

THEMIS

디지털 화폐 세계 분권화의
“알리페이”

<https://themis.network>



1. 개요	1
2. 디지털 화폐를 매체로 한 공평교환	1
2.1 부동한 유형의 디지털 화폐 상호 교환	1
2.2 디지털 화폐와 현실상품 상호 교환	2
2.3 THEMIS 의 설계목표	4
3. THEMIS 전체 구조	6
3.1 THEMIS 블럭체인	6
3.2 그룹 위탁관리 계약서	9
3.3 쟁의의 해결	12
3.4 노드의 선택책략	14
3.5 안전성 설계	15
3.6 전형적 작업절차	17
3.7 THEMIS 지갑	20
4. 관건기술	24
4.1 그룹 위탁관리를 기반으로 한 공평교환 계약서	24
4.2 검증가능한 재조정과 관련 링 서명을 기반으로 한 익명 명예 체제	26
4.3 비 인터랙션형 영지식 증명	28
4.4 우수한 병행성 서명검증을 지원하는 디지털 서명 알고리즘	30

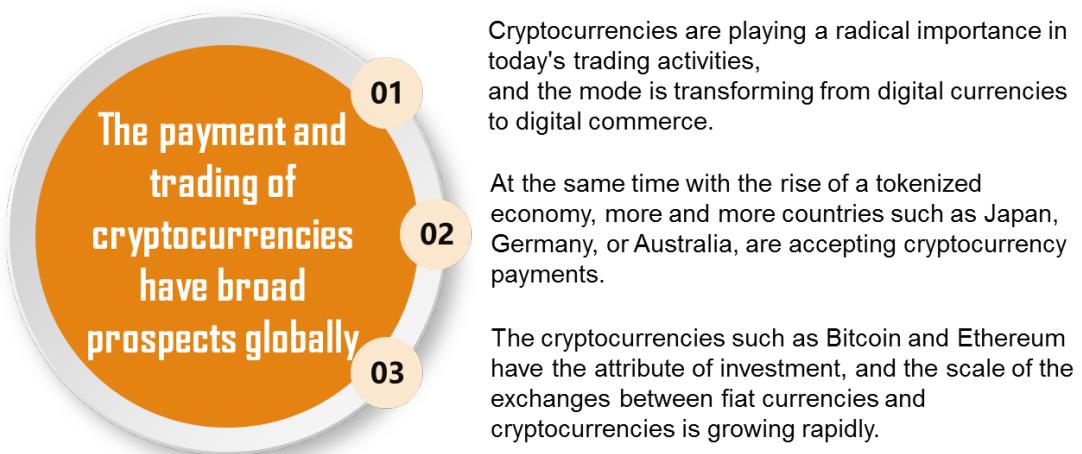


5. 사용환경	33
5.1 점 대 점 위탁관리 지불	33
5.2 디지털 화폐 거래 교환	34
5.3 감독관리 계좌 안전 위탁관리	35
5.4 다중 에이전트 거래 자산 위탁관리	37
6. 팀 소개	39
6.1 핵심팀	39
6.2 컨설턴트팀	44
6.3 파트너	47
7. 기관 투자가	49



1. 개요

블록체인에 기초한 디지털 화폐가 출기차게 발전하여 인류의 새로운 화폐형식으로 되고 있으며, 비즈니스 활동에 점점 더 깊게 침투되고 있습니다. 각종 디지털 화폐 거래소가 시대의 요구에 따라 탄생하였고, 거래규모도 신속하게 성장하고 있습니다. 또한 디지털 화폐 사용범위의 끊임없는 확대와 더불어, 점점 더 많은 국가와 지구(예하면 일본 등 국가)의 많은 상점들은 모두 디지털 화폐를 지불방식으로 받아들이고 있습니다. 전세계 범위 내에서 디지털 화폐를 사용하여 실물상품을 구매하는 것은 광활한 시장이 있다고 볼수 있습니다.



도 1.1 디지털 화폐의 발전추세

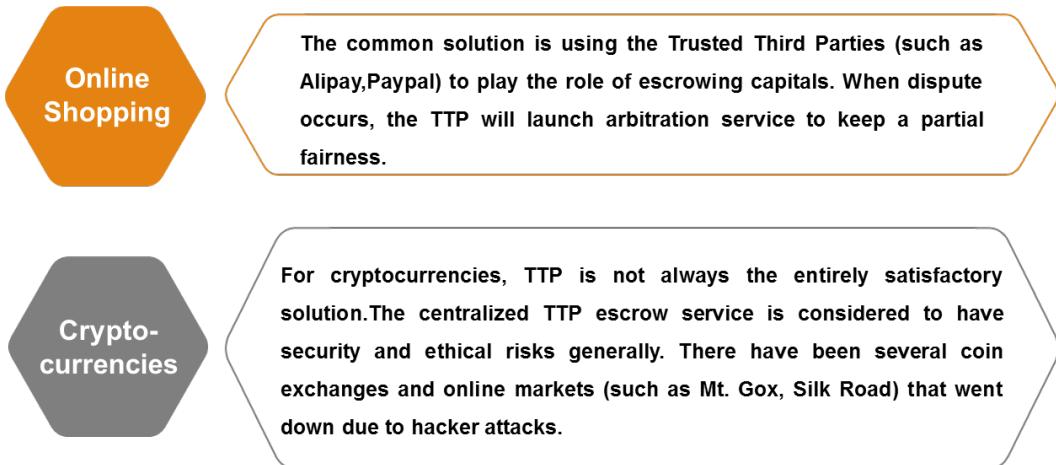
현재, 디지털 화폐 거래소와 점 대 점 거래 서비스 제고자는 대부분이 거래의 안전성에 초점을 두고 있으며, 거래의 공평성에 대한 관심이 많지 않습니다. 예하면 광범위하게 사용되고

있는 해시락 계약서(Hashed Time-lock Contract, HTLC) 기술 중에서 환불시간락은 공격자에게 이용당해 서비스 거절 공격을 할수 있어 거래 상대가 한정된 환불시간내에 교환을 완성할수 없게 합니다.



도 1.2 수요 분석

또한 디지털 화폐와 실물상품 교환 과정중에서 구매자는 상품을 받은후 대금을 지불하려고 하고, 판매자는 대금을 받은후 상품을 출하하려고 하여 거래와 교부를 동시에 달성할수 없어 공평한 원자 교환을 보증할수 없게 되었습니다. 일반적인 해결방안은 제 3 신뢰기관에 의존하는 것이나, 단일 장애 지점 문제 가 존재하므로 하나의 제 3 자에 의존하는 해결방안은 안전하고 신뢰성 있는 방안이 아닙니다. 비트코인 거래소와 온라인 시장이 해커 공격을 당해 도산(예하면 Mt. Gox, Silk Road)한 사례가 있었습니다.



도 1.3 현실상황

지난날, 전통 공평교환 프로토콜에 대한 대량의 연구는 모두 공평 교환이 제 3 신뢰기관에 대한 의존을 약화시키려고 노력해 왔습니다. 블럭체인의 탄생은 공평교환 프로토콜에 새로운 활기를 심어주었습니다. 저희는 블럭체인 기술을 이용하여 디지털 화폐를 매체로 한 공평교환 시스템 **Themis**¹를 구축하여, 분권화의 디지털 화폐 위탁관리 서비스를 제공하고, 디지털 화폐, 디지털 자산과 실물상품 간의 공평교환 문제와 같은 디지털 화폐를 매체로 한 공평교환 문제를 해결하였습니다.

Themis는 경제학 인센티브에 기반한 그룹 위탁관리 체제로서, 문턱암호, 익명명예 체제, 비 인터랙션형 영지식 증명 및 우수한 병행성 전자서명 알고리즘 등 관건기술을 사용하여 그룹 구성원중 악의적 구성원 수량이 절반 이하인 상황에서 공평교환

¹ Themis(테미스) 제우스가 가장 존중하고 신임하는 아내. 법률과 정의의 여신으로서, 질서의 창조자, 수호자임.

을 보증할수 있게 하여, 안전, 프라이버시, 분권화와 서비스 거절 공격에 저항하는 등 특성을 갖고 있습니다. Themis는 비트코인, 이더리움 및 기타 블럭체인에 기반한 암호학 디지털 화폐에 안전한 위탁관리 서비스를 제공할수 있습니다.

▶ 2. 디지털 화폐를 매체로 한 공평교환

공평교환이라 함은 서로 불신임하는 여러개 주체 사이에서 사전 약정에 따라 자산 상호 교환을 완성하는 프로토콜을 가리킵니다. 디지털 화폐를 매체로 한 교환이라 함은 교환 주체인 한쪽이 디지털 화폐를 교환대상으로 하는 상황을 가리키는 바, 예를 들면 부동한 유형의 디지털 화폐 사이의 교환 또는 디지털 화폐와 실물상품의 교환과 같은 경우입니다. 상기 상황은 모두 공평교환 프로토콜이 제공하는 안전한 보장을 필요로 합니다.

2.1 부동한 유형의 디지털 화폐 상호 교환

부동한 유형의 디지털 화폐간 교환을 실현함에 있어서 최초로 생긴것이 거래소 방식입니다. 거래소는 내부 계좌 건립을 통해 사용자간 부동한 디지털 화폐의 교환을 완성하였습니다. 즉, IOU(I Owe You) 계좌 방식입니다. 거래소 방식에서 고 빈도수 거래는 쉽게 달성이 되나, 보편적으로 다음과 같은 결함이 존재한다고 인식되고 있습니다. 첫째, 안전성 리스크. 사용자 자금을 거래소가 위탁 관리하므로 해커 공격과 도덕 리스크 존재. 둘째, 유동성 부족. 거래소가 외딴섬을 형성하여 사용자 자산은 거래소 내에서만 유동 가능. 셋째, 지불성 지연. 거래결과를 실시간으로 블럭체인에 제출하지 않아 즉시 현금화 불가.

중심화 거래소의 결함을 극복하기 위하여 사람들은 분권화 거래소 방식을 제출하였습니다. 이런 방식은 대부분이 다중 서명 방안 또는 해시락 계약서(HTLC) 방안을 기반으로 원자 거래를 보증하였습니다. 하지만 다중 서명 방안은 제 3 신뢰기관에 의존하므로 동모공격 또는 서비스 거절 공격 리스크가 존재합니다. HTLC 방안중의 환불시간락은 공격자에게 이용당해 서비스 거절 공격을 발기할수 있어 거래 상대가 한정된 환불시간내에 교환을 완성할수 없게 합니다.

2.2 디지털 화폐와 현실상품 상호 교환

기존의 중심화 거래소와 분권화 거래소는 디지털 화폐간의 교환에 주력하여 디지털 화폐와 실물상품의 공평교환 수요를 만족시킬수 없습니다. 이는 디지털 화폐와 실물상품 교환과정중, 거래와 교부를 동시에 달성할수 없어 공평을 보증하는 원자 교환이 도전에 직면하였기 때문입니다. 또한 구매자는 상품을 받은후 대금을 지불하려고 하고, 판매자는 대금을 받은후 상품을 출하하려 하여 순환 의존 문제에 직면한 것입니다. 때문에 제 3 신뢰기관을 통해 자금 위탁관리와 중재를 진행하여 거래 달성후, 교부 확인전에 구매자의 거래자금에 대해 안전한 위탁관리를 진행함으로써 공평성 요구를 만족시켜야 합니다.

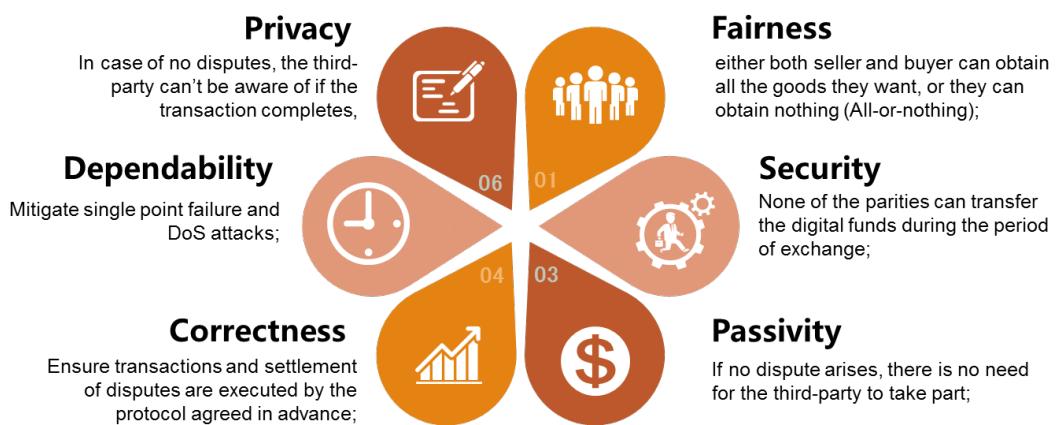
일종의 자주 보는 위탁관리 지불방식은 2-of-3 다중 서명 거래를 사용하여, 구매자, 판매자와 제3 신뢰기관이 각기 한개의 암호 키를 보유하고, 구매자가 한건의 디지털 화폐를 한개의 다중 서명의 위탁관리 주소로 지불하면 임의의 한측은 3 자중 임의의 양자의 암호 키를 제공하여 전자서명을 형성해야만 해당 자금을 사용할수 있습니다. 거래가 원활하게 진행될 경우, 구매자가 암호 키를 판매자에게 발송하면 판매자는 위탁 관리한 자금을 받을수 있고, 쟁의가 발생할 경우, 제3 신뢰기관이 중재를 진행하고 쟁의 승리자에게 암호 키를 발송하여 대금지불(또는 환불)을 완성합니다.

이러한 위탁관리 계약은 2 개의 우점이 있습니다. 1. 쟁의가 없을 경우, 매매 쌍방은 제3자와 관련되지 않는 상황에서 결산을 진행할수 있음. 2. 제3자는 위탁관리한 자금을 가져갈수 없음. 제3자에게는 한개의 암호 키만 있으며, 위탁관리 자금을 취득하려면 최소 2 개의 암호 키가 필요함.

하지만 이런 방식 또한 심각한 문제가 존재합니다. 첫째, 공모 문제. 위탁관리 계약서를 정성껏 설계하지 않을 경우, 위탁관리측은 특정 구매자 또는 판매자와 쉽게 연결하여 공모를 실시 할수 있음. 둘째, 서비스 거절 문제. 제3자가 돈을 절취할수 없다 해도 쟁의 중재를 거절할수 있어 자금 잠금 상태를 유지할수 있음.

2.3 Themis 의 설계목표

Themis 는 분권화의 공평교환 시스템으로, 디지털 화폐 세계의 알리페이와 유사하며, 디지털 화폐를 매체로 한 공평교환 문제를 해결합니다. 기술적인 측면에서 Themis 는 아래와 같은 요구를 만족해야 합니다.



도 2.1 Themis 설계목표

공평성 : 교환 종료후 교환 쌍방이 모두 원하는 목적물(예하면 디지털 화폐, 디지털 자산, 실물상품)을 얻거나 모두 얻지 못함(All-or-nothing).

안전성 : 디지털 화폐는 교환과정중 어느 누구도 함부로 가져가지 못함.

피동성 : 쟁의가 없을 경우 제3자 참여가 필요 없음.

정확성 : 거래와 쟁의의 해결이 사전 약정 규칙에 따라 집행할것을 확보함.

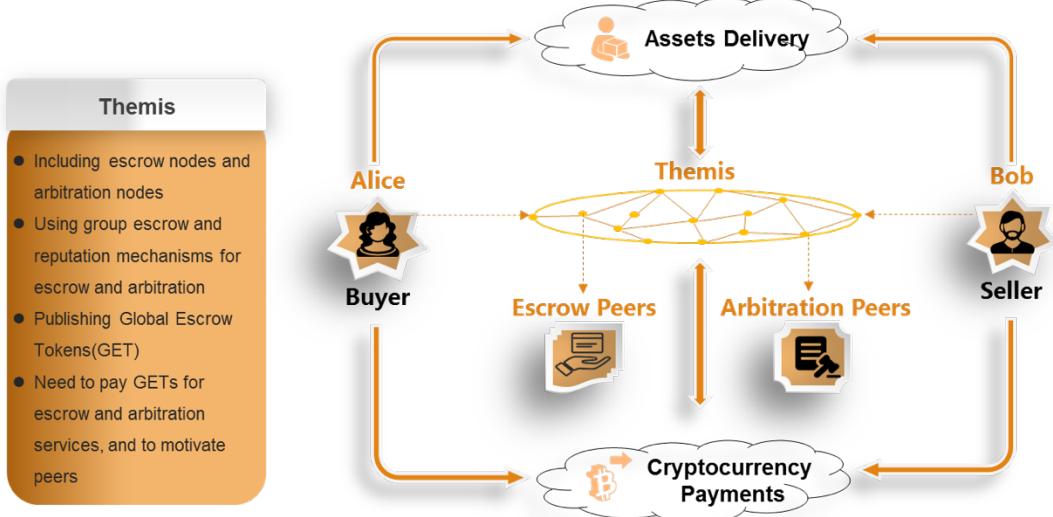
신뢰성 : 쟁의 발생후 위탁관리측이 중재 판결을 집행하지 않음으로 인한 자금 잠금 문제를 피함. 즉, 단일 장애 지점과 서비스 거절을 피함.

프라이버시성 : 쟁의가 발생하지 않은 상황에서 제3자는 거래 완성여부를 알수 없고, 비 거래 관련자는 쟁의 발생 여부를 알수 없음.

3. Themis 전체 구조

3.1 Themis 블럭체인

Themis 는 제 3 자 위탁관리 서비스(기존의 알리페이가 인터넷 쇼핑에서의 역할과 유사함)를 제공하여 체인에서 기호화폐 Global Escrow Token(GET)를 발행하고, 경제학 격려를 기반으로 한 그룹 위탁관리 체제와 명예 체제를 도입하여 블럭체인 노드를 격려하며, 위탁관리 계약서와 중재 계약서를 이용하여 디지털 화폐간, 디지털 화폐와 현실자산간의 점 대 점 공평교환을 실현합니다. 위탁관리 수수료와 중재 서비스료를 발급하는 방식을 통해 자금 위탁관리와 쟁의 중재에 참여하는 노드에 격려를 제공합니다. 사용자는 디지털 화폐를 사용하여 지불하는 과정중, GET 기호화폐를 지불하여 위탁관리와 중재 서비스를 획득해야 합니다. 위탁관리와 중재 노드에 참여하여 거래 완성후 거래측의 GET 기호화폐 수수료와 장려를 획득할수 있어 GET 기호화폐가 Themis 에서의 폐 루프 유동을 실현합니다.



도 3.1 Themis 전체 구조

DPoS 공통인식 체제. Themis는 기존의 위탁권익증명(DPoS) 프로토콜을 개선하여 신형 공통인식 체제 DPoS(Deposit based Proof of Stake and Reputation)를 제출할 예정입니다. 즉, 보증금의 권익과 명예 증명 계약을 기반으로 하여, 노드가 쟁의처리에 참여한 명예를 공통인식 체제에 가입시키고 또 노드 경쟁 수탁자 자격은 보증금을 선 지급해야 합니다. 노드가 수탁 노드로 될 확률은 납부한 보증금 및 보유한 권익과 명예와 밀접한 연관이 있습니다.

보증금 체제. 노드 경쟁 수탁자 자격은 일정한 대가를 지불해야 합니다. 즉, Themis에 보증금을 납부해야 합니다. 노드가 나쁜 짓을 할 경우, 보증금은 시스템에 의해 몰수 됩니다. 수탁자가 시스템 운영을 유지시 보수를 받게 되는바, 즉, 기타 수탁자와 블럭 거래비를 공유합니다. 보수는 그에 대해 정향적 피드

백을 형성함으로써 수탁자로 하여금 더욱 열심히 시스템 안전을 유지하도록 격려 합니다. 블럭이 수탁자에 의해 교대로 체결되었기에, 모 수탁자가 오프라인으로 인해 블럭 체결을 놓칠 경우, 기타 후보 수탁자에 대체될 리스크에 직면하게 됩니다. 때문에 이익을 보기 위해 수탁자는 반드시 충분한 온라인 시간을 보증해야 합니다.

위탁관리 노드 격려체제. 위탁관리 노드는 그가 소지한 권익에 근거하여 대응한 수량의 암호 키를 할당 받으며, 상응한 서명 할당을 계산하여 거래에 첨부시키며, 암호 키 할당비례에 근거하여 수수료를 획득합니다. 위탁관리 노드가 암호 키 할당을 정확하게 제공할 경우, 보증금과 상응한 할당의 거래 수수비용을 획득하게 되며, 오프라인 또는 암호 키 할당을 분실할 경우, 중재거래에 참여할수 없으며 또 거래 수수료도 획득할수 없습니다. 노드가 거짓 또는 잘못된 암호 키 할당을 제공할 경우, 위탁관리 신분을 취소당할수 있습니다. 상기와 같이, 격려체제는 위탁관리 노드가 정확한 암호 키 할당을 제공하고, 온라인 상태를 유지하며, 자신의 암호 키 할당을 안전하게 보관하도록 격려합니다.

명예 관리 체제. Themis 중의 노드는 쟁의의 해결에 참여하여 중재 의견을 제시하는 한면에 또 기타 사용자가 제시한 쟁의 해결 의견에 대해 지속적인 익명 평가를 진행합니다. 저희는 실용적인 익명 명예 체제를 구축하여 대규모 사용자 그룹중에서

신속하게 명예값을 업데이트 할수 있고, 사용자의 프라이버시 수요도 만족시켜 드립니다. 명예 시스템은 시스템중 기타 사용자가 모 사용자에 대한 중재의견 결과의 피드백을 정확하게 계산하고 또 해당 사용자의 명예값을 신속하게 업데이트 합니다. 명예값의 높고 낮음은 사용자가 중재 노드가 될 확률에 직접적인 관계가 있는 바, 명예값이 낮은 사용자는 중재 노드로 선택되기 어렵습니다.

일반 노드 격려체제. Themis에서 충분한 권익을 장악해야만 위탁관리 노드로 선정되어 위탁관리에 참여할수 있으며, 위탁관리 노드가 되지 못한 기타 노드는 일반노드라 불리웁니다. 일반노드는 위탁관리에 참여할수 없으나 장악한 권익을 신임할수 있는 위탁관리 노드에 위탁할수 있으며, 수탁한 위탁관리 노드는 거래소가 획득한 거래비를 검증하여 위탁 권익 비중에 따라 일반노드에 분배합니다. 위탁관리 노드가 징벌을 받을 경우, 일반노드도 상응한 손실을 감당하게 됩니다. 이와 같은 격려체제는 Themis 상의 권익 보유자가 모두 권익과 관련된 수익을 획득할 수 있음을 보증하였고 또 그들이 장악한 권익을 신임할수 있는 노드에 위탁할것을 격려함으로써 Themis 의 안전성과 안정성을 제고하였습니다.

3.2 그룹 위탁관리 계약서

Alice 와 Bob 를 예로 들자면, 거래 쌍방인 그들은 쌍방이 공유하는 2-of-2 주소를 생성하여 위탁관리 계좌 주소로 하였습니다. Alice는 그녀의 위탁관리 개인 키 x_A 를 생성하였고, Bob도 상응한 위탁관리 개인 키 x_B 를 생성하였으며, Thresh-Key-Gen 계약서²에 따라 쌍방은 각기 $y_A = g^{x_A}$ 와 $y_B = g^{x_B}$ 를 사용하여 위탁관리 공중 키 주소 : $y = g^{x_A+x_B}$ 를 획득하였습니다. Alice 와 Bob 중 누구든지 개인 키 x_A 와 개인 키 x_B 를 동시에 가지면 위탁관리 계좌를 잠금해지할수 있습니다.

Alice 와 Bob 는 블럭체인에서 그룹 위탁관리 청구를 발기하여 약간(홀수)개의 위탁관리 노드의 반응을 받았습니다. 그다음 Alice 와 Bob 는 위탁관리 노드와 인터랙션하여 각기 x_A 와 x_B 을 위해 n 개의 Shamir 암호 키 할당 3P_i 을 건립하였습니다. $n = 2t + 1$ 개 위탁관리 노드 상황에 대해 $t + 1$ 개 위탁관리 노드는 x_A 또는 x_B 관련 암호 키 할당을 제공하기만 하면 위탁관리 개인 키 x_A 또는 x_B 를 유효하게 회복할수 있습니다.

Alice 와 Bob 는 각기 매개 위탁관리 노드의 공중 키를 사용하여 각자의 위탁관리 개인 키 x_A 또는 x_B 를 암호화 하여 $c_i = E_{M_i}(P_i)$ 를 생성하여 각 위탁관리 노드로 발송하고, 암호화한 이들 암호 키 할당 $\{c_1, c_2, \dots, c_n\}$ 을 전부 상대 측에 제공하였습니다.

상기 암호 키 할당의 교환 과정중 사기를 방지하기 위하여

² Gennaro, R., Goldfeder, S., Narayanan, A.: Threshold-optimal dsa/ecdsa signatures and an application to bitcoin wallet security, In: Applied Cryptography and Network Security 2016, pp.156-174.

³ Shamir A. How to share a secret. Communications of the ACM, 1979, 24(11): 612-613.

저희는 검증이 가능한 비밀공유 방안 Feldman VSS⁴와 영지식 증명을 이용하여 Alice 와 Bob 가 상대방에게 발송한 암호 키 할당의 진실성을 보증하였습니다. 즉, 이들 암호 키 할당은 Shamir 비밀 공유 계약서를 운행한후 생성한 위탁관리 개인 키 x_A 또는 x_B 와 관련된 암호 키 할당이었습니다. Alice 가 Bob 에게 암호화 한 암호 키 할당 $c_i = E_{M_i}(P_i)$ 일 경우, 한개의 Feldman VSS 값 $w_i = g^{P_i}$ 및 이 두개 값의 일치성과 관련된 한개의 영지식 증명 을 동시에 제공해야 했습니다. 그러면 Bob 는 자신이 받은 암호 문자 데이터가 x_A 의 Shamir 비밀공유 계약서가 생성한 암호 키 할당이 맞는지를 검증할수 있습니다. 마찬가지로, Alice 도 자신이 받은 암호 문자 데이터가 x_B 의 Shamir 비밀공유 계약서가 생성 한 암호 키 할당이 맞는지를 검증할수 있습니다.

상기 작업을 완성한후, Alice 또는 Bob 는 디지털 화폐를 위탁관리 주소로 계좌이체 할수 있습니다. 쟁의가 없을 경우, 지불자는 자신의 위탁관리 개인 키를 상대방에게 분배하고, 2개 위탁 관리 개인 키를 동시에 소유한 자는 위탁관리한 자금을 가질수 있습니다.

쟁의가 발생할 경우, 위탁관리 노드는 중재 서비스를 사용 합니다. 중재중의 승리자는 매개 위탁관리 노드에 상대방으로부터 받은 상응한 암호 키 할당 데이터를 발송합니다. 위탁관리 노드 그룹중의 대부분 노드가 정상 작업하기만 하면 데이터를

⁴ Feldman, P.: A practical scheme for non-interactive verifiable secret sharing. In: 28th Annual Symposium on Foundations of Computer Science, 1987, pp. 427-438.

받은 후 그들은 중재 실패자의 위탁관리 개인 키를 재건하고 이를 승리자에게 발송합니다. 이에 승리자는 2 개의 위탁관리 개인 키를 소지하여 위탁관리 주소로부터 위탁관리한 자금을 가질 수 있습니다.

3.3 쟁의의 해결

쟁의가 발생할 경우, 즉, Alice 와 Bob 는 모두 상대방에게 자신의 위탁관리 개인 키를 제공하지 않으려고 할 경우, 누구든지 모두 Themis 에서 쟁의 해결을 신청할 수 있습니다. 쟁의가 발생 할 경우, 위탁관리시 거래 쌍방이 약정한 쟁의 해결 규칙에 근거하여 Themis 는 중재 절차를 가동합니다. 중재 서비스는 쟁의 발생시에만 가동하여 공평거래의 원가가 영에 가깝도록 보증합니다. 즉, 쟁의가 발생한 경우에만 중재비용을 지불하는 것입니다.

저희는 쟁의 해결방법을 두 가지로 나누었습니다. 첫째, 중재 스마트 계약서 집행을 통해 자동으로 중재결과 생성. 둘째, 인공이 개입하여 처리하는 방법으로, 수명의 중재인이 투표하여 중재결과를 형성.

첫번째 쟁의 해결 방법중에서 중재 스마트 계약서는 자동으로 Oracle 서비스를 사용하여 외부 입력을 획득하고, 스마트 계약서 코드를 운행하여 중재 결과를 생성합니다.

두번째 쟁의 해결 방법중에서 저희는 명예 평점을 기반으로 한 크라우드 소싱 중재 서비스를 제출하였습니다.

크라우드 소싱 중재. Themis의 명예 평점을 기반으로 한 크라우드 소싱 중재 서비스는 익명 중재자에 대한 명예 평점 체제를 통해 거래 쌍방이 신뢰성 있는 중재 서비스를 선택하도록 도우며, 중재자도 체인에서 상응한 장려를 획득할수 있습니다.

또한 Themis는 중재자 명예를 평가하는 공개 심사제도를 적용하였습니다. 중재자의 판결은 익명처리후에 분포식 장부에 제출되어 심사로 진행하게 됩니다. Themis에서 블럭체인 분포식 장부를 사용하여 중재자가 거래 쟁의 처리중의 계약 주체 사항, 사례, 판결 및 판결이유 등 정보를 열거하면 기타 사용자는 중재자의 판결에 대해 점수를 매길수 있습니다. 판결이 획득한 호평정도에 근거하여 익명 중재자는 자신의 명예값을 획득합니다. 중재권력을 남용하는 모든 행위는 모두 중재자의 전문 명예값에 신속하게 반영되므로, 명예값이 낮은 사용자는 미래의 거래 쟁의에서 중재자를 맡을 확률이 떨어지게 됩니다.

명예관리체제. Themis의 명예 시스템은 기타 사용자가 중재 결과에 대한 피드백을 신뢰성 있게 제공할수 있으며, 사용자의 신분 또는 평점 세부 정보를 누설하지 않고 또 명예값이 악의적으로 왜곡되지 않음을 보증할수 있습니다. 현재 자주 보는 명예 시스템은 기타 사용자의 피드백에 근거하여 사용자가 정보 품질을 평가하도록 도와주며, 알고리즘을 통해 명예값을 업데이트

함으로써 긍정적인 행위를 격려 합니다. 이런 명예 체제는 사용자의 평점 데이터를 통계하나, 명예값과 사용자의 장기적 신분을 연결시켜 심각한 프라이버시 누설을 초래하게 되고, 사용자의 행위기록이 악의적으로 추적당하게 하며, 중재자의 익명성과도 저촉 됩니다. 저희는 실용적인 익명 명예 시스템을 구축하여 대규모 사용자 그룹중에서 신속하게 명예값을 업데이트 함과 동시에 사용자의 프라이버시를 보증할 것입니다. 즉, Themis 의 명예방안은 관련 사용자의 장기적 신분이 필요 없습니다.

Oracle 서비스. Oracle은 중재 서비스중에서 거래 쌍방이 제공한 재료를 토론 및 검토시 필요한 체제로, 그의 본질은 현실 세계에 대응하는 진실사건의 발생결과에 대한 정보 발표입니다. 중재에 필요한 데이터와 자료는 반드시 Oracle이 결정해야 합니다. Oracle은 일련의 API를 제공하고, Themis는 Oracle API 사용을 통해 중재결과를 결정하고 그후의 작업을 실현합니다. Oracle은 중심화일수도 있고(예하면 RealityKeys) 분권화일수도 있습니다(예하면 OracleChain).

3.4 노드의 선택책략

수탁자의 선거. DPoS 공통인식 체제에서 노드는 경쟁을 통해 수탁자가 되는 자격을 얻기 위하여 우선 보증금을 납부해야

합니다. 만약 노드가 나쁜 짓을 하면 보증금은 몰수당합니다. 노드는 모 노드에 투표하여 해당 노드를 자신의 수탁자로 선거하고, 시스템은 노드가 가진 지분이 시스템에서 차지하는 비중에 따라 표수가 가장 높은 일정한 수량의 수탁자를 계산하며, 수탁자는 사전 규정 순서에 따라 차례대로 블럭 생성을 책임집니다.

위탁관리 노드의 선택. 사용자의 위탁관리 청구에 근거하여 시스템은 일치성 해쉬 알고리즘을 사용하여 홀수($2f + 1$)개 노드를 위탁관리 노드로 선택합니다.

중재 노드의 선택. 시스템은 노드의 명예값에 근거하여 가중 랜덤 알고리즘을 적용하여 홀수($2f + 1$)개의 중재 노드를 계산해 냅니다.

3.5 안전성 설계

저희 방안은 3 가지 주요 공격의 위협에 직면하고 있습니다. 첫째, 서비스 거절 공격. 즉, 제 3 자가 돈을 절취할수 없으나 쟁의 중재를 거절할수 있어 위탁관리 계좌의 잠금상태를 유지할수 있음. 둘째, 위탁관리 노드와 중재 노드의 공모 공격. 즉, 중재 노드가 Alice 와 Bob 에게 모두 중재에서 이겼다고 알려주면 쌍방이 모두 각자의 암호 키 할당을 위탁관리 노드에게 보내주며, 위탁관리 노드는 2 개의 위탁관리 개인 키를 회복할수 있어 위탁관리 계좌내의 자금을 빼갈수 있음. 셋째, DPOS 의 공모 공격.

즉, DPOS 공통인식 알고리즘 자체 이론에서 참여자 공모 공격의 위협에 직면함.

첫번째 유형의 공격에 대해 Themis 는 경제학 격려체제를 도입하여 노드 서비스 거절과 공모의 기회비용을 제고함으로써 위탁관리 노드가 시장의 힘에 의해 성실하고 도덕적인 행동을 취하게 하여 Themis 가 위탁관리와 중재 절차를 객관적으로 완성할수 있게 하였습니다.

Themis 의 격려체제는 위탁관리 노드가 유효한 서비스를 제공하고, 위탁관리에 정상적으로 참여한 모든 노드가 명예 제고를 얻게 하며, Themis 의 기호화폐 GET 를 획득하도록 격려하는 데 목적을 두었습니다. 이에 반해, 비 정상적인 위탁관리 노드는 명예와 플랫폼에 저당한 GET 리스크 보증금을 동시에 잃게 되어 나쁜짓을 할 기회비용이 대폭 증가하므로, 노드는 자신의 기존 이익과 장원한 수익을 파괴하면서 전체 네트워크를 파괴하지 않을 것이며, 이는 Themis 로 하여금 대다수 악의적인 노드의 공격을 방지할수 있게 하였습니다.

실제 사용중에서 저희는 위탁관리 노드를 신뢰할수 있는 위원회 노드, 인증을 거친 중개 대행 노드와 일반 노드 등 3 개 유형으로 나눕니다. 그중, 위원회 노드는 신뢰성 있는 기구가 유지하는 항상 온라인 상태에 있는 신뢰성 노드로서, 서비스 거절 공격을 당한후 최후의 주재 결과를 여전히 집행할수 있음을 보증합니다. 중개 대행 노드 자체는 시스템에 보증금을 입금시켜

악의적 행위를 할 경우 보증금을 몰수 당하게 되어 그의 정상적인 작업을 구속합니다.

두번째 유형의 공격에 대해 저희는 2-of-2 공유주소를 3-of-3 공유주소로 업그레이드 하고, 세번째 위탁관리 개인 키 x_c 는 Alice와 Bob 거래 쌍방이 공유하나 위탁관리 노드에게 누설하지 않게 하였습니다. 그러면 위탁관리 노드가 성공적으로 공격을 발기한다 해도 개인 키 x_A 와 개인 키 x_B 만을 획득하게 되어 위탁관리 자금을 빼갈수 없습니다.

세번째 유형의 공격에 대해 Themis 를 사용하여 위탁관리 및 중재 서비스를 진행하는 사람이 많을수록 Themis 가 감당하는 가치가 크며, 노드에서 악의적 행위를 할때의 기회비용이 높게 되므로, 전체 네트워크가 더욱 안전해 지며, 더욱 안전한 Themis 는 점점 더 많은 사람들이 위탁관리와 중재 서비스를 사용하도록 흡인할 것입니다. 이는 서로 이익을 증가하는 과정으로서, Themis 네트워크 노드수의 지속적인 확대와 함께 Themis 는 점점 더 건장해 지게 될것입니다.

3.6 전형적 작업절차

Alice 가 비트코인을 지불하여 Bob 에게서 기린 완구를 구매하는 것을 예로 하여, Themis 를 통해 아래와 같이 공평교환 과정을 완성합니다.

위탁관리전의 협상 :

Alice 와 Bob 는 한개의 비트코인 위탁관리 주소를 협상함.

Alice 와 Bob 는 Themis 에서 위탁관리 신청을 발기함. 이에
는 사전에 상의하여 결정한 쟁의의 해결방법(스마트 계약서), 수
수료와 중재 상금 등이 포함됨.

Themis 가 위탁관리 스마트 계약서를 운행하여 Alice 와 Bob
에게 위탁관리 노드 리스트를 보냄.

Alice 와 Bob 는 매개 위탁관리자에게 개인 키의 암호 키 할
당을 각기 발송함.

Alice 와 Bob 는 개인 키의 암호 키 할당을 상호 발송함.

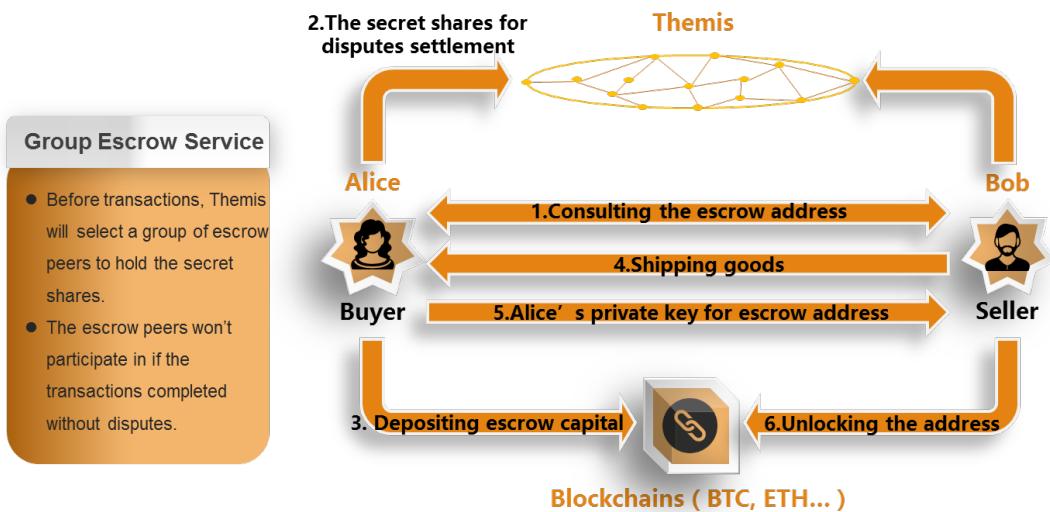
자금 위탁관리와 상품 교부 :

Alice 는 비트코인을 위탁관리 계좌에 이체하고, 이때 Alice,
Bob 와 위탁관리자 중의 어느 누구도 자금을 함부로 빼갈수 없
음.

Bob 는 완구를 Alice 에게 우편으로 보냄. Alice 는 완구를 받
아 확인한후 수금확인을 발기하고 Bob 에게 그의 위탁관리 개인
키를 발송함.

Bob 는 개인 키를 받은후 위탁관리 계좌안의 자금을 자신의
비트코인 주소로 전입함.

Themis 상의 스마트 계약서는 위탁관리자의 위탁관리 수수
료를 계산 및 분배함.



도 3.2 자금 위탁관리와 상품 교부 안내도

쟁의의 해결 :

Alice 와 Bob 는 Themis 에서 쟁의 중재 청구를 발기함.

중재측은 사전에 약정한 쟁의 해결방법에 따라 판결결과를 형성함(Alice 가 승리하고 Bob 가 실패하였다고 가정).

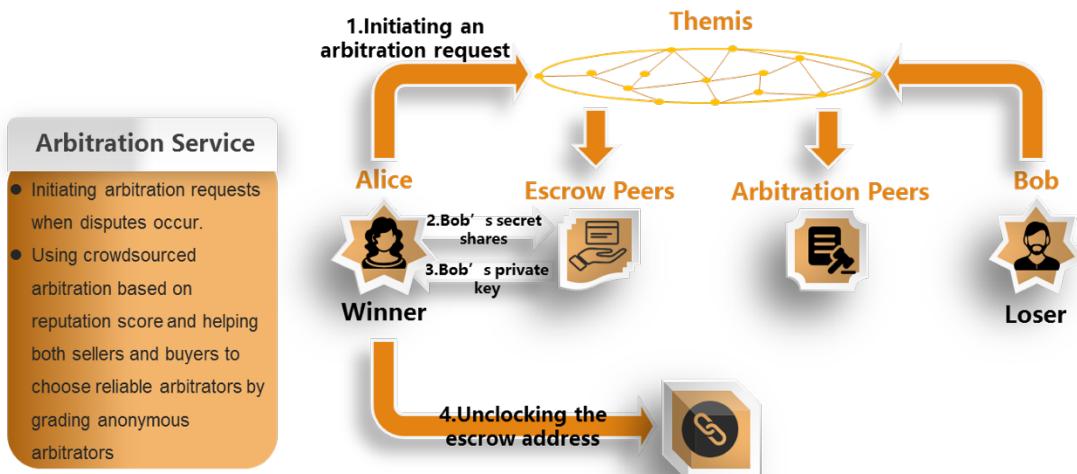
Alice 는 위탁관리측 인원에게 Bob 로부터 획득한 개인 키 암호 키 할당 정보를 발송함.

위탁관리측은 Bob 의 위탁관리 개인 키를 계산해 낸후 Alice 에게 발송함.

2 개 위탁관리 개인 키를 소지한 Alice 는 위탁관리 계좌를 잠금해지하고, 위탁관리 계좌안의 자금을 자신의 비트코인 주소에 전입함.

Themis 상의 스마트 계약서는 각 중재자의 중재 장려를 계산 및 분배함.

Themis 상의 스마트 계약서는 위탁관리측의 위탁관리 수수료를 계산 및 분배함.



도 3.3 쟁의 해결 안내도

3.7 Themis 지갑

Themis 는 신형 암호기술을 기반으로 한 등급 지갑, 즉 Themis 지갑을 제공하여 사용자에게 고 효율성, 저 저축 지출의 개인 키와 주소관리를 제공하고, Themis 블럭체인과의 데이터 인터랙션을 자동으로 완성하여 사용자가 Themis 블럭체인 위탁 관리 서비스를 사용하는데 편리하게 합니다.

Themis 의 몇가지 전형적인 환경에서 사용자는 기타 사용자가 지불하는 대금을 빈번하게 받아야 합니다. 예하면 Themis 를 통해 신뢰성 있는 디지털 화폐 거래를 진행하는 인터넷 상점은 모든 거래에서 모두 사용자가 지불하는 대금을 받게 되는데, 프

라이버시 보호를 위하여 매개 거래에 대해 부동한 주소를 생성하여 해당 주소 및 대응한 개인 키를 저장 및 관리해야 합니다. 거래가 아주 빈번하고, 거래 수량이 아주 많을 경우, 주소는 개인 키 수량과 거래 수량과 선성관계를 형성하여 개인 키와 주소에 대한 관리는 지갑 시스템에 거대한 저장과 관리 지출을 가져오게 됩니다.

지갑이 새로운 주소를 생성할 때마다 대응한 개인 키를 개인 키 저장구에 저장해야 하며, 개인 키 저장구를 방문하는 과정은 거대한 안전 리스크를 가져오게 됩니다. 개인 키 저장구의 빈번한 방문을 피하기 위하여, 기존의 지갑은 주소를 대량 생성하는 책략을 적용합니다. 즉, 한꺼번에 여러개 주소 및 대응한 개인 키를 생성한후 다시 해당 개인 키를 한꺼번에 개인 키 저장구에 저장함으로써 개인 키 저장구에 대한 방문 빈도수를 감소합니다. 예하면 비트코인 지갑은 디폴드 셋팅에서 매번 100 개의 개인 키 및 대응한 주소를 생성하여 사용자는 개인 키를 오프라인 메모리(예하면 USB 플래시 드라이브, 전용 하드웨어 설비 또는 종이에 출력) 저장하여 오프라인 저장을 선택할수 있습니다. 대량 생성한 주소는 지갑 클라이언트에서 온라인 저장됩니다. 해당 주소들을 전부 사용한후 지갑은 다시 개인 키와 주소를 대량 생성하고 오프라인 저장을 방문하여 개인 키를 저장합니다. 이런 책략은 개인 키 저장구의 방문 빈도수를 어느정도 감소하였지만 여전히 개인 키 저장구에 대한 정기적인 방문이

필요하며, 주소와 개인 키의 저장과 관리 지출을 감소하지 않았으며, 개인 키 저장구의 방문수량과 저장지출은 여전히 거래량과 선성관계가 있습니다.

Themis 지갑은 신형 암호기술을 기반으로 한 등급 지갑으로, 아래와 같은 면에서 개선을 가져왔습니다.

1. Themis 블럭체인의 API를 지원하여, Themis 노드와의 데이터 인터랙션을 자동으로 완성하고, 사용자로 하여금 Themis 블럭체인 기능을 사용하여 신속하게 위탁관리 임무를 완성하게 함.

2. 사용자를 위해 임의의 수량의 주소를 생성하고 또 사용자 개인 키 오프라인 저장은 한개 개인 키 공간만 필요함. 사용자는 기존의 개인 키 오프라인 저장방안, 예하면 종이 지갑(개인 키를 QR 코드 형식으로 종이에 출력)을 이용하거나 또는 개인 키를 하드웨어 USB Key에 저장(일반적인 경우, 암호학 화폐의 개인 키는 표준 타원 곡선 암호 개인 키이므로, 본 방안의 주요 암호 키 s를 타원 곡선 암호 개인 키 저장을 지원하는 모든 암호 설비에 저장할수 있음)하는 방식을 이용할수 있음.

3. 사용자는 수불금 과정중 개인 키 저장구 방문이 필요 없음. 이는 본 방안의 주요 암호 키가 오프라인 저장이 완전 가능함을 의미함.

4. 사용자의 공중 키 인자 행렬의 저장공간은 고정된 정수로서, 이 저장량은 주소 생성 수량의 증가와 더불어 증가하지

않음.

5. 사용자의 주소관리가 더욱 용이해짐. 사용자 주소는 지불과 관련된 모 정보에 의해 생성되며, 해당 정보는 저장이 필요 없음.

4. 관건기술

4.1 그룹 위탁관리를 기반으로 한 공평교환 계약서

공평교환이라 함은 서로 불신임하는 여러개 주체 사이에서 사전 약정에 따라 자산 상호 교환을 완성하는 프로토콜을 가리킵니다. 공평교환은 공평 쌍방이 계산한 특례로서, 주로 서로 불신임하는 쌍방이 어떻게 공동으로 협력하여 디지털 상품을 교환 할수 있는지를 연구하며, 쌍방이 모두 상대방의 상품을 얻었거나 쌍방이 아무것도 얻지 못합니다(All-or-nothing).

01

Ensure the optimistic fair exchange protocol, that means TTPs only participate when disputes appear

We use group escrow protocol to avoid single point failure issue and denial of service issue.

02

도 4.1 자금 위탁관리와 상품 교부 안내도

공평교환의 비 형식화 묘사는 다음과 같습니다.

A 와 B 두개의 프로토콜 참여자가 각기 교환대기 전자항목 i_X 및 그 묘사 d_X 를 보유하고 있다고 가정하며, 여기서 $X=A$ 또

는 $X=B$.

검증 가능한 함수 $f(*)$ 가 존재하여 $d_X=f(i_X)$ 프로토콜이 성공과 중지 두가지 종료 상태가 있으며, 참여 쌍방이 자신의 종료 상태를 판정할수 있다고 가정합니다.

비동기 인터넷 환경에서 성실한 실체 A(B)의 성실여부는 판정 불가)는 기대하는 전자항목 i_B 를 받은후에야만 자신의 전자정보 i_A 를 지급하려고 하며, 성실한 실체 B도 마찬가지 입니다. 하여 이는 조정할수 없는 모순을 형성하였습니다. 즉, A, B는 누구도 먼저 자신의 전자항목을 지급하려고 하지 않아 결국 누구도 자신이 기대하는 전자항목을 얻지 못한것입니다. 이 모순에 대한 유효한 해결방안은, 쌍방 모두가 자신의 정보를 제 3 신뢰기관 실체(TTP)에 줌으로써, TTP 를 통해 중계하거나 쟁의 발생시 TTP 가 판결을 진행할수 있게 하는 것입니다.

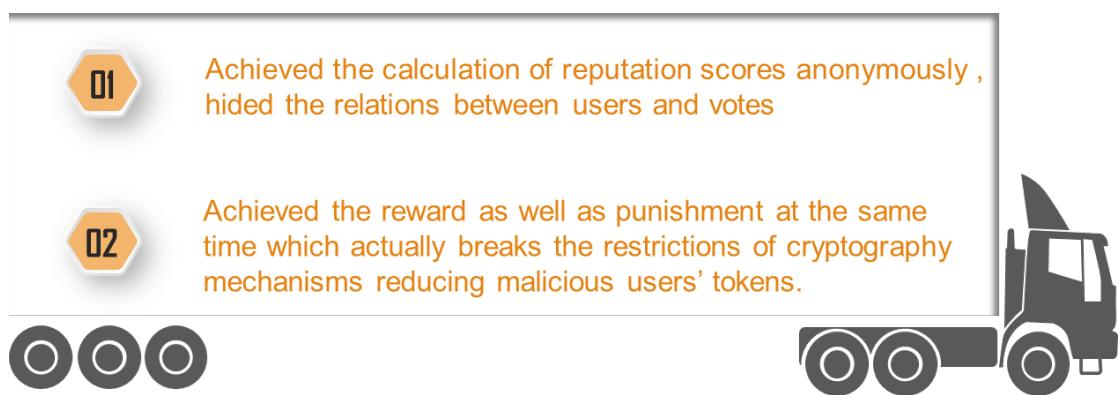
Themis의 설계는 주로 두개 측면의 문제를 해결하였습니다.

첫째, 중계방식, 즉 In-line TTP 또는 On-line TTP 방식은 TTP의 대량 참여가 필요하여 TTP의 성능과 안전이 광범위한 질의를 받게 되었습니다. 이에 대해 Themis는 낙관적인 공평교환 프로토콜을 제시하여 TTP는 쟁의 발생시에만 참여합니다.

둘째, TTP에 존재할수 있는 단일 장애 지점과 서비스 거절 공격 등 문제에 대해 저희는 그룹 위탁관리를 기반으로 한 안전교환 프로토콜을 제출하여 상기 안전 위협을 효과적으로 개선할 수 있습니다.

4.2 검증가능한 재조정과 관련 링 서명을 기반으로 한 익명 명예 체제

기존의 블럭체인중에 사용하는 격려체제는 첫째, 익명을 보증할수 없어 관찰자가 사용자의 신분과 투표 사이의 관계를 발생할수 있고, 둘째, 디지털 기호화폐를 기반으로 한 장려체제는 사용자에게 화폐를 증가하게만 할수 있지 사용자가 나쁜짓을 한 후 사용자의 화폐를 감소시킬수 없습니다. 즉, 디지털 기호화폐의 암호학 체제는 시스템이 사용자로부터 화폐를 인출해 가는것을 제한하여 징벌 목적을 달성할수 없습니다. 상기 문제를 해결하기 위하여 Themis 명예체제는 검증가능한 재조정과 관련 링 서명을 기반으로, 익명 명예 컴퓨팅을 완성할수 있으며 또 사용자의 신분을 노출시키지 않고, 장려와 징벌 격려를 실현할수 있습니다.



도 4.2 검증가능한 재조정과 관련 링 서명을 기반으로 한 익명 명예 체제

Themis 명예 시스템의 작업체제는 주로 여러 라운드 정보의 발송과 피드백입니다. 매 라운드의 시작에서 서버 유지관리에는 모든 클라이언트의 장기 데이터 베이스 신분과 각자의 암호화 명예 점수가 포함됩니다. 매 라운드에서 서버는 검증 가능한 재조정 프로토콜을 기반으로 한 스케줄링 알고리즘을 차례대로 운행하여, 명예 리스트를 일회성 가명에 기반한 익명 배열 리스트와 대응한 명문 신용 평점으로 변하게 합니다. 저희는 분권화의 스케줄링 프로토콜을 적용하여 서버와 클라이언트(소유자 제외)는 모두 일회성 가명과 장기 신분을 연관시킬수 없습니다. 클라이언트는 일회성 가명을 이용하여 익명으로 정보를 발표하고, 서버는 해당 정보와 그들과 상응하는 명예 평점을 연관시킬수는 있지만 클라이언트의 민감 정보를 파악할수 없습니다. 그다음 매개 클라이언트는 기타 사용자가 발표한 정보에 대해 피드백(예하면 투표)를 진행합니다. 모든 투표에는 모두 관련 링서명을 적용하여 서명함으로써 서버로 하여금 매개 고객이 한번만 투표했음을 검증하고 어느 고객이 투표를 제출했는지를 누설하지 않게 합니다. 이 설계로 인해 서버는 긍정적 투표와 부정적 투표를 통계할때 투표와 장기적 신분을 연관시킬수 있게 됩니다. 마지막으로 서버는 일회성 가명의 피드백 정보에 근거하여 신용 평점을 업데이트 하고, “역방향 스케줄링”을 진행하여, 해당 일회성 가명 및 업데이트한 명예를 원래의 장기적 신분과 그들의 암호화 업데이트한 명예 평점으로 회복시킵니다.

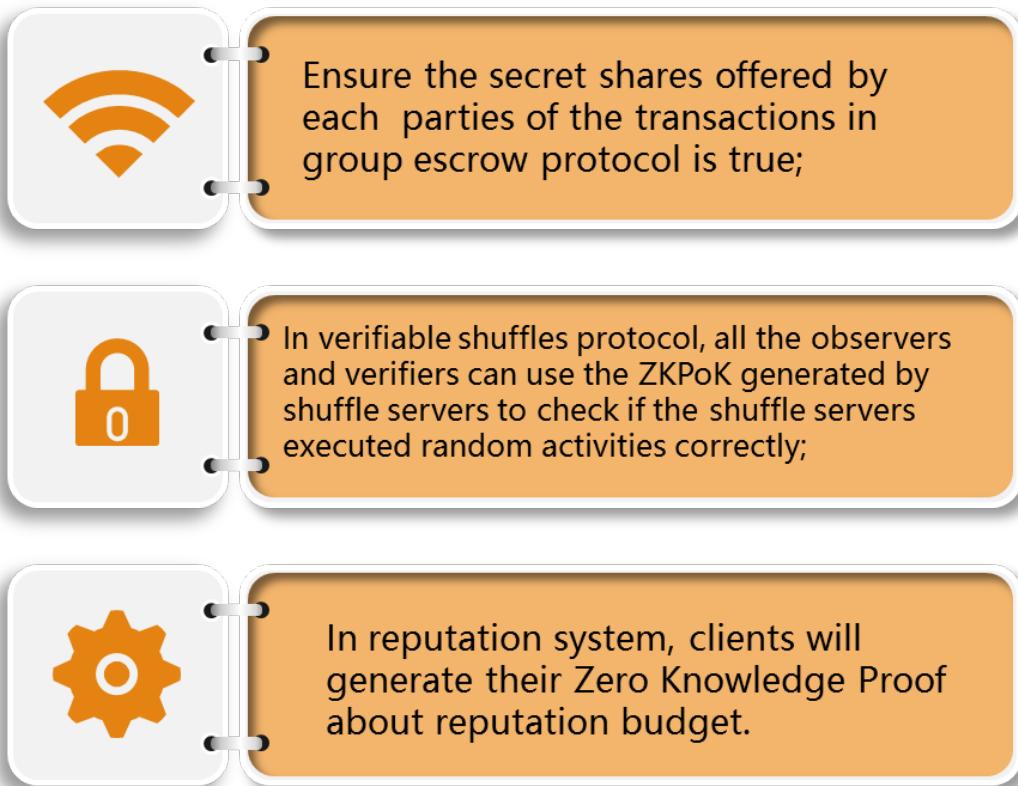
4.3 비 인터랙션형 영지식 증명

영지식 증명 시스템(Zero Knowledge Proof Systems)은 일종의 양자(증명자와 검증가)간 암호 프로토콜로서, 1983년에 탄생된 이래 이 신기한 컨셉은 이념 컴퓨터와 암호학에 깊고 원대한 영향을 가져왔습니다.

영지식 증명 프로토콜 집행을 통해 진실로 단언할 경우, 증명자는 검증자에게 증명할 수 있고 또 그로 하여금 신속하게 해당 단언의 진실성(완전성 : Completeness)을 확신하게 하며, 검증자는 해당 단언의 진실성 외에 어떠한 지식도 획득할 수 없으며 (영지식성 : Zero Knowledge), 해당 단언이 거짓일 경우, 무궁한 컴퓨팅 능력을 가진 증명자라 할지라도 무시할 수 없는 확률로 검증자를 기만하여 해당 거짓 단언을 받아들이게 할 수 없습니다 (합리성 : Soundness). 단언이 증명자가 모 비밀지식을 보유하고 있다는 단언일 경우, 영지식 증명 시스템은 영지식의 지식증명 시스템(Zero Knowledge Proof of Knowledge)으로 특화됩니다. 즉, 증명자는 검증자에게 증명하고 또 그로 하여금 자신이 정말로 자신이 주장하는 비밀정보를 갖고 있음을 확신하게 하고, 증명 과정에 어떠한 비밀정보 관련 지식을 누설하지 않을 수 있습니다. 증명자와 검증자 사이의 인터랙션 필요 여부에 근거하여, 영지식 증명 시스템은 인터랙션형 영지식 증명 시스템과 비 인터랙

션형 영지식 증명 시스템으로 진일보 구분할수 있습니다. 비 인터랙션형 영지식 증명은 통신에 대한 요구가 가장 낮아 실제 응용에 더욱 적합합니다.

저희는 영지식 증명을 이용하여 아래와 같은 세가 문제를 해결하였습니다. 1. 그룹 위탁관리 서비스 계약중에서 영지식 증명을 이용하여 거래 쌍방이 각기 위탁관리 노드에게 제공한 암호 키 할당 데이터가 진실함을 보증. 2. 검증 가능한 재조정 프로토콜에서 재조정 작업을 집행하는 것 외에 매개 재조정 서버는 모두 영지식 증명을 생성하여, 어떠한 관찰자 또는 검증자이든 모두 이를 이용하여 재조정 서버가 그의 랜덤 작업을 정확하게 집행하였는지를 검사 가능. 3. 명예 시스템에서 클라이언트가 정보 발표시 자신의 명예 예산의 영지식 증명을 생성하고, 1) 그의 실제 명예 득점이 예산값 b 보다 적지 않음을 주장, 2) b 作를 명예 점수로 하여 해당 소식을 발표하려고 함을 주장.



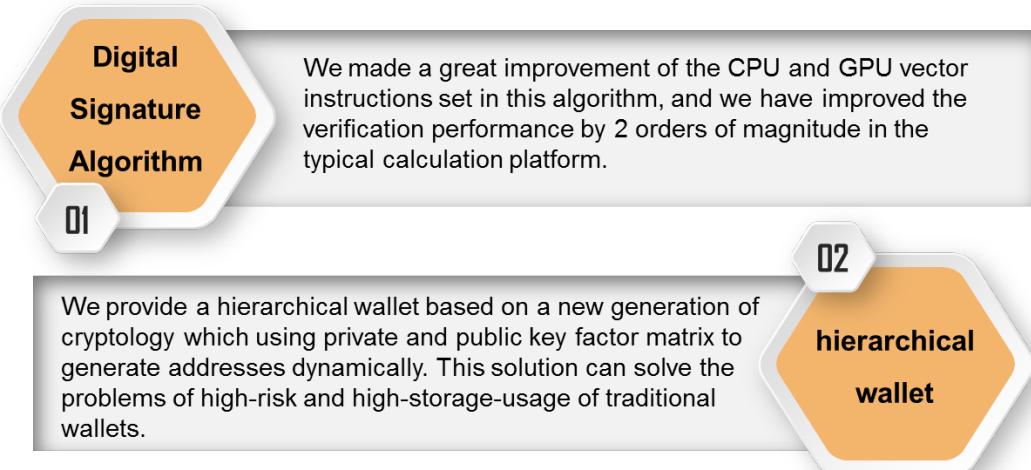
도 4.3 비 인터랙션형 영지식 증명

4.4 우수한 병행성 서명검증을 지원하는 디지털 서명 알고리즘

대량 거래 정보중 전자서명의 서명검증 컴퓨팅은 공유 블럭체인 거래 처리능력을 제약하는 주요 요소로서, 현재 블럭체인 중에서 보편적으로 적용하는 256 비트 소체 타원곡선상의 서명 알고리즘은 비록 비교적 높은 안전성을 갖고 있으나 서명검증 효율이 높지 못하며, 현재의 주류 중앙처리장치 초당 컴퓨팅이 가능한 서명검증 차수는 만회에 달하지 못합니다. 하여 네트워

크에 대량의 거래 정보가 발생할때 정보에 대한 서명검증은 노드에 매우 높은 지연을 초래하게 됩니다. 현재의 일부 연맹체인과 사유체인은 신뢰성 컴퓨팅 환경 도입 등 방식을 통해 기술도전을 피하고 있으나 이와 동시에 더욱 복잡한 안전기저를 도입하여 공유체인의 안전수요를 지탱할수 없습니다.

Themis 프로젝트는 최신 우수한 병행성 서명검증을 지원하는 디지털 서명 알고리즘을 도입하여 이 관건기술 수요를 해결하였습니다. 시스템은 여러가지 선택가능한 전자서명 방안을 지원하여 사용자와 응용의 수요에 근거하여 상응한 서명 알고리즘을 선택할수 있으며, 서명 개인 키가 한번의 환경만 사용해야 할 경우, 매우 높은 검증성능을 갖춘, 해쉬에 기반한 일회성 서명 알고리즘을 선택합니다. 전형적인 사용환경에서는 256 비트 안전등급을 보증하는 기초에서 특수성질의 타원곡선 및 서명검증 알고리즘을 선택함으로써 서명검증 노드로 하여금 곡선 파라미터와 알고리즘의 특점을 이용할수 있게 하며, 시공 균형 최적화 기술을 통해 대량 서명검증의 컴퓨팅 효율을 대폭 개선합니다. 알고리즘 실현에서는 특별히 GPU 와 CPU 를 상대로 한 벡터 명령어 조합을 최적화 하여 중앙처리장치위의 매개 트랜지스터가 가져온 컴퓨팅 능력을 충분히 이용합니다. 종합 최적화를 통해 전형적인 컴퓨팅 플랫폼에서 2 개 수량급의 서명검증 성능 제고를 실현하였습니다.



도 4.4 블럭체인을 향한 신형 암호학 알고리즘

5. 사용환경

Themis는 블럭체인을 기반으로 한 공평교환 시스템으로, 분권화의 디지털 화폐 위탁관리 서비스를 제공하고, 디지털 화폐를 매체로 한 공평교환 문제, 예하면 디지털 화폐, 디지털 자산과 실물상품 사이의 공평교환 문제를 해결합니다. Themis는 점대 점 위탁관리 지불, 디지털 화폐 거래 교환, 감독관리 계좌 안전 위탁관리, 다중 에이전트 거래 자산 위탁관리 등 여러가지 환경에 사용할수 있습니다.

5.1 점 대 점 위탁관리 지불

Themis는 P2P 인터넷 시장(예하면 OpenBazaar)에 분권화 디지털 화폐 위탁관리 지불을 제공하여 매매 쌍방의 직접거래를 실현할수 있습니다. Themis는 전자상 거래 플랫폼의 디지털 화폐 지불 시스템에 연결하여 Themis를 통해 기존 체인에서 상응한 위탁관리 계좌를 생성하며 디지털 화폐 거래행위에 대해 분권화 위탁관리를 진행합니다. 거래중, 구매자는 지불해야 할 디지털 화폐를 해당 위탁관리 계좌에 위탁관리하여, 실물상품 교부상황에 근거하여 정식 교부확인후 판매자에게 확인지령을 발송하며, 판매자는 위탁관리 계좌로부터 디지털 화폐를 획득합니

다. 이런 체제는 디지털 화폐 지불과 실물상품 교부가 동시에 완성할수 없는 난제를 효율적으로 해결하였습니다.

전자상 거래 실제 응용중에서 Themis 플랫폼은 구매자에게 선 배상 보장을 제공합니다. 예하면 상품 수령 확인후 7 일내에 판매자의 5% 자금은 스마트 계약을 통해 플랫폼 계좌에 남겨 담보금으로 하며, 7 일내에 분쟁이 발생할 경우, Themis 는 담보금으로 구매자에 대해 선 배상을 한후 플랫폼과 구매자가 환불사항에 대해 협상 합니다. 이는 구매자의 만족도를 진일보 제고함과 동시에 판매자의 신용등급을 제고할수 있습니다.



도 5.1 점 대 점 위탁관리 지불

5.2 디지털 화폐 거래 교환

Themis 는 블럭체인을 기반으로 한 공평거래 시스템으로, 디지털 화폐와 실물상품의 공평교환 수요를 만족시킬수 있을 뿐만 아니라 또 부동한 디지털 화폐간의 거래 교환 수요도 만족할수

있어, 각종 중심화와 분권화 디지털 화폐 거래 교환에 공평교환 보장을 제공합니다.

Themis 는 디지털 화폐의 장외거래를 지원하며, 비트코인, 이더리움 및 기타 블럭체인을 기반으로 한 암호학 디지털 화폐에 분권화 안전 위탁관리 서비스를 제공하여, 기존 체인에서 상응한 위탁관리 계좌 생성을 통해 부동한 디지털 화폐간 거래 교환 수요를 만족하고, 디지털 화폐의 체인간 거래에 공평교환 보장을 제공합니다.

Themis supports OTC transactions of digital currencies, and it can provide secure escrow service for cryptographic digital currencies based on blockchain



도 5.2 디지털 화폐 거래 교환

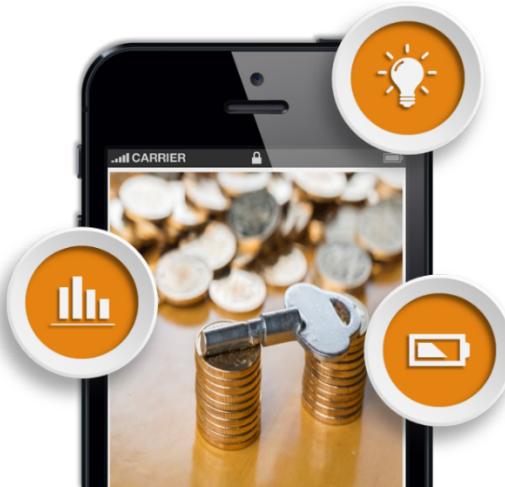
5.3 감독관리 계좌 안전 위탁관리

위탁관리 서비스는 전통 금융중 사용자 자금안전을 보장하는 중요한 수단인바, 예하면 증권사가 계좌 개설후 은행 위탁관

리 계좌를 개설해야 하며, P2P 인터넷 대출은 감독관리 계좌를 개설해야 합니다. 사모펀드, 크라우드 펀딩드 및 새로 나타난 ICO 투자펀드 등은 자금 위탁관리가 없거나 또는 제3자 중심화의 위탁관리 체제를 적용하였기에 위탁관리 자금의 투자대상, 투자비례와 투자수익이 불투명하여 정보 왜곡과 도덕 리스크를 쉽게 초래할수 있습니다.

Themis 는 고 확장성을 가진 스마트 계약 집군으로, 분포식 장부의 인터페이스를 제공하여 디지털 화폐 자금 감독관리 계좌에 분권화의 위탁관리 서비스를 제공할수 있습니다. 이를 통해 투자자금 안전, 프로젝트 자국 추적과 투자 이익 배당 합리화 등 문제를 효과적으로 보장할수 있습니다. 디지털 경제의 활발한 발전과 함께, 미래에는 디지털 화폐 대차, 디지털 화폐 선물 옵션, 디지털 화폐 ETF 펀드, 체인간 디지털 화폐 거래 등과 같은 수많은 디지털 화폐 금융상품 및 사용환경이 파생될 것이며, 이 모든것은 Themis 시스템을 통해 안전 위탁관리를 진행함으로써 자금안전을 보장할수 있습니다.

Themis can provide decentralized escrow service for cryptocurrency funds regulatory accounts, such as lenders of digital currencies



Futures of digital currencies, ETF funds of digital currencies, cross-chain transactions of digital currencies and so on, and all of these can be managed by themis system to keep security

도 5.3 감독관리 계좌 안전 위탁관리

5.4 다중 에이전트 거래 자산 위탁관리

공급사슬 금융, 부동산, 대형 설비 등 거래에서 거래 주체가 많고, 거래 단계가 길며, 거래 의존성이 강하므로 도덕 리스크와 거래 주체 왜곡 문제가 쉽게 초래됩니다.

Themis는 다중 에이전트 직책과 권의 촉발 조건 지령을 기반으로 한 스마트 계약 구축을 통해 다중 에이전트 거래중 위탁 관리가 필요한 자금, 예하면 계약금, 선수금, 수수료, 잔금 등을 디지털 화폐 형식으로 기존 체인에 위탁관리할수 있습니다. 거래가 상응한 단계까지 발전했을때, 상응한 거래 주체는 상응한 지령 입력을 통해 해당 스마트 계약을 촉발하여 공평거래 및 권리 교부를 실현합니다. 한개 거래측이 거래단계에 대해 쟁의가 생길 경우, Themis 그룹 위탁관리 서비스 계약 및 공평 중재체

제를 이용하여 중재청구를 발기할수 있으며, 그룹 위탁관리측의 모든 인원이 쟁의에 대해 중재, 투표를 진행하고 판결결과를 형성하며, 승리자는 위탁관리 계좌를 잠금해지할수 있습니다.

▶ 6. 팀 소개

6.1 핵심팀

Danish A.Alvi

Danish 는 UCL 런던대학교 블럭체인 기술센터 (CBT)의 개발인원으로, ERC223 프로토콜을 이용하여 Overled 프로젝트 ICO에 스마트 기호화폐를 작성함. Hadoop 와 Weka 를 사용한 온라인 빅데이터 검색과 저장 서비스를 홍보하였으며, 개발환경의 가상 기 자동 구성, 전단 서비스 환경의 가상기 자동 구성, 전단 서비스 CKAN / Drupal 집성과 데이터 감사를 협조 개발함. 정보과학 기술 서비스회사 Atos 에서 선도적인 연구 프로젝트를 했었고, UCLU TechSoc 에서 팀 조율 역할을 발휘하였으며, 얼굴인증 시스템 홍보에 주력하여 얼굴인증 시스템 사용을 강화하고, 대학교 출입 안전을 간소화하는 방식을 강화함.



Jennifer Chung

Jennifer 은 Agility Sciences Limited 의 CMO 및 중국-영국 블럭체인협회의 창시자임. 런던경영대학원의 경영학과 학위를 보유하고 있으며, 졸업 후 분포식 기술이 가져온 잠재적인 공업혁명에 주력함. 보스턴컨설팅회사에서 사모펀드와 벤처펀드 업무경험이 있음.



Ennan Zhai

예일 대학 박사 학위, 예일대 부교수. 그의 연구 분야에는 평판 시스템 및 대규모 분산 시스템이 포함되며 분산 시스템, 프로그래밍 언어 및 암호화 기술을 사용하여 안전하고 안정적인 컴퓨터 시스템을 구축하는 데 초점을 맞 춥니다. 현재 업무에는 매우 효율적이고 정확하며 심층적인 감사 기법을 사용하여 대규모 분산 시스템의 안정성과 보안을 향상시키는 것, 그리고 최초의 대기 시간이 짧고 익명으로 처리되는 익명 통신 시스템 인 PriFi 가 있습니다. 그의 박사 학위 논문은 클라우드 컴퓨팅 관련 신뢰성 문제를 일으킬 수 있는 근본적인 원인과 변칙적인 의존성을 사전에 감지하는 클라우드 컴퓨팅 신뢰성 감사 시스템 구축에 중점을 둡니다.



Wei Xin

Ph.D., Peking University, 중국 정보 보안 평가 센터

선임 엔지니어. 보안 취약점 탐지 및 암호화 알고리



즘 보안 분석에 중점을 두고 블록체인 자동 취약성 탐지 경험이 풍부합니다.

Takuya Koide

Takuya 는 영국 로얄할로웨이 런던대학교를 졸업하



고 현재 Unicoin에서 그로스 해커를 맡고 있으며,

시장 마케팅, 공정 연구개발, 데이터 분석 등 분야에서 풍부한

경험을 보유함. SEM 보급, 컨텐츠 마케팅, 프로그램 테스트, 수학

모델링 등 여러가지 기능을 장악하고 있으며, 다수의 블럭체인

프로젝트의 연구개발 실시와 운영 보급에 참여한 경험이 있는

블럭체인 및 금융혁신 분야의 복합형 인재임.

Yuet Ning Chau

Yuet 는 London School of Economics에서 석사 학위



를 받았습니다. Yuet 은 cryptocurrency 연구에 깊이

관여하고 있으며 다양한 blockchain 프로젝트에 대해 조언합니

다. CUKBA 의 공동 설립자 인 그는 영국의 금융 기술 기업가들

과 밀접하게 관련되어 있습니다. Yuet 는 이전에 영국 PwC 및

Capital Markets 팀의 멤버였으며, 전통적인 금융 서비스에 대한 확실한 지식과 경험을 가지고 있으며 여러 프로젝트에서 실사와 합병 및 인수에 참여하고 있습니다. Yuet 의 진정한 열정은 파괴적인 금융 기술에 있습니다. 그의 열정은 금융 기술 벤처 캐피탈 회사에서의 작업으로 시작되었으며, 심층적으로 연구하고 중국의 2 ~ 3 번째 도시 및 지방에서의 "전문 마을"개발 및 전자 도시 기술 개발을 시정부에 제안했습니다. 인프라의 잠재적 인응용 프로그램입니다.

Amir Marat



Amir 는 영국 로얄할로웨이 런던대학교를 졸업하고 블럭체인 기술과 금융 과학기술 분야에서 수년간 실제 작업 경험을 보유하고 있음. 암호화 공간과 블럭체인 지식을 깊이 파악하고, 여러개의 오픈 소스 커뮤니티에서 활약하고 있으며, 공중 키 암호학과 공통인식 알고리즘의 연구와 실현에 주력함. 또한 시장 조사와 비즈니스 사례 개발 측면에서도 풍부한 경험을 보유함. 소통능력이 뛰어나고, 세가지 언어(러시아어, 영어와 카자흐어)를 장악하였으며, 현재 중국어를 공부하고 있음.

James Johnson



James 는 App Society 의 공동 창립자 겸 공동 의장

이자 London University 의 Royal Holloway 의 컴퓨터 과학과를 졸업 한 UNIcoin 의 CTO 겸 공동 창립자입니다. James 는 광범위한 웹 개발 및 컴퓨터 시스템 관리 경험을 보유하고 있습니다. 그는 Cisco Systems의 기술 엔지니어였으며 비즈니스 관리자와 제품 주제 전문가를 계정 관리자에게 제공했습니다.

Hubertas Trinkunas

휴 버트 스는 영국 런던 대학교의 로얄 홀로 웨이 (Royal Holloway)에서 재무를 전공했으며, 로얄 홀로 웨이 (Royal Holloway)의 투자 및 재무 담당 부사장을 역임하고 현재는 UNIcoin 의 CFO 로 재직 중입니다. UNIcoin 은 학생 커뮤니티의 경제적 공유에 중점을 둔 블록 체인 기술이자 디털 화폐 기술의 시작입니다.



Evan Bian

하얼빈 공업 대학 전자 정보 공학과 졸업. 수석 IT 시스템 엔지니어, 수석 커뮤니케이션 엔지니어. Ericsson Operations Support 에서 근무했으며 전 세계 여러 사업자의 네트워크 관리 시스템을 담당했습니다. 블록 체인 산업에 합류한 후 여러 얼라이언스 체인 제품 계획 작업에 참여했습니다. 통신 시스템 설계, 솔루션 개발, 운영 지표 분석에 대한 풍부한



경험을 보유하고 있습니다.

Emma Zhu

미국 존스 홉킨스 대학 (Johns Hopkins University)

의 비즈니스 리스크 관리 석사 (Master of Business



Risk Management)는 학년도 여러 차례에 걸친 사례 연구 및 학교 특허 홍보 프로그램 개발에 참여하고 있습니다. 그녀는 광범위한 분석 및 컨설팅 경험을 보유하고 있습니다. 그는 현재 수석 블록 체인 애널리스트이며 여러 제휴 체인 제품 솔루션의 사용자 지정 및 금융 상품 디자인 분야에서의 경험에 참여하고 있습니다.

6.2 컨설턴트팀

Donald Lawrence

- 유니버시티 칼리지 런던 객원교수
- 전략 컨설팅회사 창세기회사 파트너



유니버시티 칼리지 런던 교수, 블럭체인 기술센터 프로젝트 담당, 금융 컴퓨팅연구센터 프로젝트 담당, 앨런 튜링 빅데이터 연구센터 프로젝트 담당. 시티코프, 뱅크 오브 아메리카와 아멕스 등에서 총경리 이상급의 직위를 맡았으며, UCL 기간에 중앙은행, 투자은행, 헤지펀드, 청산센터와 과학기술기업과의 프로젝트 연구와 개발 연계 등을 책임짐.

Daniele Bernardi

■ Diaman SCF 의 창시자 겸 CEO

투자자 잡지(INVESTORS' Magazine Italia) 주석

Daniele Bernardi, Diaman SCF 의 창시자 겸 CEO, 투자자 잡지(INVESTORS' Magazine Italia) 주석. 수익율이 높은 투자 전략 개발에 주력하고, 끊임없이 혁신을 추구하는 기업가임. 그의 연구방향은 수학모델의 개발이며, 투자자와 가족기업의 의사결정 과정을 간소화하고 투자 리스크를 감소함.



천중(陈钟)

■ 북경대학 교수

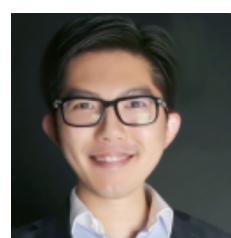
천교수는 원 북경대학 소프트웨어와 마이크로전자 학원 원장, 북경대학 금융정보화 연구센터 주임, 북경대학 네트워크와 정보안전 실험실주임임. CCF 상무이사, CCF 정보 비밀유지 전문위원회 부주임, CCF 네트워크와 데이터 통신 전문위원회 위원임.



Hui Gong

■ 중국 - 영국 블록 체인 협회 사무 총장

옥스퍼드 대학교 (University of Oxford) 박사후 연



구원, 런던 대학 (University College London)의 재무 수학 박사, 런던 대학 (University College)의 블록 체인 연구 센터 연구원, 중국 - 영국 블록 체인 협회 사무 총장. 연구 프로젝트에는 유엔 식량청 디지털 신원 프로그램, ICO 규정 및 도전 등이 포함되며 디지털 통화 금융 상품 디자인에 대한 풍부한 경험을 보유하고 있습니다.

구안 지(关志)

■ 북경 대학 준회원 연구원



북경 대학 박사, 북경 대학의 동료 연구원, 암호화 및 보안 프로토콜 전문가, 주요 개발자 및 커뮤니티 리더는 잘 알려진 비밀 알고리즘의 GmSSL 오픈 소스 프로젝트, 처음 세 북경 대학 블록 체인 방향 마스터를 육성.

선 지용(孙志勇)



■ 중국의 국유 국영 산업 혁신 전략 동맹 부위원장

북경 대학 과학 석사, 중국 국영 기업 소유의 국영 산업 혁신 전략 동맹 부회장 인 Tian Tian Chi Juntai 법률 사무소 수석 파트너, Jinfeng Capital 회장, 우 의료 공동 창업자 겸 최고 경영자, 베이징 신 제어 기술 주식 회사, 미국 비전 투자 관리 회사 관리 파트너의 부회장.

6.3 파트너

1. 심천시 Chieftin 금융과학기술연구원(<https://chieftin.org/>).

본 연구원은 심천시 나호구정부의 지원하에 설립되었으며, 원 영국 옥스포드 대학 컴퓨터학과 주임 Bill Roscoe 교수가 선도하여 블럭체인, 빅데이터, 인공지능 등 금융 과학기술 분야의 기술 연구개발과 응용 개발에 주력하였으며, 형식 검증 기술은 국제 상에서 선두적인 지위를 차지하고 있고, 관련 연구 프로젝트, 방향은 모두 심천시정부의 중점 부화 연구 프로젝트 및 산업화 방향에 속함. Themis 와 연구원의 협력은 주로 스마트 계약의 안전성 문제를 해결하는 것으로, 형식 검증 기술을 이용하여 시스템 중의 스마트 계약, 특히는 위탁관리 계약과 중재 계약의 정확성을 검사 및 검증함.



도 6.1 Chieftin 금융과학기술연구원

2. 오라클체인(<http://oraclechain.io/>). Oracle 은 중재 서비스중에서 거래 쌍방이 제공한 재료를 토론 및 검토시

필요한 체제임. OracleChain 은 블럭체인내에서 현실세계 데이터의 Oracle 서비스를 제공하며, 그의 생태 시스템은 일련의 서비스와 API 를 제한다. Themis 는 상기 서비스와 API 를 이용하여 현실세계 데이터를 블럭체인에 도입시켜 중재 결과를 결정하고 그후의 작업을 실현함.

7. 기관 투자가

Themis 는 Node Capital, Genesis, JiuDing Blockchain Lab(Jlab), Consensus Capital 및 Northern Light Venture Capital 등 여러 유명 투자 기관으로부터 투자를 받았습니다.