



WHITE PAPER

**CRYPTO MODERN ART
&
BLOCKCHAIN
MOMENTUM
HOLDINGS**



About XBC Project

Blockchain Momentum Holdings와 Crypto Modern Art가 공동으로 기획한 XBC 프로젝트는 Crypto Modern Art의 자체 개발 블록체인 기술, 결제 솔루션, 블록체인 기술기반의 게임 등과 함께 Blockchain Momentum Holdings의 금융 서비스를 제공합니다. 암호화 화폐가 단순한 투자의 대상이 아닌 실물 자산으로 자리 잡는데 있어 가장 큰 문제로 대두되는 가치의 변동을, 수익으로 전환한다는 역발상에 의해 시작되었고, 이를 위해 3가지의 다른 블록체인을 활용한 에코 시스템을 사용하고 Blockchain Momentum Holdings와의 협업으로 해결하였습니다.

본 프로젝트는 본질적으로, 치밀한 비즈니스 모델과 완성된 기술을 통한 수익의 대부분을 사용자에게 환원 하는 것에 목적을 두고 있으며, 이를 통해 본질적 의미의 탈중앙화를 구현하고자 합니다. BLOCKCHAIN MOMENTUM HOLDINGS와 CRYPTO MODERN ART는 블록체인 기술 기반의, 금융 플랫폼, 코인 개발, 결제 솔루션, 게임 등의 서비스를 제공합니다. CRYPTO MODERN ART의 자체 개발 기술로 안전한 금융 거래 환경을 제공하며 자사 디자이너를 통해 서비스의 기초적인 단계부터 관리되는 BI/BX 솔루션 또한 준비되어 있습니다.



INDEX



About XBC Project

XBC 프로젝트는 금융, 문화, 소셜네트워크 등 블록체인으로 확장 가능한 모든 영역을 아우르는 것과 동시에, 각 비즈니스에 최적화된 기술을 사용함으로써 특별한 확장성을 가지게 됩니다.

XBC 네트워크는 우선적으로 자체 플레이 스토어, 거래소 편의점, 유튜브즈 플랫폼 등을 구축 함으로써 중소기업과 개인에게 창의적이고 최적화된 환경을 제공하고, 이를 통한 수익 대부분을 참여자에게 돌려주는 환원 구조를 통해 올바른 생태계를 구축할 것입니다.

XBC 프로젝트의 심볼인 ‘콤마’는 기술, 문화, 예술을 관통하는 지점을 찾고 4차 산업혁명에 기여하고자 기획되었습니다. 소프트웨어 개발자의 상징적 기호인 ‘세미콜론’ 과 음악의 ‘숨표’ 그리고 루이스 호르헤 보르헤스 역작인 ‘픽션들’ 중 특별한 문장인 “모든 책이 서로 다를지라도 동일한 요소들로 구성되어 있다. 즉 띄어쓰기 공간과 마침표, 쉼표, 그리고 스물두 개의 철자 기호로 이루어 진다는 것이었다.” 에서 영감을 받았습니다. 특히 루이스 호르헤 보르헤스는 단편집인 픽션들로 하이퍼 텍스트의 개념을 처음 제시하였고 이를 통해 포스트 모더니즘, 현재의 인터넷까지 이르게 한 천재 작가로서, 기술, 경제, 문화, 예술을 블록체인 기술로 융합함으로써 새로운 가능성을 제시하고자 하는 XBC 프로젝트의 이념과 많은 부분 동일성을 가지고 있습니다.

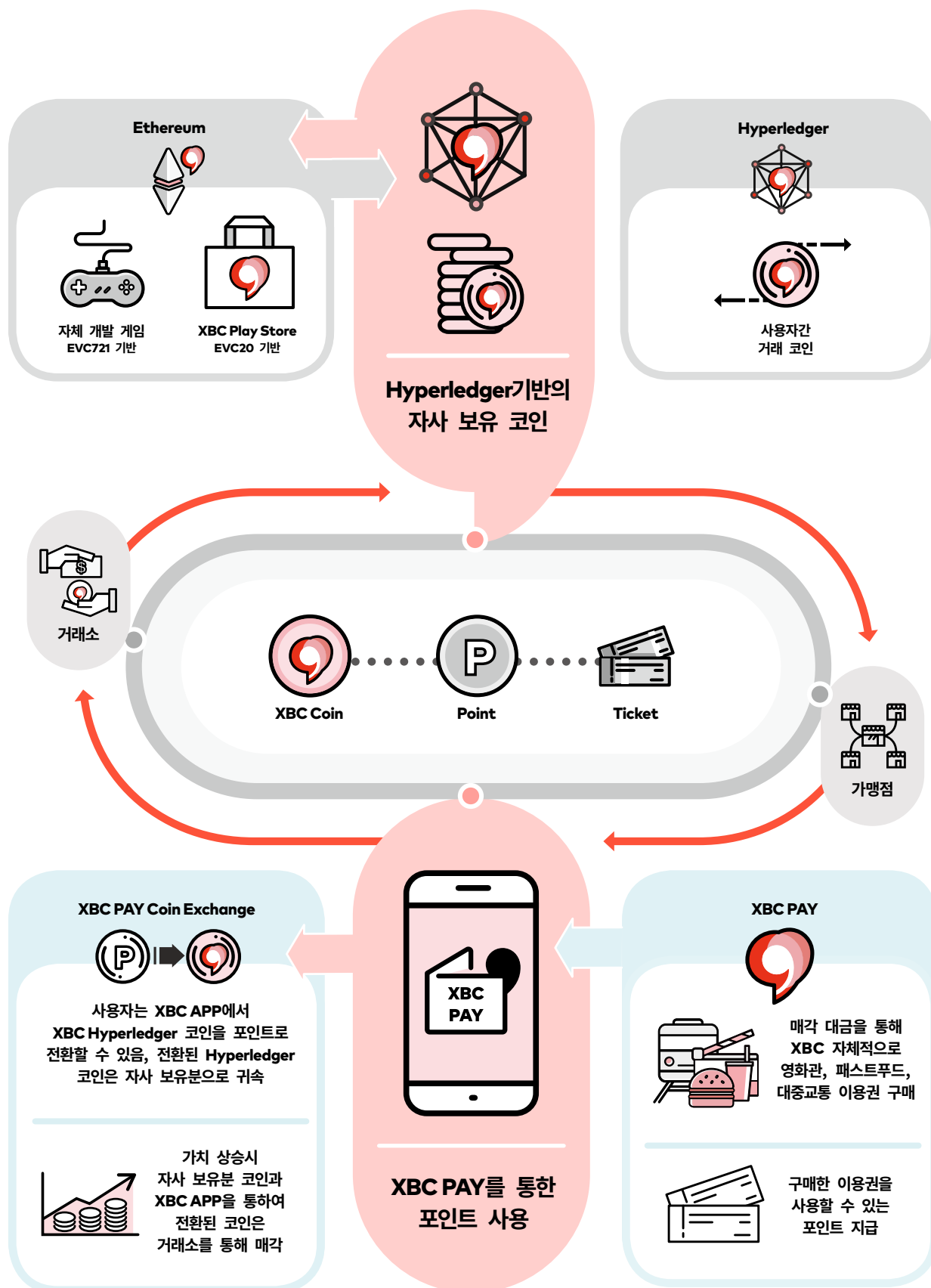




BUSINESS ISSUES



세 가지 자체 개발
코인의 장점을 활용한
에코 시스템



About XBC Project

XBC 프로젝트는 크게 3가지의 다른 특성을 가진 블록체인이 연동되어 하나의 생태계를 이루고 있습니다.

Hyperledger Fabric

그 가치가 유동적이며 거래소 상장에 사용될 XBC 코인과, 1:1의 고정 환율로 Pay Platform을 통해 대중교통/프렌차이즈 등에서 사용 가능한 XBC Pay로 나뉘게 됩니다. XBC 코인은 약 40%의 자사보유량을 유지하게 되며 가치 상승시 자사 트레이딩 시스템에 의해 매각한 뒤 매각대금을 Pay Platform 사용자 에게 나누어 주게 됩니다.

Lighting Network & Pay Platform

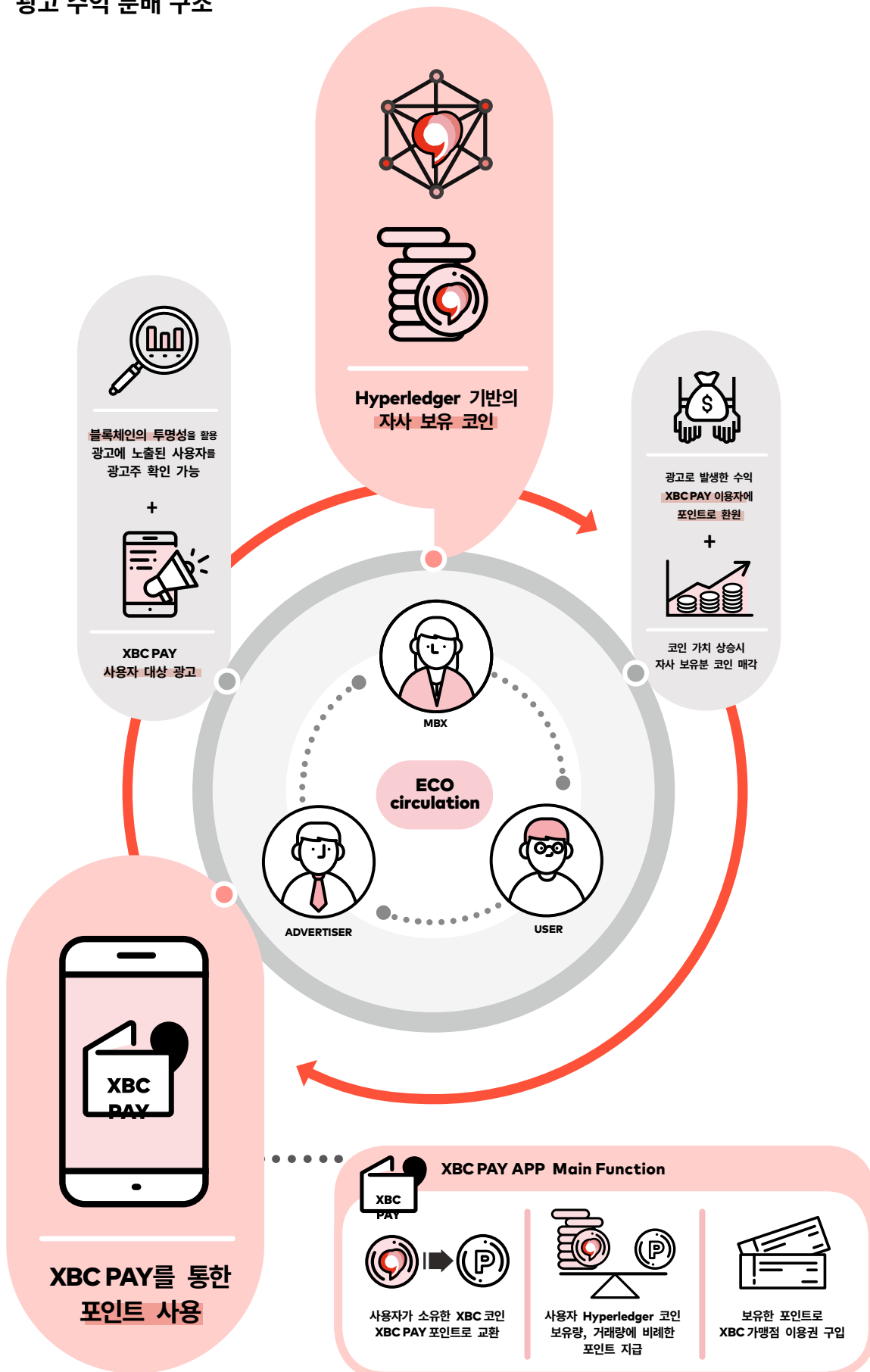
사용자가 XBC Pay를 사용하게 될 경우 XBC Pay로 전환된 XBC 코인은 다시 자사가 보유하게 되며 이를통해 효율적인 인플레이션 관리와 자사 보유량을 유지하게 됩니다.

ERC 20 & ERC 721

XBC의 자체 개발 게임과 XBC Playstore는 Ethereum 기반으로 개발된 블록체인과 ERC 20, ERC 721의 스마트 컨트랙트로 구성 되었으며 Hyperledger Fabric 기반의 코인, Pay Platform과 효율적으로 연동 됩니다. 사용자는 게임내 캐릭터, 아이템등을 경매에 붙이거나 거래할수 있기때문에 1:1 비율의 고정된 가치를 지닌 Pay Platform과 달리 해당 캐릭터의 실물가치는 유동적입니다. XBC 코인의 지분증명 방식을 통하여 XBC 코인의 사용자는 랜덤으로 XBC 게임의 캐릭터를 선물받게 됩니다. 이것이 의미하는 바는 XBC 코인 투자자는 저절로 XBC 게임에 관심을 가지게 되며, XBC 게임 이용자 에게는 자발적 XBC 코인의 투자를 유도하게 되어 지속적인 가치상승과 게임성을 누리게 됩니다.



XBC PAY의 광고 수익 분배 구조



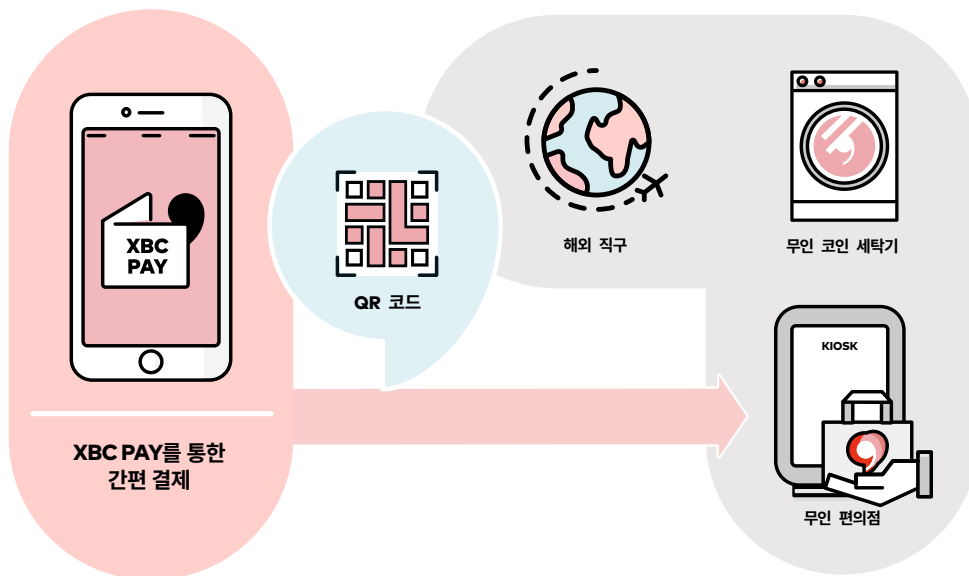
XBC의 네트워크 구조에 의하여 단순히 XBC Pay를 사용하는 것만으로도, 실사용자와 가맹점은 충분한 혜택을 누릴 수 있지만, XBC는 나아가, 블록체인 네트워크의 투명성을 백분 활용하여, 트래픽이 확보된 이후 적극적으로 기업들로부터 광고를 유치할 것입니다.

타 광고 플랫폼과 달리 블록체인 네트워크의 장점 중 하나인 실거래량, 거래금액 등의 투명성은 기업들로 하여금 매우 구체화된 광고효과를 예측할 수 있게 되며, 실사용자에게는 XBC Pay 네트워크를 이용함으로 인하여 발생한 실제 광고 수익을 확인할 수 있게 될 것입니다.

이를 통해 XBC 프로젝트의 행보는, 단기간 내 비약적 네트워크의 확장과 더불어, 4차 산업혁명의 중요한 지표로 사용될 것입니다.



XBC PAY의 무인화 서비스



XBC 네트워크는 차별화된 무인 편의점, 무인 코인세탁을 지원합니다.
사용자는 XBC Pay를 사용하여 무인편의점, 코인세탁기를 사용할 수 있습니다.

또한 XBC의 무인 편의점 플랫폼은, 그동안 사용자가 해외 직구를 하는 데 있어 소요되었던 복잡하거나 불필요한 과정을 대폭 간소화하여, 물품을 선택하고 XBC Pay App을 통해 QR 코드를 인식 하는것 만으로 간편한 구매가 가능합니다.

가장 가까운 곳에서 만나는 **스마트 쇼핑 플랫폼**

당사의 무인 편의점은 XRway와 키오스크의 기술융합을 통해 보다 편리하고 안전하며 신속한 쇼핑 서비스를 제공할 수 있는 플랫폼입니다.

Smart Shopping Platform

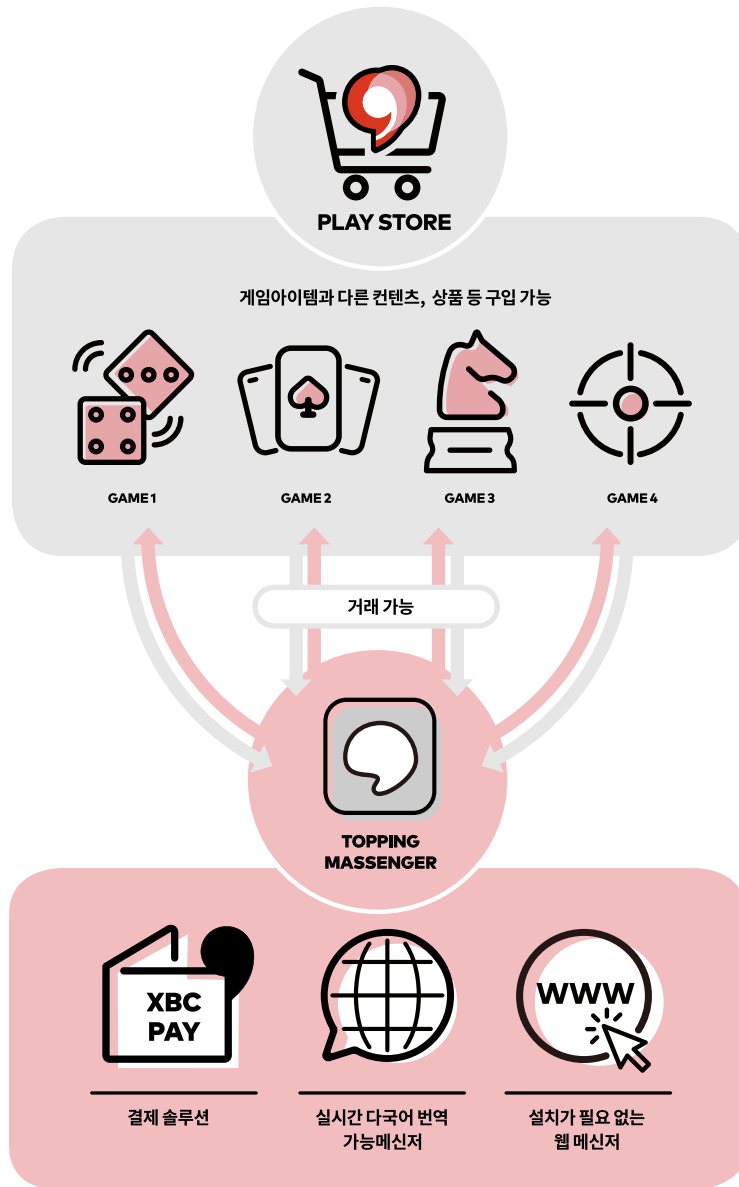
- 자동화 로봇 시스템**
포장부터 상품출고까지 전과정 자동화
- XRway**
촬영 한번으로 진행되는 간편한 결제서비스
- 키오스크 주문 시스템**
터치 한번으로 주문하는 편리한 키오스크

스마트폰 하나만 있으면 안전하게 이용 가능

최소의 공간만으로 편의점의 모든 기능 제공

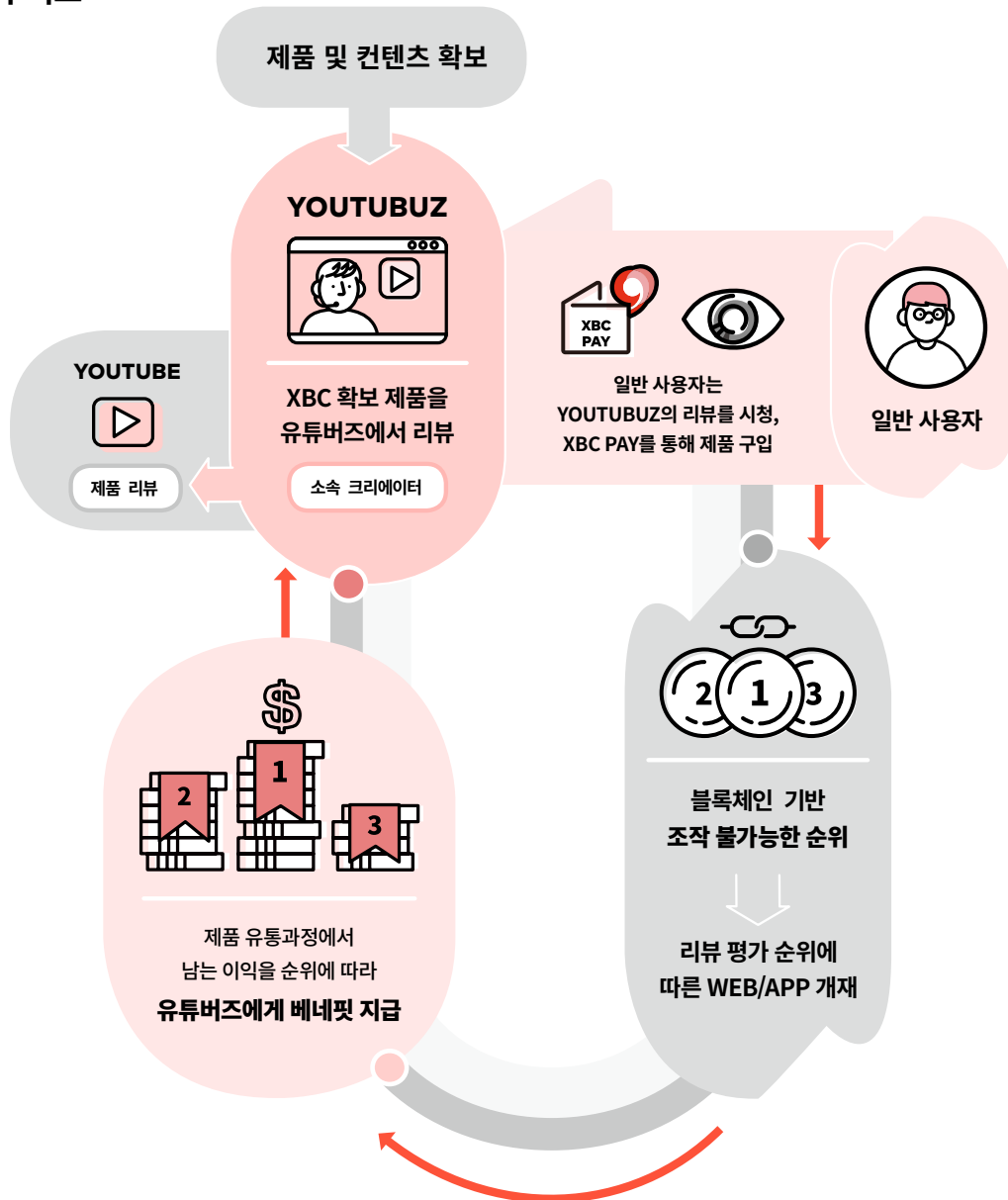
상시 근로자 없이 24시간 정상 운영





XBC 플레이 스토어는 플레이 스토어 내 등록된 게임의 포인트 결제, 게임 아이템 등의 자유로운 거래를 지원합니다. 또한 XBC 플레이 스토어의 핵심 콘텐츠 중 하나인 XBC 메신저는 설치가 필요 없는 간편한 웹 메신저로서 다국어 번역 기능을 통하여 전 세계 사용자와 커뮤니케이션이 가능하며 XBC Pay와의 연동을 통하여 편리한 결제솔루션을 제공 합니다.

나아가 XBC 플레이 스토어는 디 센트럴라이징 상거래 플랫폼인 YOUTUBUZ와 연동됩니다.



YOUtubuZ Project는 실사용자와 리뷰어에게 수익을 돌려주는 디 센트럴라이징 상거래 플랫폼입니다. XBC에서 확보한 제품이나 콘텐츠를 YOUtubuZ들이 리뷰하게 되며, 사용자들은 해당 리뷰를 보고 투표하게 됩니다. 리뷰는 사용자들에게 신뢰도 높은 순으로 노출되며, 해당 제품은 XBC Pay를 통하여 구매 가능합니다.

YOUtubuZ 플랫폼 또한, XBC 블록체인 네트워크를 사용하여 투명성이 보장 됩니다. 수익 대부분을 리뷰어에게 돌려주는 YOUtubuZ의 환원 구조는, 각 분야 전문가들의 자발적 참여를 유도 하게 되며 통해 사용자들은 신뢰도 높은 리뷰를 제공받고 제품을 구매할 수 있게 됩니다.

스트리밍 플랫폼의 성장과 스타 크리에이터의 등장

대형 크리에이터가 등장하며 스트리밍 영상을 활용한 마케팅 시장이 성장하였으나 MCN의 영향력이 매우 저조해 새로운 마케팅 플랫폼의 필요성이 대두되고 있습니다.

전세계 대표 스트리밍 플랫폼, YOUTUBE

이용자들은 카카오톡, 네이버보다 유튜브를 더욱 많이 사용하고 있습니다.



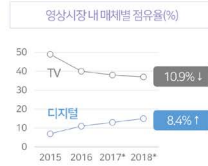
지속적인 스타 크리에이터의 등장

다양한 분야에서 수억대 매출을 가진 크리에이터가 탄생하고 있습니다.



디지털 영상광고 시장의 폭발적 성장

디지털 영상광고 점유율은 TV 대비 낮은 편이지만 점차 영향력을 높여나가고 있습니다.



... 광고주와 크리에이터, 소비자를 유기적으로 연결하는 진보된 마케팅 플랫폼의 필요성 증대 ...

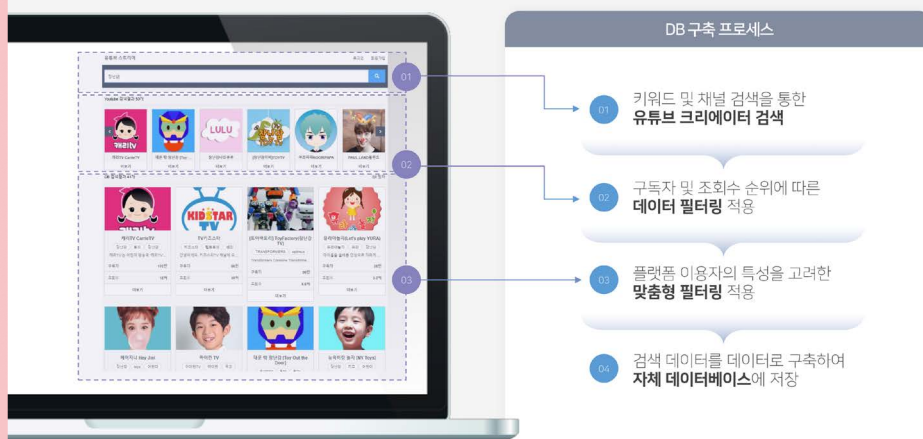
콘텐츠 마케팅 전문 브랜드, 유튜버즈

유튜버즈는 크리에이터의 발굴과 매니지먼트를 담당하는 MCN기업임과 동시에 콘텐츠를 통해 소비자와 상품을 연결하는 혁신적인 마케팅 플랫폼입니다.

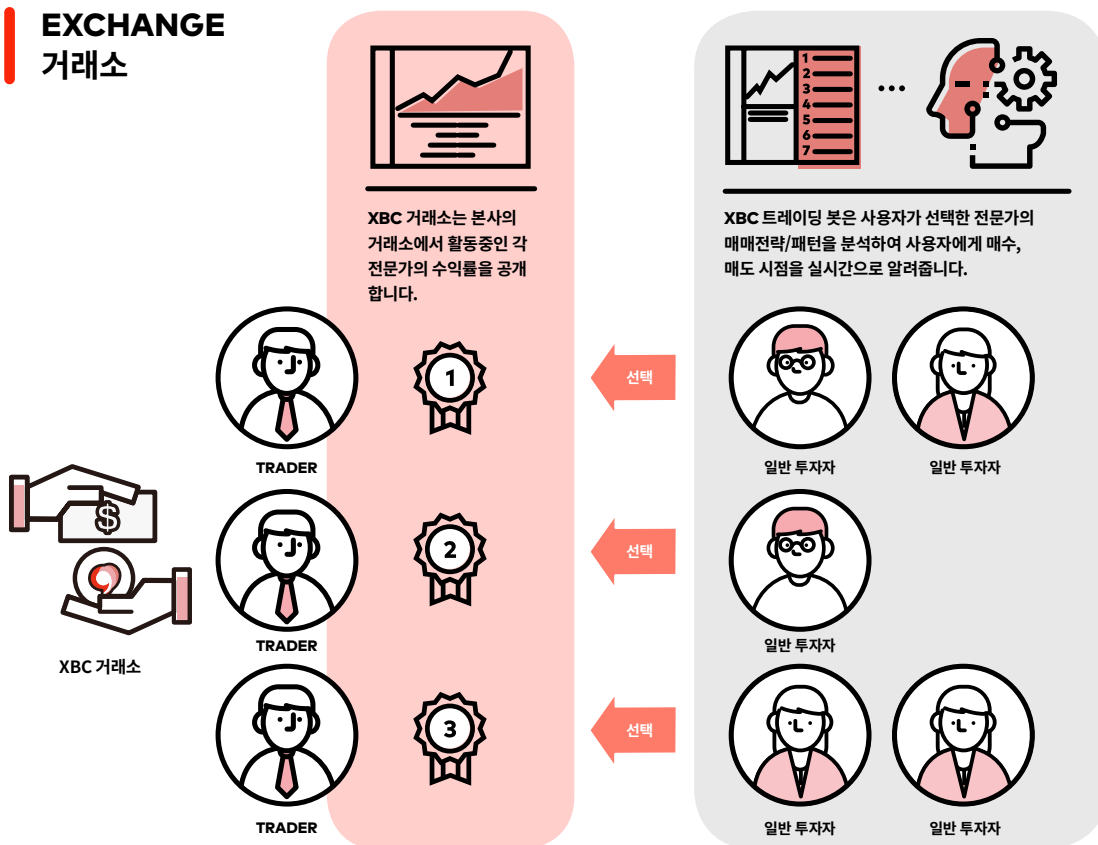


채널 및 키워드 검색을 통한 콘텐츠 DB 구축

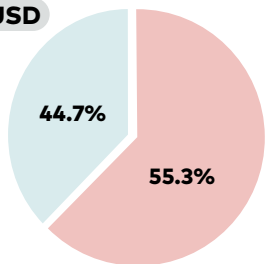
스트리밍 플랫폼 이용자들의 채널 및 키워드 검색 데이터를 수집하고 분석하여 자체 구축된 DB와 소비자의 특성에 맞게 필터링 절차를 거칩니다.



EXCHANGE 거래소



USD



USD Long USD Short

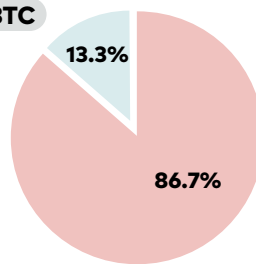
1시간 변동

LONG 23 ETH
SHORT -248 ETH

2시간 변동

LONG -121 ETH
SHORT 1031ETH

BTC



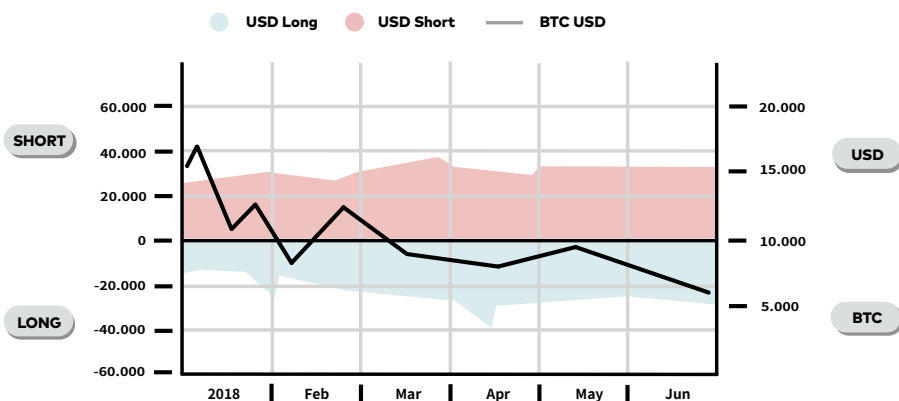
USD Long USD Short

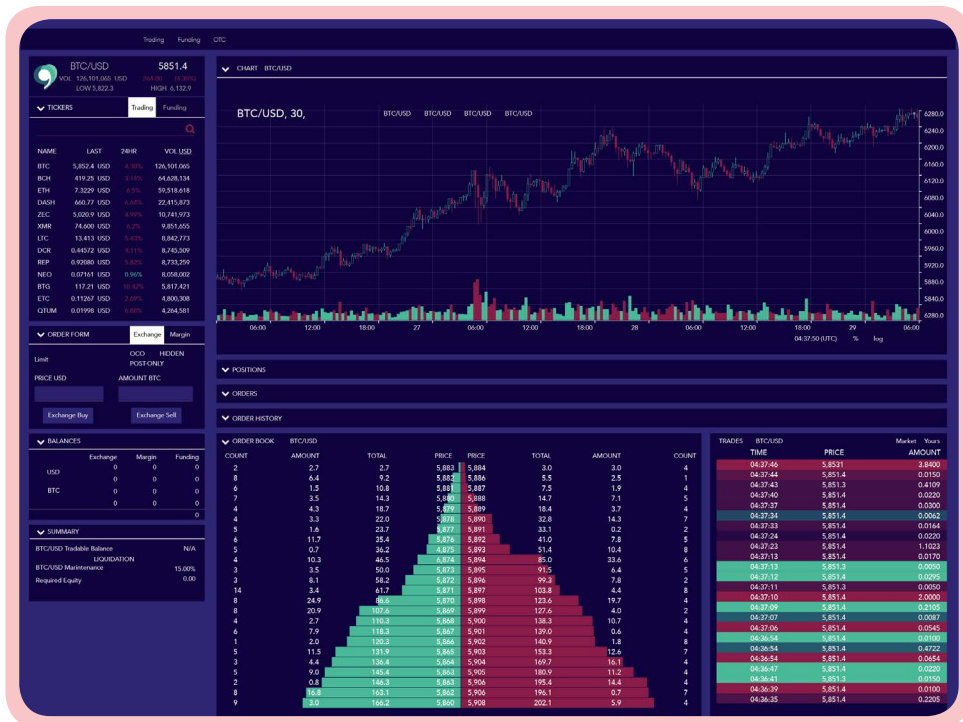
1시간 변동

LONG 79 ETH
SHORT -43 ETH

2시간 변동

LONG 85 ETH
SHORT -116 ETH





XBC 거래소는 본사의 거래소에서 활동 중인 전문가의 매도, 매수 전략을 그대로 이용할 수 있도록 각 전문가의 수익률을 공개할 예정이며, 사용자는 선택한 트레이더의 매도, 매수 전략을 활용해서 거래할 수 있습니다. 기존의 자동매매시스템의 문제를 극복하기 위하여, XBC 트레이딩 봇은 사용자가 선택한 전문가의 매매전략/패턴을 분석하여 사용자에게 적절한 매수, 매도 시점을 실시간으로 알려줍니다.

XBC 트레이딩 봇은 추세지표 비추세지표 (RSI, Bollinger Bands, Stochastic 등을 포함한 10개 이상의 보조지표)를 활용한 트레이딩 솔루션을 제공합니다. 나아가 알트코인의 가격변동은 일반적인 증권거래와는 다르게 BITCOIN의 시세와 직접적인 관계를 가지고 있기 때문에 XBC 봇은 실시간으로 cryptowat.ch의 거래소별 BITCOIN의 거래량과 변동 폭의 평균값을 계산하고, BITCOIN 과 알트코인들의 마진 비율을 실시간으로 업데이트합니다.

마진 거래란 매매대금의 일정 비율에 해당하는 증거금을 거래소나 증권회사에 예탁하고 필요한 자금 또는 주권을 차입하여 매매하는 거래방법으로, 증거금매수 (margin buying) 와 공매도(short selling)가 있습니다. 마진거래 비율을 XBC 트레이딩 봇의 알고리즘으로 책정하는 것은, 다수의 전문 트레이더들의 중요한 보조지표로 사용됩니다.





TECHNICAL ISSUES



Core Architecture

현재 사용되는 비트코인, 이더리움의 퍼블릭 네트워크는 다소 취약한 보안, 느린 트랜잭션 속도 문제로 기업이나 단체에서 쉽게 접근할 수 없습니다. 이 문제를 이해하고 해결하기 위해 리눅스 단체에서 Hyperledger Umbrella Foundation을 개설하였고 IBM에서는 Hyperledger Fabric 오픈소스 블록체인 기술을 공개하였습니다.

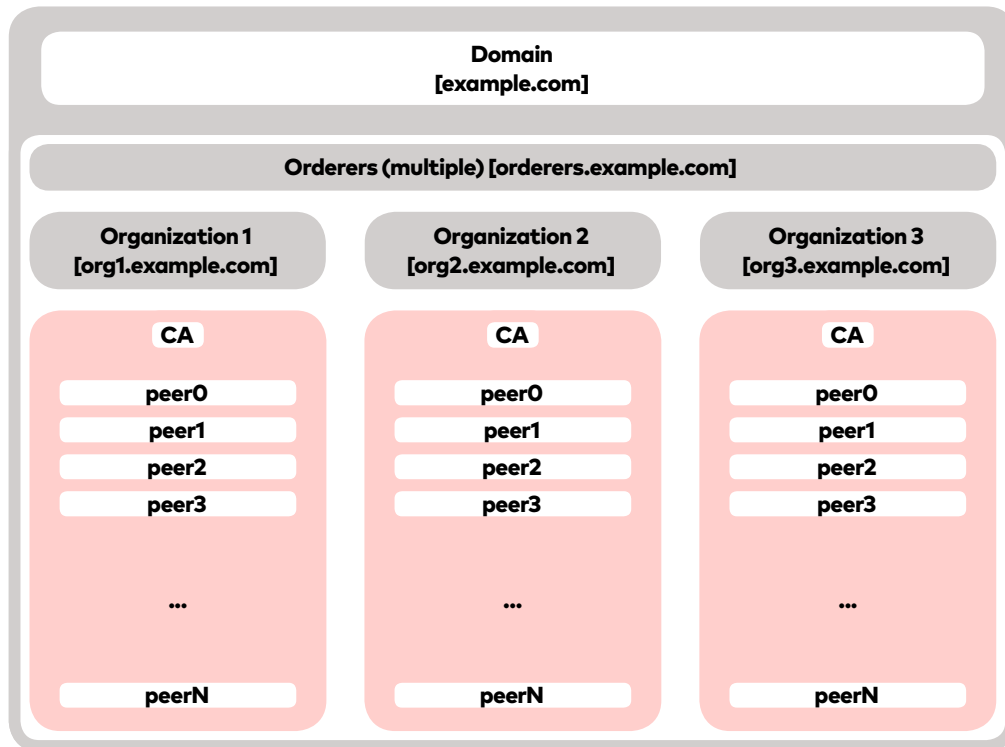
Fabric 블록체인은 산업용으로 개발된 블록체인이며 보안, Scalability, 트랜잭션 속도 면에서 뛰어난 성과를 보여주는 기술입니다. Fabric은 타 블록체인과 달리 permissioned 블록체인이며, 접속 권한은 POI (Proof Of Identity), 즉 실명제로 가입을 허가됩니다. 즉, 기존 P2P 퍼블릭 블록체인 방식을 벗어나지만, 기업에서 안전하고 빠른 블록체인 기술을 응용해서 사용할 수 있는 기술입니다.

XBC Project는 Fabric 프레임워크를 일부 활용하여 개발하였으며, XBC 만의 기술이 반영된 월렛과 페이 플랫폼을 제공합니다.



Domain

XBC 제품은 각 자신만의 도메인 명을 가지게 됩니다. 해당 도메인은 하나의 채널을 상징을 하며 모든 Hyperledger Fabric의 구성원을 포함한 프로젝트 단위로 운영 됩니다.



Orderers

모든 노드(peer)들을 관리하는 시스템입니다. 하나의 노드가 만약 트랜잭션을 일으킨다면 노드가 Proposal을 올리고 Orderers (Ordering Service)는 그 트랜잭션 정보를 올리고 모든 노드가 새로운 블록을 추가하고 업데이트 하는 일을 관리 해주는 역할을 합니다.

현재 XBC는 Kafka Cluster w/t Zookeeper Ordering Service를 도입할 예정입니다.

Organization 네트워크를 Organization 단위로 나누어 집니다. 각 Organization은 MSP 권한을 가지고 있으며 CA (Certificate Authority) 서비스를 가지고 있습니다. 즉 Organization은 노드 관리 뿐만 아니라 권한 부여, 트랜잭션 endorsement policy, 그리고 클라이언트들이 네트워크에 들어갈 수 있는 허브 시스템을 제공합니다.

XBC는 네트워크 아래에 있는 프로젝트 수에 맞춰 최적화된 Organization을 산입 합니다. 유저는 사용 XBC 제품에 따라 가입할 Organization 가 달라지지만 다른 Organization과 연결이 가능하며 서비스에 제한이 없습니다.

**CA
(Certificate
Authority)**

User Certificate을 유저와 노드들에게 제공해 주는 server-client 기술입니다. 클라이언트 요청이 허가 된다면 CA는 Certificate Public/Private 키를 제공하고 노드 정보를 서버 데이터베이스에 저장합니다. 각 Organization 당 CA 하나가 부여 됩니다.

XBC는 CA를 사용해서 유저 인증 시스템을 구축합니다. 회원 등록한 클라이언트 유저는 private 키를 가지게 되며, 키와 비밀번호를 가지고 있는 유저는 안전하게 XBC 서비스를 사용할 수 있습니다. 또한, CA 서버에 등록된 유저 정보는 블록체인 world state 데이터베이스에 등록이 되며, 인증정보는 회원의 허가 없이 바꿀 수 없습니다.



Peers

Peer는 네트워크의 상태를 유지하고 트랜잭션 proposal 올리는 역할 가지고 있습니다. 각 peer (노드) 는 최신 블록체인 데이터베이스를 가지고 있으며, 트랜잭션 업데이트와 블록이 추가 될 때마다 모든 노드는 그 데이터베이스를 새로 업데이트를 합니다. Peer는 크게 endorsing peer과 validating peer로 나뉘는데, endorsing peer는 트랜잭션에 인증 사인을 붙이는 것이며, endorsing policy에따라 endorsing peer의 권한이 필요한 트랜잭션이 달라집니다.

Validating peer는 블록 생성과 트랜잭션 정보를 validate, 즉 인정 해주는 역할을 가지고 있으며, endorsement policy를 충족하면 바로 state database를 업데이트를 합니다.

endorsing peer, validating peer 는 매우 안전하게 관리되며, XBC 제품에 가입한 고객은 validating peer 권한 아래로 활동을 하고, 각 제품마다 트랜잭션을 허가하는 endorsing peer이 존재할 것입니다. XBC의 제품에 따라 endorsing policy가 구성되며 . Endorsing policy에 따라 latency가 달라지기 때문에 XBC에서 특별히 관리 합니다.

Consensus

현재 퍼블릭 블록체인에서의 Consensus의 정의는 POW, POS, 등의 알고리즘을 사용하여 퍼블릭 블록체인 네트워크를 인증하는 하나의 블록 생성/인증 알고리즘을 뜻합니다.

하지만, Hyperledger Fabric의 경우 Consensus는 단순 트랜잭션 순서를 정하는 시스템이 아니라 전체 트랜잭션 진행 방식을 뜻합니다. Transaction proposal, endorsement, ordering 까지 모든 트랜잭션 순서를 Fabric의 Consensus Policy로 부를 수 있습니다.



**Hyperledgers
Fabric
Transaction
Process**

클라이언트 Peer가 트랜잭션 Proposal을 올립니다. Endorsing Node가 Proposal을 미리 실행하고 문제 있으면 에러값을 반환, 문제없으면 인증 사인을 붙이고 다시 validating node에게 돌려보냅니다.

만약 Query (정보 확인) 명령이라면 바로 값을 돌려 드립니다. 트랜잭션 신청 명령일 경우 endorsement signature가 부여된 체인 코드를 찍어 Ordering Service (Kafka 서비스)로 보내서 트랜잭션을 정리해서 새로 생성된 블록에 추가합니다. Ordering Service는 체인 코드 읽을 필요 없이 endorsement 사인만 확인하고 바로 블록 생성하여 추가할 수 있기 때문에 트랜잭션 일일이 확인하고 블록에 추가하는 퍼블릭 블록체인보다 속도가 월등합니다. 다시 새로 업데이트된 블록체인 상태를 validating peer (committing peer) 들에게 전달하여 endorsement policy 다시 확인하여 노드마다 state database를 업데이트합니다. 모든 노드들이 업데이트 완료 후 이벤트를 돌려주며, 클라이언트는 이벤트 정보를 확인할 수 있습니다.

이더리움, 비트코인, 등 다른 블록체인과의 가장 큰 차이점은 블록에 추가하기 전에 먼저 체인코드 (스마트 콘트랙트)를 실행하고 보안, 인증 절차가 문제없이 진행되는지 확인한 다음에 ordering service에게 올립니다. 당연히 문제가 생기면 에러값을 반환하고 atomic 형식이기 때문에 블록체인 영향이 없고, 그리고 체인코드 상 보안, 논리 문제가 있어도 블록체인과 분리가 되어 행동을 하기 때문에 불량 체인코드로 인한 네트워크 피해를 보지 않습니다.

XBC 제품은 Hyperledger Fabric 속도, 보안, 그리고 트랜잭션 설계를 사용하여 유저가 걱정 없는 간편결제, 게임 포인트, 등 유료 서비스를 이용할 수 있도록 개발합니다. 사용자의 계정은 블록체인에 안전하게 보관이 되고 있으며, 불량 입력이나 스마트 콘트랙트가 있더라도 계정에 아무런 영향을 미치지 않습니다.



Database

Hyperledger Fabric 모든 피어 노드는 World State 데이터베이스 최신 버전을 가지고 있습니다. 이 데이터베이스가 가진 역할은 현재 네트워크 상태를 알려주고 권한 설정에 따라 읽기/쓰기 명령을 실행합니다. 데이터베이스 읽기/쓰기 작업은 체인코드로 이루어지게 되며 새로 업데이트 된 데이터베이스는 새로 생성된 블록에 저장 되어 모든 피어 노드에게 전달 됩니다. 모든 노드가 새로운 트랜잭션 블록을 인정하면 그 블록이 추가를 하고, 블록 안에 데이터베이스 상태가 현재 네트워크의 최신 상태를 의미합니다.

데이터베이스 읽기/쓰기 체인코드 작업 (Query/Invoke)은 차이점이 있습니다. Query를 할 경우 데이터베이스의 현 상태 정보를 불러서 읽기 때문에 트랜잭션, 즉 블록을 생성할 필요 없고 Organization 허락하에 바로 정보를 부를 수 있습니다. 즉, 거래 정보나 현재 유저의 토큰 수를 확인하는 것은 실제 트랜잭션보다 빠르고, 유저는 바로 그 정보를 확인 할 수 있습니다. Invoke을 할 경우 어떤 작업이든 데이터베이스 상태를 바꾸는 것이기 때문에 트랜잭션으로 분류를 하고, 블록을 생성하여 Ordering Service을 통해 모든 피어 노드에게 전달이 됩니다. 이로 인하여 latency 문제가 생기는데 Hyperledger는 Scalability가 뛰어나 Invoke 작업도 시간당 100만 트랜잭션을 유지할 수 있습니다.

XBC는 CouchDB를 사용하여 네트워크에 반영합니다. CouchDB document model는 rich query를 허락하여 보다 효율적인 쿼리 쿨을 할 수 있고 API 편한 사용을 고려하여 선택 했습니다. Hyperledger CouchDB 네트워크와 같이 연동을 하여 모든 제품 비즈니스 논리에 반영하여 유저 트랜잭션 정보를 저장할 것입니다.



Smart Contracts

Hyperledger Fabric 비즈니스 논리, 즉 state database에 읽기/쓰기 명령을 보내고 실행하는 코드를 체인코드라고 부릅니다. 체인코드는 블록체인과 docker로 분리되어 실행되며, 클라이언트 요청으로 코드를 불러 비즈니스 논리를 실행합니다.

클라이언트의 API 요청으로 읽기 (Query) 체인코드를 실행할 경우 피어 노드의 권한으로 현재 데이터베이스 상태의 정보를 확인합니다. 트랜잭션이 일어나지 않기 때문에 ordering 서비스 단계를 거칠 필요가 없으며 노드가 현재 상태를 계속 유지하기 때문에 언제나 데이터를 확인할 수 있습니다. 단, CA 유저 권한으로 인해 본인 계정에 있는 정보만 확인할 수 있습니다.

체인코드 트랜잭션 실행 (Invoke)의 경우 데이터 확인하는 것 외 모든 비즈니스 논리를 실행하는 명령어를 의미합니다. 입금, 출금, 거래, 경매, 등 블록체인이 처리 해야 할 기능들은 ordering 서비스를 거쳐 블록에 추가되어 데이터베이스를 업데이트합니다. 그로 인하여 피어 노드 권한뿐만 아니라 해당 Organization 권한을 받고 트랜잭션을 실행할 수 있습니다. Validating Peer, Endorsing peer들 인증 절차를 통과한 트랜잭션은 이벤트 형식으로 데이터 반환되어 유저는 거래내역을 확인할 수 있습니다.



Query Chaincode

피어 노드가 가지는 현 블록체인 데이터베이스 상태 확인
사용자 정보를 확인 할 수 있음

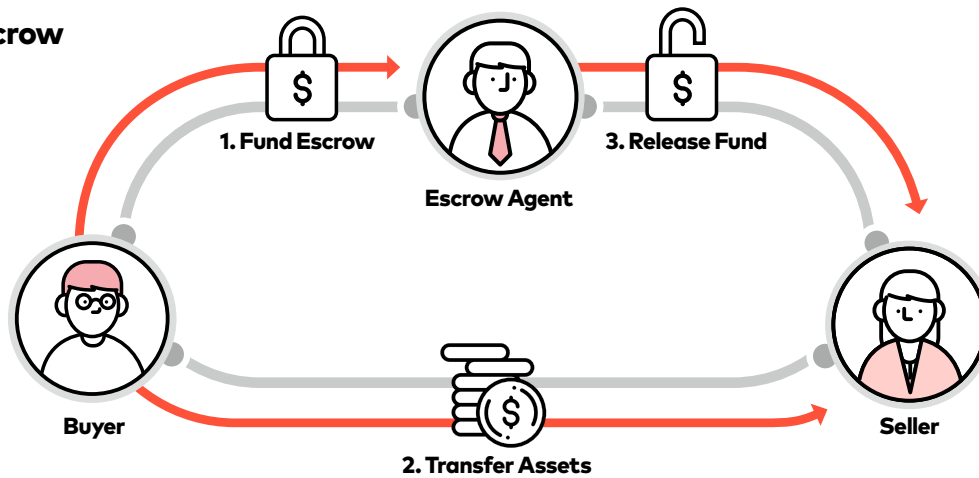
CA 서버에 등록 된 사용자는 키를 확인하고 계정 정보를 불러 줌
사용자는 계정 정보, 트랜잭션 기록, 네트워크 상태, 등 확인이
가능하지만 트랜잭션 개인 정보 확인은 2차 인증이 필요

Invoke Chaincode

모든 트랜잭션 기능 실행
피어 노드, Organization 노드, 그리고 CA 서버 등록 인증 절차를
거쳐야 실행 가능 Sanity Checks, Ordering 서비스, Endorsement
Policy 통과 해야만 데이터베이스 업데이트 가능 업데이트 된
데이터베이스는 Ordering 서비스를 통해 모든 노드들에게 전달
인증 확인 된 트랜잭션 블록은 모든 노드들이 추가를 하고 그 블록이
현 블록체인 데이터베이스 상태로 지정
이벤트로 트랜잭션 결과를 반환



XBC Escrow



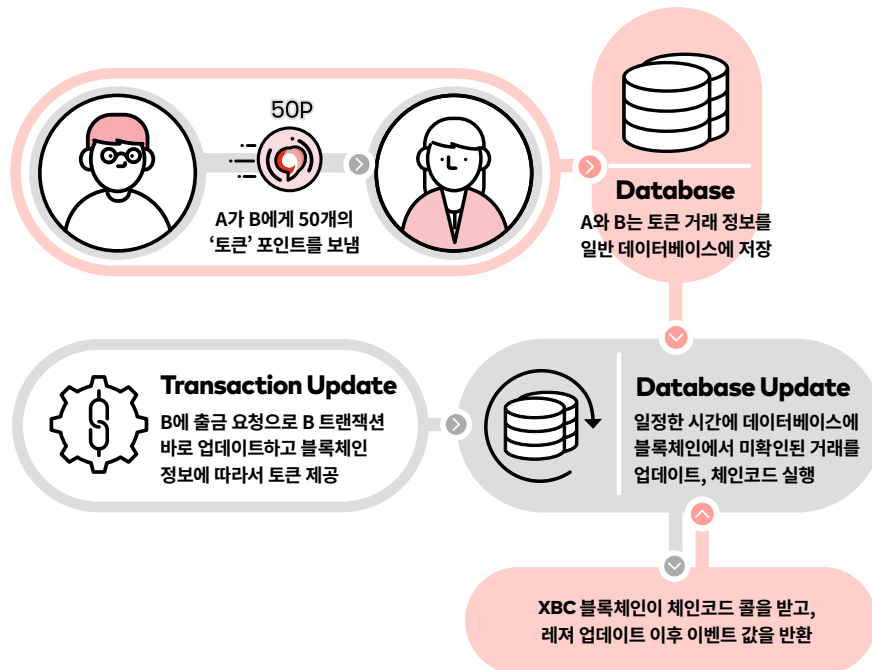
E-commerce 서비스를 이용할 경우 물건 거래를 할 때 제 3자 계약을 통해 거래가 이루어집니다. 에스크로는 돈을 받은 다음에 물건을 받는 조건으로 판매자에게 액수에 맞는 돈을 지불합니다.

만약, 판매자가 물건을 내주지 않거나 다른 물건을 보낼 경우 트랜잭션은 무효처리가 되며, 돈은 다시 클라이언트에게 돌려집니다. XBC Pay Platform뿐만 아니라 토큰으로 실거래를 할 시 에스크로 컨트랙트로 진행됩니다. Hyperledger Consensus가 블록에 추가하기 전에 먼저 실행을 시도하기 때문에 보다 빠르고 안전하게 트랜잭션을 진행하는 에스크로 체인코드를 개발 하였습니다.

XBC Lightning Network

현재 Hyperledger Fabric 네트워크 많은 양의 트랜잭션을 거의 실시간으로 처리할 수 있는 장점을 가지고 있습니다. 하지만, 네트워크 사용자가 늘고 트랜잭션 요청이 많아질수록 결코 latency, 접속 속도 충돌로 인한 네트워크 속도 저하를 경험을 할 수 있습니다. 이 문제를 해결하기 위해 XBC 는 자체 Lightning Network을 개발하였고 현재 특허등록 진행 중에 있습니다.

유저의 요청 시 마다 때마다 체인코드를 실행하는 것이 아닌 먼저 제품 노드의 인증을 받고 일반 데이터베이스에 저장 후 일정 기간을 지나면 업데이트하는 방식을 사용합니다. 업데이트 체인코드 반영 시 많은 양의 트랜잭션을 한꺼번에 올릴 수 있으며, 업데이트 시간 외에는 latency 문제없이 트랜잭션을 실행할 수 있습니다. XBC Lightning Network는 사용자의 네트워크 환경에 따라 신용카드 수준의 실시간 거래를 가능하게 합니다.



왜 Hyperledger인가?

- Hyperledger는 리눅스 재단에서 운영하며 IBM, SAP에서 지원합니다. 시간당 360만건 수준의 빠른 트랜잭션 처리가 가능하며 XBC Pay에 특화되어 있습니다.
- Hyperledger는 인증을 통한 블록체인이며, 추가 채널 기능을 통하여 데이터 안전성과 신뢰성을 높이고 있습니다.
- 산업적인 혹은 컨소시엄기반의 노드들은 공공의 채굴이 없이 필요 노드들을 정하여시스템을 구성할 수 있어야 합니다.
- 모듈화된 방식으로 구성해서 쉽게 기능을 늘려갈 수 있습니다.

Hyperledger 제한점

Hyperledger는 Scalability, 그리고 보다 빠른 트랜잭션을 자랑하면서 기업들이 안전하고 빠르게 블록체인 기술을 사용할 수 있도록 구성되어 있습니다. 하지만, permissioned 블록체인이기 때문에 일반 유저가 쉽게 접근해서 사용하기에는 권한, 인증 절차에 어려움을 겪을 수 있습니다. CA, 트랜잭션 endorsement policy, 등 보안상 필요한 절차는 기업들이 필요하고 쓸 수 있지만 빠르고 간편하게 제품을 즐기고 싶은 사용자에게 다소 불편함을 호소 할 수 있습니다.

일반 유저가 저희 모든 블록체인 제품을 편하게 사용하려면 XBC는 퍼블릭 블록체인도 반영해야 한다고 생각합니다. 퍼블릭 블록체인 장점은 누구나 가입을 할 수 있고 그 네트워크가 제공하는 서비스를 쉽게 사용할 수 있습니다. 단, Hyperledger Fabric와 다르게 채굴 시스템, 즉 POW와 같은 채굴 Consensus을 사용하기 때문에 트랜잭션 속도와 비교적 느릴 수 있습니다. 하지만, distributed network의 장점을 가지고 있는 보안을 즐기면서 애플리케이션을 사용할 수 있고, 게임, 엔터테인먼트 같은 제품은 유저 편리성을 우선이기 때문에 퍼블릭 블록체인이 적합하다고 봅니다.



What is Ethereum?

이더리움 블록체인은 비트코인 다음으로 제일 많은 거래량을 자랑하는 애플리케이션 개발이 가능한 블록체인 플랫폼입니다. 비트코인이 가지고 있는 POW 채굴 방식과 네트워크 안정성을 자랑하면서 가스값만 내면 쉽게 Decentralized Application, 즉 DAPP을 개발하여 블록체인 기술을 사용하는 웹/앱 제품을 만들 수 있습니다.

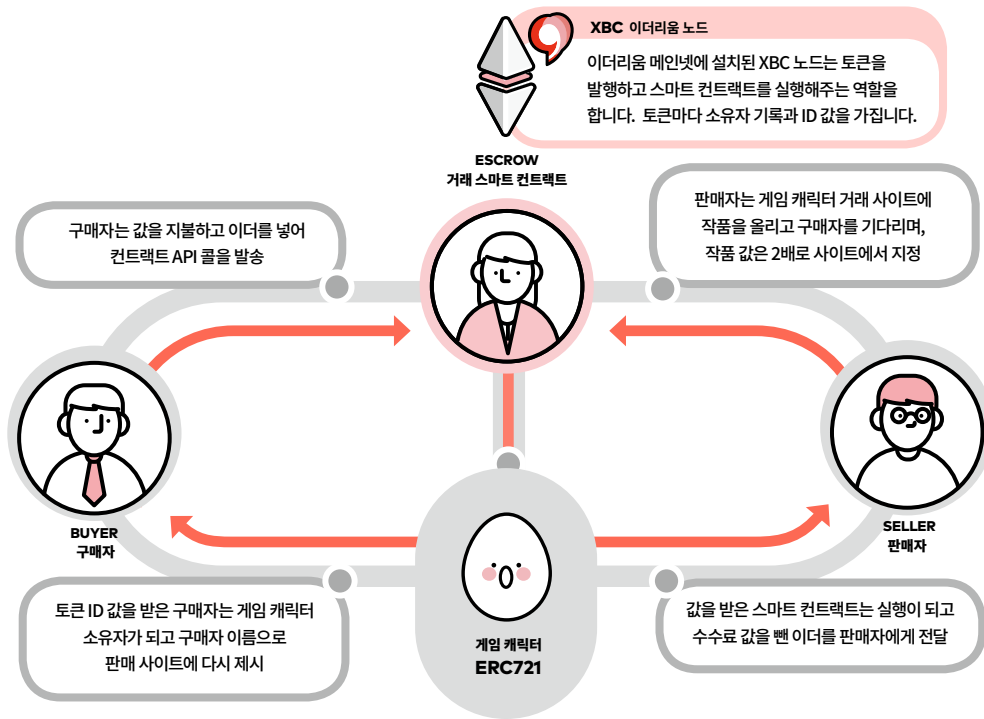
현재 이더리움 메인 넷의 경우 트랜잭션 속도를 평균 초당 10개의 트랜잭션이 실행됩니다. 블록 생성 속도는 평균 20초입니다. XBC는 메인 넷 사용을 할 예정이고 AWS 서버 인스턴스에 제품 서버와 네트워크 클라이언트 노드를 구성해 이더리움 네트워크와 연동할 계획입니다.

비교적 느린 블록생성 속도와 트랜잭션 속도를 해결하기 위해 XBC는 이더리움 기반 제품을 똑같은 lightning network 방식을 사용할 계획입니다. 스마트 계약을 개발하여 많은 양의 거래 액수를 데이터베이스에 저장하여 일정한 시간이 지나면 보다 많은 양의 가스 값을 지불하여 업데이트를 진행하는 방법을 현재 검토 중입니다.

Game Platform

CRYPTO MODERN ART는 자체 게임 개발하여 XBC 토큰을 사용하는 웹 게임을 개발하였습니다. 캐릭터를 사고 거래할 수 있는 트레이딩 시스템을 구축하여 다소 접근하기 어려웠던 블록체인 기술의 접근성을 높여나갈 계획입니다. XBC 거래 토큰은 ERC 721 토큰 기준으로 구성되어 있으며, 각 캐릭터별 하나의 토큰을 부여하여 unique한 ID 값이 부여됩니다. 캐릭터가 값을 사용해 거래 정보, 과거 트랜잭션 이력 등 정보를 불러 더 많이 거래할 수록 그 캐릭터 가치를 올리는 시스템을 구축합니다.





- **유저 등록** — 유저는 Metamask 계정으로 XBC 게임에 등록
- **캐릭터** — ERC 721 토큰 하나를 부여 받고 특유의 ID 값을 가집니다.
사용자는 여러 개의 캐릭터를 가질 수 있습니다.
- **거래** — 유저는 원하는 캐릭터 있다면 거래 신청이 가능하며 값은
현 가격의 2배를 지불하여 캐릭터를 삽니다.
- **판매** — 캐릭터는 자동으로 게임에 판매를 하게 되며, 다른 유저가 작품을
살 경우 거래 신청은 판매자에게 이벤트로 보내집니다. 판매자는
판매를 거부할 수 있는 권한을 가집니다.
- **경매** — 판매자는 또한 작품을 경매 페이지에 올릴 수 있습니다. 시간과
초기 금액을 설정한 다음에 경매 페이지에 올려 작품을 판매할 수
있습니다. 작품에 따라 가격이 몇 배 오를 수 있습니다.

게임 보안

게임이 해킹 되거나 사이트가 다운이 될 경우 유저들은 현재 가지고 있는 토큰과 그 토큰 값을 그대로 받을 수 있습니다. 블록체인에 저장되는 ID 값과 거래 기록을 확인할 수 있기 때문에 서버 문제와 해킹으로 인한 실제 이더와 토큰 손실은 없습니다.

그 외 네트워크 보안은 이더리움 블록체인 네트워크 사용해서 맞는 보안 정책과 스마트 컨트랙트 보안(ex: double spending)을 대비하고 있습니다.



XBC Hyperledger Token과 Ethereum Token 교환 시스템

XBC 아래 모든 제품은 하나의 큰 네트워크 아래에 구성할 계획입니다. 트랜잭션 속도가 필요한 Pay Platform과 XBC 월렛, 유저 편리성과 접근성이 필요한 XBC 게임과 Playstore는 각 다른 기반의 블록체인 플랫폼으로 구성 됩니다.

이더리움 토큰을 가지고 있는 유저가 XBC Hyperledger 토큰을 교환하고자 하는 경우 또는 Pay Platform이나 월렛 기능을 사용하고자 할 경우를 고려하여, 일정 트래픽에 도달하게될 경우 Hyperledger와 Ethereum 토큰 서로 교환할 수 있는 시스템이 가동됩니다. XBC Exchange는 실시간으로 시장 가격, 거래 활동 등 양쪽 프레임워크를 모니터링을 통한 일정한 비율로 교환 서비스를 제공합니다.

블록체인과 XBC PAY

블록체인기반의 코인은 코인구매수요와 공급물량에 따라 상대적으로 주식시장에 비하여 높은 가격 변동률을 가집니다. 반면 테더화 되어 고정된 통화가치로서 작용할 수 있는 XBC Pay의 포인트는 현금과 1대1로 매칭해서 구매하거나, 지불/송금등에 쓰일 수 있고, 포인트 구매의 변동요인이 없습니다. 포인트는 XBC Pay App을 통하여 XBC 코인과 교환할 수 있습니다. XBC Pay App 에서는 포인트와 1:1 교환을 위한 Hyperledger 기반 코인을 사용합니다. 코인은 ERC 20 형태로 운용됩니다. XBC Pay App와 연계된 게임에서 구매를 위한 토큰은 ERC 20 기준의 토큰 입니다. XBC 게임에서 사용되는 아이템은 ERC 721시스템을 통하여 거래되며, 아이템을 구매하거나 판매할때에는 Hyperledger 기반코인으로 거래할 수 있습니다. 전체 시스템에서는 Ethereum 기반의 코인과 Hyperledger 코인을 같이 사용할 수 있으며 거래소를 통하여 다른 코인으로 변경 가능하고, 코인을 구매하거나 판매할 수 있습니다.



- 포인트 혜택 포인트 사용처 포인트는 대중교통이나 프렌차이즈 등에서 현금처럼 1대1의 가치로 교환가능한 시스템을 구축 중입니다.

거래소 상장을 통한 수익의 발생시, 같은 기간동안 포인트를 사용한 유저에 대해 포인트 사용에 해당하는 비율의 수익분을 나누어 주어서 포인트에 대한 사용기회를 늘리고, 포인트 사용을 장려하도록 합니다. XBC 코인을 통한 구매시, 포인트 구매에 사용한 코인의 가치가 오를수록 가치증가에 대한 이익을 코인으로 사용자에게 분배함으로써 추가 혜택을 드립니다. 시스템에서 코인의 가치가 올라가면서 생기는 차액은 주기적으로 그 가치를 평가하여 그중 일정비율은 자사 블록체인을 매입하고, 그 나머지의 수익은 코인의 수익계산기간에 대한 포인트 사용량을 계산하여 비율대로 각 포인트 사용자에게 나누어 줍니다.

코인의 가치변경분에 대한 계산은 일주일 단위로 갱신하고, 기간은 변경 가능합니다. 포인트 사용자에게 나누어 주는 방법은 각 포인트 사용자들이 포인트 구매에 사용한 지갑에 추가적으로 코인 또는 포인트를 적립하는 방식이며, 수익에 대한 배분은 포인트 보유수량과 함께 포인트의 사용량에 따라 나누어 주도록 하여 포인트 사용을 장려하고, 궁극적으로는 포인트와 코인의 거래를 촉진해서 가치를 올릴수 있도록 합니다. 포인트와 코인의 사용이 늘어나면서 XBC의 시가총액이 상승하게 되면 다시 포인트와 코인의 수익을 만들어내어 포인트와 코인기반의 지불/결제시스템에서 선순환이 이루어 질 수 있도록 유도합니다.

코인을 통한 수익이 없이 코인의 가치가 하락한다면, 사용한 포인트의 비율에 맞추어 할인된 가격으로 코인을 살 수 있도록합니다. 이로써 코인의 수요를 늘리면서 전체적인 포인트 사용량을 확장해 나갈 수 있습니다. 코인의 유통과 함께 코인의 가치는 올라가거나 내려갈 수 있습니다. 하지만, 코인의 가치가 오르면서 인플레이션이 유발되거나 혹은 코인의 가치가 하락할 수 있는데, 안정적인 코인의 가치를



유지하면서 코인을 보유하거나 코인의 사용자를 확보하기 위하여, 코인
혹은 포인트를 사용하거나 보유하고 있는사람들에게 코인의 가치상승에
대한 내용중 일부분을 다시 포인트관련 소유자 혹은 사용자들에게
포인트의 소유분이나 사용량에 따라서 코인을 지급합니다.

- 지급주기는 코인의 가격확인주기이며, 지급방법은 코인 초과이익분을
분배상수(C)로 곱해서 나오는 코인의 양을 각각의 사용자들에게
포인트 보유량과 포인트 사용량의 합에 비례해서 나누어 주도록
합니다.
- 코인의 초과이익분이나 하락의 양은 가격 변화량을 전체 코인 양으로
곱한 값으로 합니다.
- 분배상수는 예측할 수 없는 코인의 가치를 가장 잘 반영하기 위해서,
중간값인 0.5로 설정을 하고, 이후에는 거래량 대비 코인의 가치변동을
확인하고, 과거 데이터를 기반으로 분배 상수를 갱신하면서 코인의
가격변동을 막는 기준이 될수 있도록 데이터를 분석하고, 상수를
정할 수 있게 합니다.
- 개인별 코인 분배량 = 분배상수(C) x 코인의 갯수로 환산된 코인 가치
증가분 x (개인의 코인 보유량+ 개인의 코인 사용량) / (전체 코인
보유량 + 전체 코인 거래량)
- 개인별 코인 분배량 = 분배상수(C) 코인의 갯수로 환산된 코인 가치
증가분 (개인의 코인 보유량 + 개인의 코인 사용량) (전체 코인 보유량
+ 전체 코인 거래량)
- 코인 구매 할인가격 = 분배상수(C) x 코인의 갯수로 환산된 코인 가치
하락분 x (개인의 코인 보유량 + 개인의 코인 사용량) / (전체 코인
보유량 + 전체 코인 거래량)



- 코인 구매 할인가격 = 분배상수(C) 코인의 갯수로 환산된 코인 가치 하락분 (개인의 코인 보유량 + 개인의 코인 사용량) (전체 코인 보유량 + 전체 코인 거래량)

XBC 코인의 상장이후 가치상승과 가치하락에 대한 데이터를 기반으로, 적절한 분배계수를 찾는 것이 중요하며, 지속적으로 거래를 모니터링하여 코인과 포인트 사용내역 및 보유량에 맞춘 보상을 지급합니다.

코인의 가치변화에 대한 정보는 일차적으로 각 사용자의 코인 보유량과 사용량을 계산하고, 분배상수를 정의합니다. 이후에는 분배상수를 정의하기 위해서 SNS에서 회자되는 코인관련 뉴스를 파악하고 긍정적인지 부정적인지 판단해서 각각의 뉴스에서 나오는 값의 평균 혹은 중앙값으로 구하면 그 값을 분배계수로 사용할 수 있을 것으로 생각됩니다. 코인관련 뉴스를 파악하거나 뉴스의 내용을 파악하는 것은 뉴스에서 가지고 있는 단어가 긍정적인지 부정적인지 판단해서 코인의 가치변화를 예측할만한 정량적인 예측값을 뽑게 되고, 이를 분배계수에 반영합니다. 게임을 통한 포인트 생성 및 코인전환 XBC Playstore와 연동된 게임을 통하여 포인트를 생성 할 수 있으며, 게임유저가 사용하는 포인트 지급과 연동됩니다.

XBC 게임에서의 포인트 변환은 게임마다 다르게 적용되어 계산될 수 있습니다. 게임마다 게임에서의 경험치를 변환하거나, 물리친 적의 수, 클리어한 게임 수, 1등 한 횟수 등 각각 다른 전환계수를 가지고 포인트로 변경되게 됩니다. XBC 게임에서의 포인트가 실제로 사용 가능한 포인트와 같은 것이며, 게임에서 유래한 포인트를 통해서 코인을 구매할 수 있습니다. 따라서 게임을 통해서 포인트를 구해서 코인으로 바꾸어서 거래소에서 이용할 수 있습니다.



게임을 통해서 생겨난 포인트에 대한 혜택역시 사용한 만큼 정산하여 혜택을 받을 수 있습니다.

게임사용자가 가지고 있는 포인트는 게임내에서 구매할 수 있는 각종 현금성 아이템을 사는데 사용될 수 있으며, 게임아이템을 구매한 이후에는 다시 포인트로 전환 할 수는 없습니다.

XBC 외 타 거래소에서 거래되는 코인을 이용해서 포인트를 구매할 경우, 거래소에서 거래되는 가격에 따라 포인트를 지급하게 됩니다. 비트코인을 포함한 알트코인을 보유한 유저는 쉽게 포인트를 구매할 수 있습니다. 반대로 포인트를 가지고 있으면 코인으로 변환하여 구매할 수 있습니다. 이 경우에 코인의 시세에 따른 환율이 적용되어 실제적으로 전자지갑으로 송금되는 코인은 고정적이지 않습니다. XBC 포인트 거래를 위한 XBC 거래소에서 포인트와 현금, 포인트와 코인의 거래를 할 수 있도록 하고, API를 통해서 특정 사용자가 다른 사용자에게 포인트를 전송하는 것을 가능하게 하며, PG 형태로 타 웹사이트나 쇼핑몰에서도 사용할 수 있도록 합니다.



XBC Pay Platform

현재의 간편 결제/송금 시장은 매년 지속적으로 성장하고 있다. 한국은행 2017년 전자지급서비스 이용현황에 따르면 간편결제/송금 서비스 이용 실적은 일평균 281만건, 1,023억원으로 전년(2016년) 대비 각각 189.1%, 212.0% 증가하였다. 간편결제/송금 시스템은 기존 시스템의 절차를 대폭 간소화하여 편의성을 제공하기 때문이다.

한계

카드사, PG시스템, 간편결제 시스템 등 연관된 시스템이 많고 각 시스템마다 유지비용과 이용료가 발생하기 때문에 발생하는 비용(운영비, 수수료)이 높다. 이로 인해 영세사업자들에게 부담이 가중되고 있다. 중앙집중식 시스템의 한계로 보안에 대한 비용이 높으며, 서비스 회사에 문제(다운타임, 파산 등)가 발생했을 경우 이용자들에게 손실 위험이 있다.

블록체인 기반 결제 시스템

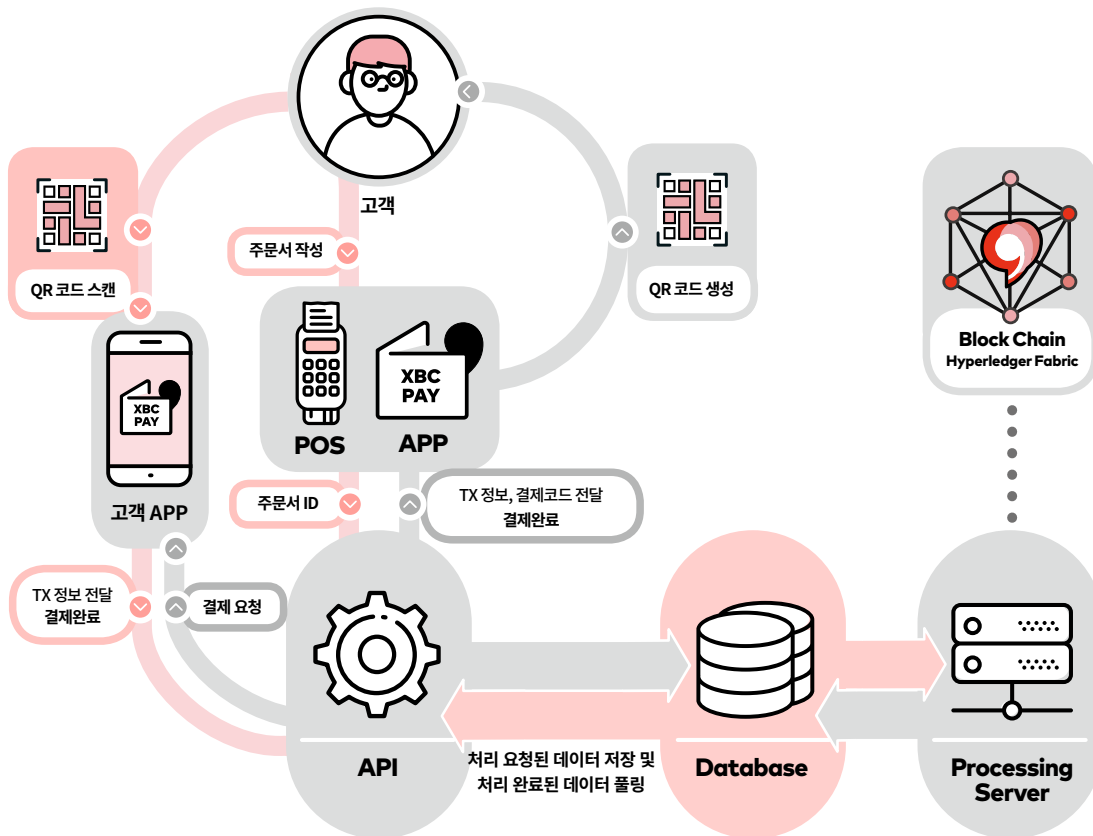
- 편리성 기존 간편결제 시스템과 동일한 수준의 절차로 편리하게 (QR코드, E-Mail, 전화번호 등을 이용하여) 간편하게 결제/송금할 수 있다. 가맹점에게는 불필요한 정산주기를 제거하여 신속한 정산이 이루어질 수 있다.
- 포인트제도 암호화폐 가치 변동에 따른 혼란을 방지하기 위해 실생활과 밀접한 관련이 있는 분야는 포인트를 이용하여 결제할 수 있다. 포인트와 암호화폐는 환전할 수 있다. 암호화폐 가치 상승 시 포인트를 소유하고 있는 사용자에게 Benefit을 제공한다.
- 저비용 블록체인 네트워크를 활용하여 기존 간편결제 시스템 대비 연관된 시스템(회사)을 간소화 하여 낮은 비용으로 운영할 수 있으며, 없거나 낮은 수수료로 이용할 수 있다.



- 안전성 체인코드(스마트컨트랙트)를 이용하여 더 안전한
에스크로 서비스를 구현할 수 있다. 판매자가 구매자에게
물건을 전달하지 않거나, 다른 물건을 전달하였을 경우
해당 거래는 무효화 되며 금액은 다시 구매자에게
전달된다. 그리고 에스크로 수수료도 발생하지 않는다.
모든 거래에 인증 절차를 거치기 때문에 부정적인 거래를
차단할 수 있다.
- 유연성 가상화폐로 운영되어 국적에 관계없는 거래가 가능하다.
체인코드(스마트컨트랙트)를 이용하여 인간이 상상할 수
있는 모든 종류의 거래에 알맞는 결제 서비스를 구현할 수
있다.
- 처리속도 Hyperledger Fabric를 이용하여 시간당 360만건
트랜잭션 처리 가능하다.
- 베네핏 서비스되는 화폐의 가치가 상승할 경우 이용자에게
베네핏을 제공할 수 있다.
- 고가용성 Docker를 활용한 다운타임 없는 고가용성 시스템을
운영할 계획이다.
- 크로스플랫폼 Android, IOS 모두 서비스할 계획이다.
POS 솔루션과 연계할 계획이다.



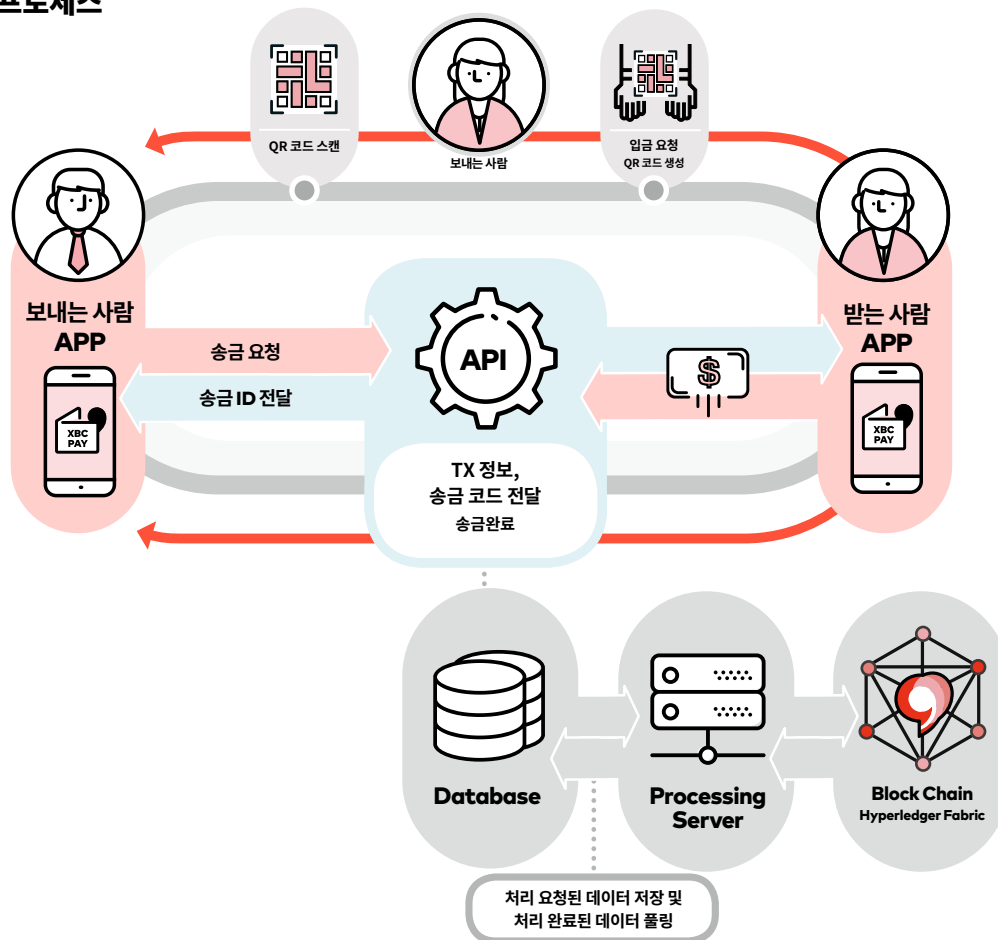
결제 프로세스 흐름



- 고객이 구매 요청시 판매자는 POS나 APP에서 주문서를 작성
- 작성된 주문서 정보를 API에 전송
- API는 해당 주문서 정보(결제요청)를 Database에 저장
- Processing Server에서 결제 요청 정보에 대한 결제 코드를 생성
- 판매자의 POS나 APP에서 결제 코드에 해당되는 QR코드를 생성
- QR코드는 판매자의 APP, POS, 영수증 프린터 등을 이용해 출력한다.
- 고객은 APP으로 QR코드를 스캔하여 암호화페나 포인트로 API에 결제 요청
- API는 고객의 잔액확인 요청을 Database에 저장
- Process Server는 고객의 잔액을 조회 후 Database에 저장
- API에서 고객의 잔액을 확인
- Database에 주문에 대한 결제 요청을 저장
- Processing Server에서 결제 요청에 대한 트랜잭션을 생성
- 생성된 트랜잭션 ID를 Database에 저장
- API에서 결제 결과를 고객(APP)과 판매자(POS or APP)에게 전달(결제완료)



송금 프로세스 흐름



- 받는사람이 APP을 이용해 QR코드를 생성
- QR코드를 보내는 사람에게 전달(직접전달, SMS, E-Mail, 주소록 등)
- 보내는 사람은 APP으로 QR코드를 스캔하여 암호화폐로 API에 송금 요청
(받는 사람 요청 없이도 받는사람 정보로 송금가능)
- API는 해당 송금요청 ID를 생성 후 정보를 Database에 저장 후
송금 ID를 보내는사람 APP에 전달
- API는 보내는사람의 잔액확인 요청을 Database에 저장
- Process Server는 보내는사람의 잔액을 조회 후 Database에 저장
- API에서 보내는사람의 잔액을 확인
- Database에 송금 요청을 저장
- Processing Server에서 송금 요청에 대한 트랜잭션을 생성
- 생성된 트랜잭션 ID를 Database에 저장
- API에서 송금 결과를 보내는사람(APP)과 받는사람(POS or APP)에게
전달(송금완료)

