 향상할 수 있습니다. 본 백서에서는 한 가지 목표에 중점을 두고 원래의 비트코인 프로토콜을 기반으로 일련의 수정을 제안하여 최고의 가치를 창출하고자 합니다.

온라인 결제 시스템으로의 경쟁력에 중점을 두지 않으면 수수료나 트랜잭션 처리량에 치중할 필요가 없습니다. 어쨌든, 금은 운송 비용이 많이 들며, 대체로 장기 투자 목적으로 구입합니다. 우리가 특히 노력하게 될 특성은 트랜잭션 확인 시간입니다. 이러한 점에서, 평균 10분 정도인 비트코인의 확인 시간을 크게 늘리는 등의 절충을 하면 중요한 이점을 확보할 수 있습니다. 우리가 10분 안에 금을 다른 곳으로 배송할 수 있을 것으로 기대하지 않기 때문에 이러한 희생은 자연스러워 보입니다.

3. 도난 문제

가치 저장 수단의 핵심 요건은 보존 가능성입니다. 도난은 가치 있는 품목을 취급할 때 발생하는 손실의 주요 위험 중 하나입니다. 금은 이와 관련하여 오히려 더 나은 특성을 보입니다. 금을 현실에서 훔치는 것은 디지털 자산에 대하여 가상 공격을 하는 것보다 훨씬 위험합니다. 또한 훔친 자가 금을 숨기는 데 있어서, 특히 국경을 이동하여 상당량의 훔친 금을 숨기는 데 어려움을 겪습니다. 대량의 훔친 금을 익명으로 세탁하고 매각하는 것도 간단한 일이 아닙니다.

유감스럽게도, 비트코인은 상대적으로 열악합니다. 자금은 프로토콜에 의해 암호화 개인 키 세트로 보호됩니다. 공격자가 이러한 키에 대한 전자 액세스 권한을 확보하면 모든 자금을 원격으로 즉각 돌이킬 수 없이 차지하게 됩니다. 트랜잭션이 익명으로 이루어지고, 믹서를 사용하여 추적을 방해할 수 있으며[6], Sybil 아이덴티티를 대량으로 생성할 수 있기 때문에 훔친 자금의 세탁도 훨씬 쉽습니다. 그 결과로, 2018년에 10억 달러를 도난당하는 등 암호화폐 도난이 증가하고 있습니다[7]. 커뮤니티에서 선별한 주요 사건 목록[8]을 보면 최신 보안 관행에 정통한 전문 기관조차도 공격에 취약하다는 것을 알 수 있습니다.

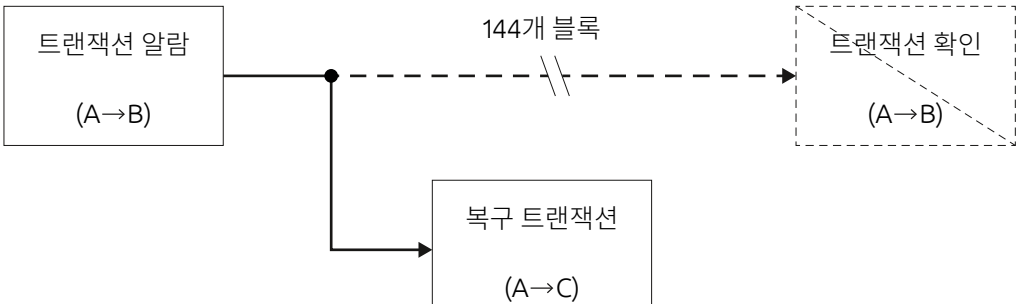
최종 사용자가 개인 키를 안전하게 관리하는 것이 비트코인의 주요 과제 중 하나인 것으로 나타나고 있습니다. 자금과의 상호 작용을 위해 키를 정기적으로 사용해야 하고 서명한 트랜잭션을 인터넷을 통해 전송해야 하므로 모든 키는 결국 취약해지기 마련입니다. "핫" 월렛과 "콜드" 월렛 간에 자금을 분할하는 등의 보안에 민감한 관행은 번거로우며 문제를 근본적으로 해결하지 못합니다. 발생한 사건을 살펴보면 핫 월렛은 불가피하게 많은 양을 보유하고 있으며[9, 10] 콜드 월렛을 사용하면 키와의 상호 작용은 줄어들지만, 완전히 없앨 수는 없습니다[11].

4. 도난 방지 솔루션

도난을 없애는 방안으로 새롭고 정교한 잠금 스크립트 및 프로토콜 수정에 기반한 솔루션을 제안합니다. 새 잠금 스크립트를 사용하여 수행한 트랜잭션은 기본적으로 24시간 동안 지연됩니다. 채굴자가 새 블록에 트랜잭션을 추가하면 트랜잭션이 더 이상 즉시 커밋되지 않습니다. 대신, 144개의 블록 지속 시간 동안 알람으로써 온 체인에서 추가됩니다(블록 시간 10분 가정). 144개의 블록 동안 방해받지 않으면 트랜잭션 상태가 알람에서 "확인됨"으로 변경됩니다.

온 체인 알람의 장점은 코인이 옮겨질 때마다 검열 불가한 사전 통지를 코인 소유자가 받을 수 있다는 것입니다. 소유자는 24시간 이내에 알람에 대해 조치를 취해야 하며 승인되지 않은 경우 이전을 무효로 할 수 있습니다. 지연 인출은 관리 지갑과 전통적인 은행 시스템에서 효과가 입증된 도난 방지 업계 표준입니다. 예를 들어 코인베이스 볼트(Coinbase Vault)[12]의 대기 시간은 48시간입니다. 당사에서 제안하는 솔루션은 신뢰할 수 있는 타사 없이 동일한 보호 기능을 제공합니다.

알람 상태인 트랜잭션의 긴급 무효화에는 특별한 복구 트랜잭션이 필요하며 24시간의 지연 없이 즉시 수행됩니다. 복구 트랜잭션에는 지갑 생성 중 잠금 스크립트에 통합되어야 하는 특수 복구 키가 필요합니다. 지정한 지갑에 복구 키를 한 번 등록하면 변경할 수 없습니다.



긴급 무효화에 사용된 개인 복구 키는 이전에 사용된 적이 없는 새로운 키입니다. 이 키는 오프라인에서 생성할 수 있으며, 인터넷에 연결하거나 장치에 입력해서는 안 됩니다. 등록 프로세스에는 이 키의 공개 부분만 필요하므로 개인 키를 사용하지 않은 채로 유지할 수 있습니다. 가끔 사용해야 하며, 따라서 도난에 취약한 콜드 월릿 키와는 달리, 복구 키는 긴급 무효화 자체에서만 처음으로 사용하므로 도난 방지 기능을 완전히 이용할 수 있습니다. 사용 후의 복구 키는 손상된 것으로 간주하며, 모든 자금은 즉시 새로운 미사용 복구 키로 보호되는 새 지갑으로 이체해야 합니다.

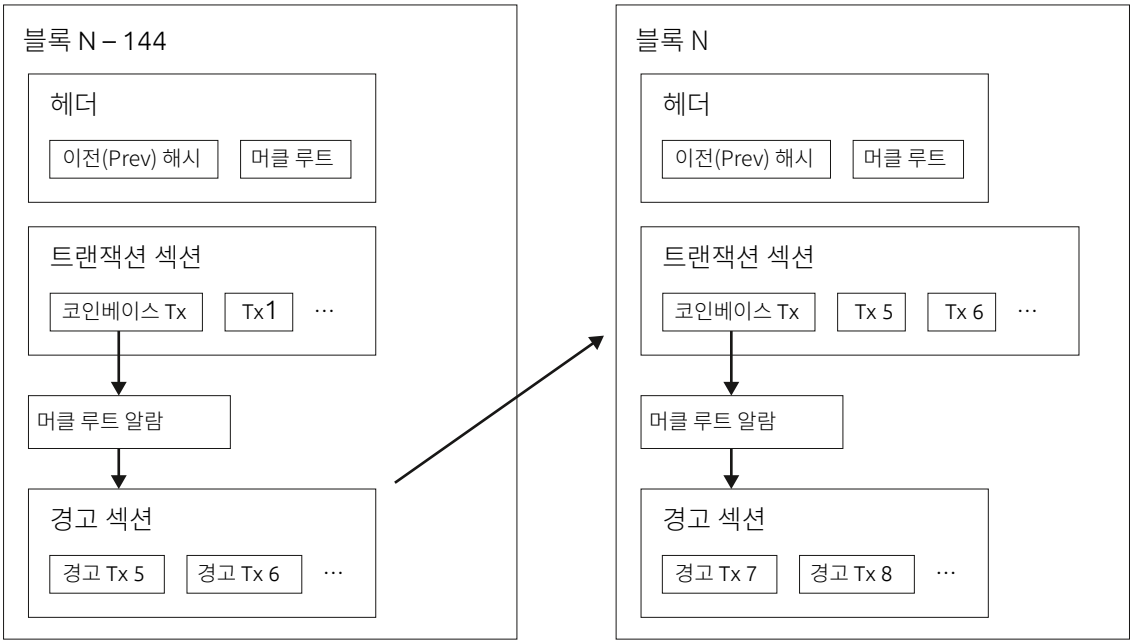
비트코인 로얄(Bitcoin Royale)의 원래 디지털 금 개념은 시스템의 모든 트랜잭션을 24시간 동안 지연시켜 코인을 안전하고 느리게 움직이는 가치 저장소로 만들었습니다. 우리는 이 개념을 확장하여 보안에 대한 타협 없이 두 가지 세계 (디지털 금 및 디지털 화폐)를 최대한 활용할 계획입니다.

느리게 진행되는 알람와 함께 우리는 빠르게 움직이는 "인스턴트" 트랜잭션을 조건부로 유지합니다. 최고의 보안을 제공하기 위해, 그러한 트랜잭션을 보내려면 사용자가 지갑 생성 중 제공된 세 번째 키를 사용하여 블록체인 기반의 2FA를 수행해야 합니다.

5. 블록

원래의 비트코인 프로토콜과 마찬가지로 모든 블록에는 확인된 트랜잭션 목록이 포함되어 있으며 이러한 트랜잭션의 머클(Merkle) 루트 해시를 블록 헤더에 보유합니다. 일부 트랜잭션은 24시간 온 체인을 기다려야 하므로 블록의 트랜잭션 섹션에 즉시 추가할 수 없습니다. 그 대신 원래의 비트코인 프로토콜에 존재하지 않는 새로운 특수 섹션인 알람 섹션에 추가됩니다. 알람 섹션의 머클 루트 해시는 원래의 비트코인과 블록 헤더 호환성을 유지하는 코인베이스 트랜잭션의 입력에 저장됩니다.

새로운 블록이 채굴될 때, 채굴자는 144개의 블록을 되돌아보고 블록 N-144의 알람 섹션을 검사합니다. 여전히 유효한 트랜잭션에 대한 모든 알람이 확인되고 새 블록의 트랜잭션 섹션을 채웁니다.



채굴 블록 N의 단계는 다음과 같습니다.

1) 블록 N 알람 섹션에 새로운 일반 트랜잭션을 추가합니다(확인되지 않음).
2) 블록 N 트랜잭션 섹션에 새로운 인스턴트 트랜잭션을 추가합니다(확인됨)
3) 블록 N 트랜잭션 섹션에 새로운 복구 트랜잭션을 추가합니다(확인됨).
4) 블록 N-144 알람 섹션으로 이동하여 블록 N 트랜잭션 섹션에 유효한 트랜잭션을 추가합니다(확인됨).

6. 스크립트

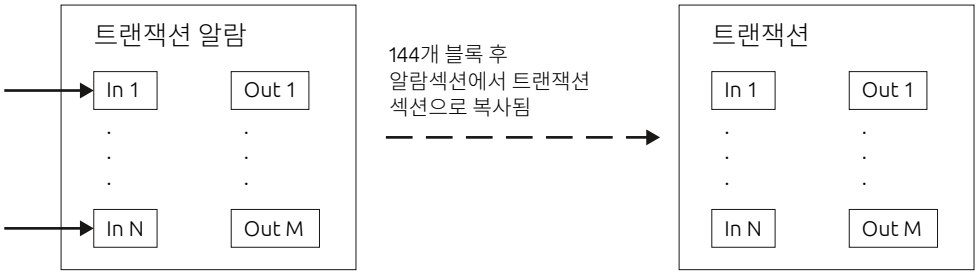
비트코인 볼트의 핵심 기능은 정교한 잠금 스크립트를 통해 사용할 수 있으며 잠금 해제 스크립트에 표시되는 서명 수에 따라 다르게 작동합니다. 다음의 두 가지 변형을 사용할 수 있습니다.

1. 알람 잠금 스크립트 - 한 개 또는 두 개의 서명이 필요합니다. 한 개의 서명이 표시되면 알람 트랜잭션이 생성됩니다. 두 개의 서명이 표시되면 복구 트랜잭션이 생성됩니다.

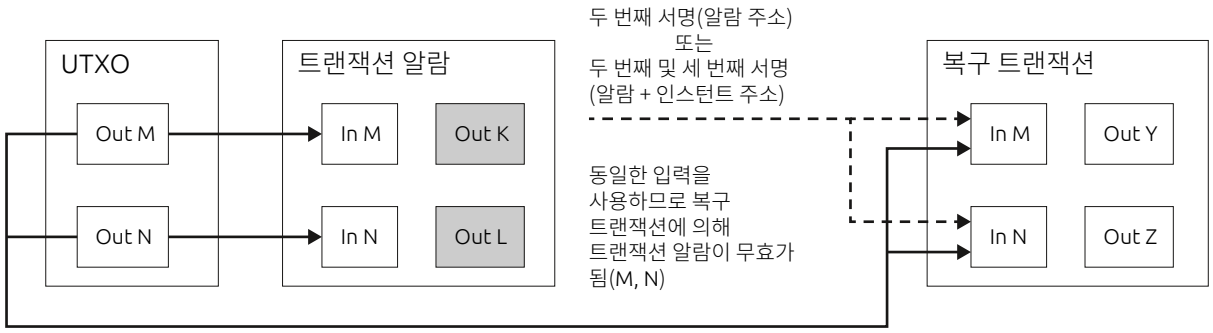
2. 알람 + 인스턴트 잠금 스크립트 - 한 개, 두 개 또는 세 개의 서명이 필요합니다. 한 개의 서명이 표시되면 알람 트랜잭션이 생성됩니다. 두 개의 서명이 표시되면 인스턴트 트랜잭션이 생성됩니다. 세 개의 서명이 모두 표시되면 복구 트랜잭션이 생성됩니다.

7. 트랜잭션

코인 전송은 비트코인 프로토콜과 동일한 일반 트랜잭션을 사용하여 수행됩니다. 알람 섹션에서 트랜잭션 섹션으로 이동해도 형식이 변경되지 않습니다.



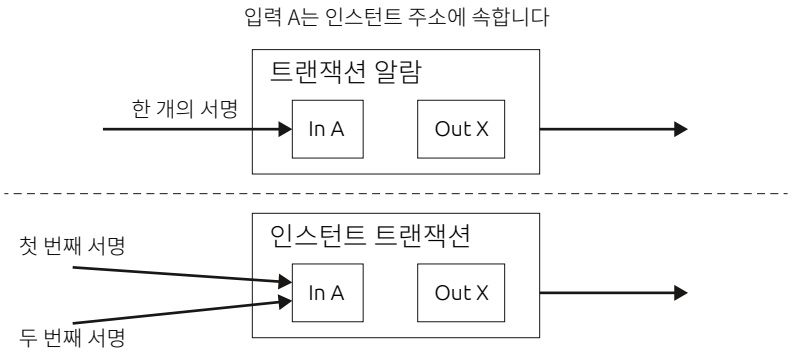
7.1. 복구 트랜잭션



복구 트랜잭션은 복구된 경고와 동일한 UTXO를 사용합니다. 차이점은 동일한 UTXO에 더 많은 서명을 제공한다는 것입니다. 알람 잠금 스크립트의 경우 2개, 알람 + 인스턴트 잠금 스크립트의 경우 3개. 복구 트랜잭션이 처리되면 복구된 UTXO가 소비되므로 이 UTXO에 의존하는 기존 알람이 무효가 되고 트랜잭션의 24시간 지연이 지난 후에 경고 확인이 방지됩니다.

7.2. 인스턴트 트랜잭션

인스턴트 트랜잭션을 통해 트랜잭션 확인에 대한 기본 24시간 지연을 무시하고 트랜잭션 확인 속도를 약 10분으로 단축할 수 있습니다. 그 메커니즘은 멀티시그(multisig) 지갑과 유사합니다. 이때 별도의 위치에 안전하게 저장해야 하는 별도의 개인 키에서 추가 서명이 필요합니다. 그래서 인스턴트 트랜잭션은 특별한 P2SH 주소(알람 + 인스턴트 잠금 스크립트에서 생성된 인스턴트 주소)에서만 보낼 수 있습니다.



8. 호환성

우리의 구상은 그 프로토콜을 표준 비트코인 프로토콜과 최대한 호환시키려는 것입니다. 기본적인 목표는 기존 비트코인의 전체 노드, 지갑, 풀, 채굴자 등에 대하여 필요한 코드 변경을 최소화하는 것입니다. 그렇지만 기존의 블록체인에서 그러한 변경을 수행하려면 하드포크가 필요합니다

블록 헤더의 형식을 변경해서 코인이 비트코인 ASIC 채굴자와 호환이 불가능해지는 것을 피하기 위하여 경고 섹션의 머클 루트 해시는 표준 코인베이스 트랜잭션의 입력에 저장됩니다.

하드포크가 필요한 경우 기존의 코인 사용자가 최대한 쉽게 전환할 수 있게 하는 것이 우리의 목표입니다. 기존의 모든 스크립트 유형의 동작은 변경되지 않으므로 하드포크 이전에 존재하는 모든 코인은 일반적인 방식으로 사용할 수 있습니다. 그렇지만 보다 안전한 새 스크립트로 전환하는 것을 강력하게 권장합니다.

9. 인센티브

본 시스템은 지난 10년 동안 성공한 것으로 입증된 인센티브 모델을 비트코인으로부터 차용했습니다. 알람을 통합하려면 이 모델을 조금 수정해야 합니다. 채굴자는 생산량과 투입량의 차이를 바탕으로 계산되는 수수료 약속에 의해 트랜잭션 알람을 블록에 포함하도록 장려됩니다. 수수료는 향후 블록 트랜잭션에서 계산되어 트랜잭션 알람을 포함하여 원래 채굴자에게 분배됩니다.

미래의 채굴자는 여전히 새로운 블록 채굴, 신규 인스턴트, 등록, 복구 트랜잭션 등에 대하여 블록 보상을 받으며, 트랜잭션 경고로부터 향후 수수료를 받게 된다는 약속을 받습니다. 미래의 채굴자는 합의된 규칙에 따라 N-144 블록에서 복구된 것을 제외하고 트랜잭션 섹션에 대한 모든 알람을 포함해야 합니다.

알람이 취소된 경우, 그 경고에 대한 원래 채굴자의 수수료는 복구할 수 없으며 총비용은 원래 경고의 수수료에 복구 트랜잭션에 대한 수수료를 더한 금액입니다.

10. 관련된 작업

우리는 비트코인 약정(Bitcoin Covenants)에 관한 Malte M ser 등의 작업에 특히 깊은 인상을 받았습니다[13]. 이들이 비트코인 스크립트 언어를 확장함으로써 향후 코인 사용에 대한 제한이 가능해졌고, 이 제한은 다양한 보안 조치를 실행하는 데 사용될 수 있습니다. 그중 주요한 사항은 볼트(Vault) 트랜잭션으로, 우리가 제안하는 지연 인출 메커니즘과 유사합니다.

우리는 지갑에 의해 실행될 재귀 배열의 커스텀 스크립트가 필요 없는 더 단순한 실행을 선택했습니다. 우리의 제안은 선택적인 확장 이상이며, 트랜잭션에 광범위한 의무적 영향을 미치는 프로토콜을 근본적으로 변화시키는 것입니다. 실행의 부담을 채굴자가 지게 하고 최종 사용자의 트랜잭션 경험을 기본 사항과 동일하게 유지하면 진정한 디지털 골드를 창출하는 임무를 더 잘 수행할 수 있습니다.

참고 자료

1. Ian Duoteli Fleming, https://bitcoinroyale.org/bitcoinroyale.pdf
2. S. Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System”, https://www.bitcoin.org/bitcoin.pdf, 2008.
3. Litecoin Project, “Litecoin, open source P2P digital currency”, https://litecoin.org, 2014.
4. “Bitcoin Cash”, https://www.bitcoincash.org, 2018.
5. bitcoingold.org, “Bitcoin Gold”, https://bitcoingold.org, 2018.
6. J. H. Ziegeldorf, F. Grossmann, M. Henze, N. Inden, and K. Wehrle, “Coinparty: Secure multi-party mixing of bitcoins”, In: *CODASPY ’15*, 2015.
7. CipherTrace, “Cryptocurrency Anti-Money Laundering Report, 2018 Q4”, https://ciphertrace.com/crypto-aml-report-2018q4, 2019.
8. “BLOCKCHAIN GRAVEYARD”, https://magoo.github.io/Blockchain-Graveyard, 2019.
9. C. Zhao, “Binance Security Breach Update (May 7 2019)”, https://binance.zendesk.com/hc/en-us/articles/360028031711, 2019.
10. J. Buck, “Coincheck: Stolen $534M In NEM Were Stored On Low Security Hot Wallet“, https://cointelegraph.com/news/coincheck-stolen-534-mln-nem-were-stored-on-low-security-hot-wallet, 2018.
11. J. Preissler, “Important Notice: Only trade TIO on trade.io”, https://medium.com/@trade.io/important-notice-only-trade-tio-on-trade-io-823d59fd7104, 2018.
12. KM. Cutler, “Coinbase Launches A More Secure Bitcoin Storage Option Called ‘Vault’”, https://techcrunch.com/2014/07/02/coinbase-vault, 2014.
13. M. M ser, I. Eyal, E. G n Sirer, “Bitcoin Covenants”, In: *Financial Cryptography and Data Security, FC 2016, Lecture Notes in Computer Science*, Vol. 9604. Springer, Berlin, Heidelberg.