Bitcoin Vault 백서

Eyal Avramovich, Kacper Wiśniewski, Piotr Kozłowski, Radek Popiel et Anon

백서 v1.0

개요

2009년 익명의 사람 또는 익명의 개발팀은 블록체인 기술을 기반으로 사용자 간 익명의 해시 주소로 자금을 이체하는 최초의 P2P 네트워크를 만들었습니다. Bitcoin 혁명이 시작된 것입니다. 결과적으로 기존 개념에 일련의 포크를 만들어내게 되었습니다.

그중 하나가 Bitcoin Vault라는 개념으로 이어졌습니다.

개발자로서 저희의 목표는 지갑 주소 관리, 개인 및 공개 키 저장, 개인 간 자산 이체 등에 사용자의 제어권을 강화하고 보안 수준을 높일 수 있는 유일한 기능으로 기존 블록체인을 업그레이드하는 것이었습니다. 암호화폐가 주는 유연성을 훼손하지 않고 사용자가 쉽고 편리한 방법으로 자산을 최대한 제어할 수 있는 부가 기능과 함께 Bitcoin의 모든 장점을 제공하는 코인을 만들고 싶었습니다.

분산형 Ledger의 핵심 기능인 블록체인의 불변성을 통해 장점뿐 아니라 손실, 분실, 또는 도난과 같은 위험도 경험해 보았습니다. 코딩을 여러 번 변경하고 개인 키 및 공개 키가 해당 블록체인 생태계에서 사용되는 방식을 통해 블록체인의 불변성을 훼손하지 않고 되돌릴 수 없었던 거래를 되돌리는 아이디어를 생각해냈습니다.

내용

소개

Bitcoin Vault (BTCV) 는 알파 체인으로 2019년에 출시되었습니다. BTCV는 2019년 12월부터 2020년 11월 사이에 크게 발전했고 이 기간에 해당 블록체인에서 거래를 되돌릴 수 있도록 하는 주요 기능이 공개되었습니다.

Bitcoin Vault는 사용자가 블록체인에 거래를 기록하고 취소할 수 있는 세계 최초의 암호화폐입니다. 이러한 혁신적인 접근 방식은 144 블록(또는 약 24시간) 내에 결제를 확인하는 맞춤형 블록체인 프로토콜을 통해 가능합니다. 이 기능은 키 도난이나 실수 혹은 버그로 인한 사용자의 자금 손실을 방지합니다.

Bitcoin Vault는 Bitcoin Royale의 하드포크이며 개인 키 하나를 더 추가해 총 3개의 키가 있습니다. 2019년에 출시된 이후 2022년 이후까지 확장되는 야심 찬 로드맵에 따라 기술과 시장 기반을 확대했습니다.

문제 기술서

CipherTrace의 2020년 봄 암호화폐 범죄와 자금 세탁에 관한 보고서에 따르면, 2020년 첫 5개월 동안 암호화 도난, 해킹, 사기 등은 총 13억 6천만 달러였습니다.

암호화폐 거래소는 실수로 잘못된 주소로 송금된 사용자의 자금을 매일 복구해야 합니다. 이 경우 시간과 비용이 소요되며 사용자 자금의 복구는 보장되지 않습니다.

매일 암호화 자산, 코인, 토크가 잘 알려진 사기 주소나 해커로 또는 중간자 유형의 공격으로 얼마나 많이 분실되고 있는지에 대한 믿을 만한 출처가 없습니다.

사용자가 실수했거나 자산이 도난당했거나 누군가가 암호화폐 지갑에 무단으로 액세스한 것을 알게 되는 즉시 거래를 취소하고 되돌릴 수 있다면 언급했던 피해 사례 중 상당 부분은 피할 수 있을 것이라 믿습니다.

미션 & 비전

BTCV는 사용자가 블록체인에서의 특정 유형의 거래를 되돌릴 수 있는 3-Key 보안 솔루션을 기반으로 추가 보안 수준을 제공하기 위해 개발되었습니다. 사용자 투명성과 자유 등의 중요한 기능을 추가함과 동시에 Bitcoin의 모든 편리한 것을 제공합니다. Bitcoin Vault는 지난 10년 동안 암호화 커뮤니티가 직면한 다음의 문제에 대한 저희의 해결책입니다.

1. 해킹이나 사용자 개인 키 액세스로 인한 지갑 무단 액세스,
2. 암호화 자산을 잘못된 지갑 주소로 보내거나 이체 금액을 잘못 입력하거나 다른 이체 금액과 합쳐서 송금하는 등의 실수,
3. 암호화폐 소프트웨어와 관련된 오류, 버그 및 기타 문제.

BTCV의 개발은 사회의 상당 부분이 글로벌 암호화 커뮤니티에 참여하는 것을 방해하는 것은 보안 및 안전 기능, 사용자 편의와 사용자 경험의 부족이라 믿어 해당 사항의 개발에 중점을 두고 있습니다.

BTCV 접근법

암호화폐는 사용자가 P2P 네트워크를 통해 자금을 저장하고 관리하며 전송하는 방법에 대한 자유와 책임을 사용자에게 부여했습니다. 본 백서에서는 모든 암호화폐 사용자가 개인 키 및 공개 키의 개념을 숙지하고 키를 안전하게 저장하고 보호하는 방법을 알고 있다고 가정합니다. 이 가정을 기점으로 다양한 유형의 거래에서 키 관리 및 사용에 대한 새로운 접근 방식을 개발했습니다.

3-Key 보안 솔루션

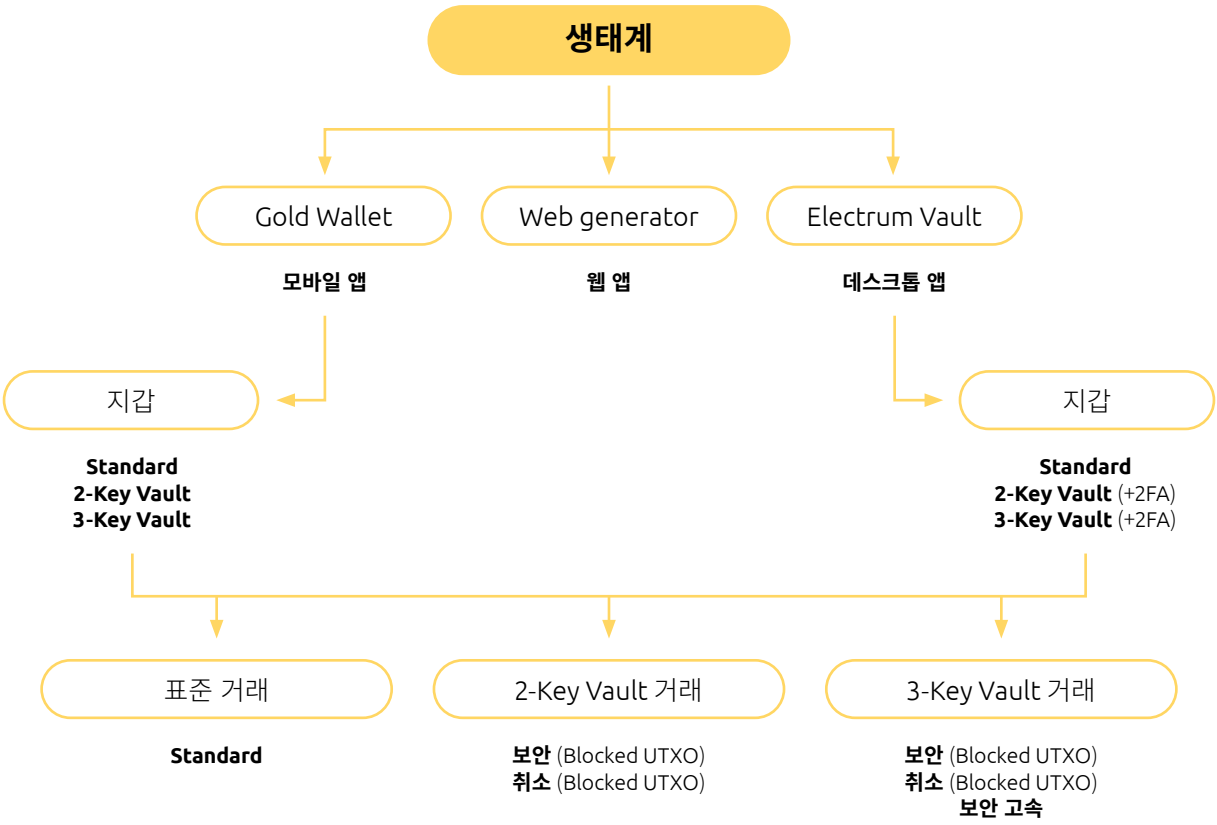
Bitcoin Vault는 사용자가 세 개의 ECDSA(Elliptic Curve Digital Signature Algorithm) 키를 생성해야 하는 3-Key Security Solution을 개발했습니다. 하나는 앱 내에 자동으로 저장되고 다른 두 개는 사용자가 관리해야 합니다. 현재 Bitcoin Vault의 설정을 통해 사용자는 시작된 거래를 취소하고 기존 또는 새 지갑 주소로 되돌릴 수 있습니다.

솔루션은 생태계에서 서로 다른 역할을 하는 세 가지 ECDSA 키를 지원합니다:

- 표준 거래 키는 자동으로 생성되며 백그라운드에서 작동합니다. 모든 거래를 시작하고 해킹이나 기술적 문제가 발생할 경우 지갑을 복구하는 데 필요합니다.
- 취소 거래 키를 사용하면 사용자는 블록 144개가 생성된 후 약 24간 안에 취소 거래를 수행할 수 있습니다.
- 빠른 거래 키를 사용하면 몇 분 만에 보안 고속 거래를 수행하고 BTCV를 전송할 수 있습니다.

Bitcoin Vault 생태계

Bitcoin Vault의 생태계에는 BTCV의 저장 및 관리를 목적으로 만들어진 세 개의 자체 앱이 포함되어 있습니다. 세 개의 앱은 보안, 투명성 및 자유도에서 더 높은 표준을 보장하는 강력한 도구를 형성합니다.



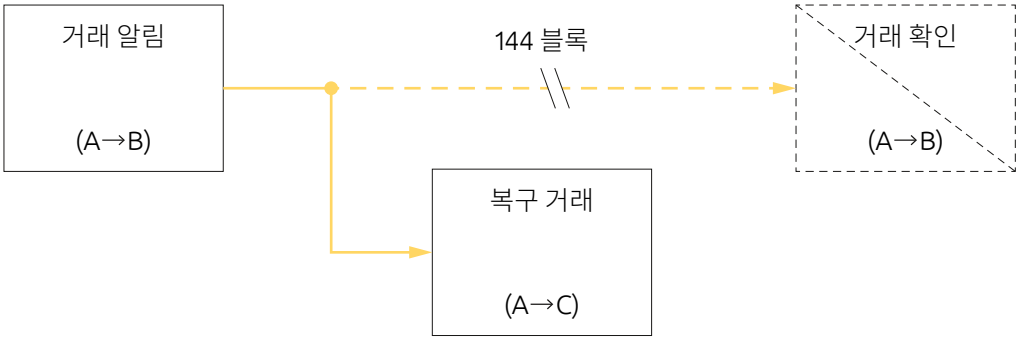
Gold Wallet
Gold Wallet은 BTCV를 저장하고 보내고 받기 위해 설계된 모바일 장치용 앱입니다. 사용자들이 세 가지 유형의 지갑을 생성할 수 있게 하며 보안 고속, 보안, 취소 거래를 포함한 다양한 유형의 거래를 수행할 수 있게 해줍니다. Gold Wallet은 Electrum Vault 데스크톱 앱의 이중인증(2FA) 인증기로도 사용할 수 있습니다.

Key Generator
Key Generator는 지갑을 설정하고 거래를 수행하는 데 필요한 개인적인 공개 키 및 개인 키를 생성하는 웹 기반 앱입니다. 이 앱은 로컬 리소스만 사용합니다. 즉, 키 생성 프로세스나 키 자체는 사용자의 장치를 떠나지 않습니다. 어디에도 저장되지 않으며 온라인으로 액세스할 수 없습니다. 키는 오프라인으로 저장되므로 최상의 안전성을 제공합니다.

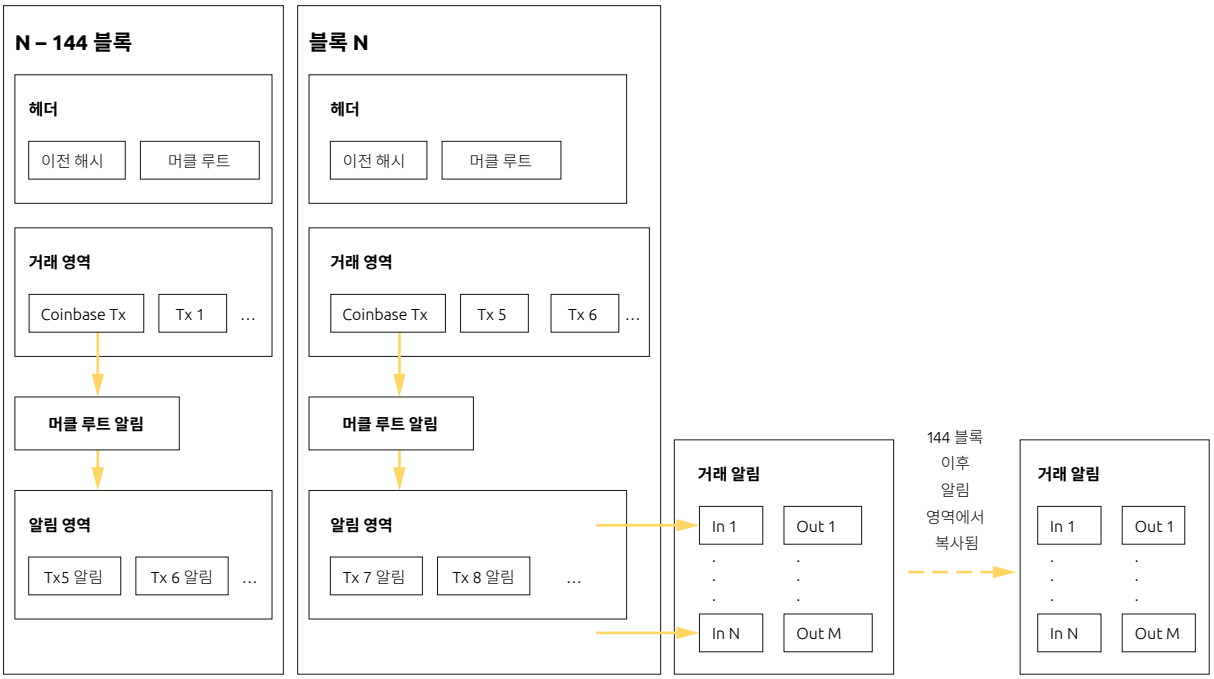
Electrum Vault
Electrum Vault는 오픈 소스 Electrum Wallet 기반의 데스크톱 애플리케이션입니다. Gold Wallet의 모든 기능을 갖추고 있어 BTCV 저장, 송수신, 지갑 생성 및 거래(보안 고속, 취소 거래 포함) 수행에 사용할 수 있습니다.

기술 개요

Locking script, 144개 블록의 기본 지연, 온 체인 알림 거래:



알림 영역이 있는 BTCV 블록 구조(저장 방법, 알림에서 확인으로 거래 상태가 변경될 때 생기는 일, 거래 상태 변경 시 채굴자 확인 방법)



거래 알림은 UTXO의 수명 주기를 변경합니다.

표준 버전에서 UTXO는 '사용 안 됨' 과 '사용됨'(기본적으로 제거됨을 의미)이라는 두 가지 상태가 있습니다. 새로운 버전의 Bitcoin Vault가 '확인됨'이라는 새로운 상태를 도입했습니다. 이것은 UTXO가 데이터베이스에 저장되는 방식을 변경합니다. 이제부터 '확인됨' 상태는 UTXO가 데이터베이스에서 제거되고 사용된 상태가 UTXO를 잠그고 사용된 블록 높이에 대한 정보를 저장하는 시간입니다. 이렇게 하면 시스템은 UTXO를 제거하기 전에 거래 알림이 확인될 때까지 기다립니다.

이는 확인을 받을 때까지 거래 알림이 복구 거래로 복구될 수 있기 때문에 필요한 접근 방법입니다(잠긴 UTXO만 입력으로 사용). 애플리케이션에서 UTXO의 수명 주기를 변경하는 가장 좋은 방법은 사용 후 높이에 대한 정보를 저장하는 것입니다. 이 새로운 정보는 UTXO의 상태를 다음과 같이 결정합니다.

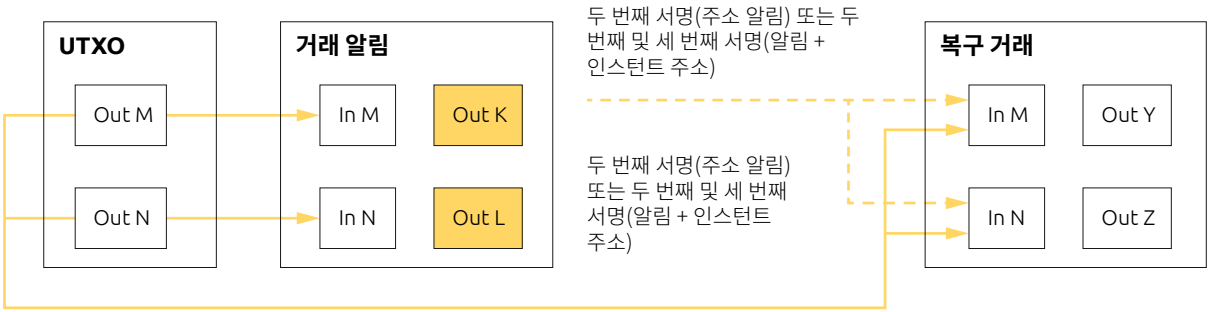
- 0 (사용하지 않은 경우),
- >0 (사용한 경우),

또한, Undo 구조에서도 동일한 정보를 고려해야 합니다. Undo 목록은 이전 UTXO의 상태 정보를 저장하고 체인 재구성이 발생할 때 이런 정보를 활용합니다.

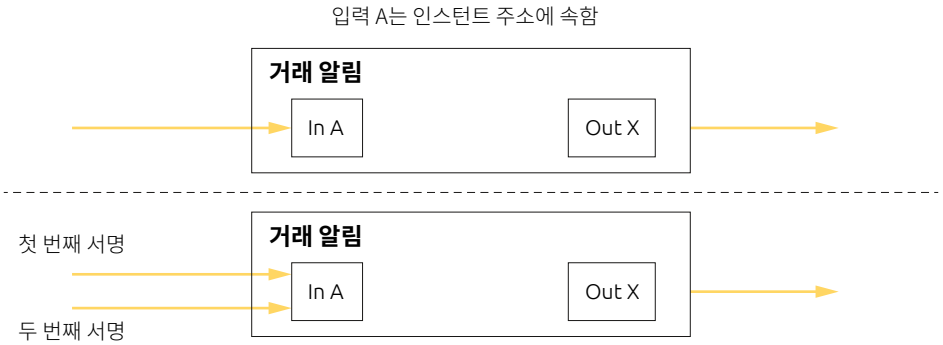
새로운 UTXO 상태 및 거래 유형도 사용자에게 표시되는 잔액에 영향을 미칩니다. 사용된 상태에 있는 UTXO는 확인된 잔액에서 표시되는 새로운 잔액으로 간주하여야 합니다. 이 잔액은 채굴되지 않고 소비할 수 있는 거래와

관련이 있기 때문에 미확인 잔액으로 간주할 수 없습니다. 이 아이디어는 잔액(사용할 수 없지만, 정보를 주는)을 생성하는 것입니다.

- 발신 알림 - 거래 알림에 의해 잠긴 사용 상태의 UTXO에서 제외됩니다,
- 수신 알림 - 거래 알림 확인 후 사용할 수 있게 될 UTXO에 포함됩니다.



빠른 거래의 작동 방식(24시간 지연 우회에 관한 설명, 이를 가능하게 하는 것 - 다중 서명):



작업증명(PoW)

Bitcoin Vault는 Bitcoin Royale 오픈 소스 코드를 기반으로 한 작업 증명(PoW) 코인입니다. 2020년 11월 17일에 하드포크가 수행되면서, Bitcoin (BTCV) 과의 병합 채굴이 구현되었습니다.

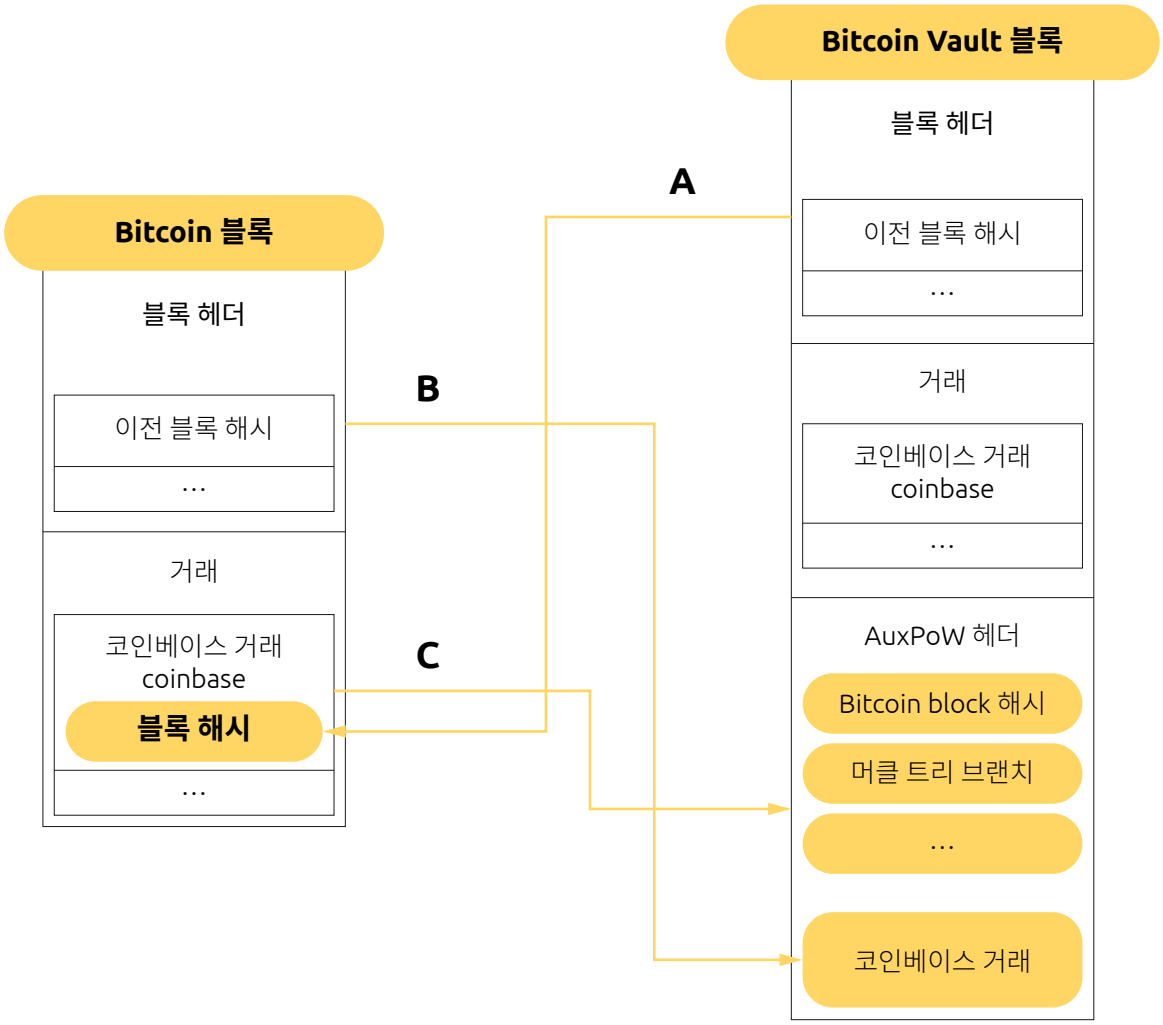
병합 채굴

블록 번호 58,420에서 BTCV 프로토콜의 주요 업데이트와 함께, Bitcoin Vault는 병합 채굴을 수용하도록 조정되었습니다. 보조적인 작업 증명이라고도 하는 병합 채굴은 채굴자가 동일한 계산 능력을 갖추고 최소 두 개의 분리된 암호화폐의 PoW를 동시에 찾는 프로세스입니다. 상위와 보조라는 블록체인 간에 이러한 관계를 구축하려면 보조 체인이 변화될 준비가 됐을 때가 가장 쉽습니다.

Bitcoin Vault에서는 병합 채굴이 Bitcoin과 함께 구현되었는데 이는 두 개의 암호 화폐가 모두 SHA-256 해시 함수를 사용하기 때문입니다. 이 경우, BTC는 상위 체인이고 BTCV는 보조 체인입니다.

결과적으로, Bitcoin(상위)의 작업 증명 솔루션을 사용하여 보조 작업 증명(AuxPoW) 합의 메커니즘으로서 Bitcoin Vault(보조 체인)를 검증할 수 있습니다.

블록 구조 및 BTC와 BTCV 블록 간의 관계에 대한 그래픽 예시를 포함한 기술 설명:



프로토콜에 병합 채굴을 구현하면 BTCV 채굴자는 BTC와 BTCV 블록체인 모두에서 두 블록 보상을 얻을 수 있는 가능성이 있기에 장려됩니다. 또 다른 이유로는 더 높은 해시 레이트로 비트코인 네트워크를 업어줌으로써 네트워크에 추가된 해시 파워 덕분에 네트워크 보안이 강화된다는 점에서 장려됩니다.

블록 보상

Bitcoin Vault는 총 2,100만 개의 코인이 공급되며, 하나의 블록을 채굴하는 데에는 약 10분 정도의 시간이 소요됩니다.

Bitcoin Vault 블록 보상은 가상화폐 개발 초기 단계에서 발생한 특정 문제를 제거하기 위해 설계되었습니다. 다음 두 가지 주요 문제가 확인되었습니다.

신규 참여자를 유치하기 위한 초기 기간은 프로젝트의 지속 가능한 개발에 필요한 적절한 수의 커뮤니티 구성원에 도달하기에는 너무 짧습니다.

초기 기간 이후 블록 보상이 급격히 감소합니다. 이로 인해 채굴자들이 채굴 과정에 더 이상 참여하지 못하게 되고 해시파워가 현저히 떨어질 수 있습니다.

이러한 위협을 방지하기 위해 Bitcoin Vault는 다음과 같은 솔루션을 제안했습니다.:

- 블록 보상이 더 높은 기간을 46개월까지 연장.
- 이 기간을 6개월마다 9개의 짧은 하위 기간으로 나누고 블록 보상 감소.

이를 통해 프로젝트 이면의 팀은 충분한 개발 시간을 가질 수 있습니다. 커뮤니티는 상당한 숫자로 증가할 수 있는 기회를 가지고 있으며, 초기의 채굴자들은 더 오랜 기간 동안 네트워크에 참여하도록 장려되며, 블록 보상의 급격한 감소를 야기하지 않으면서 코인의 수가 비트코인을 따라잡을 수 있는 충분한 시간이 있습니다.

이 기간의 블록 보상 감소는 다음과 같은 방식으로 계획됩니다.

날짜	BTCV 보상 감소	하위 기간 번호	블록 보상	하위 기간 시간	하위 기간 블록
2020년 5월	175 > 150	1	175	6개월	29850
2020년 11월	150 > 125	2	150	6개월	26600
2021년 5월	125 > 100	3	125	6개월	26600
2021년 11월	100 > 75	4	100	6개월	26600
2022년 5월	75 > 50	5	75	6개월	26600
2022년 11월	50 > 25	6	50	6개월	26600
2023년 5월	25 > 12.5	7	25	6개월	26600
2023년 11월	12.5 > 6.25	8	12.5	6개월	26600
2024년 5월	6.25 > 3.125	9	6.25	6개월	26600

결과적으로 이 기간에 19,687,500개의 코인이 배포되어 4번째 반감기(2024년 3월 11일 추정)까지 Bitcoin의 수를 따라잡을 것으로 예상됩니다. 그 후, BTCV 블록 보상은 Bitcoin의 반감기 일정과 동일하게 진행될 것입니다.

Bitcoin Vault 개발

BTCV 개발 단계

2019년 5월 – 2019년 12월	사전 알파
2019년 12월 – 2020년 9월	알파
2020년 9월 – 2020년 11월	베타
2020년 11월	메인넷

메인넷
메인넷은 블록 높이 번호 58,420으로 2020년 11월 17일에 성공적으로 출시되었습니다.

로드맵
2020년 12월, BTCV 개발팀은 2021-2022년에 대한 새로운 로드맵을 발표했습니다. 추가 BTCV 개발을 6개의 작업 흐름으로 나누었습니다.

작업 흐름 #1 – 개발 업그레이드
개발 작업 흐름은 Bitcoin Vault에 추가될 모든 블록체인 업그레이드와 관련이 있습니다. 이 작업 흐름의 주요 목표는 2021년 말까지 Ethereum 2.0을 둘러싼 Dapp 생태계에 랩핑 BTCV(wBTCV)로 참여하는 것입니다.

- 2021년 1분기
  - wBTCV ERC-20 토큰 – wBTCV 이면에 대한 분석 및 토크노믹스
- 2021년 2분기
  - Ledger 통합
- 2021년 3분기
  - wBTCV ERC-20 토큰 베타 테스트 단계
- 2021년 4분기
  - wBTCV 출시
  - DeFI 생태계와 통합 시작
- 2022년 1분기
  - DeFI 생태계와 통합 완료
  - Dapps 개발
- 2022년 2분기~
  - Dapps 개발

작업 흐름 #2 – 보안 업그레이드

Bitcoin Vault에는 내부에 블록체인 보안 전문 팀이 있습니다. 메인넷의 블록체인 무결성은 여러 차례 확인되었으며, 2021년에는 코드를 강화하고 외부 파트너의 지원을 받아 버그와 취약점을 식별하는 것이 주요 목표입니다. 내/외부적인 침투시험 후 개발자를 위한 바운티 프로그램을 운영하고 'white hat' 커뮤니티와 긴밀히 협력할 것입니다.

- 2021년 1분기
  - 전체 코드 감사 (내부 및 외부)
- 2021년 2분기
  - 침투 테스트 (내부)
- 2021년 3분기
  - 침투 테스트 (외부)
- 2021년 4분기
  - 보안 감사 CIS/20
  - 클라우드 보안 매트릭스
- 2022년 ~
  - 추가 보안 개선 및 감사
  - 해커톤
  - 바운티 프로그램

작업 흐름 #3 – 사용자 경험 업그레이드

사용자 경험은 제품 사용 및 채택의 가장 중요한 요인 중 하나입니다. 저희 목표는 애플리케이션을 더욱 개발하고 업그레이드하여 커뮤니티의 피드백을 바탕으로 다양한 사용자의 요구에 맞게 조정하는 것입니다.

- 2021년 1분기 및 2분기
  - GoldWallet 모바일 앱 UX 개선
  - Electric Vault 모바일 앱 쉬운 모드 및 전문가 모드 전환
- 2021년 3분기
  - GoldWallet 사용자 알림
- 2021년 4분기
  - 타사 앱과 GoldWallet 통합
- 2022년~
  - 추가 UX 개선

작업 흐름 #4 – 상품

IT 개발과 함께 시장 채택에 파이프라인이 되는 새로운 상품에 매우 주목하고 있습니다. 2021년에는 BTCV 파트너의 지원을 통해 스테이킹 상품을 출시하고 법정 통화에 BTCV 생태계를 연결하고 싶습니다.

- 2021년 1분기
  - 타사를 통한 새로운 스테이킹 상품
  - 새로운 트레이딩 상품
- 2021년 2분기
  - 새로운 결제 게이트웨이
  - FIAT 통합

- 2021년 3분기
  - 데이터 분석 플랫폼 (빅 데이터)
- 2021년 4분기
  - wBTCV 토큰 관련 상품
  -
- 2022년~
  - 새로운 3-Key 기능
  - dApps 상품

작업 흐름 #5 – 마케팅 활동

2021년에는 현재와 미래의 BTCV 사용자뿐만 아니라 전 세계 암호화 커뮤니티를 대상으로 글로벌 인식 및 참여 캠페인을 시작할 계획입니다. BTCV 블록체인의 보안을 강화하고 BTCV가 양자 연구를 앞서갈 수 있도록 하는 새로운 파트너십을 모색할 것입니다.

- 2021년 1분기
  - 새로운 웹사이트 출시
- 2021년 2분기 및 3분기
  - 글로벌 인식 및 참여 캠페인
- 2021년 4분기
  - 전략적 보안 파트너십
- 2022년 ~
  - 전략적 과학 파트너십

작업 흐름 #6 – 기타 업그레이드

BTCV 생태계 추가 업그레이드를 통해 커뮤니티와 연결되고 참여하며 2021년 2분기 초에 완전히 시작될 새로운 에어드롭 메커니즘을 통해 호들러를 위한 새로운 옵션을 제공하고자 합니다. 저희의 장기적인 관점은 또한 양자 컴퓨팅과 그것이 블록체인의 암호화에 영향을 미칠 수 있는 잠재력에 관한 것이 될 것입니다.

- 2021년 1분기
  - 새로운 에어드롭 메커니즘 개발 및 출시
  - 에어드롭 지갑 잠금
- 2021년 2분기
  - 에어드롭 플랫폼 / 앱
- 2021년 3분기
  - 블록체인 분석 플랫폼
- 2021년 4분기~
  - 양자 연구
  - 과학 파트너십 보조금 프로그램

양자 컴퓨팅과 분산 Ledger 기술(DLT) – 비전

대부분의 블록체인 개발자처럼 우리는 양자 기술의 진보에 진정으로 관심이 있습니다. 블록체인과 같은 분산 Ledger 기술(DLT)을 연구하는 연구자와 개발자는 모든 블록체인 솔루션에 필수적인 공개 키 암호화와 해시 함수에 의존합니다.

Bitcoin Vault 블록체인은 ECDSA 및 SHA-256과 같은 강력한 암호화 알고리즘에 의해 보호되며, 이는 Bitcoin을 비롯한 다른 많은 암호 화폐에도 사용됩니다. 현재 사용되는 암호화 알고리즘은 기존의 계산 방식보다 충분히 강력합니다.

양자 컴퓨팅의 위협

양자 기술을 통해 컴퓨팅 성능을 기하급수적으로 향상하면 공개 키를 크래킹하여 개인 키 해시를 계산하거나 SHA-256 알고리즘을 해제하여 필요한 블록의 일회성 해시값 블록을 얻는 것이 이론적으론 가능할 수 있습니다. 이 분야의 많은 전문가에 따르면, 여전히 안정된 양자 컴퓨터를 개발하는 것에 대한 연구를 수년째 해오고 있다고 합니다. 그리고 개발이 된다고 하더라도 특정 암호화 알고리즘을 크래킹하기 위해서는 컴퓨터 코드를 적절하게 코드화해야 합니다.

양자 컴퓨팅의 기회

양자 컴퓨팅의 위협보다는 그 기회에 초점을 맞추고 싶습니다.

이론적으로, 양자 컴퓨터가 신뢰할 수 있는 계산을 수행하기에 충분히 안정적인 수준이 된다면 양자 컴퓨터는 암호화 알고리즘을 개선하는 데 사용될 수 있을 것입니다. 이것이 우리가 보는 블록체인의 미래입니다.

현재 양자 증명 코인의 목표 달성을 위해 다양한 방법을 생각할 수 있습니다.

- 격자 기반 암호화 시스템,
- 다중 변수 기반 공개 키 암호화 시스템,
- 초단일 타원 곡선 동위 원소 암호화 시스템,
- 해시 기반 디지털 서명 암호화 시스템
- Google에서 테스트한 솔루션(CECPQ1 및 CECPQ2)과 같은 하이브리드 솔루션
- 그 외 다수.

적절한 반양자 솔루션을 찾고 포스트 양자 시대에 대비한 BTCV 코인을 준비하기 위해, 우리 개발팀은 필요한 온-키 압축 기법과 특정 유형의 코드 및 코딩 기법의 사용에 관한 연구를 더 많이 진행해야 합니다.

그런데도, 오늘날에는 작은 용량의 키 크기, 짧은 서명/해시 크기, 빠른 실행, 낮은 계산 복잡도 및 낮은 에너지 소비를 동시에 제공하는 포스트 양자 블록체인 알고리즘이 없습니다. 이러한 요인들은 사물 인터넷에서 사용되는 것과 같이 자원이 제한된 임베디드 장치에 특히 중요합니다.

향후 3년에서 5년 동안 우리 BTCV 개발자들은 다양한 기업, 신생 기업 및 기술 대학의 전문가들과 새로운 파트너십을 통해 양자 내성에 대한 운영 준비태세에 도달하는 데 주력할 것입니다.

Bitcoin Vault 설립자

Bitcoin Vault는 아시아와 유럽에 위치한 암호화 채굴 시설의 세계적인 운영사 중 하나인 Minebest의 CEO인 Eyal Avramovich가 설립했습니다.

Minebest에 대한 자세한 정보는 다음 링크에서 확인할 수 있습니다. https://minebest.com/

Bitcoin Vault 이면의 팀에 대한 자세한 정보는 다음의 공식 웹사이트에서 확인할 수 있습니다.
https://bitcoinvault.global/

관련 작업

Bitcoin Vault 개발로 이어진 Bitcoin Royale 제작자의 콘셉트 아이디어에 감사를 드립니다.

Bitcoin Royale 백서: https://bitcoinroyale.org/bitcoinroyale.pdf

BTCV 출처:

프로젝트에 대한 추가 정보는 다음과 같습니다.

https://bitcoinvault.global/
https://twitter.com/vaultbitcoin
https://medium.com/bitcoin-vault-btcv
https://t.me/Bitcoin_Vault
https://www.facebook.com/bitcoinvaultofficial
https://www.instagram.com/bitcoinvaultofficial
https://www.youtube.com/c/BitcoinVault

참고 문헌

1. Bitcoin Whitepaper, Satoshi Nakamoto, https://bitcoin.org/bitcoin.pdf
2. Bitcoin Royale: Peer-to-Peer No-Theft Electronic Gold, Ian Duoteli Fleming, https://bitcoinroyale.org/bitcoinroyale.pdf
3. Cryptocurrency Anti-Money Laundering and Crime Report, Spring 2020, https://ciphertrace.com/cryptocurrency-anti-money-laundering-and-crime-report-spring-2020/
4. The Chainalysis 2020 Crypto Crime Report, https://go.chainalysis.com/2020-Crypto-Crime-Report.html
5. Bitcoin, crypto-coins, and global anti-money laundering governance, Malcolm Campbell-Verduyn, https://www.researchgate.net/publication/322596368_Bitcoin_crypto-coins_and_global_anti-money_laundering_governance
6. Namecoin project, https://www.namecoin.org/
7. Bitcoin Wiki, Merged Mining Specifications, https://en.bitcoin.it/wiki/Merged_mining_specification
8. Adam Back, Hashcash – A Denial of Service Counter-Measure, http://www.hashcash.org/papers/hashcash.pdf

9. Phil Daian, Rafael Pass, Elaine Shi; Snow White: Robustly Reconfigurable Consensus and Applications, https://eprint.iacr.org/2016/919.pdf
10. Wrapped Tokens A multi-institutional framework for tokenizing any asset https://wbtc.network/assets/wrapped-tokens-whitepaper.pdf
11. Smart Contract Extensibility with Wrapped Tokens https://yos.io/2019/07/13/smart-contract-extensibility-wrapped-tokens/#:~:text=Wrapped%20Tokens%20is%20a%20design,two%20versions%20at%20any%20time.
12. Aleksei Pupyshev, Ilya Sapranidi, Elshan Dzhafarov, Shamil Khalilov, Ilya Teterin, Graviton: interchain swaps and wrapped tokens liquidity incentivisation solution, https://arxiv.org/ftp/arxiv/papers/2009/2009.05540.pdf