



## Viacoin Whitepaper

Viacoin Dev Team

September 12, 2017

Viacoin은 2014년에 오픈소스 암호화폐입니다 그리고  
120 바이트 확장 된 OP\\_RETURN의 임베디드 컨센서스를 지원하는 Bitcoin  
프로토콜입니다.

Viacoin의 특징은 Scrypt Merged mining,Auxiliary proof of work 또는 AuxPoW라고도 하며  
Bitcoin보다 25 배 빠른 트랜잭션입니다.

Viacoin 채굴 보상은 6개월에 한 번씩 이루어지며 총 공급량은 23,176,392.41459개입니다.  
상승률과 채굴 보상은 매우 낮습니다.

Viacoin의 블록 보상이 낮기 때문에 채굴자들은 Merged mining(AuxPoW)을 통해  
인센티브를 받습니다.

Viacoin은 현재 매우 높은 해시 비율을 갖고 가장 큰 mining pools(F2Pool)중 하나에 의해  
채굴됩니다.

다른 기능으로는 Kimoto의 Gravity Well (DarkGravityWave)의 결함을 처리하는 마이닝  
난이도 조정 알고리즘,  
한 번에 29 개의 Soft Fork 변경 사항을 구현할 수 있는 Versionbits, Segwit 및 Lightning  
Network입니다.

small Note: The whitepaper, documentation, designs are in research and development phase  
and subject to change.



## Viacoin Whitepaper

### 1. Scrypt

암호학에서, Scrypt에서는 Colin Percival이 만든 암호 기반 키 유도 함수입니다. 이 알고리즘은 대량의 메모리가 필요하므로 대규모 사용자 지정 하드웨어 공격을 수행하는데 많은 비용이 듭니다. 2012년에 알고리즘은 IETF에서 정보 RFC로 의도된 인터넷 초안으로 발행되었지만 Scrypt 버전은 이제 Viacoin과 같은 크립토 통화 (cryptocurrencies)에 의한 proof of work로 사용됩니다.

Scrypt는 메모리 하드 키 파생 함수로, 합리적으로 많은 양의 Random Access Memory를 평가해야합니다.

따라서 특수 목적의 맞춤 하드웨어 (ASIC)를 구현하려면 Viacoin을 채굴하는 목적으로 구축하기가 불필요한 VLSI 영역이 더 필요합니다. Scrypt 알고리즘의 요구 사항은 메모리에 보유 될 의사 랜덤 비트의 큰 배열과 이로부터 파생 된 키입니다. 이 알고리즘은 TMTO (Time-Memory Tradeoff)를 기반으로합니다. Viacoin의 ASIC 이점은 Bitcoin과 비교하여 10 배 감소합니다.

Scrypt는 다음 매개 변수를 사용하여 파생 키를 생성합니다:

- Passphrase: 해시에 문자의 문자열
- Salt: 함수에 제공된 임의의 문자열
- N: 메모리 / CPU 비용 매개 변수
- P: 병렬화 파라미터
- R: 블록 크기 매개 변수
- dkLen: 키에서 파생 된 키의 예상 길이 (바이트)

kd = scrypt(P, S, N, P, R, dkLen)

Viacoin 매개 변수 (N = 1024, R = 1, P = 1 및 S = 256 바이트 출력의 256 바이트 생성)

### 2. Merged Mining AuxPoW

Viacoin Merged 채굴은 다른 Scrypt 동전의

채광력을 재사용하여 Viacoin블록체인에 보안을 추가하는 것을 목표로합니다.

채굴자는 동시에 하나 이상의 블록 체인을 채굴 할 수 있습니다. 예를 들어 채굴자는 Viacoin과 Litecoin 또는 다른 Scrypt 동전을 Viacoin과 함께 채굴할 수 있습니다.

채굴자가 기여하는 모든 해시는 두 크립토의 총 해시에 대한 것이며 더 안전한 블록 체인을 만듭니다.

AuxPoW 블록은 두 가지 차이점이 있는 표준 Bitcoin 블록과 유사한 블록 유형입니다. 블록 헤더의 해시가 블록 체인의 난이도를 충족시키지 못합니다.

둘째, 블록을 만든 채굴자가 상위 블록 체인에서 마이닝을 수행하고



## Viacoin Whitepaper

블록 체인의 난이도를 충족시키는 것을 보여주는 추가 데이터 요소가 있습니다.

채굴자들은 Viacoin 채굴에 대한 인센티브를 가지고 있습니다.

다른 Scrypt 동전을 동시에 채굴 할 수 있기 때문에 보상이 낮아도

"무료"로 Viacoin을 사용할 수 있습니다. Viacoin 채굴은 대규모 블록

보상으로 운영되지 않으므로 Viacoin은 merged mining을

지원하지 않는 다른 암호화폐들과 비교하여 낮은 인플레이션을 보입니다.

### 3. DarkGravityWave

Dark Gravity Wave (DGW) 오픈 소스 난이도 있는 알고리즘입니다.

DGW는 X11 / Darkcoin / Dash의 개발자이자 개발자인 Evan Duffield가 저술했습니다.

이 알고리즘은 Kimoto Gravity Wave 알고리즘의 Time warp 공격과 같은 결함을

처리하도록 설계되었습니다.

Dark Gravity Wave는 Dash (Darkcoin)에서 처음 소개되었습니다.

DGW는 재조정 메커니즘을 부드럽게하기 위해 여러 지수 이동

평균 및 단순 이동 평균을 사용합니다.

$2222222 / (((\text{Difficulty} + 2600) / 9)^2)$

Dark Gravity Wave 버전 3은 최신 버전으로 잘 알려진 Kimo Gravity Well

알고리즘과 비교하여 난이도를 개선 할 수 있습니다.

### 4. Segwit

Viacoin에는 Segwit (BIP 141)<sup>10</sup> 활성화되었습니다.

분리 된 Witness은 거래 규모를 축소하고 UTXO 성장에 대처하는 데 도움이 됩니다.

분리 된 Witness은 Witness 데이터가 트랜잭션과 분리 된 트랜잭션 형식입니다. 또한 블록  
당

트랜잭션 처리량을 2 또는 3 배로 높이는 동시에

새로운 노드에 대해 블록 동기화를 더 빠르게하는 것을 목표로 합니다.



## Viacoin Whitepaper

Viacoin에서의 Segwit 구현의 주된 목적은 용량을 늘리는 것이 아니라 유연성을 수정하고 스크립팅을 쉽게 업그레이드하는 것입니다. 유연성을 수정하면 \cite{atomic}atomic swaps, 양방향 지불 채널 및 Bitcoin과의 Viacoin 상호 운용성을 높일 수 있는 Lightning 네트워크와 같은 Viacoin의 기능을 추가 할 수 있습니다.

Segwit에는 스크립트 용 버전 관리가 포함되어 있으므로 (일반적으로 비 segwit 트랜잭션에서 하드 포크가 필요한) 추가 opcode가 대신 사용될 수 있습니다. 스크립트 opcode를 보다 쉽게 변경하면 Viacoin을 더 쉽게 사용할 수 있습니다. Schnorr 서명, 사이드 체인, MAST 및 기타 기능이 가능합니다.

### 5. The Lightning Network

The Lightning Network는 블록 체인에서 스마트 계약 기능을 사용하여 Viacoin 블록 체인 위의 계층에서 작동하는 전송 네트워크로 참가자 네트워크에서 즉시 지불 할 수 있습니다.

이를 통해 컨센서스 원장 외부의 트랜잭션 대부분을 지불 채널로 이동시킴으로써 트랜잭션 처리량을 수주 단위로 향상시킬 수 있습니다.

이를 통해 네트워크에서 초당 수십억 건의 트랜잭션을 처리 할 수 있습니다. 용량은 기존 지불 레일을 보낸다.

이는 당사자가 디지털 서명을 공유하여 상태를 업데이트하고 블록 체인에 증거를 제시하여 종료 할 수 있는 양 당사자 간의 스테이트 풀 계약을 체결하는 온 체인 스크립트를 지원함으로써 가능합니다.

Lightning Network는 예외적으로 낮은 수수료를 허용합니다. 가치가 낮은 거래의 경우, Lightning Network는 묘책입니다. 그것은 새로운 종류의 상거래를 허용합니다. 많은 당사자와 함께 지불 채널을 열면 LN의 참가자는 완전히 연결된 지불 채널로 이어지는

다른 사람의 지불을 라우팅하기 위한 중심점이 될 수 있습니다. 지불은 감소하는 시간 잠금을 통해 원 자성을 강요하는 스크립트를 사용하여 시행됩니다.

또 다른 이점은 원자 간 연쇄 거래의 가능성으로, 사용자는 viacoin, bitcoin, litecoin 및 기타 Segwit coin을 즉각적으로 거래 할 수 있어 매우 효율적이고 분산 된 교환 또는 분산 형태의 'Shapeshift.io'를 허용합니다.



## Viacoin Whitepaper

### 6. Schnorr Signature

Schnorr 서명 집계는 곧 개발 될 예정입니다. 이 기능은보다 효율적인 알고리즘이므로 ECDSA의

후속 제품으로 Bitcoin에서 제안되었습니다. 최근까지 Viacoin과 다른 많은 cryptocoins에서 하드포크없이

Schnorr 서명을 구현하는 것은 불가능했습니다. Segwit의 유연성으로 이제 가능합니다. 모든 서명 데이터가 감시 서버로 이동됩니다.

Viacoin은 현재 ECD (Elliptic Curve Digital Signatures)를 하나의 출력에서 다른 출력으로 전송하는 권한을 부여하기 위해 소유권 증명으로 사용했습니다. 2015 년에

Daniel J. Bernstein은 Elliptic Curve 위에 Schnorr와 같은 서명을 사용하도록 제안했습니다.

몇 가지 장점:

- 기본적 가정 하에서 안전하게 보호
- 유연성에 대한 내성
- 해시 함수 충돌에 대한 내성
- 속도 향상을 위한 일괄 검증
- 기본 k-of-k Multisignatures \dots

배치 유효성 검사를 지원합니다. 즉, 단일 키가 아닌 공개 키 메시지 서명 쌍의 그룹이 있는 경우 개별적으로보다 빠른 속도로 그룹 전체의 신뢰성을 전체적으로 확인할 수 있습니다.  
블록은 유효성 검사를 위한 서명 일뿐입니다.

네이티브 k-of-k 멀티 서명 인 Schnorr의 아이디어는 여러 개의 키를 함께 사용할 수 있고 모든 서명이 서명 된 단일 서명을 가질 수 있다는 것입니다.

group cat은 키 합계에 유효한 서명을 만듭니다.

U1, U2 및 U3은 사용자입니다. 두 라운드 상호 작용 체계가 있습니다. 이 둘은 모두 n 번째로 k1, k2, k3으로 나오며 모두 해당 공개 지점

R1, R2, R3을 계산합니다. 그들은 서로 의사 소통하고 전반적인 R 값을 더합니다. 이 전반적인 R 값은 S1, 2, S3을 결과로하는 자체 키를 사용하여이 논스에 서명 한 다음 모든 S 값을 하나의 최종 S로 결합합니다.

해당 키의 합계에 유효한 서명입니다.

이것은 k-of-k multisig의 이점이 있습니다.

$$\begin{array}{c} U_1 \rightarrow k_1, R_1 \\ U_2 \rightarrow k_2, R_2 \\ U_3 \rightarrow k_3, R_3 \end{array} \left| \rightarrow R \right| \begin{array}{c} U_1 \rightarrow (R, s_1) \\ U_2 \rightarrow (R, s_2) \\ U_3 \rightarrow (R, s_3) \end{array} \rightarrow (R, s) \quad (1)$$



## Viacoin Whitepaper

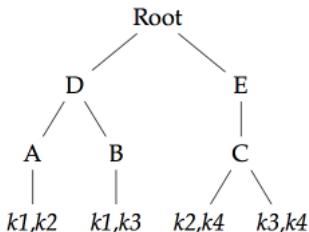
k-of-k상황이 없는 경우에도, 키 조합의 어떤 조합이 서명할 수 있는 다른 정책이 있다.  
하나의 요구 사항은 merkle tree와 Schnorr이 트리를 추가하고 빌드하는 기능입니다.  
여기에서 트리의 모든 노드 리프는  
서명 할 수 있는 키 조합입니다. 이것들은 함께 해시 될 필요가 있고 루트는 주소입니다.  
OP\\_CHECKSIG \& OP\\_CHECKMULTISIG는 수정되어 pubkeys를 스택하고,  
유효성이 검증 된 입력을 delinearize 및 연관 시키며,  
블록 크기가 20 % 감소 된 트랜잭션에 대한  
결합 서명을 생성합니다.

2 out of 4 (k1...k4)

O(1) verification time\nnewline

O(log n) signature size\nnewline

O(n) signing time



단일 트랜잭션에서 모든 시그니처에 대해 집계를 수행 할 수 있습니다. 그 배경은 Viacoin 노드와 같은 시스템 검사기가 모든 트랜잭션의 모든 입력에 대해 단일 키를 계산할 수 있게하는 것입니다.

### 7. Non-atomic flushing

시스템을 강력하게 만들려면 디스크의 상태를 블록으로 유지해야합니다.

예기치 않게 지갑을 종료하면 내부에서 시작하고 롤백하거나

롤 포워드 할 수 있으며 디스크에서 일관된 텁을 얻을 수 있습니다.

일반적으로 캐시가 가득 찰 때마다 플러시가 강제 실행됩니다.

시작시에 존재한다면, flush 중에 추락했다는 것을 의미하고, 진행하기 전에 디스크에 일관된 텁을 얻기 위해 롤백 / 롤 포워드 블록을 사용합니다.



## Viacoin Whitepaper

### 8. Colored Coins

Viacoin 스크립팅 언어를 사용하면 자산 조작 지침을 나타낼 수 있는 소량의 메타 데이터를 블록 체인에 저장할 수 있습니다. Viacoin 트랜잭션은 새로운 자산의 x 단위가 발행되고 Viacoin 주소로 대변되는 x 단위로 인코딩 될 수 있습니다.

기간은 동전의 명목상 양을 착색하는 아이디어에서 파생됩니다. Viacoin을 이용하면 회사 주식이나 실제 상품처럼 사용자가 원하는 모든 것을 나타낼 수 있는 토큰이 됩니다. 이것은 '상대방'과 매우 유사하지만 몇 가지 주요 차이점이 있습니다. Viacoin 블록 체인을 사용합니다. (e.g NXT).

보조 코인은 발행하지 않습니다 (예 : 거래 상대방 및 마스터 코인).  
metadata는 색깔의 동전 거래에 의미를 부여하는데  
보통 OP\_RETURN opcode 중 하나에 저장됩니다.  
OP\\_RETURN을 포함하는 출력을 마커 출력이라고 합니다.  
이 마켓 아웃은 0 또는 0이 아닌 값을 가질 수 있습니다.  
마커 출력은 OP\_RETURN opcode로 시작하며 구문 분석 가능한  
열린 자산 시장 페이로드를 포함하는 PUSHDATA opcode를 포함해야하는  
모든 opcode 시퀀스가 뒤따를 수 있습니다.  
자산 수량 목록 필드는 자산의 각 출력량을 결정하는 데 사용되며  
각 정수는 LEB128 인코딩을 사용합니다.  
이 값이 9 바이트를 초과하면 시장 산출물은 유효하지 않은 것으로 간주됩니다.  
산출물의 최대 자산 수량은  
 $\$2^{63} - 1$ 입니다.  
colored coins Open Asset Protocol은 Viacoin 프로토콜 위에 위치합니다.  
Viacoin 프로토콜 자체를 변경할 필요가 없습니다.



## Viacoin Whitepaper

### 9. Merkelize Abstract Syntax Trees

Viacoin 트랜잭션 유효성 검사 스크립트를 구문 분석된 형태로 저장하고

노드가 MerkleTree와 상호 작용할 수 있도록 허용합니다.

"소비자는 사용할 수 있는 분기점만 제공할 수 있으며,

이를 통해 분기점을 고정된 크기의 Merkle루트에 연결할 수 있습니다.

이것은 상환 스택의 크기를  $O(n)$  to  $O(\log n)$  ( $n$  as the number of branches)에서 줄입니다.

이것은 스크립트 크기 및 연산 코드 제한으로 인해 현재 불가능한

복잡한 상환 조건을 가능하게하고, 실행되지 않은 지점을 숨김으로써 프라이버시를

향상 시키며 추가 비용이 매우 적거나 전혀 없는 비 합의 된 데이터를

포함시킬 수 있게 해줍니다."

MAST는 블록 체인을 막히지 않고도 스마트 계약을 생성 할 수

있기 때문에 중요합니다. 보통 모든 현명한 계약은 블록 체인에서

볼 수 있으며 공간을 차지합니다. MAST를 사용하면 완료된 스마트 계약 만

표시 할 수 있으므로 노드가 Merkle Tree의 최상위

레이어를 읽어야하기 때문에 공간을 절약 할 수 있습니다.

Ethereum의 현명한 계약 시스템에는 익숙해 보일 수도 있지만 차이점이 있습니다.

Ethereum은 VIA가 RootStock (RSK)을 통해 VM에 대한 액세스 권한을 얻는 VM에 직접 액세스합니다.

RSK는 Ethereum이 해야 할 일, 즉 분권화 된 Turing-complete 스마트 계약 플랫폼을 목표로 합니다.

### 10. Viacoin RSK smart contracts

Rootstock은 양방향 페그가 있는 스마트 계약 플랫폼입니다.

아이디어는 스마트 계약으로 작동하도록하는 것입니다. Rootstock은 가상 머신

Rootstock Virtual Machine (Ethereum 가상 머신과도 호환됩니다!)이라고 불리는 완벽한 가상

머신을 실행하고 견고한 컴파일 된 스마트 계약을 실행할 수 있도록 합니다.

병합 마이닝과 Viacoin을 함께 사용하면 RSK 블록 체인이 Viacoin과

동일한 보안 수준을 가질 수 있습니다. 그것은 초당 약 2,000건의 트랜잭션과

초당 2,000건의 트랜잭션을 처리할 수 있어야 합니다.



## Viacoin Whitepaper

### 11. Anonymous transactions

Tumblebit을 기반으로하는 Viacoin의 Unlinkable 익명 Atomic Payment Hub.  
<https://github.com/viacoin/documents/blob/master/whitepapers/styx/Viacoin-Styx-Whitepaper.pdf>