CLOAK

ENIGMA V2.1

백서 (개정판)

2018년 2월

ENIGMA

CloakCoin의 안전하고 사적이며

추적이 불가능한 교환 시스템

1. 개요

CloakCoin은 Enigma를 이용해 사적이고 안전하며 추적이 불가능한 분산된 이송을 추진하게 디자인된 크립토커런시입니다.

Cloak은 이제 지분증명 단계에 있는 듀얼 작업증명/지분증명 코인입니다.

Enigma는 미래 발전의 근본을 개설하고 CloakCoin 네트워크의 분산된 애플리케이션을 위해 기본적인 교환 시스템을 제공하는 사적이고 안전하며 추적이 불가능한 시스템의 CloakCoin입니다.

프라이버시는 어느 때보다 중요합니다. 기술 발전의 엄청난 속도는 우리 모두의 시야를 넓혔고 전례 없는 새로운 세상을 연결했습니다. 2009년 비트코인의 출시 이후 크립토커런시는 꾸준히 주류로 여겨지고 이제 블록체인의 힘을 사용하여 순식간에 크립토커런시를 전세계에 안전하게 전송할 수 있게 되었습니다.

크립토커런시 채택이 더욱 널리 보급되는 동시에 증가된 규제가 불가피해집니다. 이 규정이 어떠한 형태로 이루어질지 아직까지 알지 못하지만, 많은 사람들은 과도하게 엄격할 수 있고 자유주의론 측면에서 크립토커런시의 일부를 질식 시키도록 고안되어 있다고 우려하고 있습니다.

ENIGMA

Enigma는 CloakCoin 네트워크의 사용자가 사적이고 안전하게 Cloak을 전송할 수 있게 해주는 분산형 오프 블록체인 혼합 서비스입니다. 믹싱 프로세스가 제 3자 관찰자에게 안전하고 추적할 수 없도록 설계되었습니다. 이렇게 하면 전송 중에 사용자의 CloakCoin이 안전하게 유지되고 발신자와 수신자가 묶이거나 연결될 수 없게 됩니다. Cloaking (클로킹) 중에는 CloakCoin이 중개자에게 넘겨지지 않으므로 코인은 안전하게 유지됩니다. 우리는 또한 Enigma 시스템이 Cloaking 전송을 지원하는 사용자에게 보상을 제공하고 프로세스를 지속적으로 개선하고 적극적인 참여자에게 동기를 제공하기 위해 노력했습니다. CloakCoin이 있는 사람은 누구나 Cloaking 작업에 참여할 수 있습니다. Cloaking 작업을 통해 Staking/ Cloaking 모드에서 지갑을 실행 상태로 두어 수동으로 Cloaking 을 지원하고 상당한 보상을 얻을 수 있습니다.

2. ENIGMA V1.0 개요

Enigma는 Cloak의 사적이고 안전하며 추적할 수 없는 지불 시스템에 대한 최초의 공개 반복입니다. Enigma 거래는 다른 사용자들에 의해 은폐하고 그들은 도움을 준 대가로 보상을 받습니다. 다른 사용자는 Enigma 거래에 대한 입력과 출력을 제공하여 Cloak 전송의 실제 출처와 목적지를 결정하는 것을 불가능하게 만듭니다. 네트워크의 모든 Enigma 메시지는 데이터 보안 및 무결성을 보장하기 위해 CloakShield를 사용하여 수신자에 대해 해시되고 암호화됩니다. 자세한 내용은 섹션 3: 'CloakShield'를 참조해주세요.

2.1 ENIGMA 프로세스 (ENIGMA 활성화된 노드들을 위해)

ENIGMA 공지

Enigma 노드는 Cloak 네트워크를 통해 통신하고 노드는 다른 활성 Enigma 노드를 추적합니다. Enigma 공지 방송은 세션 키와 현재 Enigma 클로킹 잔액의 다른 Enigma 노드에 알림을 방송합니다.

ENIGMA 클로킹 요청

사용자가 Cloaked Enigma 거래를 보내려고 할 때 Enigma 노드를 충분히 선택하여 클로킹에 도움을 요청합니다. Enigma 노드는 클로킹을 돕기 위해 요청자에게 수용 응답을 보냅니다. Enigma 노드가 클로킹에 참여하지 않거나 적시에 응답하지 않으면 대체 Enigma 노드가 선출되고 연락됩니다.

DDoS 보호는 나머지 세션 동안 오작동하는 노드를 블랙리스트에 올립니다. 노드가 Enigma 교환에 서명하는 것을 반복적으로 거부하거나 Enigma 메시지 릴레이를 거부하는 경우, 노드는 오작동하는 것으로 간주됩니다. Enigma 클로킹 노드는 Elliptic Curve Diffie Hellman (ECDH) 키 교환을 사용하여 클로킹 노드와 송신 노드 사이에서 대칭 RSA-256 데이터 암호화를 위한 공유 비밀 키를 생성하는 데 사용되는 Enigma 개시 노드와 공유 된 비밀을 유도합니다.

ENIGMA 클로킹 허용

Enigma 노드가 '클로킹'요청을 수락하면 Enigma 트랜잭션에 사용할 트랜잭션 입력 및 출력 목록을 제공합니다. 클로킹 노드가 제공 한 입력 값은 Enigma 전송 금액 (또는 모든 수수료)보다 크거나 같아야합니다. Enigma 트랜잭션의 실제 출력과 가능한 한 가깝게 일치하도록 출력을 신중하게 선택합니다. Enigma 출력 주소가 이전에 사용되지 않았 으면 'Cloaker'에 의해 새 변경 주소가 생성됩니다. Enigma 산출 주소가 이전에 자금을 수령 한 경우 유사한 활동을하는 기존 주소가 'Cloaker'에 의해 선택되어 투입 자금을 반환하고 Enigma '클로킹'보상을받습니다.

은신된 ENIGMA교환

Enigma 발신자는 Enigma Cloaker(클로커) 노드에서 제공하는 입력과 출력을 사용하여 은폐된 교환을 생성합니다. Enigma 보내는 이는 클로킹을 용이하게 하기 위해 모든 교환 입력과 출력을 섞기 전에 교환에 자신의 입력과 출력을 추가합니다. 이렇게 클로킹된 교환은 암호화되어 CloakShield를 사용하여 각 참여 클로커에게 전송됩니다. 클로커 노드는 교환을 확인하여 교환이 제공 한 입력과 출력이 은폐된 교환에 존재하는지 확인하고 하나 이상의 출력에도 충분한 수수료가 지급되는지 확인합니다.

거래 검사가 통과하면 거래가 서명되고 (SIGHASH_ ALL + SIGHASH_ ANYONECANPAY), 암호화되어 다시 Enigma 보내는 이에게 전달이 됩니다. 모든 Enigma 클로커들이 거래에 서명하면 Enigma 보내는 이는 서명된 거래가 유효하고 서명됐음을 확인합니다. 이 모든 과정이 완료되면 은폐(Cloak)된 거래는 네트워크에 제출할 준비가 됩니다.

2.2.1. ENIGMA 클로킹 노드 추적

Cloak 네트워크의 Enigma 활성화된 노드들은 다른 노드로 알림을 방송합니다. 이 Enigma 공지에는 노드의 공용 ec-key ID와 현재 Enigma 클로킹 작업에 사용할 수 있는 잔액이 포함되어 있습니다. 노드는 클로킹 목적으로 통신 할 수 있도록 네트워크상의 다른 활성 Enigma 노드 목록을 유지 관리합니다. 노드 ID는 세션 단위로 생성됩니다. 클라이언트를 다시 시작하면 현재 ID가 새로 고쳐집니다.

1. 각 지갑은 시작할 때 세션에 대한 공용/암호 (secp256k1) 키 쌍을 작성합니다.

2. 지갑은 Cloak 네트워크의 다른 노드에 주기적으로 세션의 공개 키와 클로킹 잔여를 알립니다.

3. 노드는 다른 활성 Enigma Cloaking 노드를 추적하며 (CloakShield Onion Routing을 통해) 직접 또는 간접적으로 노드와 통신 할 수 있습니다.

2.2.2. ENIGMA 거래 개시

앨리스는 5 믹서 노드를 사용해 밥에게 10 CLOAK을 보내기를 원합니다.

1. 앨리스는 Enigma 요청을 네트워크에 방송하고 Enigma 세션 키와 전송하려는 CLOAK의 수를 포함합니다. 그녀의 요청은 일련의 5개의 Enigma 노드를 통해 안전하게 전달되어 발신자를 숨길 수 있습니다.

2. 캐서린은 'Cloaking Mode' (클로킹 모드)를 활성화하고 앨리스와의 안전한 통신을 위한 안전한 CloakShield의 암호화 채널을 생성합니다. 캐서린은 Enigma 응답 패킷을 구성하여 안전하게 앨리스에게 보냅니다. 응답에는 앨리스가 거래를 은폐하는데 사용할 캐서린의 입출력 목록이 포함되어 있습니다.

3. 앨리스는 캐서린의 Enigma 응답을 해독하고 처리하고 캐서린의 입력과 출력의 혼합된 고유한 입력과 출력을 사용하여 Enigma 거래를 생성합니다. 이것은 암호화되어 서명을 위해 캐서린에게 보내집니다.

4. 캐서린은 Enigma 거래를 해독하고 거래에 대한 무결성 검사를 수행하여 그녀가 제공 한 입출력이 올바르게 사용되고 충분한 보상을 받았는지 확인합니다. Enigma 거래가 테스트를 통과하면 캐서린이 서명하고 암호화하여 앨리스에게 전송합니다.

5. 앨리스는 서명한 거래를 서명하기 전에 추가로 확인합니다. 거래는 블록에 포함시키기 위해 네트워크 (Enigma 노드를 통해 안전하게 라우팅됨)에 제출됩니다.

6. 거래가 완료되면 밥은 앨리스에게서부터 자금을 수령하고 캐서린은 Enigma 거래를 도운 대가로 클로킹 보상을 받게 됩니다.

7. 앨리스의 입력과 출력을 반영하는 캐서린의 입력과 출력 때문에, Enigma 거래의 진정한 발신자와 수신자를 확인할 수 없습니다.

ENIGMA 거래 예

앨리스는 밥에게 익명으로 코인을 보내고 싶어합니다.

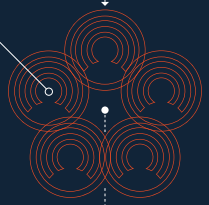
앨리스 (–10.0992) CLOAK

(–10) CLOAK + (–0.0992) Enigma 수수료
= (–10.0992) 총 CLOAK

Enigma 믹서 노드가 커뮤니케이션을 시작합니다.

캐서린

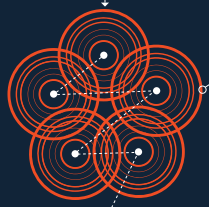
모든 코인 보유자는 믹서 노드, 혹은 '클로커'로 자신들을 공개합니다.



각 참여자는 익명으로 남고 암호화된 채널을 통해 소통합니다.

앨리스의 지갑은 이제 믹서 노드들에게 연결되었습니다.

각 믹서 노드는 거래 주의에서 셔플을 함으로써 앨리스는 도웁니다.



이 노드 네트워크는 TOR Onion Routing에 비슷한 분산된 익명화를 생성합니다.

믹서 노드들은 앨리스의 거래를 클로크한 대가로 보상을 받습니다.

(+0.0992) CLOAK

0.2% (>1000 코인) 에서부터 1% (0코인)의 일차적 수수료가 모든 참여하는 클로커들에게 나눠집니다.

완전한 익명성과 개인성을 위해 계속해서 ¬시스템이 일합니다.

이렇게 밥은 앨리스의 암호화된 지불을 받습니다.

밥 (+10) CLOAK

밥은 성공적으로 10 CLOAK을 익명자로부터 받습니다.

3. CLOAKSHIELD

CloakShield는 Elliptic Curve Diffie Hellman key exchange (ECDH)에 의해 지원되는 대칭 RSA 암호화를 사용하여 Cloak 네트워크의 노드 간에 보안 통신을 제공합니다. 이를 통해 노드는 데이터를 안전하게 교환하고 스누퍼 (중개자)와 임포저 (Sybil 어택)로부터 보호합니다. CloakShield는 Enigma와 분산 CloakCoin 응용 프로그램을 모두 보호하도록 설계되었으며 가능한 비공개로 데이터를 유지합니다.

CloakShield는 하나 이상의 수신자에게 암호화된 데이터 전송을 허용합니다. 단일 수신자에게 전송할 때 페이로드는 ECDH 공유 암호를 사용하여 RSA 암호화됩니다. 여러 명의 받는 사람에게 보낼 때 페이로드는 일회성 키를 사용하여 암호화 된 다음 ECDH/RSA 방법을 사용하여 받는 사람마다 암호화됩니다.

공유된 암호화키 생성

앨리스와 밥이 안전하게 통신하려면 공유 암호화 키에 동의해야 합니다. CloakShield는 ECDH를 사용하여 다음을 수행합니다:

- 앨리스는 Enigma 개인 키 dA와 Enigma 공개 키 QA = dAG (G는 타원 곡선의 생성자 임)가 있습니다. 밥은 Enigma 개인 키 dB와 Enigma 공개 키 QB = dBG를가집니다.
- 앨리스는 클로킹 지원 가능성을 발표하기 위해 네트워크에 보내는 Enigma 발표에서 밥의 Enigma 공개 키 dB를받습니다. 그녀는 개인 비밀 키 dA와 Bob의 공개 키 QB를 사용하여 공유 비밀 dAQB = dAdBG (OpenSSL의 ECDH_compute_key)를 계산합니다.
- 그런 다음 앨리스는 비밀의 SHA256 해시를 만들고 OpenSSLEVP_BytesToKey 메소드에 해시를 전달하여 암호화 키를 얻고 IV를 사용하여 Bob의 데이터를 암호화합니다 (대칭 RSA 암호화 사용).
- 이제 앨리스가 밥에게 CloakShield 보안 메시지를 생성 할 수 있게 되었습니다.

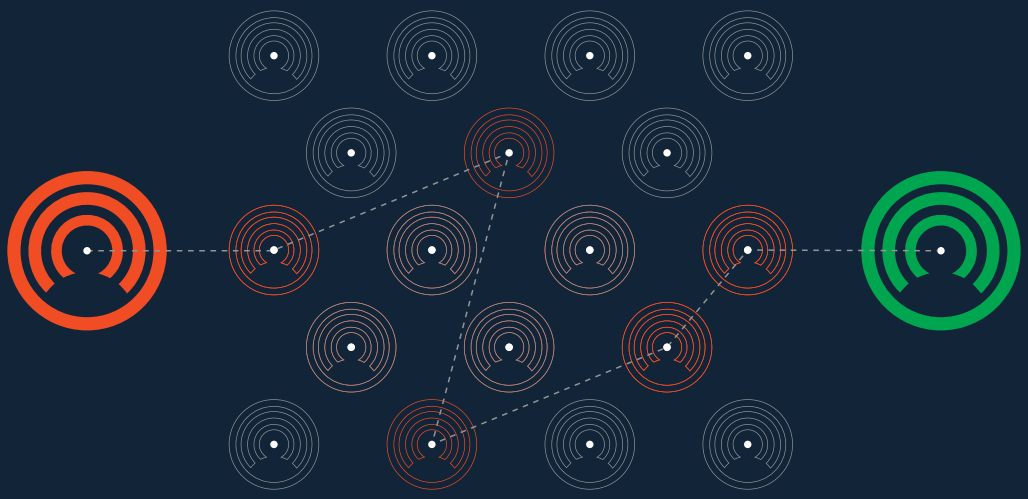
밥은 앨리스로부터 Cloak Shielded 메시지를 받으면 메시지 헤더에서 앨리스의 공개 키를 읽은 다음 위 단계 (앨리스의 키 대신 자신의 비밀 키로)에서와 동일한 앨리스의 공유 키를 생성합니다.

Cloak Wallet은 활성 CloakShield 키 목록을 유지 관리하며 목록을 생성하기 전에 기존 CloakShield 키를 확인합니다.

CLOAKSHIELD 데이터

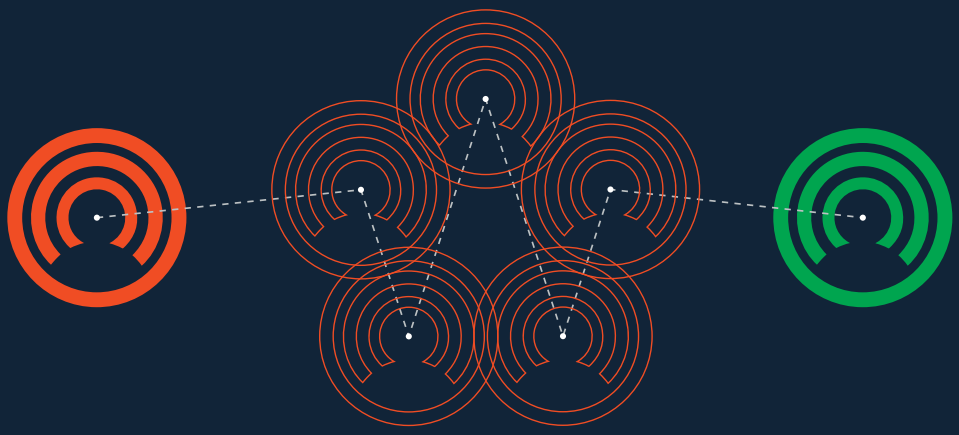
CloakShield를 사용하면 모든 Cloak 데이터 객체를 하나 이상의 수신자에게 안전하게 직렬화하고 전송할 수 있습니다. CloakShield 데이터 패킷 헤더는 보낸 사람의 Enigma 공개 키와 수신자의 공개 키 해시를 포함합니다.

CloakShield 헤더에는 보낸 사람의 공개 키와 암호화되지 않은 원시 데이터를 사용하여 생성되는 확인 해시가 들어 있습니다. 이 해시는 헤더의 수신자 정보가 암호화 키와 일치하는지, 그리고 데이터가 변경되지 않았는지 확인하기 위해 CloakShield 데이터를 해독하는 동안 확인됩니다.



CLOAKSHIELD ONION ROUTING (어니언 라우팅)

어니언 라우팅은 컴퓨터 네트워크를 통한 익명 통신을 위한 기술입니다 (TOR에서 사용). 어니언 네트워크에서 메시지는 양파 레이어와 유사한 암호화 계층으로 캡슐화됩니다. 암호화된 데이터는 어니언 라우터라고하는 일련의 네트워크 노드를 통해 전송되며 각 노드는 단일 레이어를 "벗겨내어"데이터의 다음 대상을 찾습니다. 최종 계층이 암호 해독되면 메시지는 대상에 도착합니다. 각 중개자는 바로 앞뒤의 노드의 위치 만 알고 있기 때문에 보낸 사람은 익명으로 유지됩니다.



어니언 라우팅 유사

Enigma 네트워크 (CloakShield 사용)에 어니언 라우팅 기능을 추가하면 노드가 트래픽 분석을 우회하기 위해 간접적으로 통신 할 수 있습니다. 이는 어느 노드가 서로 통신하고 있는지 또는 어떤 노드가 CloakCoin 네트워크에 거래를 제출 하는지를 결정하려는 시도를 방해합니다. Enigma 노드는 다른 Enigma 노드와 통신하기를 원할 때 통신을 위한 릴레이 역할을 하는 다른 Enigma 노드를 선택합니다. 각 암호화 된 계층은 [특정 계층이 암호화 된] 의도 된 릴레이에 의해서만 해독 될 수 있습니다. 레이어를 해독 한 후 릴레이는 데이터를 다음 릴레이 노드로 전달합니다. 이 라우팅은 데이터가 의도 된 수신자에 도달하고 모든 계층이 선택된 중계 노드에 의해 해독 될 때까지 계속됩니다. Enigma 네트워크의 자체 특성으로 인해 종료 노드는 필요하지 않으며 CloakShield는 중계 노드가 암호화 된 데이터를 읽거나 변경할 위험이 없음을 보장합니다.

4. 은폐된 주소들

CLOAK은 사적이고/안전한 거래를 추진하기 위해 Enigma 시스템을 이용합니다.

CLOAKSHEILD – 노드에서부터 노드 소통

각 클록 지갑은 개인 키와 수신자의 공개 키를 사용하여 ECDH를 사용하여 임시 비밀을 파생시킬 수 있도록 [NID_secp256k1] 키 쌍 (클로킹 암호화 키 / CEK)을 생성합니다. 이 통신은 Enigma와 관련된 모든 노드 간 통신의 기초를 형성합니다. 자세한 내용은 'src / enigma / cloakshield.h / .cpp'를 참조하십시오. 이 ECDH 기반 암호화 통신은 CloakShield에서 처리하는 어니언 라우팅 데이터에도 사용됩니다.

어니언 라우팅이 활성화되면 클라이언트는 알고있는 Enigma 피어 목록을 사용하여 데이터에 대한 유효한 어니언 경로를 구성하려고 시도합니다. 노드는 Enigma 피어에 직접 연결할 수는 없지만 CloakData (CloakShield로 라우팅하기 위해 압축 된 데이터) 패킷은 피어 투 피어로 릴레이 됨으로 필요하지 않습니다. 어니언 루트는 대개 경로 당 3 개의 노드 홉이 있는 대상 노드에 대한 3 개의 별개의 라우트로 구성됩니다. 라우팅 노드가 오프라인 상태로 되는 상황에 대처하기 위해 여러 경로가 사용됩니다.

노드는 주기적으로 Enigma Announcement (src / enigma / enigmaann.h)를 전송하여 어니언 라우팅에 대한 서비스를 광고합니다. 네트워크의 다른 노드는 알림이 만료되거나 업데이트로 대체 될 때까지 저장하고 어니언 경로를 구성하는 데 사용합니다.

은폐된 주소 거래 예

노드가 은폐된 주소에 Enigma거래를 보냈을 때 다음의 경우가 발생합니다:

1. 보내는 이는 보낸 금액, Enigma보너스 및 네트워크 수수료 (1000 코인 이상의 경우 0 % 코인에서 1 %)를 입력으로 생성합니다.
2. 보내는 이는 CloakingRequest 객체 (이 요청에 대해 고유 스텔스 넌스 포함)를 생성합니다.
3. 보내는 이는 받는 이의 스텔스 주소를 사용하여 2 회에서 4 회까지의 일급 스텔스 지불 주소를 생성하고 보낸 금액을 주소 간에 임의로 나눕니다.
4. 보내는 이는 사용할 참가자 수를 결정합니다. 5-25 명의 참가자가 선택 될 수 있습니다 (각 참가자는 동일한 Enigma 요금의 80-120 %를 받습니다).
5. 보내는 이는 어니언 루트 Cloak 네트워크에 요청합니다. 요청에는 송금액이 포함되어 있으므로 클로커는 자신이 얼마를 보유할지 알 수 있습니다.
6. 클로커가 CloakRequest를 선택하고 참여하기로 결정합니다.
7. 클로커는 X 입력을 보내는 이에게 보내고 스텔스 주소와 스텔스 해시를 변경합니다.
8. 클로커는 CloakingAcceptResponse를 보낸 사람에게 보냅니다. 여기에는 스텔스 주소, 스텔스 넌스 및 TX 입력이 포함됩니다.
9. 보낸 사람은 충분한 클로커가 받아 들일 때까지 기다립니다.
10. 보낸 사람은 충분한 클로커가 받아 들일 때까지 기다립니다.
11. 보낸 사람은 모든 클로커들에 관한 TX 출력을 만듭니다. 출력물은 무작위로 변경 사항을 분할하여 반환합니다. 이것은 또한 클로커들에게 클로킹 보상을 할당합니다.

12. 발신자는 Enigma TX에 대한 고유 한 변경 반품을 생성합니다. 이것은 일회성 은폐 지불 주소입니다.

13. 보내는 이는 네트워크 TX 수수료를 계산하고 자신의 변경 반환 값에서 이 값을 뺍니다.

14. 보내는 이가 Enigma TX를 클로커에게 싸인을 하기 위해 보냅니다.

15. 클로커들은 TX가 입력 내용이 정확하고 올바른 지, 입력 금액을 초과하는 지불로 스텔스 주소 중 하나에 연결된 일회성 지불 주소가 있는지 확인합니다.

16. 클로커는 텍사스에 서명 또는 거부하고 서명을 보내는 이에게 보냅니다.

17. 송신자는 서명을 대조하고 최종화되고 서명된 TX를 네트워크로 전송합니다.

18. 노드는 스텔스 지불 및 Enigma 지불을 위해 수신 트랜잭션을 스캔하고 지불 또는 변경을 감지합니다. 일치하는 지불에 대해 키 쌍 및 주소가 생성되고 생성 된 키/주소는 로컬 지갑에 저장됩니다.

5. ENIGMA의 미래 – 더한 발전

Enigma는 클로크코인(CloakCoin)의 핵심을 형성하며 클로크코인으로 발전함에 따라 계속 개발되고 개선 될 것입니다. 다음은 향후 개정을 위해 계획된 일부 기능입니다.

발전된 지분증명 알고리즘

지분증명은 블록에 서명하기 위해 동전의 소유권을 보여주는 사용자에게 의존하는 크립토커런시 네트워크를 보호하는 방법입니다.

장기적으로 블록에 서명 할 확률은 소유 한 동전의 양에 비례하며, 동전 공급의 1 %를 소유 한 사람은 모든 스테이크 블록 증거 중 1 %를 서명 할 수 있습니다. 증명 작업 방식과 비교할 때, 스테이크 증명은 계산력이 훨씬 적어 에너지 사용량이 훨씬 적습니다.

코인 에이지, 그리고 일차적(선형) 지분증명

클로크코인을 포함하여 지분증명의 대부분의 구현에 기본이 되는 것은 코인 에이지의 개념입니다. 본질적으로, 이것은 코인 홀더가 지출이나 이동없이 코인에 얼마나 오래 붙들었는지를 측정한 것입니다. 거래가 완료된 시점부터 해당 거래의 일부인 코인은 코인 나이를 축적하기 시작합니다 (0부터 시작). 선형 코인 시대라는 가장 간단한 형태로, 코인은 매분/시간/일/년의 동전 연령의 분/시간/일/년을 축적합니다. 예를 들어, 365 코인을 100 일 동안 보유하고있는 사람은 36,500 개의 코인 일 또는 약 100 년 코인을 축적합니다 (코인 주년은 윤년을 설명하기 위해 정의되었으므로 정확히 365 일이 아니고 약 365.24 일입니다).

일차적 지분증명 디자인은 코인 시대와 관련하여 비판을 받았습니다. 많은 사람들이 선형 증표가 코인의 축적을 장려한다고 주장합니다 (무역 및 이전 물량에 악영향을 미칠 수 있음). 선형 증명 증거에 대한 또 다른 유효한 불만은 네트워크 보안에 미칠 수 있는 영향과 관련이 있습니다. 일차적 지분 증명은 종종 사용자가 정기적으로 망내 네트워크에 연결하여 코인을 걸고 모든 코인 시대가 파괴되면 연결을 끊기 때문에 어려움을 겪습니다. 그런 다음 사용자는 연결 스테이크 분리 프로세스를 반복하기 전에 코인 에이지가 보충 될 때까지 기다립니다. 이는 네트워크에 대한 최상의 보안을 제공하지 못하며 빈번하거나 일정한 스테이징을 보상하는 지분증명 알고리즘이 클로크코인과 관련된 지분증명 통화에 가장 유익합니다.

Enigma Cloakers가 최대한 충실한 보상을 받으려면 CloakCoin의 Proof-of-Stake 알고리즘에서 Coin Age를 제거해야합니다. 이것은 Cloakers가 Stake 보상과 Enigma Cloaking 보상을받을 수 있도록합니다. 스테이 킹 보상을 계산할 때 속도 요소를 추가로 통합하면 Enigma Cloaking 노드를 추가로 보상 할 수 있으므로 사용자가 Enigma Cloaking에 참여하여 얻은 클로킹 보상과 함께 획득 이익을 추가로 높일 수 있습니다.

개선 된 Proof-of-Stake 알고리즘은 적극적으로 참여하는 사용자에게 더 많은 보상을 제공 할뿐만 아니라 앞서 언급 한 네트워크 보안 기능 향상을 제공합니다.

ENIGMA 거래의 분열과 결합

Enigma는 현재 전송 당 하나의 은폐된 거래를 생성합니다. 우리는 현재 여러 개의 Enigma 거래를 Enigma 슈퍼 거래로 결합 할 수 있는 Enigma 프레임 워크에 대한 업데이트 작업을 하고 있습니다. 이렇게 하면 여러 은폐된 거래가 효과적으로 포함되어 Cloak 사용자에게 훨씬 더 많은 익명 성을 제공합니다. 이 확장을 통해 사용자는 클로커들의 수 이외에 필요한 Enigma 거래의 수를 선택할 수 있습니다.

물론이 과정은 완전히 분산되고 개인적이고 안전하게 유지됩니다. 클로킹 팀이 현재 강화하고있는 또 다른 'Enigma'는 클로킹을 대량의 클로킹을 더 작은 일련의 작은 Enigma 거래로 은폐 처리하는 것입니다. 이를 위해 사용자는 은폐된 코인을 주소로 보내려는 클로크의 양을 선택합니다. 그런 다음 클로크코인은 백그라운드에서 일정량의 Cloak 네트워크에 제출할 수있는 일정량의 작은 Enigma 거래를 생성합니다. 이 일괄 처리 프로세스는 결합된 Enigma 거래와 호환되므로 전송을 위한 클로킹 보호를 제공합니다.

6. FAQ

Q. 클로커들이 ENIGMA 거래를 어떻게 도우나요?

클로커들은 보내는 이의 입력을 망가뜨리는데 사용되는 하나 이상의 입력을 제공합니다. 클로커들은 일련의 반환 주소를 제공하여 클로커에게 요금을 지불하고 보상을 제공합니다. 반환 주소는 활동이 있는 주소의 우선 순위를 정할 때 신중하게 선택됩니다. 이를 통해 블록 체인 분석을 수행하는 사람이 Enigma 거래의 실제 출력을 정확히 찾아내는 것이 더 어려워집니다. Enigma 시스템은 또한 목표 주소를 확인하여 은폐된 출력이 가능한 가깝게 실제 출력을 반영하도록 합니다.

Q. ENIGMA 거래를 완료하는데 얼마나 시간이 걸리나요?

Enigma 거래는 현재 1 분 내에 완료됩니다. Enigma 거래를 은폐하는데 도움이 되는 클로킹 노드는 Enigma 거래가 완료되거나 할당된 시간이 만료 될 때까지 필요한 자금을 예약합니다. 만료되었거나 중단된 Enigma 거래의 경우, 자금은 재사용을 위해 지역적으로 잠금 해제됩니다.

Q. ENIGMA가 스테이킹에게 어떻게 영향을 주나요?

Enigma 거래 (발신자 또는 클로커)에 사용 된 모든 코인에는 코인 보관함 초기화가 적용됩니다. 그러나 클로킹에 참여하는 것은 스테이크보다 훨씬 더 많은 수익을 제공해야 한다는 점에 유의해야합니다. Cloak 팀은 곧 출시 될 하드 포크 (Enigma 1.1)에 대한 Enigma 알고리즘을 수정하려고 합니다. 자세한 내용은 섹션 5 - 'Enigma의 미래 - 더한 발전'을 참조하십시오.

Q. ENIGMA 클로커가 되기 위해 나의 지갑 잔고에 일정량의 클록 금액이 필요합니까?

클로크코인 지갑의 잔고와 상관없이 클로킹 서비스를 제공 할 수 있습니다. Enigma 클로킹이 활성화되면 클로크코인은 Enigma 클로킹에 참여하기 위해 저울의 일부를 예약합니다. 그러면 클로킹 보상을 받게됩니다. 기본 예약 금액은 약 50%이지만이 값은 사용자가 조정할 수 있습니다. 광고된 클로킹 잔액으로 Enigma 공고의 연결을 방지하기 위해 값이 무작위로 선택됩니다.

더 높은 잔고를 가진 지갑은 더 큰 Enigma 거래에 필요한 클로킹 잔액을 가질 확률이 높기 때문에 클로커로 선택 될 확률이 더 높습니다.

Q. 이 제품은 특정 입력과 출력을 위해 블록체인을 누군가가 보았을 때를 기본으로 하여 어떻게 보호됩니까?

Enigma 거래는 출력을 그룹화하고 수신자의 출력을 은폐하기 위해 일치하는 출력을 여러개 보유하도록 보장됩니다.

Q. 서명 순서를 결정하기 위해 스크립트 서명을 검토하여 ENIGMA 거래의 기원자를 결정할 수 있습니까?

서명 과정에서 서명을 결합 할 때 스크립트 서명 순서가 무작위로 지정됩니다. 보낸 사람과 참여하는 클로커가이 작업을 수행합니다.

Q. 몰래 엿듣는 이가 네트워크를 모니터링하여 발신자를 알아내기 위해 보내는 ENIGMA 거래가 네트워크에 전송되는지 감시 할 수 있습니까?

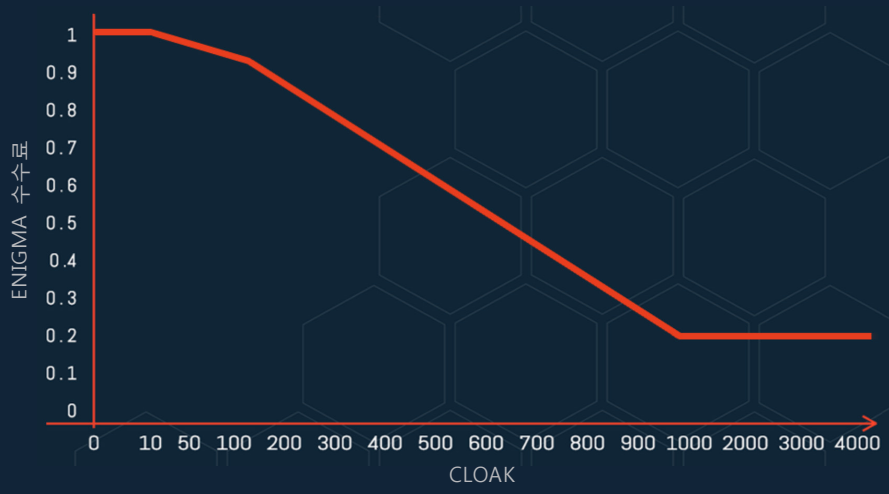
할 수 없습니다. 임의의 순서로 모든 당사자가 네트워크에 Enigma 거래를 제출합니다. 이것은 그러한 도청 공격에 대한 완화를 제공합니다.

Q. ENIGMA 거래의 수수료 값은 무엇입니까?

1000 코인 이상에서 0 코인에서 1 % .2 %. 이는 Enigma 거래를 은폐하는 데 도움이 되는 Enigma 노드를 보상하는 데 사용됩니다. 수수료는 거래와 혼합되어 클로커 사이에서 분리됩니다. 참가자들에게만 주는 보상은 아닙니다. 거래 금액의 결정을 어렵게 하는 데 도움이 됩니다. 각 참여자는 동등하게 분할 된 수수께끼 거래의 80-120 %를 받습니다.

Q. ENIGMA 수수료는 어떻게 결정됩니까?

Enigma 수수료는 거래 당 기준으로 다음 요금으로 청구됩니다:



TX 금액	Enigma 수수료	CLOAK 수수료
0	1.00	0
10	0.992	0.0992
50	0.96	0.48
100	0.92	0.92
200	0.84	1.68
300	0.76	2.28
400	0.68	2.72
500	0.60	3.00
600	0.52	3.12
700	0.44	3.08
800	0.36	2.88
900	0.28	2.52
1000	0.20	2.00
2000	0.20	4.00
3000	0.20	6.00

Q. ENIGMA가 클로크 네트워크의 하드포크를 요구합니까?

아니요. 오래된 클로커코인 고객은 문제없이 에니매이션 거래를 처리 할 수 있지만 해당 거래를 생성하거나 은폐 할 수는 없습니다. 그러나 Enigma의 다음 개정판에서는 기본 지분증명 알고리즘의 변경 때문에 시장 기능 (Block Escrow와 같은)에 대한 추가 스크립트 opcode 지원으로 인해 하드 포크가 필요합니다.

Q. ENIGMA 거래가 부담할 수 있는 최대의 클로커 금액이 무엇입니까?

클로커들의 최대 수는 25로 고정되어 있습니다. Enigma 시스템은 유연하며 이 숫자는 쉽게 확장 할 수 있습니다.

Q. ENIGMA는 연기자(사기꾼)들에게서부터 어떻게 보호를 합니까?

Enigma 시스템은 세션 기간 동안 '차단 목록' 노드에 대한 광범위한 DDoS 보호 기능을 제공합니다. Enigma 노드가 반복적으로 서명을 거부하면 현재 세션의 나머지 부분에 대한 Enigma 클로킹 초대에서 제외됩니다. 우리는 현재 비협조적인 Enigma 노드를 추가 처벌하기위한 추가 방법론을 연구 중이며 노드가 Enigma 거래를 차단하려고 시도 할 때 페널티로 주장 할 수 있는 명목상의 환불 가능한 수수료를 클로커들이 에스크로하여 요구하는 시스템을 구현할 것입니다. 악의적인 노드는 Enigma 거래를 방해하려고 시도 할 수 있지만 어떤 자금도 도용하거나 부당하게 사용할 수는 없습니다.

Q. 은폐된 거래와ENIGMA 거래는 어떻게 발견/받아집니까?

모든 들어오는 거래를 검사합니다. 스텔스 거래는 먼저 검색됩니다 (임의의 OP_RETURN TX 출력에 포함된 임시 pubkey 사용). 그런 다음 Enigma 거래가 검색됩니다. Enigma 거래는 또한 임시 epuberal pubkey를 사용하지만 지불은 추가 파생 키와 관련된 추가 단계를 사용합니다. Enigma 출력은 일시적인 pubkey의 해시, 개인 스텔스 주소 해시 및 출력 색인을 사용하여 생성됩니다.

Enigma 거래를 검색 할 때 각 소유 스텔스 주소 [HASH (ephemeral_pubkey, hash_stealth_secret, 0)]에 대해 제로 인덱스 지불 주소가 생성됩니다. 스텔스 주소의 0 색인과 일치하는 항목이 발견되면 나머지 색인 [num_tx_outputs]에 대해 추가 주소가 생성되고 이러한 주소는 검색을 위해 검색됩니다. 자세한 정보는 wallet.cpp의 FindEnigmaTransactions를 참조하십시오.

Enigma TX 에 서명하기 전에 비슷한 방법으로 클로커들을 고용하여 정확하게 환불을 받을 수 있습니다. 자세한 정보는 wallet.cpp의 GetEnigmaOutputsAmounts를 참조하십시오.

7. 참조

[01] http://bitcoin.org

[02] https://en.bitcoin.it/wiki/Category:Mixing_Services

[03] https://wiki.openssl.org/index.php/Elliptic_Curve_Diffie_Hellman

[04] http://blog.ezyang.com/2012/07/secure-multiparty-bitcoin-anonymization

[05] https://bitcointalk.org/index.php?topic=279249.0 (CoinJoin: Bitcoin Privacy for the Real World)

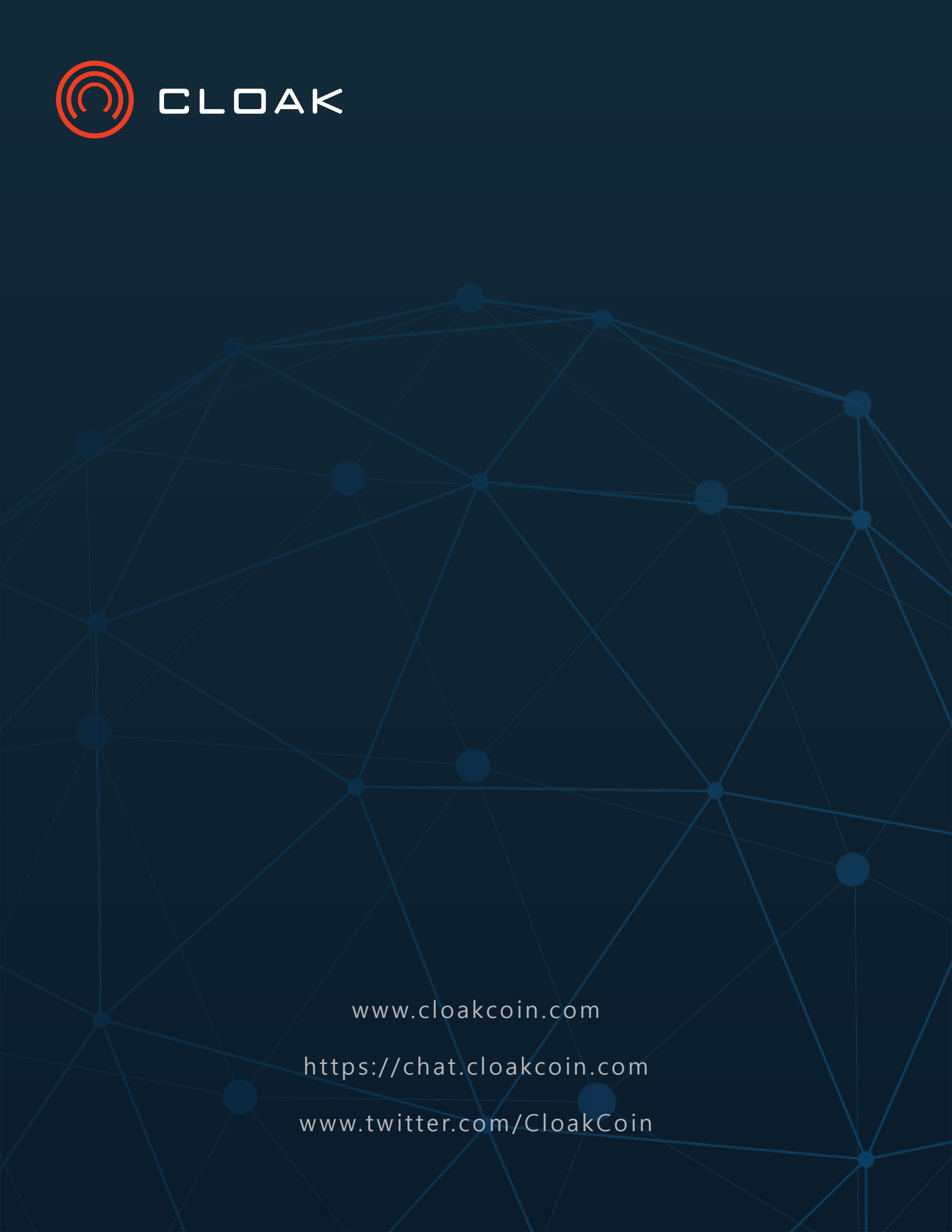
[06] https://bitcointalk.org/index.php?topic=27787.0 (Proof of Stake Instead of Proof of Work)

[07] https://en.bitcoin.it/wiki/Proof_of_Stake

[08] https://en.bitcoin.it/wiki/Deterministic_wallet

[09] https://github.com/bitcoin/bips/blob/master/bip-0032.mediawiki

[10] http://www.onion-router.net



www.cloakcoin.com

https://chat.cloakcoin.com

www.twitter.com/CloakCoin