

이더리움을 통해 본, Smart Contract 기반의 금융업 혁신 모델

[요약문] 금융 IT 동향 특별 기고



2017. 1. 3 | 금융 IT Lab

김세형 수석컨설턴트
sehyoung.kim@samsung.com

박대현 주임컨설턴트
d0930.park@samsung.com

1. 블록체인 플랫폼, 이더리움의 탄생과 진화

이더리움은 무엇인가?

이더리움(Ethereum)은 비트코인(Bitcoin) 기술에 자극을 받은 19세 러시아 청년 Vitalik Buterin이 '14년에 개발한 범용 블록체인 플랫폼이다. 모든 거래 참여자들이 동일한 거래 기록을 나누어 갖는 분산 원장 체계를 갖추고 있으며, 네트워크에서 통용되는 독자적인 가상화폐 단위¹⁾를 사용한다는 점에서 두 블록체인 기술은 유사점을 가진다.

하지만 기술적인 면에서 몇 가지 중요한 차이가 존재한다. 우선 1MB로 블록 크기가 고정되어 있던 비트코인과는 달리 이더리움은 블록 크기에 제한을 두지 않는다. 또한 블록 생성 주기를 약 12초까지 줄여 10분에 한 번꼴로 블록 생성 과정이 일어났던 비트코인에 비해 훨씬 더 빠른 데이터 검증이 가능하게 되었다.

비트코인 대비 이더리움의 가장 눈부신 발전은 Smart Contract 기능의 도입에서 찾을 수 있다. 이더리움 블록체인의 경우 블록에 데이터뿐만 아니라 조건, 반복 구문 등의 실행코드를 포함시켜 로직의 실행을 자동화할 수 있다. Smart Contract를 구현하기 위한 contract code는 EVM(Ethereum Virtual Machine)이라는 독립된 실행 환경에서 실행된다.

이더리움 플랫폼의 발전

이더리움 플랫폼은 모든 사용자에게 열려 있기 때문에 누구나 공개된 소스코드를 활용해 이더리움 기반의 어플리케이션을 개발할 수 있다. 이러한 개방성과 이더(ether) 가치의 급속한 상승에 따라 이더리움 어플리케이션은 빠른 속도로 개발되어 공유되기 시작하였다.

'16년 12월 기준 이더리움 어플리케이션 수는 총 327개이다²⁾. 이는 연구를 진행한 '16년 9월 대비 약 35% 증가한 수치이다. 서비스 상태 별로 보더라도 컨셉 단계나 프로토타입 단계에 머물러 있던 어플리케이션 대비 실제 서비스 단계에 접어든 어플리케이션의 비중이 크게 증가하였다. 아울러 이더리움 초기의 어플리케이션들이 도박이나 게임을 구현하는 데에 집중되어 있었던 것에 비해 비즈니스 로직이 구현된 어플리케이션의 수도 눈에 띄게 늘어 이더리움 블록체인 기술의 성숙도를 가늠할 수 있었다.

1. 비트코인의 경우 '비트코인(BTC)'이라는 가상화폐를, 이더리움의 경우 '이더(ETH)' 라는 가상화폐를 사용하고 있다.

2. EtherCasts 웹 페이지(<http://dapps.ethercasts.com/>)에 등록된 어플리케이션 기준

2. Use Case 분석

327개 이더리움 어플리케이션의 추적 조사를 통해 실행 가능성(feasibility)과 파급력(impact), 확장성(expandability) 측면에서 심층 분석이 필요하다고 생각되는 8개 Use Case를 선별하였다. 각각의 사례들을 리서치하며 다양한 산업 영역에서 블록체인 기술의 적용 가능성을 확인할 수 있었다.

La'Zooz는 사용자 운행 정보를 활용한 서비스 확장 가능성이 돋보였고, WeiFund와 Etherplan의 경우 금융 거래 시 법적 계약을 코드화하여 자동화한 부분에서 혁신성이 발견되었다. Provenance와 EthIdent는 모두 블록체인의 비가역적인 거래 기록 관리에 초점을 맞춘 서비스로서 관련 비즈니스 영역에 빠르게 적용될 여지가 있었다. Otonomos 및 Augur는 구성원의 참여가 적극적으로 요구되는 모델로 기존 의사결정 및 정보 수집 과정을 근본적으로 변화시킬 수 있는 아이디어라고 판단하였으며, 마지막으로 EtherEx는 異種의 가치 저장 수단을 표준화된 방식으로 교환할 수 있는 플랫폼이라는 점에서 시장 파급력과 확장성이 높다고 보았다.

| 서비스 명 | 기능 유형 | 서비스 개요 | 서비스 상태 |
|------------|------------|--|----------|
| La'Zooz | 비즈니스 서비스 | 별도 가상화폐를 통해 중개자 없이 탑승자와 운전자를 매칭하는 카 셰어링 플랫폼 | 컨셉 단계 |
| WeiFund | 비즈니스 서비스 | 이더리움 계좌와 연동하여 자금 수요자와 투자자를 직접 연결하는 크라우드 펀딩 플랫폼 | 프로토타입 단계 |
| Etherplan | 비즈니스 서비스 | 다양한 펀드 상품을 하나의 플랫폼에서 투자할 수 있도록 도와주는 글로벌 자산관리 모델 | 개발 단계 |
| Provenance | 비즈니스 서비스 | 블록체인 원장에 상품 생산 및 유통 과정을 기록 / 관리하는 상품 이력 트래킹 서비스 | 컨셉 단계 |
| EthIdent | 이더리움 보조 도구 | KYC 데이터를 이더리움 계좌와 연계한 이더리움 네트워크 內 신원 검증 서비스 | 서비스 단계 |
| Otonomos | 비즈니스 서비스 | 분산 환경 하에서 실제 기업의 주식 발행 및 의사결정이 진행되는 기업 운영 서비스 | 서비스 단계 |
| Augur | 이더리움 보조 도구 | 집단 지성을 통해 특정 사건의 발생 가능성을 추정하는 온라인 예측 시장 플랫폼 | 프로토타입 단계 |
| EtherEx | 비즈니스 서비스 | 다양한 종류의 가상화폐 및 디지털화된 자산을 사용자 間 교환할 수 있는 P2P 거래 플랫폼 | 프로토타입 단계 |

3. 금융업 혁신 모델 발굴

이더리움이 만들어가는 디지털 혁신의 의미

이더리움 Use Case들은 개방형 생태계를 바탕으로 블록체인의 특성을 활용하여 오랜 기간 비즈니스 관행으로 고착화된 여러 제약을 넘어설 수 있는 새로운 가능성을 제시하고 있다. 또한 디지털 혁신을 통해 실현될 미래 금융의 모습을 생각해볼 수 있는 기회를 제공한다.

시스템이 서로 완전히 단절되어 있어 서비스 연계가 어려웠던 기존의 중앙집중식 시스템에 비해 상호 공조가 편리한 이더리움은 산업 융·복합이나 플랫폼 사업을 위한 기술 개방의 중요성을 보여 준다. 또한 중개자가 배제된 진정한 의미의 P2P 네트워크 형성이 가능하다는 점에서 디지털 경제가 향해갈 하나의 이정표를 제시하고 있다. 아울러 비트코인이 구성원들의 합의(consensus)에 의한 화폐 발행으로 '경제 권력 분산화' 가능성을 제시하였다면, 이를 이어받은 이더리움은 거래의 안전성과 신뢰성을 확보하는 진정한 디지털 민주화를 지향하고 있다.

블록체인 Smart Contract의 비즈니스 가치

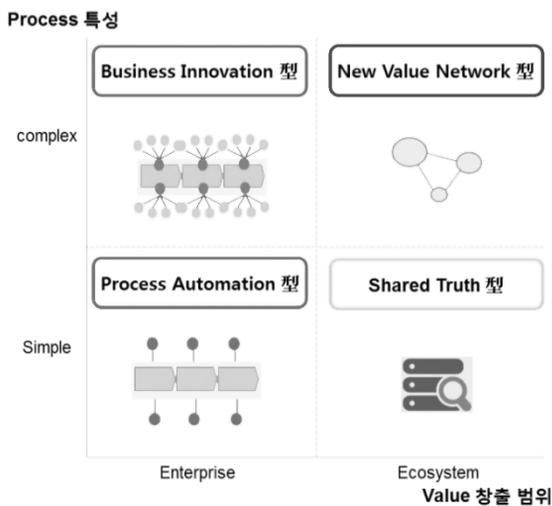
블록체인 Smart Contract 본연의 특징은 오랜 기간 동안 비즈니스 관행으로 고착화된 여러 제약을 넘어설 수 있는 사고의 파괴를 유도하고 나아가 새로운 가치를 창출할 수 있는 원천이다. 크게 Cost, Time, Risk 관점에서 Smart Contract의 비즈니스적 가치가 도드라진다.

| 블록체인 특징 | 분산된 상호 인증 | | | 확장성 | 자동화 |
|-------------|------------|-------------------------|---------------|--------------|------------|
| | 보안성 | Middle man 대체 | 투명성 | | |
| 적용 효과 | | | | | |
| Cost | • 보안 비용 절감 | • 수수료 절감 | • 규제 비용 절감 | • IT 구축비용 절감 | |
| Time | | • 데이터 정확성, 무결성 검증 시간 단축 | | | • 신속한 거래처리 |
| Risk | • 해킹 위험 제거 | | • 이중 지불 위험 제거 | • 신사업 서비스 확장 | • 에러율 감소 |

현안과 이슈를 블록체인의 특징을 통해 해결하고자 하는 다양한 시도에 대한 조사와 유형화를 통해 블록체인 Smart Contract 적용 가능 영역 발굴을 위한 기능 적용 Matrix를 설계할 수 있다. 기본적으로 블록체인 Smart Contract 적용을 통해 Value가 생성될 수 있는 분야는 상호 거래 및 검증이 빈번하거나, Data Ownership 및 보안이 민감하며 정형화된 절차를 통해 처리될 수 있는 업무 특성을 가지고 있다.

블록체인 기능 적용 Matrix는 이를 발전시켜 Value 창출의 범위와 Process 특성을 중심으로 New Value Network型, Shared Truth型, Business Innovation型, Process Automation型으로 혁신 기회를 분류할 수 있는 도구이다.

블록체인 기능 적용 Matrix



- **Shared Truth 型** : Provenance, EthIdent
개인 또는 공공 정보의 기록, 권리의 저장, 인증, 활용
- **Process Automation 型**: Otonomos
정형화된 프로세스 중 데이터 정합성, 무결성의 상호 확인을 요하는 업무의 자동화
- **Business Innovation 型** : Etherplan, EtherEx
중개자 배제 등을 통한 거래 구조 혁신 또는 Supplier, 서비스 제휴사 등 모든 Value Chain의 정보 가시성 확보
- **New Value Network 型** : La'Zooz, Augur, WeiFund
생태계의 확장, 신기술과의 결합을 통한 신규 사업 및 서비스 창출 수단으로 활용

금융업 혁신 모델의 발굴

지금까지 우리는 이더리움의 특징과 주요 Use Case, 기술적 잠재력에 대해 검토하고 혁신 기회 발굴의 접근 방법에 대해 살펴 보았다. 블록체인의 기술적 특성을 감안할 때 비즈니스 영역에 미칠 파급력은 부인할 수 없는 사실이며, 실제 사업 영역의 현실적인 이슈들을 반영함으로써 혁신 가능성을 현실화 할 수 있다.

이제 블록체인 기능 유형 분류를 통해 도출한 Matrix를 바탕으로 금융 현실을 분석하고 새로운 가치를 만들어낼 수 있는 현실적 Use Case에 대한 고민이 필요하다. 마지막으로 금융 현실 및 환경을 반영하여 고객의 새로운 금융 경험을 제공할 수 있는 몇 가지 금융向 Smart Contract 적용 모델들을 제시해보고자 한다.

| 예시 모델 | 블록체인 기능적용 Matrix | | | | 서비스 가치 | 이더리움 참조 모델 |
|------------------------|------------------|--------------------|---------------------|-------------------|--|------------|
| | Shared Truth | Process Automation | Business Innovation | New Value Network | | |
| KYC | ✓ | | | ✓ | 보안 및 고객 프라이버시가 담보된 금융사 통합 KYC 데이터 관리 서비스 | EthIdent |
| 로그인 대행 및 본인 확인 | ✓ | | | ✓ | 참여자間 공유된 고객 정보로 회원가입 / 로그인 간편화 및 신규 마케팅 기회 발굴 | EthIdent |
| 생체인식 연계 사용자 인증 | ✓ | ✓ | | | 생체인식 사용자 인증의 고객 편의 수준은 유지하며 블록체인으로 추가적인 보안 확보 | EthIdent |
| 전자문서 진위 판별 및 원본 확인 | ✓ | | ✓ | | 신뢰할 수 있는 데이터 / Timestamp 관리 및 보다 안정적인 서비스 운영 | Provenance |
| Insurance Claim | ✓ | ✓ | | | 보험 관계자들에게 보험 관련 문서 및 데이터가 Single View로 제공되어 시간 및 비용 절감 | Provenance |
| Loyalty Reward Program | ✓ | | | ✓ | 제휴사間 리워드 거래 정보의 실시간 공유 / 정산으로 비용 절감 및 고객 retention 강화 | EtherEx |
| Crowd Funding | | ✓ | | ✓ | 다른 Dapp 間的 연동으로 Compliance 달성 및 지분형 크라우드 펀딩 모델로의 확장 | WeiFund |
| Supply Chain Finance | ✓ | | ✓ | | 공유된 무역 문서를 바탕으로 Supplier에게 펀딩 기회 제공 및 중개자 제거로 비용 절감 | Etherplan |

insight to **!nspiration**  삼성SDS

<http://www.samsungsds.com>

Copyright © 2017 Samsung SDS Co., Ltd. All rights reserved