Y2 (에틸 자일 렌)

아랍 연맹 Y2 새로운 에너지 연료 실험실 똑똑한 계약

재생 불가능한 자원을 재생 가능 자원으로 전환

아랍 리그 엠블럼 리그, Y2 동전 로고, Y2 새로운 에너지 연료 실험실 로고

아랍 연맹 사무 총장

Ahmed Aboul Gheit 서명 확인 Y2

요약 :

Satoshi 가 2009 년 1 월에 Bitcoin 블록 체인을 시작했을 때 그는 세계에 두 개의 새로운 테스트되지 않은 혁신적인 개념을 도입했습니다. 첫 번째는 비트 코인으로, 자산 보증, 본질적 가치 또는 중앙 발급 기관없이

가치를 유지하는 분산 된 피어 - 투 - 피어 온라인 통화입니다. 지금까지 Bitcoin 은 대중의 주목을 많이 받았다. 정치 측면에서는 중앙 은행이없는 통화로 가격 변동이 컸다.

그러나 Satoshi Nakamoto 의 위대한 실험은 Bitcoin 에서도 똑같이 중요합니다. 작업 증명을 기반으로하는 블록 체인 개념은 사람들이 거래 순서에 대한 합의에 도달 할 수있게합니다. 응용 프로그램으로 Bitcoin 은 first-to-file 시스템으로 설명 될 수 있습니다. 한 사람이 50 개의 BTC 를 보유하고 동시에 50 개의 BTC 를 A 와 B 로 보내는 경우 첫 번째 확인 된 트랜잭션 만 적용됩니다. 이 두 가지 거래 중 어느 것이 먼저 도착 하는지를 결정하는 고유 한 방법이 없기 때문에이 문제는 수년 동안 분산 된 디지털 통화의 발전을 방해했습니다. Nakamoto 의 블록 체인은 신뢰할 수있는 최초의 분산 솔루션입니다. 이제 개발자의 관심이 비트 코인 기술의 두 번째 부분으로 빠르게 이동하기 시작하고 블록크 체인이 돈이 아닌 영역에서 어떻게 사용되는지 살펴 봅니다.

자주 언급되는 응용 프로그램에는 사용자 지정 통화 및 금융 도구 (색의 동전), 특정 기본 물리적 장치 (스마트 자산)의 소유권 및 도메인 이름 (도메인 통화)과 같은 대체 할 수없는 자산을 나타내는 체인상의 디지털 자산의 사용, 또한 분산 형 교환기, 금융 파생 상품, 포인트 투 포인트 (point-to-point) 도박, 체인 신원 및 평판 시스템과 같은 고급 애플리케이션.

또 다른 중요한 영역은 사전 정의 된 규칙에 따라 디지털 자산을 자동으로 전송하는 "스마트 계약"입니다. 예를 들어, "A 는 하루에 X 동전까지 인출

할 수 있고, B 는 하루에 Y 까지 가질 수 있으며, A 와 B 는 자유롭게 함께 추출 할 수 있으며 A 는 B 의 출금 권리를 철회 할 수 있습니다"형태로 저장 계약을 체결 할 수 있습니다. 이러한 종류의 계약을 논리적으로 확장하는 것은 분산 된 자율 조직 (DAO) - 조직의 자산을 포함하고 조직의 규칙을 인코딩하는 장기 스마트 계약입니다. Y2 코인의 목표는 내장 된 성숙한 Turing 완전한 언어로 블록 체인을 제공하는 것입니다.이 언어는 임의의 상태 전이를 인코딩하는 계약을 생성하는 데 사용할 수 있습니다. 사용자는 몇 줄의 코드를 사용하여 간단하게 로직을 구현할 수 있습니다. 위에서 언급 한 모든 시스템과 우리가 상상할 수 없었던 많은 시스템을 생성하십시오.

디렉토리

● **연혁**

○ **상태 전이 시스템으로서의 Bitcoin**

○ **Merkel Tree**

○ 대체 블록 체인 적용

○ 스크립트

● **Y2** 통화

○ **Y2** 통화 계정

○ 뉴스 및 거래

○ **Y2** 코인 상태 변환 기능

○ 코드 실행

● 신청

○ 토큰 시스템

○ **Y2** 에너지 파생 상품

○ 신원 및 평판 시스템

○ 분산 파일 저장

○ 지방 자치 단체

○ 추가 신청

● 기타 및주의

○ 향상된 고스트 프로토콜 구현

○ 수수료

○ 계산 및 튜링 완료

○ 통화 및 발행

○ 확장 성

● 개요 : 분산 응용 프로그램

● 결론

● 코멘트 및 고급 읽기

————

역사

재산 등록의 대체 적용과 같은 분산화 된 디지털 통화의 개념은 수십 년 전에 제기되었습니다. 1980 년대와 1990 년대의 대부분의 익명의 전자 현금 거래는 Chaumian 눈부신 기술에 기반을두고있었습니다. 이러한 전자 현금 거래는 높은 개인 통화를 제공하지만이 프로토콜은 모두 중앙 중개자에 의존하기 때문에 인기가 없습니다. 1998 년 B-돈 다이 웨이 (웨이 다이) 먼저 계산 도전과 분산 합의를 해결하여 돈을 만들 수있는 아이디어를 소개하지만, 제안하는 방법을 중심으로 주어진 합의를 달성하는 방법을 지정하지 않습니다. 2005 년, Hal Finney 는 b money 의

사고와 Adam Back 의 계산 상 어려운 해시 현금 (Hashcash)을 모두 사용하는 "재사용 가능한 작업 증명"개념을 도입했습니다.) cryptocurrency 통화를 생성하는 데 어려움이 있습니다. 그러나이 개념은 백엔드로서의 신뢰할 수있는 컴퓨팅에 의존하기 때문에 이상화에서 다시 손실됩니다.

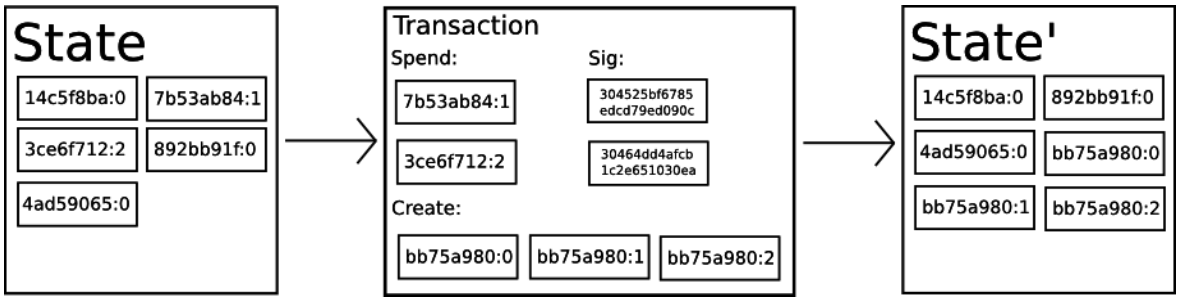
통화가 사전 신청 응용 프로그램이기 때문에 거래 순서가 중요하므로 분산된 통화는 분권화 된 합의를 도출 할 수있는 방법을 찾아야합니다. 모든 전자 화폐 프로토콜 이전에 주요 장애물 비트 코인은 보안 (비잔틴 결함 허용) 년 동안 지속했다을 만드는 방법에 대한 합의 비잔틴 결함 허용 문제에도 불구하고, 멀티 파티 시스템의 연구가 발생하지만, 이러한 계약은 절반 문제를 해결 . 이 프로토콜은 시스템의 모든 참가자가 알고 있다고 가정하고 "N 당사자가 시스템에 참여하는 경우 시스템이 N / 4 의 악의적인 참가자를 용인 할 수 있습니다"와 같은 보안 경계 양식을 생성합니다. 그러나,이 가상의 질문, 익명을 조건으로, 보안 경계가 공격자가 하나의 서버 또는 봇넷에 수천 개의 노드를 만들 수 있기 때문에, 마녀를 공격, 그렇게 만들 취약한 시스템에 의해 설정되어 있는지 확인 당신은 일방적인의 대부분이 공유.

Nakamoto 의 혁신은 매우 단순한 노드 기반의 분산 된 합의 프로토콜과 작업량 증명 메커니즘을 결합한 개념의 도입입니다. 노드는 작업량 증명 메커니즘을 통해 시스템에 참여할 수있는 권한을 얻게되며 트랜잭션은 10 분마다 "블록"으로 패키지화되므로 끊임없이 커지는 블록 체인이 생성됩니다. 운영자는 노드의 큰 힘이 더 영향을 가지고 있지만, 그것은

백만 노드를 만드는 것보다 더 많은 전체 전력 네트워크 사업자보다 얻는 것이 훨씬 더 어렵다. 비트 코인 블록 체인 모델은 매우 간단하지만은 향후 5 년에, 쉽게 충분히 입증했지만, 그것은 세계의 통화 및 프로토콜의 200 개 이상의의 초석이 될 것입니다.

상태 전환 시스템으로

Bitcoin



기술적 관점에서 Bitcoin 서적은 기존의 모든 Bitcoin 소유 상태와 "상태 전달 함수"를 포함하는 상태 전이 시스템으로 간주 될 수 있습니다. 상태 전이 함수는 현재 상태와 트랜잭션을 입력으로 받아 새로운 상태를 출력합니다. 예를 들어, 표준 은행 시스템에서는 상태가 대차 대조표입니다 .A 계좌에서 B 계좌로 X 달러를 송금하려는 요청은 트랜잭션이며, 상태 전달 함수는 A 계좌에서 X 달러를 뺀 다음 B 계좌에 추가합니다. X 달러. A 계정의 잔액이 X 달러 미만인 경우 상태 전 환 함수는 오류 메시지를 반환합니다. 따라서 다음과 같이 상태 전이 함수를 정의 할 수 있습니다.:

```
APPLY(S,TX) > S′ or ERROR
```

전술 한 은행 시스템에서, 상태 전이 함수는 다음과 같다:

```
APPLY({ Alice: $50, Bob: $50 },”send $20 from Alice to Bob”)
= { Alice: $30,Bob: $70 }
```

그러나:

```
APPLY({ Alice: $50, Bob: $50 },”send $70 from Alice to Bob”)
= ERROR
```

Bitcoin 시스템의 "상태"는 파기되어 소비되지 않은 모든 Bitcoin (기술적으로 "미사용 트랜잭션 출력 또는 UTXO"로 알려짐)의 모음입니다. 각 UTXO 에는 액면가와 소유자 (20 바이트 암호화 공개 키의 주소로 정의됨)가 있습니다. 트랜잭션은 하나 이상의 입력 및 하나 이상의 출력을 포함합니다. 각 입력에는 기존 UTXO 에 대한 참조와 소유자 주소에 해당하는 개인 키로 생성 된 암호화 서명이 포함됩니다. 각 출력에는 새 UTXO 가 상태에 추가됩니다.

비트 코인 시스템에서, 상태 전이 함수 APPLY (S, TX) -> S '는 대략 다음과 같이 정의 될 수있다.

1. 거래의 각 입력 :

● 참조 된 UTXO 가 현재 상태 (S)에 존재하지 않으면 오류 메시지가 반환됩니다

● 서명이 UTXO 소유자의 서명과 일치하지 않으면 오류 메시지가 반환됩니다

2. 모든 UTXO 입력 패싯 양이 모든 UTXO 출력 패싯 금액보다 적 으면 오류 메시지가 리턴됩니다

3. 새로운 상태 S '로 돌아가서 모든 입력 UTXO 가 새로운 상태 S'에서 제거되고 모든 출력 UTXO 가 추가됩니다.

첫 번째 단계의 첫 번째 부분은 트랜잭션의 보낸 사람이 존재하지 않는 Bitcoin 을 사용하지 못하도록하고 두 번째 부분은 트랜잭션의 보낸 사람이 다른 사람의 Bitcoins 를 보내지 못하게합니다. 두 번째 단계는 값의 보전을 보장합니다. Bitcoin 의 결제 계약은 다음과 같습니다. Alice 가 Bob 11.7 BTC 를 보내려고한다고 가정합니다. 실제로 앨리스는 정확히 11.7 BTC 를 가질 수 없습니다. 그녀가 얻을 수있는 Bitcoin 의 최소량은 6 + 4 + 2 = 12 라고 가정하십시오. 그래서 그녀는 3 개의 입력과 2 개의 출력으로 트랜잭션을 생성 할 수 있습니다. 첫 번째 출력에는 11.7 BTC 의 이름이 있고 소유자는 Bob (Bob 의 Bitcoin 주소)이고 두 번째 출력에는 0.3 BTC 의 이름이 있으며 소유자는 변경된 Alice 자신입니다.

신뢰할 수있는 중앙 집중식 서비스 조직이 있다면 상태 전이 시스템을 쉽게 구현할 수 있으며 위 기능을 간단하게 정확하게 코딩 할 수 있습니다. 그러나 우리는 분산 된 통화 시스템으로 비트 코인 시스템을 구축하고자합니다. 모든 사람이 거래 순서에 동의하도록하려면 상태 전환 시스템을 컨센서스 시스템과 통합해야합니다. Bitcoin 의 분산 된 합의 프로세스는 네트워크의 노드가 트랜잭션을 "블록"으로 꾸리는 데 끊임없이 노력하도록 요구합니다. 네트워크는 약 10 분마다 블록을 생성하도록

설계되었으며 각 블록에는 타임 스탬프, 난수, 이전 블록 (예 : 해시)에 대한 참조 및 이전 블록이 생성 된 이후 발생한 모든 트랜잭션이 포함됩니다. 목록. 이러한 방식으로 시간이 지남에 따라 지속적으로 증가하는 블록 체인이 생성되며 Bitcoin 북의 최신 상태를 나타 내기 위해 지속적으로 업데이트됩니다.

이 패러다임에 따르면 블록이 유효한지 여부를 확인하는 알고리즘은 다음과 같습니다.

1. 블록이 참조하는 이전 블록이 존재하고 유효한지 확인하십시오.

2. 블록의 시간 소인이 이전 블록의 시간 소인보다 빠르며 다음 2 시간 이전인지 확인하십시오.

3. 블록의 작업 부하가 유효한지 확인하십시오.

4. 이전 블록의 최종 상태를 S [0]에 지정하십시오.

5. TX 가 n 개의 트랜잭션을 포함하는 블록 트랜잭션 목록이라고 가정합니다. 0 ... n-1 에 속하는 모든 i 에 대해, 상태 전이 S [i + 1] = APPLY (S [i], TX [i])가 수행된다. 트랜잭션 i 가 상태 전이에서 실수를하면 프로그램을 종료하고 오류를 리턴하십시오.

6. 리턴은 정확하다. 상태 S [n]은이 블록의 최종 상태이다.

본질적으로 블록의 모든 트랜잭션은 올바른 상태 전이를 제공해야합니다. "상태"는 블록으로 코딩되지 않습니다. 그것은 어떤 블록이 (제대로 인해) 각 블록에 대한 세계 상태, 순서의 기초에서 플러스 거래 당 시작 현재 상태를 계산할 수 있습니다에 대한 순수한 추상화 체크 노드는 기억 될 것입니다. 또한 거래가 블록에 포함되는 순서에주의해야합니다. 두 개의 트랜잭션이 A, B 가있는 경우 A 는 B 가 이전 인 경우, 비용은이 블록이 유효하지 않습니다,이 블록 그렇지 않으면, 유효, UTXO A B 생성된다. 블록

블록 확인 알고리즘 흥미로운 개념은 "작업 증명"이다 : 각 블록에 대한 SHA256 해시 될 결과 해시 끊임없이 동적으로 조정해야하는 목표 값보다 작은 값의 256 비트의 길이로 간주 이 책을 쓰는 시점에서 대상 번호는 약 2 ^ 190 입니다. 목적은 부하함으로써 악의적 인 공격자 마녀 재생성 블록 사슬을 방지하는 블록을 생성하는 것이 곤란하게 입증한다. SHA256 때문에 의사 랜덤 함수 전혀 예측할 효과적으로 생성을 차단할 수있는 유일한 방법은 새로운 해시 값이 목표 값보다 작은 볼 난수의 값을 증가시키기 위해 계속해서 간단히 시행 착오이다. 현재 대상 값이 2 ^ 192 이면 유효 블록을 생성하기 위해 평균 2 ^ 64 시도가 필요함을 의미합니다. 일반적으로 Bitcoin 네트워크는 2018 블록마다 목표 값을 재설정하여 10 분마다 평균 블록을 생성합니다.

Bitcoin 네트워크에 악의적 인 공격자가있을 때 어떤 일이 발생하는지 분석해 보겠습니다. Bitcoin 의 암호화 기반은 매우 안전하기 때문에

공격자는 암호화로 직접 보호되지 않는 부분 인 트랜잭션 순서를 공격합니다. 공격자의 전략은 매우 간단합니다.

상품을 구매하기 위해 판매자에게 100BTC 를 보냅니다 (특히 우편으로 보낼 필요가없는 전자 제품).

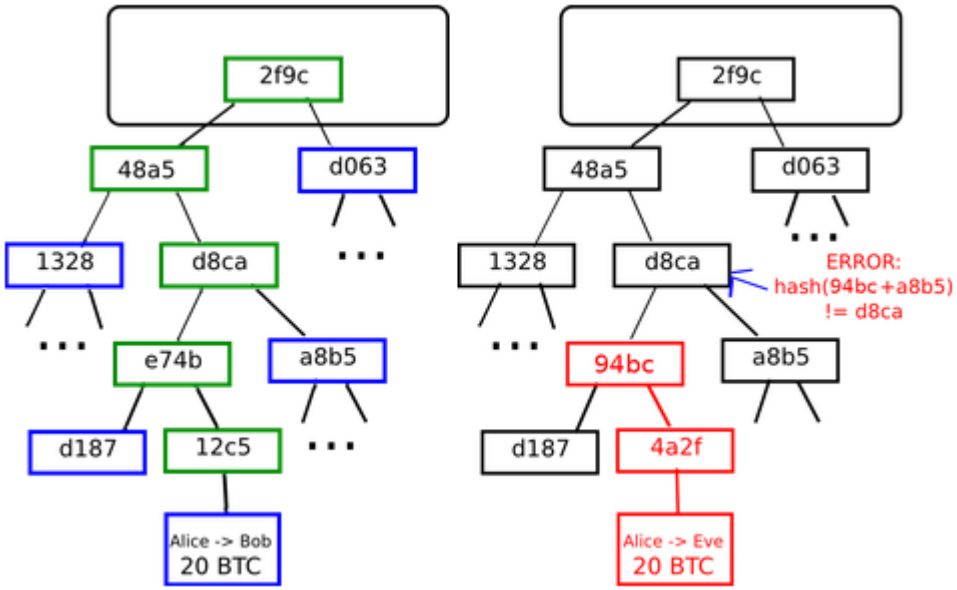
1. 상품이 발행 될 때까지 기다리십시오.

2. 다른 거래를 생성하고 동일한 100BTC 를 귀하의 계좌에 보냅니다.

3. Bitcoin 네트워크가 자신의 계정으로 전송 된 트랜잭션이 처음으로 전송되었다고 생각하게합니다.

단계 (1)이 발생하면 270000 번째 블록을 가정하고 트랜잭션이 몇 분 내에 블록으로 패키징됩니다. 약 1 시간 후,이 블록 뒤에 5 블록이있을 것이며, 각각은 트랜잭션을 간접적으로 가리켜 트랜잭션을 확인합니다. 현재 판매자는 지불액을 수령하여 구매자에게 발송했습니다. 이 제품이 디지털 제품이라고 가정하기 때문에 공격자는 즉시 제품을받을 수 있습니다. 이제 공격자는 다른 트랜잭션을 생성하고 동일한 100BTC 를 자신의 계정으로 보냅니다. 공격자가이 메시지를 전체 네트워크에만 브로드 캐스팅하면이 트랜잭션은 처리되지 않습니다. 상태 전이 함수 APPLY (S, TX)가 실행되고이 트랜잭션은 더 이상 상태가 아닌 UTXO 를 취하는 것으로 판명됩니다. 따라서 공격자가 체인 분기를 차단, 부모 블록으로 첫번째 269,999 블록은 처음 27 블록, 이전 거래를 대체 할 새로운 계약이 블록을 재생합니다. 블록 데이터가 다르기 때문에 작업 부하 증명이 필요합니다. 첫 번째 블록에 원래 제 270,001 270,005 이 가리 키지 않도록 새로운 제 270,000 블록 공격자 다른 해시를 생성했기 때문에 또한, 공격자 너무 신구 블록 블록 사슬이 완전히이었다 분리. 블록 사슬이 분기의 블록 사슬의 길이는 기존의 합법적 인 제 270,005 블록 따라 것이다 정직 블록 사슬로 간주 될 때 분기 270 000 의 새로운 블록에 하나 침입자 발생 . 그에게 블록의 긴 사슬을하기 위해 공격자는, 그 횟수 (즉, 51 %의 공격)를 잡기 위해 그의 더 힘뿐만 아니라 전체 네트워크에 이상을 가질 필요가있다.

메르켈 트리



왼쪽 : Merkle tree 에 소수의 노드 만 제공하면 분기에 대한 법적 증거가 충분합니다.

오른쪽 : Merkel tree 의 어떤 부분을 변경하려는 시도는 체인의 어딘가에서 결국 불일치로 이어질 것입니다.

Bitcoin 시스템의 중요한 확장 성 기능 중 하나는 블록이 다중 레벨 데이터 구조에 저장된다는 점입니다. 사실, 단지 블록 해시 해시 헤더 영역, 루트 해시 길이의 모든 거래를 타임 스탬프, 임의의 숫자, 해시 블록을 포함하고 나무 메르켈 블록에 저장 영역 헤더 약 200 바이트의 데이터.

Merkel 트리는 리프 노드 집합, 중간 노드 집합 및 루트 노드로 구성된 이진 트리입니다. 최하위 수의 리프 노드는 기본 데이터를 포함하고 각 중간 노드는 두 개의 하위 노드의 해시이며 루트 노드는 두 개의 하위 노드의 해시이며 Merkel 트리의 최상위를 나타냅니다. 메르켈 목적 산발적으로 전송 될 수있는 트리 데이터 블록을 허용한다 : 소스 노드는 데이터가 올바른지 모두 확인할 수 아직도 이와 다운로드 추가 소스 트리 연관된 다른 부분으로부터 헤더 영역으로부터 다운로드 할 수 있지만 . 이 때문에 때문에 확산 해시 업 : 나무의 아래쪽 지역에서의 악의적 인 사용자 시도가 가짜 거래를 추가하는 경우, 변경은 결국 루트로 이어지는 트리의 상위 노드 (upper node)에 의해 발생하는 변화뿐만 아니라 상위 계층 노드의 변화로 이어질 것 블록 해시의 변경 및 변경으로 계약에서이를 완전히 다른 블록으로 기록합니다 (거의 틀림없이 잘못된 작업량 증명과 함께).

Merkel 의 합의는 Bitcoin 의 장기적인 지속 가능성에 결정적인 요소입니다. 2014 년 4 월, 전체 노드에서 네트워크 비트 코인 - 노드 저장 및 모든 블록의 모든 데이터를 처리 - 필요 메모리 공간을 최대 15GB 까지 걸릴뿐만 아니라, GB 이상 매달 성장률. 현재이 저장 공간은 데스크톱 컴퓨터에서 사용할 수 있지만 휴대 전화에서는 이러한 대용량 데이터를로드 할 수 없습니다. 앞으로는 상업적 조직과 열광 자만 완전한 노드로 활동할 것입니다. 결제 확인을 단순화 (SPV)이 프로토콜은 다른 노드의 존재가,이 노드가 "빛 노드"는, 만 무역 관련 메르켈 트리 "분기를 다운로드 증명 작업 부하를 확인하기 위해 헤더 영역을 사용하여 헤더 영역을 다운로드입니다 수 있습니다 ". 이를 통해 라이트 노드는 전체 블록 체인 중 일부만 다운로드하여 Bitcoin 트랜잭션의 상태와 계정의 현재 잔액을 안전하게 결정할 수 있습니다.

기타 블록 체인 어플리케이션

블럭 체인이라는 아이디어를 다른 영역에 적용하려는 아이디어는 오래 전부터 등장 해왔다. 2005 년 사브 닉은 "제목과 재산의 소유권 '의 개념을 제시 용지는 데이터베이스 기술의 개발, 불법 잠식 예를 들어, 체인 기반 시스템은 토지 소유권의 등록에 적용 할 수있는 블록을 복사 포함한 재산권을 만드는 방법에 대해 설명합니다 조지아 및 토지 세와 같은 개념에 대한 자세한 프레임 워크. 그러나 불행히도 당시에는 실용적인 사본 데이터베이스 시스템이 없었기 때문에이 프로토콜은 실용화되지 않았습니다. 그러나 2009 년 Bitcoin 시스템의 성공적인 분산 된 합의 개발

이후, 블록 체인의 다른 많은 응용 프로그램이 빠르게 등장하기 시작했습니다.

● namecoin - 2010 년에 만들어지며 분산 된 이름 등록 데이터베이스라고합니다. Tor, Bitcoin 및 BitMessage 와 같은 분산 형 프로토콜에는 다른 사용자가 사용자와 상호 작용할 수 있도록 계정을 확인하는 몇 가지 방법이 필요합니다. 그러나 모든 기존 솔루션에서 유일하게 사용할 수있는 ID 는 1LW79wp5ZBqaHW1jL5TciBCrhQYtHagUWy 와 같은 의사 랜덤 해시입니다. 이상적으로 사람들은 "조지"와 같은 이름의 계정을 갖고 싶어합니다. 그러나 문제는 누군가 "조지"계정을 만들 수 있으면 다른 사람들도 "조지"계정을 만들어서 가장 할 수 있다는 것입니다. 유일한 해결 방법은 first-to-file 이며 첫 번째 등록자 만 성공적으로 등록 할 수 있으며 두 번째 등록자는 동일한 계정을 다시 등록 할 수 없습니다. 이 문제는 Bitcoin 의 합의 프로토콜을 사용할 수 있습니다. 도메인 이름 통화는 블록 체인을 사용하여 이름 등록 시스템을 구현하는 가장 초기의 성공적인 시스템입니다.

● 착색 된 동전 - 착색 된 동전의 목적은 사람들에게 Bitcoin 블록 체인 또는 더 중요한 통화 - 디지털 토큰에 자신의 디지털 통화를 생성 할 수있는 기능을 제공하는 것입니다. 컬러 통화 계약에 따르면 사람들은 특정 Bitcoin UTXO 에 색상을 할당하여 새로운 통화를 발행 할 수 있습니다. 이 프로토콜은 다른 UTXO 를 재귀 적으로 트랜잭션 입력

UTXO 와 동일한 색으로 정의합니다. 이는 특정 색을 유지하기 위해 사용자가 다시 UTXO 블록 사슬 판정받은 모든 색상을 통해 비트로 정규 코인 전송 등 UTXO 보내 UTXO 만 포함 할 수 있습니다.

● Metacoins - Metacoins 의 아이디어는 비트 동전 트랜잭션을 사용하여 통화 트랜잭션을 저장하지만 다른 상태 전달 함수 APPLY '를 사용하여 Bitcoin 블록 체인에 새 프로토콜을 만드는 것입니다. 적용 할 경우 비트 코인 블록 체인에 유효하지 않은 프로토콜 요소 통화 거래를 막을 수 없습니다 달러짜리 지폐는, 규칙이 증가하기 때문에 (S, TX) = S. '(S, TX 가) 오류를 반환, 기본 프로토콜은 적용' 이것은 Bitcoin 시스템에서 구현할 수없는 임의의 고급 암호화 통화 프로토콜을 만드는 간단한 솔루션을 제공하며 네트워크의 문제가 이미 Bitcoin 프로토콜에 의해 처리되므로 개발 비용이 매우 낮습니다.

따라서 일반적으로 컨센서스 프로토콜을 수립하는 두 가지 방법이 있습니다. 독립 네트워크를 구축하고 Bitcoin 네트워크에 대한 계약을 수립하는 것입니다. 같은 도메인 동전으로 첫 번째 방법을 사용하여 응용 프로그램은 성공적이었다, 그러나 각 응용 프로그램이 모든 상태 전환 및 네트워크 코드를 별도의 블록 체인을 만들 빌드, 테스트 할 필요가 있기 때문에 메서드의 구현은 매우 어렵지만. 또한, 우리는 지수 법칙 분포, 대부분의 응용 프로그램은 무료 블록 체인의 안전을 보장하기 위해 너무 작은 것 컨센서스 예측 기술의 중심에 적용, 우리는 또한 특히 분산, 분산

애플리케이션의 많은 수의 발견 자율적 인 조직은 응용 프로그램과 상호 작용해야합니다.

한편, 비트 코인에 기초한 방법의 단점이 있고,이 상속되지 않는 특성이 크레디트 결제합니다 (SPV)를 확인을 간략화 할 수있는 비트. Bitcoin 은 유효성 확인 에이전트로 블록 체인 깊이를 사용할 수 있으므로 지불 확인을보다 쉽게 할 수 있습니다. 어떤 시점에서 거래의 조상이 충분히 멀리 떨어져 나간 후에는 합법적 인 국가의 일부로 간주 될 수 있습니다. 반대로 Bitcoin 블록 체인을 기반으로하는 통화 교환 프로토콜은 통화 체인 교환 프로토콜을 준수하지 않는 트랜잭션을 차단하도록 강제 할 수 없습니다. 따라서 안전한 통화 프로토콜의 간단한 지불 확인은 특정 트랜잭션이 유효한지 여부를 확인하기 위해 블록 체인의 초기 지점까지 모든 블록을 역방향으로 검색해야합니다. 현재 비트 코인 프로토콜은 신뢰할 수있는 서버에 의존 위안 통화의 구현에 모든 "빛"의 주요 목적 중 하나 암호 통화 측면에서 신뢰의 필요성을 제거하는 것입니다 데이터를 제공하지만, 오히려 하위 최적의 결과.

스크립트

Bitcoin 프로토콜이 확장되지 않더라도 어느 정도 "현명한 계약"을 성취 할 수 있습니다. Bitcoin 의 UTXO 는 둘 이상의 공개 키에 의해 소유되거나 스택 기반 프로그래밍 언어로 작성된보다 복잡한 스크립트에 의해 소유 될 수 있습니다. 이 모드에서 UTXO 를 사용하면 스크립트를 만족하는 데이터를 제공해야합니다. 사실, 공공 소유의 기본 메커니즘은 스크립트를

통해 이루어집니다 : 입력으로 스크립트 타원 곡선 서명, 그렇지 않으면 0 을 반환 1 을 반환, 트랜잭션을 확인하고 성공하면 UTXO 의 주소를 가지고있다. 더 복잡한 스크립트는 다른 여러 응용 프로그램 시나리오에 사용됩니다. 예를 들어, 사람들은이 스크립트는 매우 유용합니다, 어셈블리, 스크립트 무역 확인 (다중 서명), 회사의 계정, 저축 계정 및 특정 상업 에이전트에서이 3 개인 키를 필요로 만들 수 있습니다. 스크립트를 사용하여 계산상의 문제를 해결하는 사용자에게 보상을 보낼 수도 있습니다. "당신은 당신이 지불 확인의 내 강아지 단순화 증거 일정 금액을 보내 가지고 제공 할 수있는 경우, 비트 코인 UTXO 이는 당신입니다"하나는 심지어 본질적으로 이러한 스크립트를 만들 수 있으며, 비트 코인 시스템은 서로 다른 암호를 수 통화로 분권화 된 교환을 배우십시오.

그러나 비트 코인 시스템의 스크립팅 언어에는 몇 가지 심각한 제한이 있습니다.

• Turing Completeness 누락 - 비트 script 스크립팅 언어가 여러 계산을 지원할 수 있지만 모든 계산을 지원할 수는 없음을 의미합니다. 주요 결함은 루프 문입니다. 루프 문을 지원하지 않는 목적은 트랜잭션 확인시 무한 루프를 피하는 것입니다. 어떤주기가 예를 들어, 길의 문 경우 반복에 의해 모델링 할 수 있지만, 이렇게하면 스크립트 공간의 비효율적 인 사용으로 이어질 것입니다 때문에 이론적으로, 스크립트 프로그래머,이 장애물은, a 의 구현을 극복 할 수있다 대안적인 타원 곡선 서명

알고리즘은 아마도 매번 별도의 인코딩을 요구하는 256 회 반복의 곱셈을 요구할 것이다.

가치 실명. UTXO 스크립트는 계정 철수 금액에 대한 세부적인 제어를 제공하지 않습니다. 예를 들어, 강력한 응용 프로그램의 신탁 계약 (신탁 계약) 계약을 회피하고, A 와 B 는 각각 계약을 헤지하기 위해 비트 코인 년에 $ 1,000 값을 보내 30 일 후, 스크립트는 B 에게 A 를 $ 1,000 bitcoins 을 전송 나머지 비트 코를 보냅니다. 필요가 헤지 계약의 신탁을 구현할 수 있지만 (오라클) 얼마나 많은 통화 달러 비트를 결정하지만 지금은 완전히 중앙 집중식 솔루션에 비해,이 메커니즘은 신뢰와 인프라를 줄이는 엄청난 진행하고있다. UTXO 가 불가분 때문에,이 계약의 실현을위한 유일한 방법은 UTXO 많은 다른 교 매우 비효율적으로 사용하는 것이다 (예를 들어, K (30)의 각각에 대한 최대에 대응하는 2 ^ k 개의 UTXO 임) 및 오라클이 A 와 B 에 보낼 올바른 UTXO 를 예측하도록하십시오.

누락 된 상태 - UTXO 는 소비되거나 낭비 될 수 없으므로 다른 내부 상태가 필요한 다중 단계 계약 또는 스크립트를위한 공간이 없습니다. 따라서 다단계 옵션 계약, 분산 교환 제안 또는 2 단계 암호화 약정 계약 (계산 보상 보장에 필수)을 구현하기가 어렵습니다. 이것은 또한이 달성 달러 계약 어렵게 분산 된 조직보다 복잡한 상태를 가지고 같은 UTXO 은 단순 일회성 계약이 아닌 계약을 설정하는 데 사용할 수 있다는 것을

의미한다. 이진 상태와 가치 장님이 결합 됨으로써 또 다른 중요한 응용 프로그램 인 철수 제한이 달성 될 수 없음을 의미합니다.

Blockchain-blindness - UTXO 는 난수와 이전 블록의 해시와 같은 블록 체인 데이터를 보지 않습니다. 이 결함은 게임과 같은 다른 영역의 애플리케이션을 심각하게 제한하는 무작위성을 기반으로 잠재적 가치의 스크립팅 언어를 박탈합니다.

우리는 암호화 통화에서 고급 응용 프로그램을 구축하기 위해 세 가지 방법을 검토 한 다음 비트 코인 블록 체인에 스크립트를 사용하여, 새로운 블록 체인을 구축, 블록 체인 비트 코인 위안 통화의 설립에 합의. 새로운 블록 체인을 구축하는 방법은 임의의 기능을 자유롭게 구현할 수 있습니다. 비용은 개발 시간과 노력을 조장하는 것입니다. 스크립트를 사용하는 방법은 구현 및 표준화가 매우 쉽지만 그 기능은 제한적입니다. 통화 교환 프로토콜은 구현하기가 쉽지만 확장 성이 떨어지는 단점이 있습니다. Y2 코인 시스템에서 우리의 목표는이 세 가지 모드의 모든 장점을 동시에 가질 수있는 공통 프레임 워크를 구축하는 것입니다.

Y2 통화

Y2 통화는 원유 재생 가능 자원의 분배를 변경하는 중동 아랍 연맹의 디지털 통화를 기반으로합니다. Y2 Y2 돈을 새로운 에너지 연구소 디지털 통화, 새로운 연료 첨가제, 연료 첨가제의 출시를 가속화하기위한 발행 Y2 의 Y2 를 실행하여 새로운 Y2 는 2035 년 약 20 배 저장 기존 Y2 를

업그레이드합니다, 2020 년 데뷔 할 것으로 예상된다 170 개 이상의 배를 달성, Y2 로 통화 1 병이 동일, 글로벌 신 재생 자원을 보호하기 위해, 세상을 구원 (가치, 기술은 튜링 완전성을 가지고 (유엔의 자원 구조 계획, 구원의 계획과 미국의 Y2 공동 스폰서라는) 가치 인식, 블록 체인 인식 및 다중 상태 추가 기능은 비트 코 스크립트가 제공 할 수있는 스마트 계약보다 훨씬 강력합니다.

Y2 계정

Y2 코인 시스템에서 상태는 "accounts"(각 계정은 20 바이트 주소 임)라는 개체와 두 계정간에 값과 정보를 전송하는 상태로 구성됩니다. Y2 코인 계정에는 네 부분으로 구성되어 있습니다.

• 트랜잭션 당 한 번만 처리 할 수있는 카운터를 결정하는 데 사용되는 난수

• 계정의 현재 Y2 잔액

• 계정의 계약 코드 (있는 경우)

• 계정 저장 (기본값은 비어 있음)

Y2 통화는 신 에너지 Y2 내의 주요 암호화 연료이며 거래 비용을 충당하기 위해 사용됩니다. 일반적으로 Y2 동전에는 두 가지 계정이 있습니다. 모든 외부 계정 (개인 키로 제어 됨)과 계약 계정 (계약 코드로 제어 됨)입니다. 모든 외부 계정에는 코드가 없으므로 사람들은

트랜잭션을 만들고 서명하여 외부 계정에서 메시지를 보낼 수 있습니다. 계약 계정에 메시지가 수신 될 때마다 계약 내의 코드가 활성화되어 내부 상점을 읽고 쓸 수 있으며 다른 메시지를 보내거나 계약서를 작성할 수 있습니다.

뉴스 및 거래

Y2 코인 뉴스는 비트 코인 거래와 다소 비슷하지만이 둘 사이에는 세 가지 중요한 차이가 있습니다.

첫째, Y2 코인 메시지는 외부 엔티티 또는 계약에 의해 생성 될 수 있지만 비트 코 트랜잭션은 외부에서만 생성 될 수 있습니다.

둘째, Y2 코인 메시지는 선택적으로 데이터를 포함 할 수 있습니다.

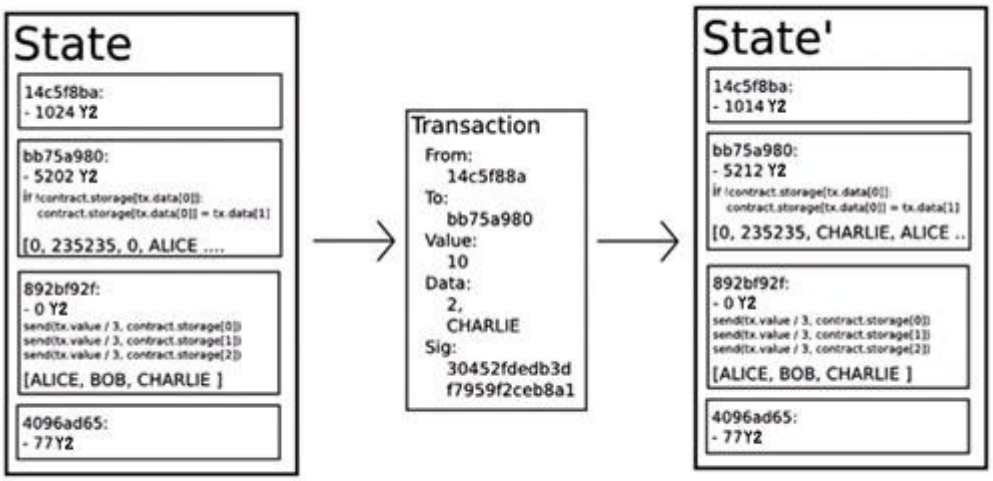
셋째, Y2 코인 메시지의 수신자가 계약 계정 인 경우 응답하도록 선택할 수 있습니다. 즉, Y2 코인 메시지에도 기능 개념이 포함됩니다.

Y2 통화의 '거래'는 외부 계정에서 보낸 메시지를 저장하는 서명 데이터 패킷을 의미합니다. 트랜잭션 메시지 송신자, Y2 현재 계좌 잔액의 서명을 검증하기위한 수신기를 포함하며, 데이터를 송신하고, 두 값의 GASPRICE STARTGAS 을 칭한다. 코드의 지수 폭발 무한 루프를 방지하기 위해, 각 트랜잭션은 트리거 실행을 코딩하는 단계를 계산해야 - 초기 메시지를 포함하고 메시지는 모두의 실행에 의해 트리거 - 제한 사항을 확인합니다. STARTGAS 는 한계이며, GASPRICE 는 각 계산 단계의 비용입니다.

거래가 실행되는 동안 "연료가 모두 사용 된 경우"모든 상태 변경 사항이 원래 상태로 복원되지만 이미 지불 한 거래 수수료는 복구 할 수 없습니다. 거래가 중단 될 때 연료가 남은 경우, 연료는 발송인에게 반환됩니다. 생성 계약에는 별도의 트랜잭션 유형과 해당 메시지 유형이 있으며 계약의 주소는 계정의 난수 및 트랜잭션 데이터의 해시를 기반으로 계산됩니다.

메시징 메커니즘의 중요한 결과는 Y2 통화의 "기본 시민"속성입니다. 계약에는 메시지를 보내고 다른 계약을 만들 수있는 권한을 포함하여 외부 계정과 동일한 권한이 있습니다. 예를 들어, 사용자는 분산 된 조직 (계약)의 구성원을 조정 계정 (다른 계약)으로 만들거나 파란색의 편집증 사용에 대한 양자 기반 인증을 사용자 정의 할 수 있습니다 Porter 서명 (세 번째 계약)을 가진 개인과 다섯 개의 개인 키 (네 번째 계약)로 보안이 설정된 계정을 사용하는 자체 서명 엔티티는 중개 서비스를 제공합니다. Y2 코인 플랫폼의 장점은 분산 된 조직 및 대행사 계약이 각 계약 참가자가 어떤 유형의 계정인지 신경 쓸 필요가 없다는 것입니다.

Y2 통화 상태 전달 함수



Y2 통화 상태 전달 함수: `APPLY(S,TX) -> S'`, 다음과 같이 정의 할 수 있습니다.:

1. 1. 트랜잭션의 형식이 올바른지 (즉, 올바른 값인지), 서명이 유효하며 임의의 숫자가 보낸 사람의 계정의 임의 번호와 일치하는지 확인하십시오. 그렇지 않으면 오류가 리턴됩니다.
2. 2. 수수료 = STARTGAS * GASPRICE 를 계산하고 서명에서 보낸 사람의 주소를 결정하십시오. 발신자의 계좌에서 거래 수수료를 뺀 후 발신자의 난수를 늘리십시오. 계좌 잔액이 부족하면 오류가 반환됩니다.
3. 3. 초기 값 GAS = STARTGAS 를 설정하고 트랜잭션의 바이트 수에서 일정량의 연료 값을 뺍니다.
4. 4. 보낸 사람의 계정에서받는 사람의 계정으로 값을 전송합니다. 수신 계정이 아직없는 경우이 계정을 만드십시오. 수신 계정이 계약 인 경우 코드가 만료되거나 연료가 모두 소모 될 때까지 계약 코드를 실행하십시오.
5. 5. 송금인의 계좌에 돈이 충분하지 않거나 계좌 이체가 끝나고 송금이 실패하면 원상태가 복구되지만 거래 수수료도 지불해야하며 계좌에 거래 수수료가 추가됩니다.
6. 6. 그렇지 않으면, 남아있는 모든 연료를 발송인에게 반환하고 사용 후 핵연료는 거래 수수료로 배송 센터로 보내야합니다.

코드 실행

Y2 코인 계약 코드는 저급 스택 기반 바이트 코드 언어로 작성됩니다. 코드는 일련의 바이트로 구성되며, 각 바이트는 연산을 나타냅니다. 일반적으로 코드 실행은 무한 루프입니다. 프로그램 카운터는 1 씩 증가하고 (초기 값은 0 입니다) 코드가 완료되거나 오류가 발생하거나

STOP 또는 RETURN 이 발생할 때까지 실행됩니다. 이 작업은 데이터 저장을위한 세 가지 종류의 공간에 액세스 할 수 있습니다.

스택, 마지막 선입 선출 데이터 저장소, 32 바이트 값을 스택에 푸시 할 수 있습니다.

● 메모리, 무한히 확장 가능한 바이트 대기열.

● 계약의 장기 저장, 비밀 키 및 값의 저장, 비밀 키 및 값이 모두 32 바이트 인 경우 계산 완료시 재설정되는 스택 및 메모리와 달리 저장된 내용은 오랜 시간 동안 유지됩니다.

코드는 블록 헤더 데이터에 액세스 할 때와 마찬가지로 수신 된 메시지의 값, 보낸 사람 및 데이터에 액세스 할 수 있으며 코드는 데이터의 바이트 대기열을 출력으로 반환 할 수도 있습니다.

PCM 코드의 공식 실행 모델은 놀라 울 정도로 간단합니다. Y2 코인 가상 머신이 실행 중일 때 완전한 계산 상태는 튜플 (block_state, 트랜잭션, 메시지, 코드, 메모리, 스택, pc, 가스)으로 정의 할 수 있습니다. 여기서 block_state 는 모든 계정 잔액과 저장 공간을 포함하는 전역 상태입니다. . 각 실행 라운드는 코드의 첫 번째 pc (프로그램 카운터) 바이트를 호출하여 현재 명령어가 발견되고 각 명령어가 튜플 자체에 미치는 영향을 정의합니다. 예를 들어, ADD 는 두 요소를 튀기고 그 합을 스택에 푸시하고 가스 (연료)를 줄이고 pc 를 하나에 추가 한 다음 SSTORE 는 맨 위 두 요소를 팝하고 첫 번째 요소를 두 번째 요소에 삽입합니다 각 요소는 계약

저장 위치를 정의하여 가스 값을 최대 200 까지 줄이고 pc 를 1 씩 증가시킵니다. Just-In-Time 컴파일을 통해 Y2 코인을 최적화하는 방법은 많지만 Y2 코인의 기본 구현은 수백 줄의 코드로 구현할 수 있습니다.

응용 분야

일반적으로 Y2 이상의 두 가지 응용 프로그램이 있습니다. 첫 번째 범주는 원유를 필요로하는 모든 국가, 기관 및 개인에게 재생 가능 에너지 지원을 제공하고 판매, 투자 및 기타 관련 응용 분야에 사용할 수있는 신 에너지 Y2 적용입니다. 두 번째 유형은 금융 애플리케이션이며 Y2 는 자원에서 금융으로 전환 할 수 있습니다. 미래는 분명히 글로벌 금융 전문가들이 선호하는 재정적 + 에너지 복합체가 될 것입니다.

토큰 시스템

체인상의 토큰 시스템에는 미국 달러 또는 금과 같은 자산을 나타내는 하위 통화에서 회사 주식, 스마트 자산을 나타내는 개별 토큰, 안전한 위조 쿠폰 및 기존 값과는 관계없는 많은 응용 프로그램이 있습니다. 보상 포인트를위한 토큰 시스템. Y2 동전에 토큰 시스템을 구현하는 것은 놀랍도록 쉽습니다. 요점은 모든 통화 또는 토큰 시스템이 근본적으로 다음 작업을 포함하는 데이터베이스라는 것을 이해하는 것입니다. A 에서 X 단위를 빼고 X 단위를 B 에 더합니다. 단, (1) A 거래 전에 적어도 X 단위가 있고 (2) 거래가 A.에 의해 승인되었습니다. 토큰 시스템을 구현하는 것은 이러한 논리를 계약에 구현하는 것입니다.

뱀 언어로 토큰 시스템을 구현하기위한 기본 코드는 다음과 같습니다:

```
from = msg.sender

to = msg.data[0]

value = msg.data[1]

if contract.storage[from] >= value:

contract.storage[from] = contract.storage[from] value

contract.storage[to] = contract.storage[to] + value
```

이것은 본질적으로이 기사에서 자세히 설명 할 "은행 시스템"상태 전이 함수의 최소 구현입니다. 초기 및 기타 주변 상황에서 통화를 배포 할 수있는 기능을 제공하려면 추가 코드를 추가해야합니다. 다른 계약에서 주소의 잔액을 조회 할 수있는 기능을 추가하는 것이 이상적입니다. 충분하다. 이론적으로, Y2 동전에 기초한 어린이 통화로 작동하는 토큰 시스템은 비트 동전 기반 체인 통화에서 부족한 중요한 기능인 거래 수수료를 직접 지불하는 데 통화를 사용할 수있는 기능을 포함 할 수 있습니다.

안정된 가치를 지닌 파생 상품 및 통화

금융 파생 상품은 "스마트 계약"의 가장 일반적인 응용 프로그램이며 코드를 사용하여 구현하기가 가장 쉽습니다. 금융 계약을 성취하는 주된 도전 과제는 대다수가 외부 가격 발행자를 참조해야한다는 것입니다. 예를 들어 매우 까다로운 응용 프로그램은 Y2 (또는 기타 암호 유포)를 달러

가격에 대해 헤지하기위한 현명한 계약입니다. 그러나 계약은 미국 달러 대비 Y2 의 가격을 알아야합니다. 가장 쉬운 방법은 기관이 필요에 따라 계약을 업데이트하고 다른 계약에서 (예 : 나스닥과 같은) 계약서를 보내도록 설계된 특정 조직 (나스닥과 같은)이 유지 관리하는 "데이터 제공"계약을 이용하는 것입니다. 계약서에 가격 정보가 포함 된 답장을 보내라는 메시지.

이러한 핵심 요소가 모두 갖추어지면 헤지 계약은 다음과 같습니다.

A 가 1000 Y2 통화를 입력 할 때까지 기다립니다. .

B 가 1000 Y2 통화를 입력 할 때까지 기다리십시오.

데이터 제공 계약을 조회하면 1000 Y2 동전의 달러 값 (예 : x 달러)이 메모리에 기록됩니다.

30 일 후에 A 또는 B 는 $ x 가치의 Y2 동전을 보내고 (새로운 가격에 대한 계약을 제공하고 계산할 데이터를 재 계산하여) A 로 보내고 나머지 Y2 동전을 B 로 보내도록 계약을 "재 활성화"할 수 있습니다

이러한 계약은 암호화 사업에 특별한 잠재력을 가지고 있습니다. cryptocurrency 의 한 가지 문제점은 가격 변동성입니다. 많은 사용자와 기업이 암호화 자산의 보안과 편의성을 필요로 할 수 있지만, 하루에 23 %의 자산 감소를 기꺼이 덜 느끼게됩니다. 가치의 상황. 지금까지 가장 일반적으로 권장되는 솔루션은 게시자의 자산 보증이었습니다.

그러나 실제로는 발행사가 항상 신뢰할만한 것은 아니며, 경우에 따라 은행 시스템이 너무 연약하거나 정직하지 않아 그러한 서비스를 불가능하게 만들 수 있습니다. 금융 파생 상품은 대안 솔루션을 제공합니다. 더 이상 자산을 지원하기위한 준비금을 제공 할 별도의 발행사가 없으며 암호화 자산의 가격을 인상하려는 투기꾼으로 구성된 분산 된 시장이 될 것입니다. 발행자와 달리 투기자는 헤지 계약으로 계약 준비금을 동결하기 때문에 거래 할 권리가 없습니다. 가격 정보를 제공하는 신뢰할 수있는 데이터 소스가 여전히 필요하기 때문에이 방법은 완전히 분산되지는 않지만 여전히 인프라 요구 사항을 줄이는 것은 논란의 여지가 있습니다 (게시자와 달리 가격 게시자는 라이센싱 및 언론의 자유로 분류 될 수 있음) 잠재적 사기 위험을 줄이기위한 커다란 진전입니다.

신원 및 평판 시스템

가장 초기의 대체 통화 인 도메인 이름 동전은 사용자가 공통 데이터베이스의 다른 데이터에 이름을 등록 할 수있는 이름 등록 시스템을 제공하기 위해 비트 코 유사 블록 체인을 사용하려고했습니다. 가장 일반적인 사용 사례는 "bitcoin.org"와 같은 도메인 이름 (또는 도메인 이름 통화의 "bitcoin.bit")과 IP 주소를 가진 도메인 이름 시스템입니다. 다른 응용 사례로는 전자 메일 검증 시스템 및 잠재적으로 고급 전자 평판 시스템이 있습니다. 다음은 Y2 통화로 도메인 이름 통화와 유사한 이름 등록 시스템을 제공하기위한 기본 계약입니다:

```
if !contract.storage[tx.data[0]]:

contract.storage[tx.data[0]] = tx.data[1]
```

계약은 매우 간단하며 Y2 코인 네트워크에 추가 할 수는 있지만 수정할 수 없거나 제거 할 수없는 데이터베이스입니다. 누구나 값으로 이름을 등록 할 수 있으며 결코 변경할 수 없습니다. 보다 복잡한 이름 등록 계약에는 다른 계약을 조회 할 수있는 "기능 조항"과 이름의 "소유자"(즉, 첫 번째 등록자)가 데이터를 수정하거나 소유권을 이전 할 수있는 메커니즘이 포함됩니다. 평판과 신뢰 네트워크 기능을 추가 할 수도 있습니다.

분산 스토리지

지난 몇 년 동안 사용자가 하드 드라이브 백업을 업로드하고 백업 스토리지 서비스를 제공하며 사용자가 월간 사용자 요금에 액세스 할 수 있도록 허용하는 인기있는 온라인 파일 스토리지 신생 업체가있었습니다. 그러나 파일 저장 시장은 때로는 상대적으로 비효율적 인 경우도 있지만, 기존 서비스를 매우 자세히 살펴보면 여유 공간과 엔터프라이즈 급 사용자 할인이없는 Mystic Valley 20-200GB 수준에서 특히 유용합니다. 매월 파일 저장 비용은 한 달 안에 전체 하드 디스크를 지불하는 비용을 의미합니다. Y2 법안은 분산 형 스토리지 에코 시스템을 개발할 수있게하여 사용자가 하드 드라이브 나 사용하지 않은 네트워크 공간을 임대하여 소액의 수익을 창출함으로써 파일 저장 비용을 절감 할 수 있도록합니다.

이러한 시설의 기본 구성 요소는 "분산 된 Dropbox 계약"입니다. 계약은 다음과 같이 작동합니다. 먼저 누군가 업로드 된 데이터를 청크로 분할하고 개인 정보를 보호하기 위해 각 데이터를 암호화하며 Merkel 트리를 만듭니다. 다음 규칙을 사용하여 계약을 생성합니다. 계약은 N 블록마다 Merkel 트리에서 무작위 색인을 추출하고 (계약 코드가 액세스 할 수있는 이전 블록의 해시를 사용하여 무작위를 제공합니다) 엔티티 X Y2 코인은 트리의 특정 인덱스에서 비슷한 단순 지불 확인 (SPV)을 사용하여 블록의 소유권 증명을 지원합니다. 사용자가 파일을 다시 다운로드하려는 경우 마이크로 지불 채널 프로토콜 (예 : 32kbytes 당 1 Saab 지불)을 사용하여 파일을 복구 할 수 있으며 가장 비용 효율적인 방법은 마지막 트랜잭션을 게시하지 않은 사람에게 비용을 지불하는 것이지만 32k 바이트마다 원래의 트랜잭션을 동일한 난수로 비용 효율적인 트랜잭션으로 대체하십시오.

이 계약의 중요한 특징은 한 사람이 파일을 잃을 준비가되어 있지 않은 많은 무작위 노드를 신뢰하는 것처럼 보이지만 그는 비밀리에 많은 작은 블록으로 파일을 공유 한 다음 계약을 모니터링하여 각 블록이 여전히 노드에 의해 저장됩니다. 계약이 여전히 지불 중이라면 누군가가 문서를 저장하고 있다는 증거를 제공합니다.

분산 된 자율기구 (DAO)

일반적인 의미에서, 분산 형 자율 조직 (DAO)의 개념은 일정한 수의 회원이나 주주가있는 가상 개체를 말하며, 예를 들어 67 %의 다수가

비용을 지출하고 코드를 수정하기로 결정합니다. 회원들은 조직이 자금을 어떻게 할당 할 것인지를 결정할 것입니다. 자금 배분 방법은 보상, 임금 또는 내부 통화로 보람있는 일과 같은 더 매력적인 메커니즘 일 수 있습니다. 이것은 단순히 암호화 블록 체인 기술을 사용하여 전통적인 회사 또는 비영리 단체의 법적 중요성을 근본적으로 복제합니다. 지금까지 DAO 를 둘러싼 많은 논의는 배당금 공유 주주와 유통 가능한 주식을 가진 "분산 형 자치 단체"의 "자본주의"모델을 중심으로 이루어졌으며 대안으로 "분산 형 자치 커뮤니티"단체는 모든 회원들이 의사 결정 과정에서 동등한 권리를 가질 수있게하며, 회원을 추가 또는 삭제할 때 67 %의 다수 동의를 요구합니다. 모든 사람은 하나의 회원 만 가질 수 있으며,이 규칙은 그룹에 의해 시행되어야합니다.

다음은 코드를 사용하여 DO 를 구현하는 방법에 대한 개요입니다. 가장 단순한 디자인은 구성원의 3 분의 2 가 동의하는 경우 자체 수정하는 코드입니다. 코드는 이론적으로 변경 될 수 없지만 코드 스켈레톤을 별도 계약에 배치하고 계약 전화 주소를 변경 가능한 저장소로 지정하면 코드를 쉽게 수정할 수 있습니다. DAO 계약의 간단한 구현에는 거래에서 제공하는 데이터로 구별되는 세 가지 거래 유형이 있습니다.

● [0, i, K, V] 등록 색인은 저장소 주소 색인 K 의 내용을 v 로 변경하기위한 제안입니다.

● [0, i] 제안 i 에 대한 투표를 등록합니다.

● [2, i] 충분한 투표가있을 경우 추천을 확인하십시오.

그런 다음 계약에는 각 항목에 대한 특정 조건이 있습니다. 모든 공개 스토리지 변경 사항에 대한 기록과 투표 한 사람의 테이블을 유지 관리합니다. 또한 모든 구성원의 테이블이 있습니다. 저장된 내용의 변경 사항에 대해 2/3 이상의 다수 동의를 얻으면 최종 거래가 변경을 실행합니다. 좀 더 복잡한 프레임 워크는 트랜잭션을 보내거나 회원을 늘리거나 줄이거 나 임명 된 민주주의와 같은 투표 대표를 제공하기 위해 내장 된 투표 기능을 추가합니다 (즉, 누구나 자신을 대신하여 다른 사람을 위임 할 수 있으며 이러한 종류의 위임 관계가 전달 될 수 있으므로 A 가 B 를 위임 한 다음 B 가 C 를 위임하면 C 가 A 의 투표를 결정합니다. 이 디자인은 DAO 가 분산 된 커뮤니티로서 유기적으로 성장할 수있게 해 주므로 사람들은 현재 시스템과 달리 궁극적으로 적합한 후보자를 전문가에게 선출하는 작업을 넘겨 줄 수 있습니다. 커뮤니티 구성원이 팀 시간을 지속적으로 변경함에 따라 전문가가 쉽게 등장하게됩니다. 그리고 사라집니다.

대안적인 모델은 회사의 분권화이며, 어떤 계정도 0 에서 더 많은 주식을 가질 수 있으며, 결정은 주식의 3 분의 2 다수가 동의 할 것을 요구합니다. 완전한 프레임 워크에는 자산 관리 기능 (주식 매매 주문 주문 및 인수 수락)이 포함됩니다 (계약서에 주문 일치 메커니즘이있는 경우). 대의원은 여전히 임명 민주주의의 형태로 존재하며 "이사회"의 개념을 갖습니다.

앞으로 더욱 발전된 조직 거버넌스 메커니즘이 구현 될 수 있으며 이제 분산 형 조직 (DA)은 분산 형 자치 조직 (DAO)에서 시작할 수 있습니다. DO 와 DAO 의 차이점은 모호합니다. 일반적인 분계선은 정치적으로 유사한 프로세스 또는 "자동화 된"프로세스를 통해 거버넌스를 달성 할 수 있는지 여부입니다. "직관적 인 테스트는"보편적 인 언어 없음 "표준입니다. 같은 언어 기관이 여전히 효과가 있습니까? 분명히 단순한 전통적인 지주 회사는 실패 할 것이며, 이와 같은 작은 협정은 성공할 것입니다. Robin Hansen 의 예측 시장을 통한 거버넌스 구성 메커니즘 인 "futarchy" "자율적인"거버넌스가 어떻게 보이는지에 대한 좋은 예입니다. 모든 DAO 가 모든 DO 보다 우월하다고 가정 할 필요는 없으며, 자율성은 일부 특정 시나리오에서는 큰 이점이있는 패러다임 일 뿐이지 만 다른 곳에서는 필연적 인 것은 아닙니다. 많은 준 DAO 가 존재할 수 있습니다.

추가 신청

1. 지갑 저장. Alice 는 돈이 안전한지 확인하려고하지만 개인 키를 분실하거나 해킹 당할 우려가 있습니다. 그녀는 Y2 코인을 Bob 과 계약을 맺습니다. 아래 그림과 같이 계약은 은행입니다 :

앨리스는 매일 최대 1 %의 자금을 인출 할 수 있습니다.

Bob 은 매일 최대 1 %의 자금을 추출 할 수 있지만 Alice 는 개인 키를 사용하여 Bob 의 철수 권한을 취소하는 트랜잭션을 생성 할 수 있습니다.

Alice 와 Bob 은 임의로 자금을 인출 할 수 있습니다.

일반적으로 Alice 는 하루에 1 %만으로 충분합니다. Alice 가 더 많은 금액을 인출하기를 원하면 Bob 에게 도움을 요청할 수 있습니다. Alice 의 개인 키가 도난당한 경우, Bob 은 즉시 새 계약으로 자금을 이체 할 수 있습니다. 그녀가 개인 키를 잃어 버리면, Bob 은 돈을 천천히 올릴 수 있습니다. 밥이 악의를 나타내면 철수 권을 끌 수 있습니다.

2. 작물 보험. 데이터 엔트리로 가격 지수 대신 기상 조건을 사용하여 금융 파생 계약을 쉽게 체결 할 수 있습니다. 아이오와 농부가 아이오와의 강수량에 따라 지불금을 되돌릴 수있는 금융 파생 상품을 구입하면 가뭄이 발생하면 농부는 자동으로 지불금을 받고 강우량이 충분하면 그의 작물이 아주 좋기 때문에 아주 행복합니다.

분산 된 데이터 게시자. 차이 기반 금융 계약의 경우 "Xerin point"프로토콜을 전달하여 데이터 게시자를 분산시킬 수 있습니다. X-Lindidian 의 작동 원리는 다음과 같습니다. N-Party 는 지정된 데이터 (예 : Y2 / USD 가격)에 대해 시스템에 입력 값을 제공하고 모든 값이 정렬되며 25 %와 75 % 사이의 값을 제공하는 각 노드는 보상을 받으려면 모든 사람들이 다른 사람들이 제공 할 답변을 제공 할 동기가 있습니다. 많은 수의 플레이어가 실제로 동의 할 수있는 답은 기본적으로 정답입니다. 이론적으로 사용할 수있는 값 (예 : Y2 / USD, 베를린 온도)을 구성합니다. 심지어 특히 계산이 어려운 결과의 중앙 집중식 프로토콜.

4. 다중 서명 스마트 계약. Bitcoin 은 다중 서명 기반 거래 계약을 허용합니다. 예를 들어, 5 개의 개인 키를 사용하여 자금을 수령 할 수

있습니다. 예를 들어 5 개의 개인 키를 사용하여 총 4 개의 자금을 수령 할 수 있으며, 3 개의 계정 만 매일 자금의 10 %를 사용하는 경우 2 개만 매일 자금의 0.5 % 만 지출 할 수 있습니다. . 또한 Y2 코인의 다중 서명은 비동기 적입니다. 즉, 양 당사자가 서로 다른 시간에 블록 체인에 서명을 등록 할 수 있으며 서명이있는 경우 마지막 서명이 자동으로 전송됩니다.

5. 클라우드 컴퓨팅. 또한 PCM 기술을 사용하여 사용자가 계산을 수행하도록 초대 한 다음 임의로 선택한 검사 점에서 올바르게 계산 된 증거를 선택적으로 요청할 수있는 검증 가능한 컴퓨팅 환경을 만들 수 있습니다. 이를 통해 모든 사용자가 데스크톱, 랩톱 또는 전용 서버에 참여할 수있는 클라우드 컴퓨팅 시장을 만들 수 있습니다. 현장 검사 및 보안 보증을 사용하여 시스템이 신뢰할 수 있는지 확인할 수 있습니다 (즉, 어떤 노드도기만 당할 수 없음). 리). 이러한 시스템은 모든 작업에 적합하지 않을 수 있지만 예를 들어 고급 프로세스 간 통신이 필요한 작업은 대규모 노드 클라우드에서 쉽게 수행되지 않습니다. 그러나 다른 작업을 사용하면 병렬 처리를 쉽게 구현할 수 있으며 SETI @ home, folding @ home 및 유전자 알고리즘은 이러한 플랫폼에서 구현하기가 쉽습니다.

6. 포인트 투 포인트 도박. 프랭크 스테 자노 (Frank Stajano)와 리처드 클레이튼 (Richard Clayton)의 사이버 디이스 (Cyberdice)와 같은 Y2 코인을 차단하기 위해 피어 투 피어 (Peer-to-Peer) 도박 계약을 수만큼 이동할 수 있습니다. 가장 단순한 도박 계약은 실제로 해시 값과 다음

블록의 추측 값 사이의 차이를 내기 위해 사용되는 단순한 계약이므로 거의 복잡한 도박 계약을 통해 거의 제로 비용을 달성 할 수 있으며 사기성 도박 서비스가 아닙니다.

7. 시장 예측. Schering 통화가 포함 된 예측 시장은 분산 된 조직 관리 계약으로 "futarchy"의 첫 번째 주류 응용 프로그램이 될 수 있습니다.

8. 체인은 정체성과 평판 시스템에 기반한 중앙화 된 시장으로 이동합니다.

기타 및주의

개선 된 고스트 프로토콜 구현

"유령"계약 ("욕심 무거운 관측 하위 트리"(GHOST) 프로토콜) 혁신을 소개하는 12 월 2013 년 Yonatan Sompolinsky 과 소할 아비브입니다. 고스트 프로토콜 의욕 때문에 낮은 보안 문제의 대상이 유효하지 않은 블록의 높은 속도의 빠른 현재 블록 체인을 확인하기 위해 제안, 그것은 무효가 높은 경우 (세트 t)는, 전체 네트워크로 확산 일정 블록이 걸리기 때문에, 단순한를 컴퓨팅 력의 높은 점유율 때문에 더 효율적입니다.

계산 블록도 포함하는 경우 바와 Sompolinsky 및 소할 된 바와 같이 스트랜드로 "긴"은 폐기물 유령 프로토콜 감소 네트워크 보안의 제 문제를 해결했다, 즉 단 하나 개의 블록, 말하자면 부모 블록과 이전의 조상은 사용되지 않는 블록 자손의 조상 블록 ("차 블록"이라고 Y2 기간 크레딧)

계산 지원 블록을 가지고 믹스에 추가 할 작업의 최대 크기는 또한, 차단 증거. 우리는 계약 Sompolinsky 하르을 넘어 두 번째 문제 해결하기 위해 기술 -에 넣어, 중앙 경향, 블록 보상의 87.5 %를 기여하는 폐기물의 새로운 블록의 신원을 확인하기 위해 "차 블록"에 지불 Y2 돈을 계산 된 "쓰레기 수거통 블록"은 보상의 12.5 %를 받게되지만 거래 수수료는 삼촌 블록에게 주어지지 않습니다.

Y2 동전은 5 층으로 내려가는 고스트 프로토콜의 단순화 된 버전을 구현합니다. 그 특성은 차 폐기물 블록 만 (예를 들면, 젊은 부모 6 세대 면적을 차단 오히려 젊은 세대 블록 먼 관계보다는, 이하의 블록의 제 5 세대의 두 번째 세대가 부모에 의해 차단할 수 있기 때문에, 아르 할아버지 블록의 블록 또는 3 세대 자손 블록이 계산에 포함됩니다. 이것에는 몇 가지 이유가 있습니다. 첫째, 무조건 고스트 프로토콜은 주어진 블록의 삼중 블록이 정당한 계산에 과도한 복잡성을 부여합니다.

비용

블록 체인으로 릴리스 된 각 트랜잭션은 다운로드 및 검증 비용을 감당하므로 스팸 거래를 방지하려면 트랜잭션 비용을 포함한 규제 메커니즘이 필요합니다.

그러나 간소화에 대한 덜 구체적인 정확한 가정이 주어지면이 시장 기반 메커니즘의 허점이 그 영향을 기적적으로 제거했다. 인수는 다음과 같습니다. 가정 :

1. 무역은 R 이 상인에 의해 설정되고 k 와 R 이 모두 (대략적으로) 가시적인 무역을 포함하는 누군가에게 보상 kR 을 제공하는 k 단계를 가져온다.

2. 각 단계를 처리하는 노드 당 비용은 C 입니다 (즉, 모든 노드의 효율성이 일정합니다).

3. N 개의 노드가 있으며, 각 노드는 동일한 컴퓨팅 성능 (즉, 전체 네트워크 전력의 1 / N)을 갖습니다.

그러나 이러한 가정과 실제 상황에서 몇 가지 중요한 편차가 있습니다.

도 1 에 도시 된 바와 같이, 여분의 검증 시간은 블록의 방송을 지연시키고 블록이 폐기물 블록이 될 확률을 증가 시키므로, 트랜잭션을 다른 검증 노드보다 더 많이 처리한다.

2. 실제로 힘의 분배는 극도로 고르지 않을 수 있습니다.

3, 자신의 정치적 반대자와 미친 사람으로 네트워크를 파괴하는 투기꾼이 존재하며, 그들은 비용이 다른 검증 노드보다 훨씬 낮아 지도록 지능적으로 계약을 설정할 수 있습니다.

위의 첫 번째 요점은 더 적은 트랜잭션을 포함 시켰고 두 번째 요점은 NC 를 추가 했으므로이 두 점의 영향이 서로 부분적으로 상쇄되었습니다 .3 및 4 점이 주요 문제이며 솔루션으로 간단하게 부동 상한 : 블록에 BLK_LIMIT_FACTOR 배에 장기 지수 이동 평균 이상을 포함 할 수 없습니다. 특히:

```
blk.oplimit = floor((blk.parent.oplimit * (EMAFACTOR - 1)
+ floor(parent.opcount * BLK_LIMIT_FACTOR)) /EMA_FACTOR)
```

BLK_LIMIT_FACTOR 및 EMA_FACTOR는 일시적으로 65536 및 1.5

상수로 설정되지만 추후 분석 후 조정할 수 있습니다.

계산 및 튜링 완료

JUMP 명령은 프로그램이 코드 어딘가에 뛰어 돌아갈 수있게하며, x <27 : x = x * 2 와 같은 조건문을 허용하는 JUMPI 명령은 조건부 점프를 구현합니다. 둘째, 계약은 재귀를 통해 루프를 달성 할 수있는 잠재력을 지닌 다른 계약을 호출 할 수 있습니다. 이것은 자연스럽게 문제가됩니다 : 악의적 인 사용자가 전체 노드가 무한 루프에 들어가게하여 강제로 종료 할 수 있습니까? 이 문제는 컴퓨터 과학의 문제로 인해 정전 문제로 인해 발생합니다. 일반적으로 특정 프로그램이 제한된 시간 내에 끝날 수 있는지 여부를 알 수있는 방법이 없습니다.

상태 전이 섹션에서 설명했듯이 우리의 솔루션은 각 트랜잭션에 대해 실행될 최대 계산 수를 설정하여 문제를 해결합니다. 초과하면 계산이 원래 상태로 돌아가지만 여전히 수수료가 유지됩니다. 뉴스는 같은 방식으로 작동합니다.

공격자는 send (A, contract.storage [A]); contract.storage [A] = 0 과 같은 계약이 포함 된 계약을보고 첫 번째 단계를 수행하기에 충분하지만 두 번째 단계를 수행하기에 충분하지 않은 상태로 보냅니다. 거래 (즉,

인출이지만 계좌 잔액을 줄이지는 않음). 계약 작성자는 실행이 중간에 중단되면 모든 변경 사항이 되돌려지기 때문에 비슷한 공격을 방어하는 것에 대해 걱정할 필요가 없습니다.

재정 계약은 위험을 최소화하기 위해 9 명의 개인 데이터 게시자의 중간 값을 추출하여 작동합니다. 공격자는 데이터 제공 업체 중 하나를 인수 한 다음 DAO 섹션에 설명 된대로이 가변 주소 호출 메커니즘을 변경 가능하도록 설계합니다. 이 금융 계약에서 자금을 요청하려는 시도를 유도하기 위해 무한 루프를 돌리는 데이터 제공 업체는 연료 고갈로 인해 일시 중지됩니다. 그러나 금융 계약은 이러한 문제를 방지하기 위해 메시지에 연료 제한을 설정할 수 있습니다.

Turing 을 완전히 대체하는 것은 Turing 불완전합니다. JUMP 및 JUMPI 명령어가 존재하지 않으며 주어진 시간에 호출 스택 내에 각 계약의 사본 하나만 존재하도록 허용됩니다. 그러한 시스템에서 계약 이행 비용은 그 규모에 따라 결정되므로 위에서 언급 한 수수료 시스템과 우리를 둘러싼 해법의 효율성에 대한 불확실성은 필요하지 않을 수 있습니다. 또한 Turing 은 불완전하거나 큰 제한이 아니며 지금까지 구상 한 모든 계약 예제에서 하나만 순환시켜야하며이 사이클조차도 26 개의 단일 라인 코드 세그먼트를 반복하여 대체 할 수 있습니다. Turing Complete 가 가져온 심각한 문제와 제한된 이점을 고려하여 단순히 Turing 불완전한 언어를 사용하지 않는 이유는 무엇입니까? Turing 이 불완전하다는 사실은 간결한 솔루션에서 멀리 떨어져 있습니다. 왜? 다음 계약을 고려하십시오:

```
C0: call(C1); call(C1);

C1: call(C2); call(C2);

C2: call(C3); call(C3);

…

C49: call(C50); call(C50);

C50: (run one step of a program and record the change in
storage)
```

이제, 이러한 거래는 재귀 호출에 대한 다른 계약 단계의 최대 수를 유지하고 수행하는 모든 계약 시도 할 수 있습니다, 계약 계산 (250 개) 조치를 취하고 51 개 거래에서, 우리가, 있도록하는 A 를 보내 이 같은 논리 폭탄을 검출하는 단계를 수행하지만,이 (생성으로 26 계약 위에서 쉽게 분리 계약 내에 배치 될 수 실행)가 계약 다른 금지 계약을 생성 할 수 있도록 계약이 미리 계산 될 수있다. 또 다른 문제는 메시지의 주소 필드 변수이기 때문에, 일반적으로도 사전에 다른 계약 어느 호출 될 계약을 알 수 없습니다 말하는 것입니다. 그래서, 마침내 우리는 놀라운 결론이 : 놀라 울 정도로 쉽게 튜링 - 완벽한 관리를하지만, 관리 제어 튜링의 부족이 불완전 놀라 울 정도로 어려운 동시에 - 왜 계약 튜링이 그것을 완료하지?

통화 및 발행

Y2 통화 네트워크는 자체 내장 화폐 성 Y2 는, Y2 통화는 주로 자산 기반의 에너지 거래의 다양한 유동성을 제공하는 이중 역할을 포함, 더

중요한 것은 거래 비용의 지불을위한 메커니즘을 제공합니다. 순서 촉진하고 미래 동안 논쟁 (현재 MBTC / uBTC / 사토시 토론 참조) 피에, 다른 교단의 이름이 사전에 설정됩니다 :

이것은 "메타"와 "점"또는 "비트 코인"과 "콩"개념의 확장 버전으로 취급되어야한다, 가까운 미래에, 우리는 "Y2 통화는"일반 거래로 사용되는 기대한다 "피니" 구현 비용에 대한 토론과 합의를위한 마이크로 거래, "사브"와 "웨이"에 사용됩니다.

배경 소개 :

아랍 국가 연맹은 아랍 국가 들간의 협력과 협력을 강화하기 위해 설립 된 지역 국제기구이다. 약어 아랍 리그 또는 아랍 리그. 년 3 월 1945 년 카이로에서 열린 이집트, 이라크, 요르단, 레바논, 사우디 아라비아, 시리아, 예멘 일곱 개 아랍 국가의 대표가 채택 된 "리그 아랍 국가의 조약,"얼라이언스 선언했다. 1993 년까지 22 개 회원국이 있었다. 그것은 아랍 국가의 독립과 주권을 유지하기 위해 회원국 간의 밀접한 협력을 강화 자신의 활동을 조정하는 것을 목표로하고있다. 11 월 중순 2011 년 아랍 연맹은 시리아의 회원 자격을 정지 년 11 월 27 일 같은 년, 아랍 연맹은 즉시, 이집트의 수도 카이로에서 나중에 장관급 회의를 개최 시리아에 대한 경제 제재를 부과하기로 결정했다. 사우디 주도의 아랍 연맹은 성명을 발표에 2017 년 6 월 5 일는 카타르가 조직에서 제외했다고 발표했다. 미션 : 회원국 간의 긴밀한 협력이, 서로들 사이에서 정치 활동을 조정하는 아랍 국가의 독립과 주권을 방어하고, 아랍 국가의

전반적인 이해는 경제, 금융, 교통, 문화, 건강에 기여 증진, 사회 복지 회원국, 국적, 여권, 비자, 사법 등 국가 정치 체제에 대한 회원국 상호 존중, 분쟁은 다른 국가가 다른 국가에 구속력과 회원국 체결, 조약 및 협정을 해결하기 위해 강제로 의존하지 않는다.

현재 22 개 아랍 연맹의 회원은 다음과 같습니다 알제리, 아랍 에미리트, 오만, 이집트, 팔레스타인, 바레인, 지부티, 쿠웨이트, 레바논, 리비아, 모리타니, 모로코, 사우디 아라비아, 수단, 소말리아, 튀니지, 시리아, 예멘, 이라크, 요르단, 지점 모로우. 2011 년 11 월 16 일, 시리아 3 월 26 일, 2013 년 아랍 연맹 공식적으로 중단 회원, 아랍 연맹, 시리아, 시리아, "국가 연합"아랍 연맹의 반대 좌석을 부여하기로 결정하지만, 아직 구현 증명했다 않았습니다.

배포 모델은 다음과 같습니다.

●, Y2 동전 활동, 개발을 목표로하고 통화를위한 연구 개발 조직의 자금 조달에 대한 지불을 판매하여 1 Y2 = 202 디르함 통화 당 판매 가격에있을 것입니다 다른 암호화 이미 Y2 Y2 새로운 에너지 연료 첨가제 메커니즘 통화 플랫폼에서의 성공적인 사용. 초기 구매자는 완벽하게 개발자와 연구자 급여 및 보상, 프로젝트 암호화 생태계 및 Y2 새로운 에너지 연료 첨가제에 넣어 돈을 지불하는 데 사용됩니다 BTC, ETH (순중량 변경)의 판매 결과, 더 큰 할인 혜택을 즐길 수 세계적인 발달, 순환 및 거주.

세계에서 처음으로 총 2 억 7 천만 개가 배포되었고, 3,450 만 개가 Exchange 에 배포되었습니다.

초기 발행 국가, 수량 및 비율:

국가	수량 (단위 : 만)	회계
미국	1356.6	19.38%
한국	910	13%
중국	900	12.85%
러시아	800	11.42%
영국	520	7.42%
EU	320	4.57%
일본	300	4.28%
프랑스어	250	3.57%
사우디 아라비아	250	3.57%
호주	250	3.57%
인도	250	3.57%
이탈리아	200	2.85%

인도네시아	200	2.85%
캐나다	200	2.85%
독일	150	2.14%
남아프리카 공화국	100	1.42%
멕시코 사람	100	1.42%
터키	100	1.42%
브라질	100	1.42%
아르헨티나	50	0.71%

아랍 연합 사무 총장 Ahmed Aboul Gheit 은 세계를 구원 할이기구에 모든 사람을 가입시킬 것을 촉구했다.

2003 년에 설립 된 Y2 신 에너지 연료 실험실 (이전의 아랍 연맹 특별 시험실)은 2017 년에 Y2 연구소로 개명되었습니다. 15 년 동안 아랍 연맹 및 중동 국가에 대한 기술 지원 (과학 특허)이 1,000 개가 넘었습니다. Y2 는 아랍 연맹 회원국에 봉사하고 연합에 대한 우려를 공유하는 것을 목표로하며, Y2 는 아랍 연맹 (UAE) 하부 기관 총무부 소속이다.

Y2 의 출시로 세계 에너지가 20 배 이상 증가 할 것이고, 2020 년까지 에너지 사용량을 10 배에서 25 배 절약 할 수 있으며, 2030 년에는 에너지 사용량을 170 배 이상 절약 할 수 있습니다.

2018 년 4 월 1 일 - 6 월 6 일은 전 세계적인 행사의 시작입니다.

Y2 동전은 4 월 7 일과 6 월 30 일에 OKEX, BitMEX, Binance, GDAX, K-net, B-net, HitBTC, YOKI, Bit-Z 및 P-net 등 7 개의 거래소에서 전세계로 발행되었습니다. 가격은 295 디르함입니다.

발급 기관 : Y2 새로운 에너지 연료 실험실（Y2 بر تـ مخ ة قـ طا الـ دة يـ جد الـ ود قـ وا لـ）

교장 선생님：

Y2 Lab 수석 과학자, Y2 통화 CEO 2011 년 노벨 화학상 수상, 아라비아 디지털 통화 재단 공동 위원장： Shechtman（ شـ يخ تمان ）

사우디 아라비아의 왕세자, 살만 왕의 아들, Y2 통화 수석 전략 책임자:

Mohammad bin Salman Al Saud（سعود ألسلمان بن محمد）

Y2 통화 기술 컨설턴트, PayTabsCEO, Y2 통화 담당 최고 기술 책임자 (Chief Technology Officer): Abdulaziz Al Jouf（الجوف عبدالعزيز）

Y2 Lab 과학자, 노벨 화학상 2016, Y2 통화 담당 최고 운영 책임자 El Sovar (مالا سوير)

단 지원 : BTC, ETH (가격 변동)

예 : 1 BTC = 46,000 위안, 즉 1 BTC = 133.33333333 Y2

예 : 1ETH = 2500 위안, 즉 1 ETH = 7.24763681 Y2

● 0.099x (x 는 판매의 총량) ETH 전에 초기 기여자의 개발에 참여는 BTC 에 할당됩니다 (실제 가격 변경) 및 현금 자금이나 다른 금융 확실성의 성공은 또 다른 0.099x 장기 연구 프로젝트에 할당됩니다 .

분해 분해

영구적 인 선형 성장 모델은 Bitcoin 에서 부의 과도한 집중의 위험을 줄이고 현재와 미래에 거주하는 사람들에게 Y2 동전을 획득하고 보유하는 인센티브를 유지하면서 공정한 기회를 얻음으로써 장기적으로 "통화 공급 증가율"이 0 으로 떨어지는 것을보십시오. 우리는 또한 시간이지나면서 부주의와 죽음으로 인해 동전이 항상 잃어 버리게 될 것이라고 추론한다. 동전의 손실이 연간 화폐 공급의 고정 비율 인 경우, 최종 총 순 환율의 화폐 공급은 안정적 일 것이다. 연례 자금 순환을 손실률로 나눈 값과 같습니다 (예를 들어, 손실률이 1 % 일 때, 공급량이 30 배에 도달 할 때마다 매회 0.3x 가 빠져 나가고 매년 0.3x 가 손실되어 평형을 이룹니다).

선형 발행 방법 외에도 Bitcoin-like Y2 동전의 공급 증가율은 장기적으로 0 이되는 경향이 있습니다.

확장 성

확장 성 문제는 Y2 동전의 공통 관심사이며 Bitcoin 과 마찬가지로 Y2 동전도 각 트랜잭션이 네트워크의 모든 노드가 이러한 딜레마를 처리해야한다는 사실 때문에 어려움을 겪고 있습니다. Bitcoin 의 현재 블록 체인 크기는 약 20GB 이며 시간당 1MB 의 속도로 증가합니다. Bitcoin 네트워크가 Visa 급 2000tps 트랜잭션을 처리하는 경우 3 초마다 1MB 로 증가합니다 (시간당 1GB, 연간 8TB). 단순 통화 인 Bitcoin 보다는 Y2 블록 체인 위에 많은 응용 프로그램이 있기 때문에 Y2 동전도 비슷한 또는 더 나쁜 성장 패턴을 경험할 수 있지만 Y2 동전은 완전한 블록 체인 역사의 사실은 상황을 개선했습니다.

대규모 블록 체인의 문제점은 중앙 집중화의 위험입니다. 블록 체인 크기가 100TB 로 증가하면 일반 사용자는 가벼운 SPV 노드를 사용하는 반면, 매우 작은 수의 대형 상인 만 전체 노드를 실행하게됩니다. 이로 인해 전체 노드 파트너십에서 사기의 위험에 대한 우려가 제기됩니다 (예 : 블록 보상 변경, BTC 제공). 라이트 노드는이 사기를 즉시 감지 할 방법이 없습니다. 물론 정직한 노드 하나 이상이있을 수 있으며, Reddit 와 같은 채널을 통해 유출 된 사기성 정보는 몇 시간 후에 유출 될 수 있습니다. 그러나 이미 일반 사용자가 이미 생성 된 블록을 폐지하도록하기에는 너무 늦습니다. 그들은 모두 성공적인 51 % 공격의 개시와 같은 규모의 거대한 실현 불가능한 조정 문제에 봉착하게 될 것입니다. Bitcoin 에서는 이것이 문제이지만, Peter Todd 가 제안한 변화로이 문제를 완화 할 수 있습니다.

최근 Y2 동전은이 문제를 해결하기 위해 두 가지 추가 전략을 사용합니다. 특정 수의 전체 노드가 보장됩니다. 둘째, 더 중요한 것은, 각 트랜잭션을 처리 한 후 중간 상태 트리의 루트를 블록 체인에 포함시키는 것입니다. 정당한 검증 노드가있는 한 블록 검증이 중앙 집중화 되더라도 검증 프로토콜에 의해 집중화 된 문제를 피할 수 있습니다. 잘못된 블록이 발행된 경우 블록의 형식이 잘못되었거나 S [n] 상태가 잘못되었습니다. S [0]은 정확하기 때문에 첫 번째 오류 상태 S [i]가 있어야하지만 S [i-1]은 정확하다. 유효성 검사 노드는 처리 APPLY (S [i- 1], TX [i]) -> S [i] 필요한 패트리샤 트리 노드의 서브 세트. 이러한 노드는 결과 S [i]가 이전에 제공한 값과 일치하는지 확인하기 위해 계산의이 부분을 수행해야합니다.

또한 불완전한 블록을 악의적으로 공격하여 공격하기가 더 복잡하여 블록이 올바른지 여부를 판단하기에 불충분 한 정보가 생성됩니다. 해결책은 챌린지 - 응답 프로토콜이다. 검증 노드는 목표 트랜잭션 인덱스에 도전하고 챌린지 정보를 수신하는 라이트 노드는 다른 노드 또는 검증자가 패트리샤 노드의 서브 세트를 올바른 것으로 제공 할 때까지 해당 블록을 신뢰하지 않는다. 증거.

검토 : 분산 된 응용 프로그램

위의 계약 메커니즘을 사용하면 한 사람이 전체 네트워크에서 "하드 디스크"로 액세스 할 수있는 상태를 변경할 수있는 가상 컴퓨터의 글로벌 네트워크 합의를 통해 명령 줄 응용 프로그램 (근본적으로 말하면)을 만들 수 있습니다. 그러나 대부분의 사람들은 트랜잭션 전달 메커니즘으로 사용되는 명령 줄 인터페이스의 사용자 편의성 부족으로 인해 분권화가 매력적인 대안이되었습니다. 전체 크레딧, 동전 및 다른 시스템 Y2 (의 조합을 사용하는지 마지막으로, 완전한 "분산 된 응용 프로그램은"Y2 에서 기본 비즈니스 로직 구성 요소를 [포함되어야한다, 예를 들어, 클라이언트 프로그램은 Y2 학점으로하는 P2P 메시지 층, 수명 말기 또는 기타 시스템 전용 모드] 및 상위 그래픽 사용자 인터페이스 구성 요소가 포함됩니다. Y2 동전 클라이언트는 웹 브라우저로 설계되지만, "PC"자바 스크립트 API 의 객체에 대한 지원을 포함하여, 클라이언트는 통화 Y2 블록 체인과 상호 작용하는 특정 웹 페이지에서 볼 수 있습니다. 블록 체인 (blockchain)과 다른 분산화 된 프로토콜은 사용자가 시작한 요청을 처리하기 위해 서버를 완전히 대체하기 때문에 "전통적인"웹 페이지의 관점에서 보면이 웹 페이지는 완전히 정적 인 내용입니다. 마지막으로, 분권화 된 프로토콜은 웹 페이지를 저장하기 위해 Y2 동전 형태를 사용할 것을 약속합니다.

결론

Y2 통화 프로토콜은 원래 그런 생각 도박 시장 통화 암호화의 업그레이드 버전으로 매우 다양한 언어, 인출 제한 및 금융 계약의 고급 기능을 통해 체인으로 계약 제안으로 개발되었다. Y2 코인 프로토콜은 모든 응용 프로그램을 직접 "지원"하지 않지만 Turing Complete Programming Language 의 존재는 이론적으로 임의의 계약이 모든 트랜잭션 유형 및 응용 프로그램에 대해 만들어 질 수 있음을 의미합니다. 그러나, Y2 통화에 더 흥미, Y2 통화 협정뿐만 아니라 유사한 개념의 수십 설립으로 중앙으로 예측 프로토콜 컴퓨팅의 중심으로 시장의 중심으로, 상점의 중심을 이동 단순한 돈보다 더 갈 것입니다 응용 프로그램, 근본적으로 컴퓨팅 업계의 효율성을 향상시키고, 경제 P2P 프로토콜의 또 다른 레이어를 추가하여 처음으로 강력한 지원을 제공 할 수있는 잠재력을 가지고 궁극적으로 다수의 응용 프로그램은 또한 돈과는 아무 상관이 나타납니다 없습니다.

Y2 크레딧 임의의 상태 프로토콜 변환의 개념은 고유 한 인터넷 잠재력을 제공하며 데이터 저장, 도박 또는 직불 다른 단일 목적의 설계와 같은 프로토콜 폐쇄, Y2 는 디자인의 오픈 학점이며, 우리는 다가오는 해에 나타날 수많은 재무 및 비재무 협약을 지원하는 기본 계층으로 매우 적합하다고 생각합니다.

댓글 및 고급 독서

메모

1. 경험이 풍부한 독자는 실제로 주소 비트 코인 타원 곡선 공개 키 해시보다는 대중 그 자체이지만, 대중의 공개 키 암호화 해시라는 학문 언어의 관점에서 사실에 완전히 합리적인 것을 알 수 있습니다. 이것은 비트 암호화 토큰은 사용자의 디지털 서명 알고리즘은 공개 키 해쉬 조성물 곡선의 타원 공개 키, 타원 곡선 공개 키 서명을 서명 연결 조성물하여 타원 곡선으로 간주 될 수 있기 때문이고, 공개 인증 알고리즘을 포함로서 타원 곡선 공개 키를 이용하여 타원 곡선 공개 검사에 의해 제공되는 공개 키, 타원 곡선 해시 키, 타원 곡선 후 서명을 검증하고있다.

2. 기술적으로 말하면, 처음 11 블록의 중앙값.

내부 3. 2 "찰리는"디지털 ^ 0-2 256-1 에서 큰 base256 인코딩 형식 후, 숫자이다.