RUEDA

We don't just roll
We roll for the happy future of the human world today.

WHITE PAPER v2.0.4

LEGAL NOTICE

백서의 목적은 잠재적 코인 보유자에게 중요하고 상세한 정보를 제공하여 회사에 대한 신뢰성을 높이며, RUEDA 코인 최초 제공에 대한 결정을 가능하게 하는 것이다. 본 문서에서 제공하는 모든 정보는 COIN 배분 또는 투자 제안서로 해석될 수 없다.
RUEDA COIN은 어느 사법권 아래에서, 어떠한 종류의 증권으로도 매매 제안이 이루어지지 않는다.
본사는 개인 또는 법인, ICO에 참여하고 COIN은 법률에 따라 구매할 수 있는 충분한 법적 능력을 갖고 있지 않은 사람에게 제공하지 않는다. 보다 자세한 사항은 법률, 재정, 세금 또는 기타 컨설턴트에게 문의 바람.

이 문서는 투자자를 보호하기 위해 고안된 관할권의 법률 또는 규제 행위와 상관없이 작성되었으며,
투자자 규제를 받지 않는다.
이 백서의 진술, 계산 및 재무 지표 중 일부는 예상되는 예비 정보이다.
이는 알려져 있거나, 알려져 있지 않은 위험 요소와 불확실성을 기반으로 한다. 때문에 실제 상황과 결과는 이러한 예비 예측과 직접 또는 간접적으로 크게 다를 수 있다.

TABLE OF CONTENTS

01 ABSTRACT

Rueda?

루에다는 바퀴라는 의미를 가지고 있습니다.

바퀴는 인류 문명에게 중요한 의미와 가치를 지니고 있습니다. 바퀴의 발명으로 인해 인류는 고도의 발전을 이루게 되었고 더불어 생산성이라는 측면에서도 이전과는 확연한 차이를 보이게 되었습니다.

바퀴의 발명으로 자동차, 운송 등의 산업이 특히 비교할 수 없게 발달했고 그 결과 건설/산업은 비약적인 발전을 하게 되었습니다.

이렇듯 바퀴(Rueda)는 인류 문명에만이 아니라 특히 고도의 산업화를 함축적으로 이루어낸 대한민국을 상징하는 또 하나의 키워드라고 할 수 있습니다.

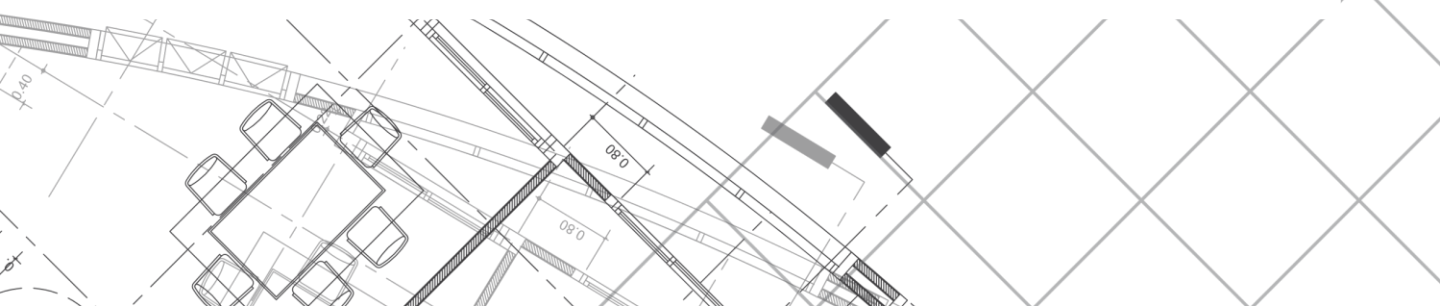
SOC의 근간이 되며 전체 산업의 기둥이라 할 수 있는 이 영역에 또 한 번 혁신의 바퀴 자국을 남길 첫걸음을 루에다 코인이 시작해보려 합니다.

이렇게 중요한 건설/산업현장에는 자재, 장비 대여, 임금 등의 결제가 월별/주별/일별로 이루어지며 그 결제의 종류 또한 굉장히 복잡한 체계로 이루어져 있고 지급 방법 역시 현금, 수표, 신용카드, 어음 등으로 다양한 형태를 가지고 있습니다.

산업현장에서 발생하는 결제 지연, 어음 및 수표 등의 지불 형태가 현금 회전율을 늦추게 하고 이는 회사의 부도, 인건비 연체, 산업 종사자들의 생활고 등으로 이어져 사회 전반에 악영향을 초래하게 됩니다.

루에다는 이런 문제점 등을 극복하고자 탄생하였습니다. 사용자와 보유자는 누에다 코인을 결제 수단으로 사용함으로써 효율적인 자금관리가 가능하고 코인의 가치 상승은 추가적인 이익 증대를 도모할 수 있게 합니다. 또한 비트코인, 이더리움, 리플 등 스테이블 코인과의 교환까지 확장하여 코인 자체의 가치도 상승하게 될 것입니다.

전통적인 산업이라고 부를 수 있는 건설 산업에 블록체인 결제 플랫폼을 도입함으로써 새로운 시대를 대비하는 동시에 현재 가지고 있는 산업의 비효율을 해결하는 솔루션이 되길 루에다가 희망합니다.



01 INTRODUCTION

건설/ 산업 현장 결제 솔루션을 위한
가상화폐

기존의 온·오프라인에 의한 건설 수주 및 각종 건설 자재 지불결제 수단은 1.5~4.5%의 가맹점 수수료와 0.15~0.3%의 지불 대행 수수료로 구성되어 있다. 또한 당, 타행 발, 송금의 경우 금액별로 차이가 있으나, 건당 15~20%의 송금수수료가 발생한다.

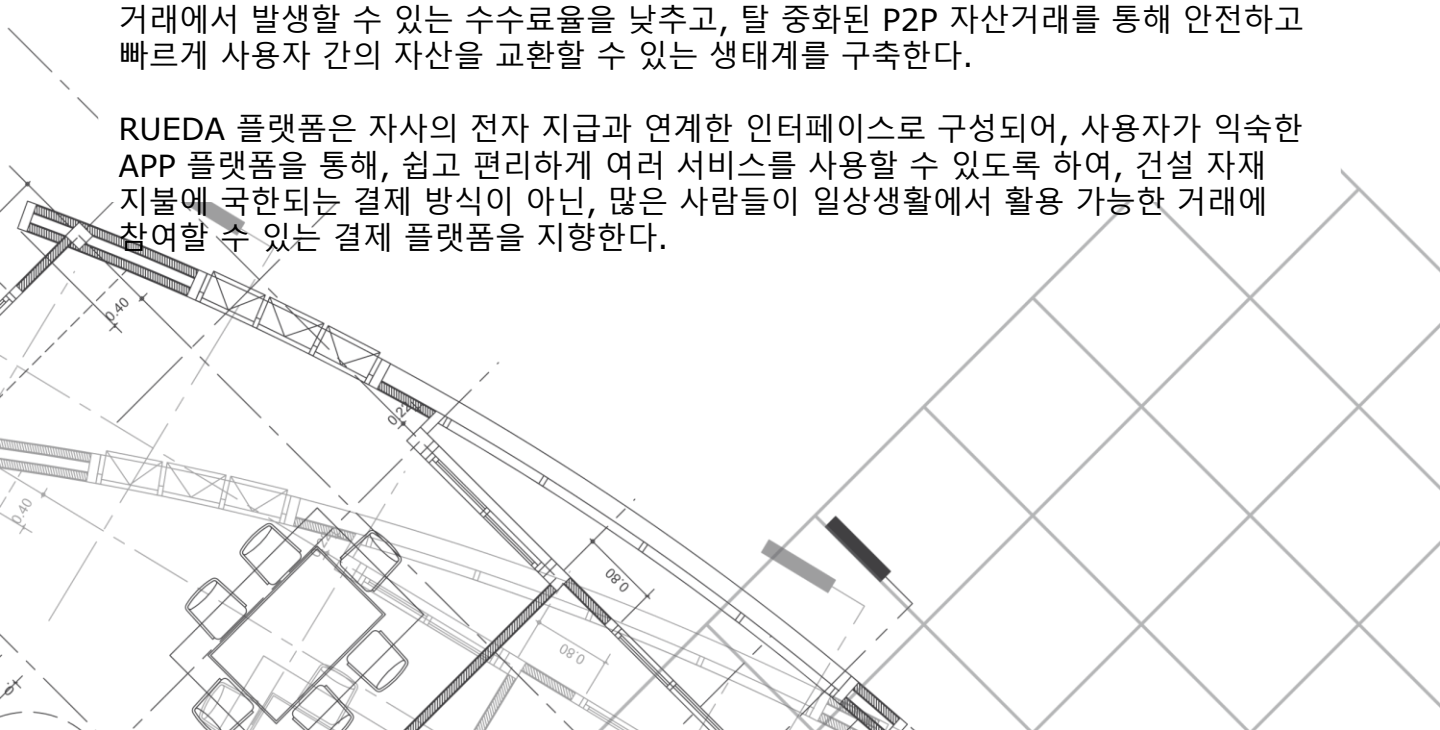
이러한 수수료로 인해 거래 시 일정한 비용이 부과되고 모든 이익이 금융사에 귀속된다. RUEDA코인은 이러한 거래수수료를 최소화하여 거래에서 발생한 이익을 사용자에게 돌려줄 수 있는 블록체인 기반 플랫폼이다.

또한, 자산의 독립적 분권화는 자산의 저장 및 교환에 혁명을 일으킬 수 있다. 자산이 분권화된 시장에는 국내외 불문하고 전 세계의 사용자가 서로 자유롭게 상호 작용이 가능하다.

분산화는 개별 참가자의 공격 및 결탁 시도 뿐만 아니라 무작위 오류에 대한 견고성을 향상시킨다. 분권화를 통해 사용자는 제 3자를 신뢰하지 않고도 자금을 완전 통제할 수 있다. RUEDA 플랫폼은 탈 중앙화된 P2P 자산 거래를 통하여 안전하고 빠르게 자산을 상호교환 할 수 있도록 한다.

RUEDA는 블록체인 기술을 통해 전통적인 금융 세계와 암호 경제학을 한데 모아 거래에서 발생할 수 있는 수수료율을 낮추고, 탈 중화된 P2P 자산거래를 통해 안전하고 빠르게 사용자 간의 자산을 교환할 수 있는 생태계를 구축한다.

RUEDA 플랫폼은 자사의 전자 지급과 연계한 인터페이스로 구성되어, 사용자가 익숙한 APP 플랫폼을 통해, 쉽고 편리하게 여러 서비스를 사용할 수 있도록 하여, 건설 자재 지불에 국한되는 결제 방식이 아닌, 많은 사람들이 일상생활에서 활용 가능한 거래에 참여할 수 있는 결제 플랫폼을 지향한다.



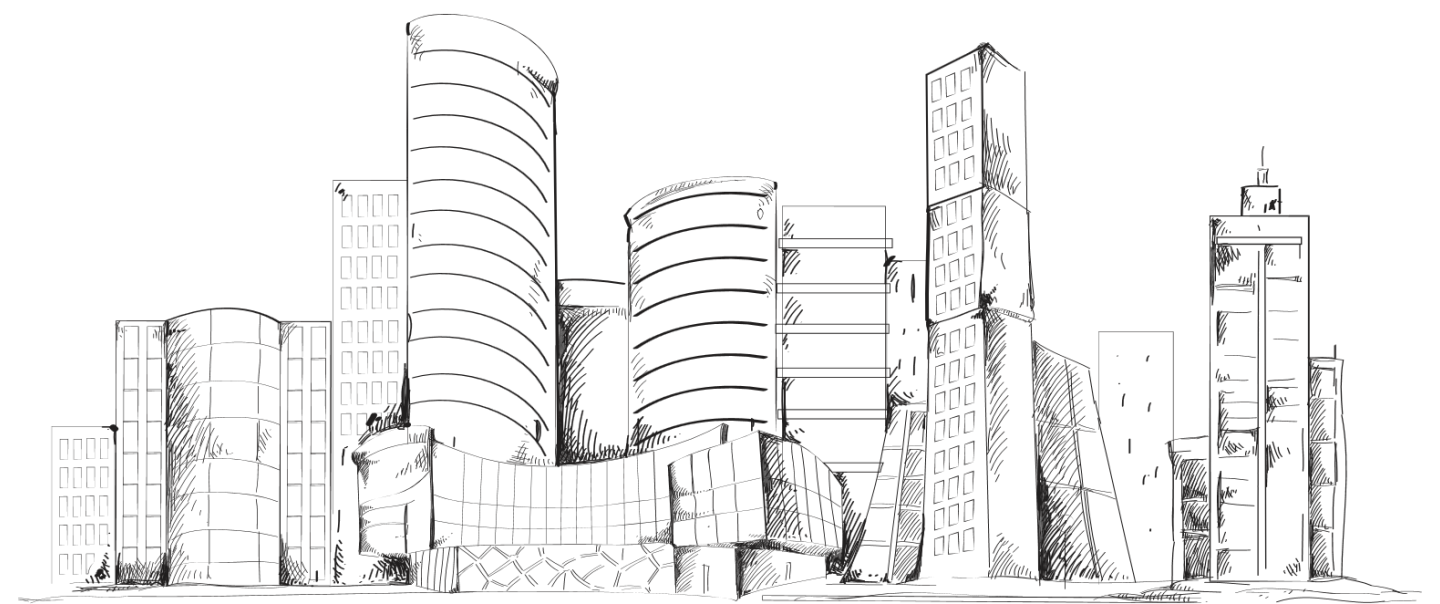
02 시장현황

2-1 국▪내외 건설 산업 시장의 현황

2-2 암호화폐 시장 규모

2-3 온▪오프라인 결제 시장 현황

2-4 현행 자금 이체

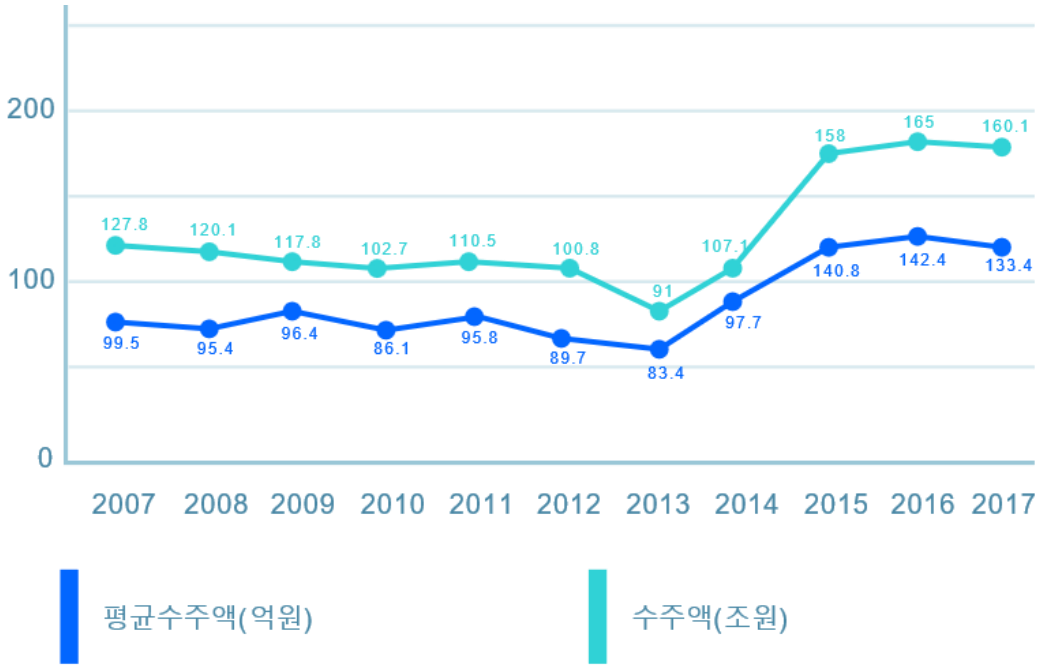


02 시장현황

2-1 국내외 건설 산업 시장의 현황

▶ 국내 산업 현황

종합 건설업체 국내 건설수주 및 업체당 평균 수주



발주자 별 / 공종 별 계약 액·기성 액 현황

단위 : 억원

구분		계약액		기성액	
		2015년	2016년	2015년	2016년
전체		1,824,985	1,620,155	1,501,495	1,656,680
공공		403,911	374,364	443,396	410,108
	토목	210,005	187,235	224,718	217,568
	건축	149,472	151,964	162,588	149,370
	산설·조경	44,430	35,159	56,085	43,165
민간		1,421,071	1,245,789	1,058,095	1,246,570
	토목	51,715	107,747	65,317	124,686
	건축	1,238,450	1,080,954	874,037	1,025,504
	산설·조경	130,904	57,085	118,740	96,378

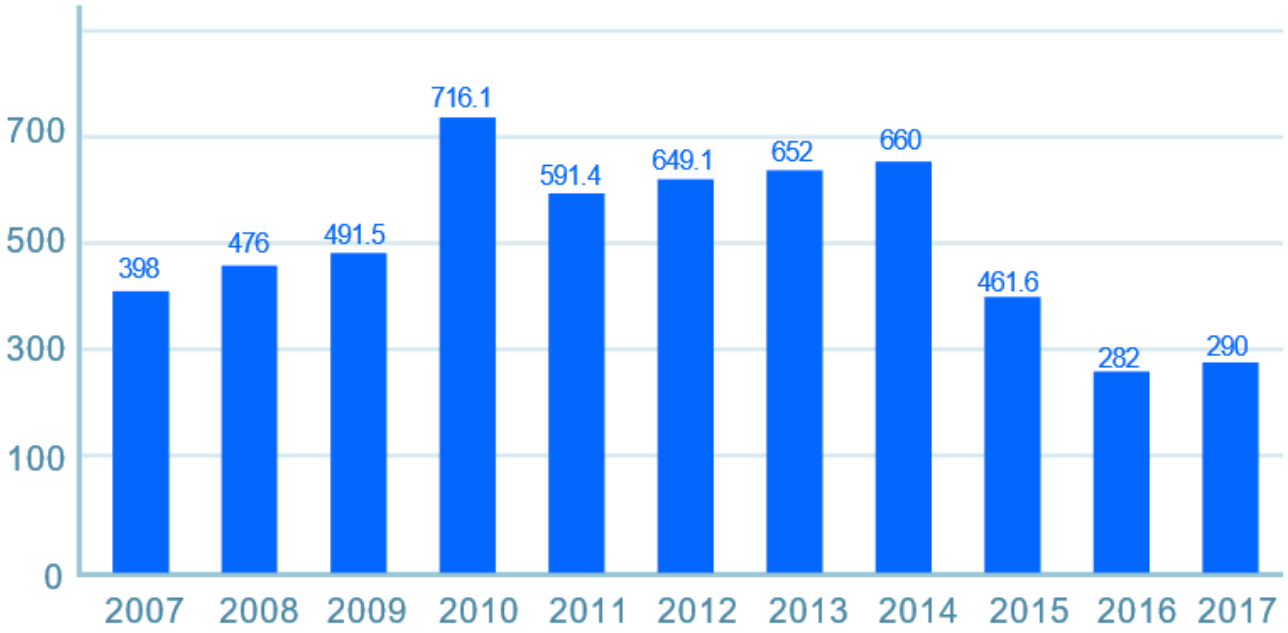
02 시장현황

2-1 국내외 건설 산업 시장의 현황

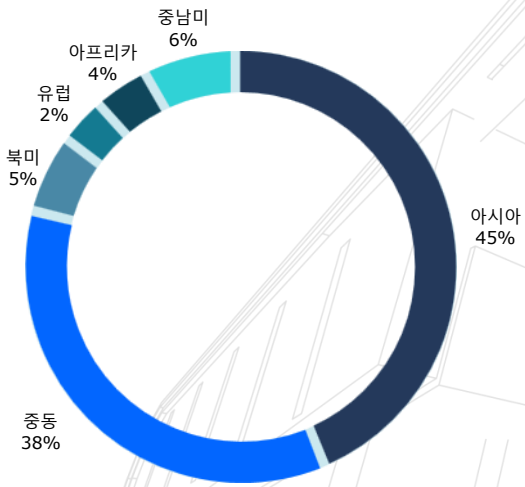
▶ 해외 산업 현황

해외 건설 수주 현황

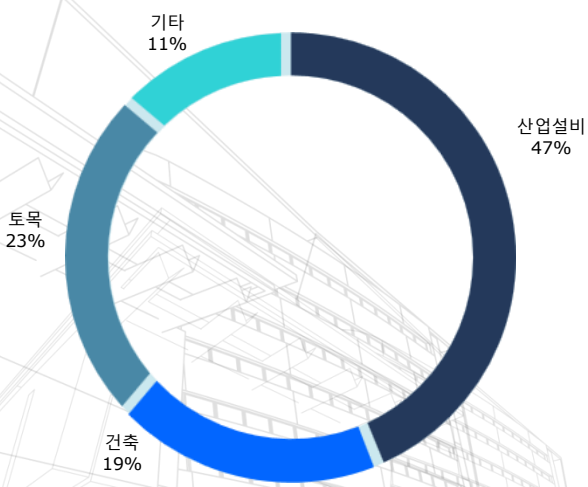
(단위 : 억 달러)



해외 수주 지역별 구성



해외 건설 수주 공종별 구성



02 시장현황

2-1 국내외 건설 산업 시장의 현황

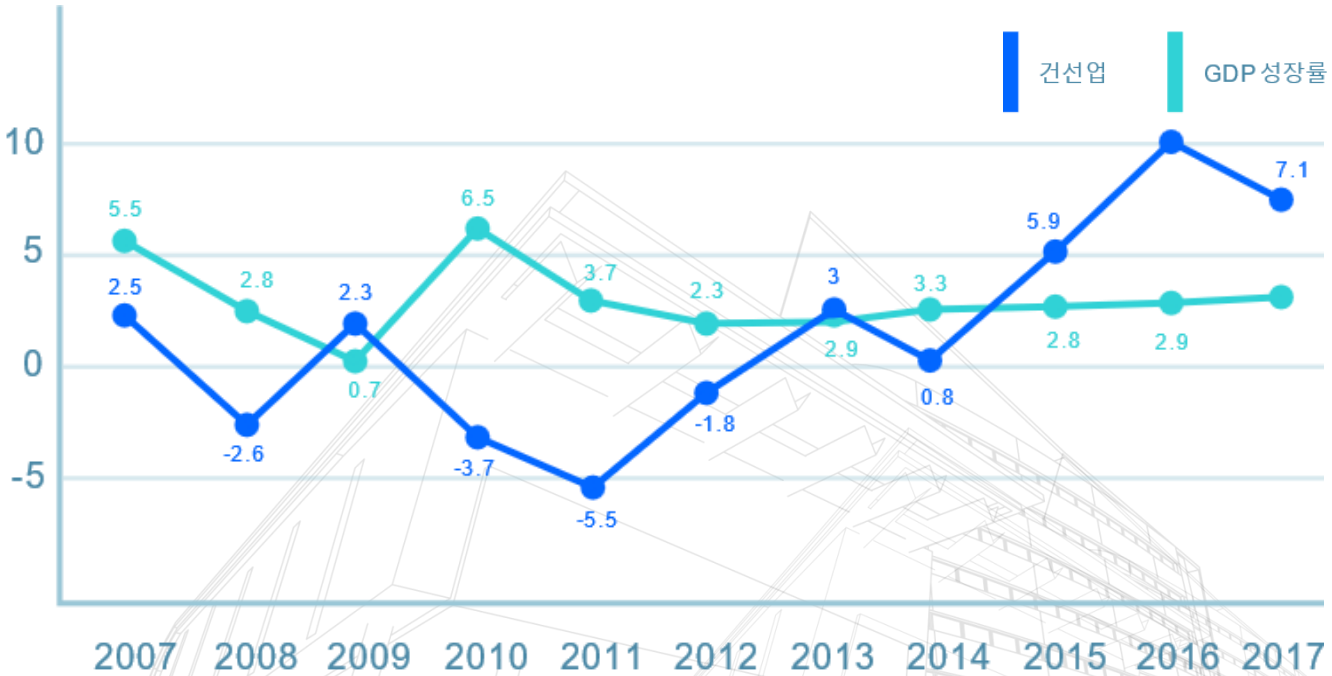
▶ GDP 동향

산업별 경제 성장률

(단위 : %)

년도	07	08	09	10	11	12	13	14	15	16	17
GDP성장률	5.5	2.8	0.7	6.5	3.7	2.3	2.9	3.3	2.8	2.9	3.1
건설업	**2.5**	**-2.6**	**2.3**	**-3.7**	**-5.5**	**-1.8**	**3.0**	**0.8**	**5.7**	**10.1**	**7.1**
제조업	8.4	3.7	-0.5	13.7	6.5	2.4	3.6	3.5	1.8	2.4	4.4
농림어업	4.1	5.6	3.2	-4.3	-2.0	-0.9	3.1	3.6	-0.4	-2.8	0.3
서비스업	5.2	3.2	1.5	4.4	3.1	2.8	2.9	3.3	2.8	2.5	2.1

경제 성장률 및 건설업 총생산

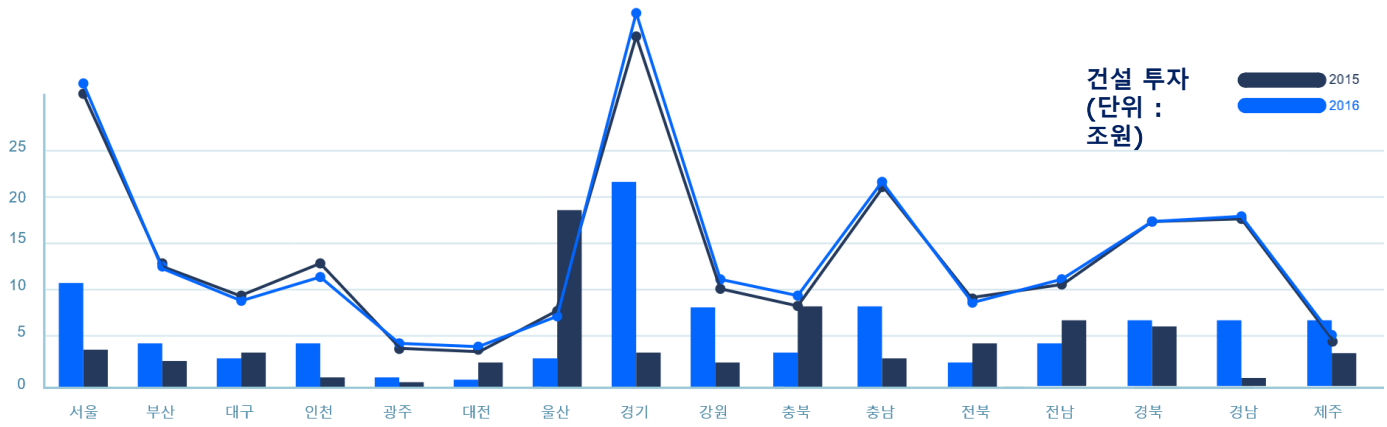


02 시장현황

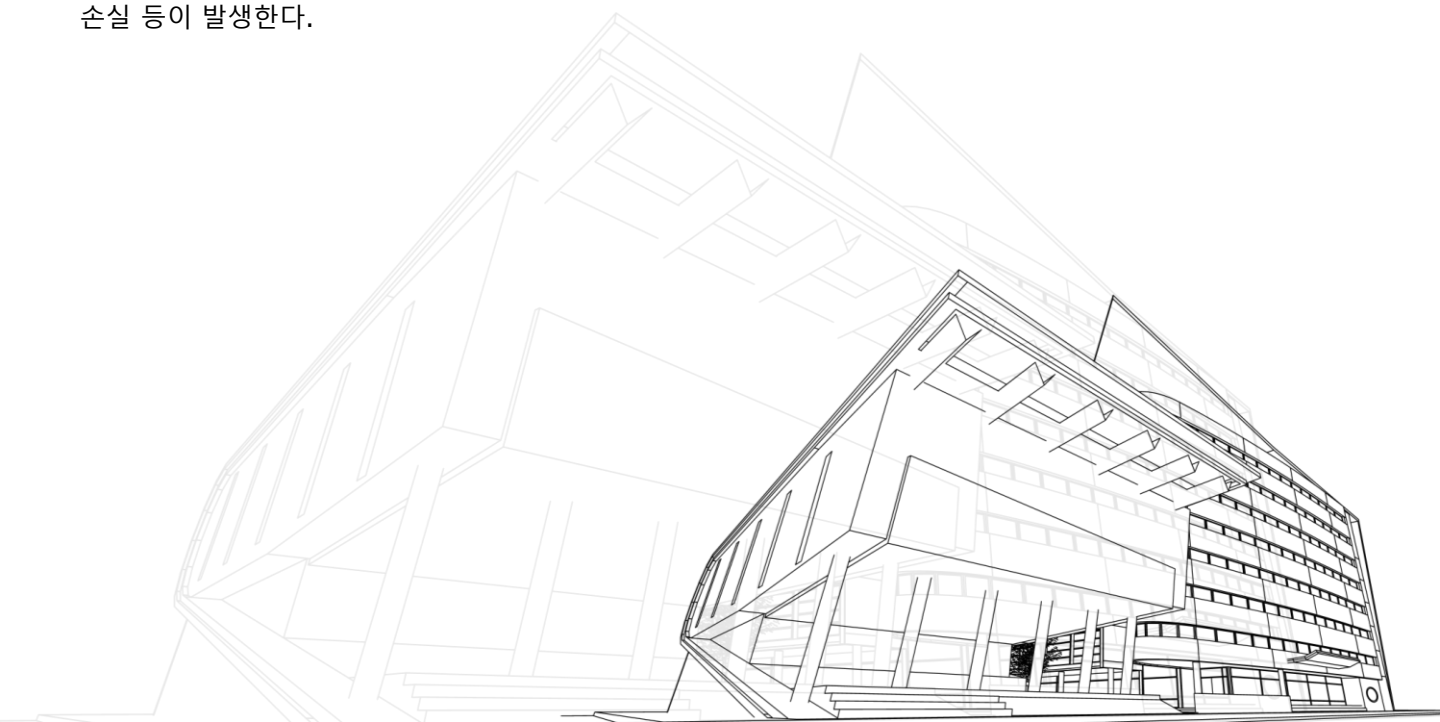
2-1 국내외 건설 산업 시장의 현황

GDP 동향

산업별 경제 성장률



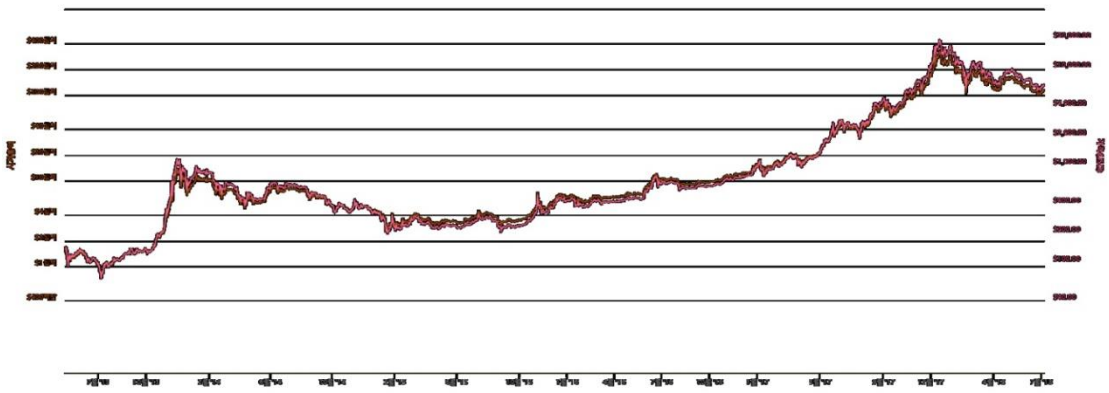
국내외의 GDP동향의 경우 건설업 분야의 비중이 매우 높으며,이에 따른 자금 이동 및 결제 또한 상당하다. 하지만 중개 기관의 개입과 각종 세금 등으로는 자유롭지 않으며, 각종 수수료에 의한 공사대금의 지불에서 손실 등이 발생한다.



02 시장현황

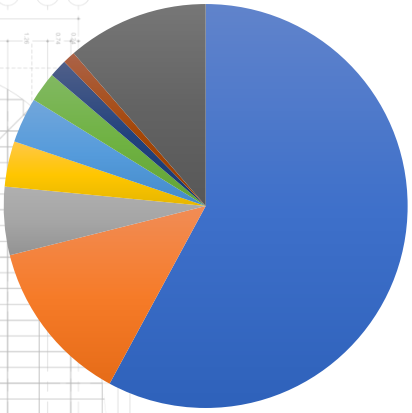
2-2 암호화폐 시장 규모

암호화폐 시장은 급속도로 확장 및 심화되고 있으며, 세계 암호화폐 시장의 규모는 2018년 기준 7천 2백억 달러이다.



암호화폐의 장점과 잠재력은 충분히 인정하고 있지만, 암호화폐 관련 거래를 지원하는 금융기관이 부족하다는 이유로 익명성은 더욱 광범위한 주류 화폐로의 편입에 장애물이 되어왔다.

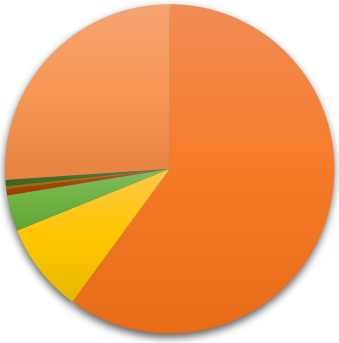
암호화폐 시가 총액 점유율(%)



비트코인
이더리움
비트코인 캐시
리플
라이트코인
IOTA

주 : 2017년 12월 13일 기준
자료 : COIN DANCE

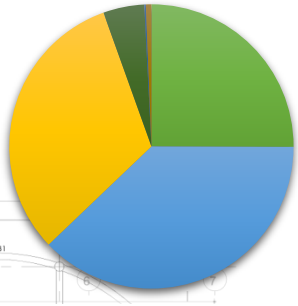
비트코인 통화별 거래량(%



JPY
KRW
EUR
USDT
ALD
GBP

주 : 2017년 12월 13일 기준
자료 : COIN DANCE

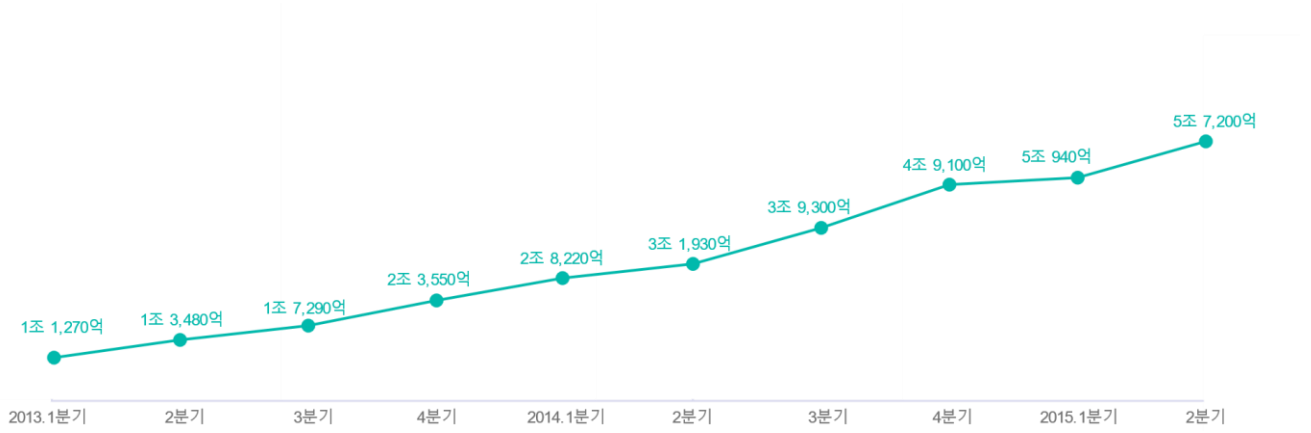
이더리움 통화별 거래량(%



KRW
BTC
USD
EUR
SGD
JPY

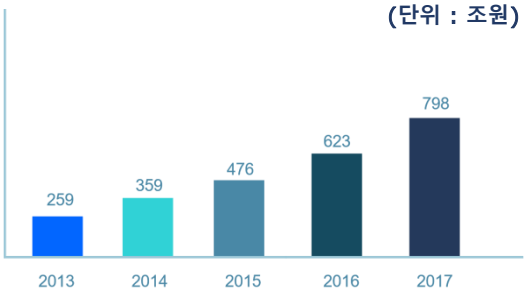
02 시장현황

2-3 온·오프라인 결제 시장

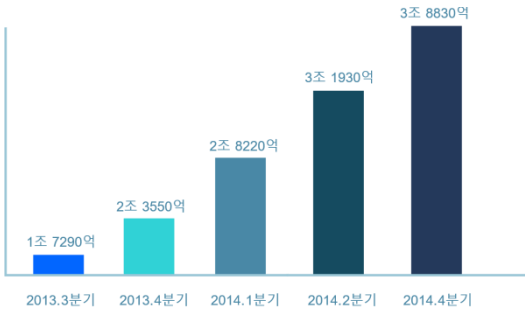


급성장하는 세계 모바일 결제 시장

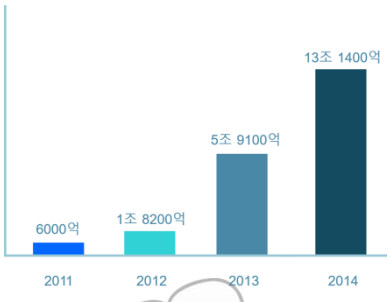
(단위 : 조원)



커지는 국내 모바일 결제 시장

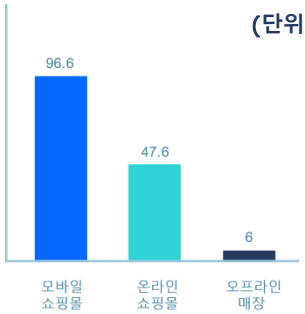


스마트폰으로 쇼핑하는 시대



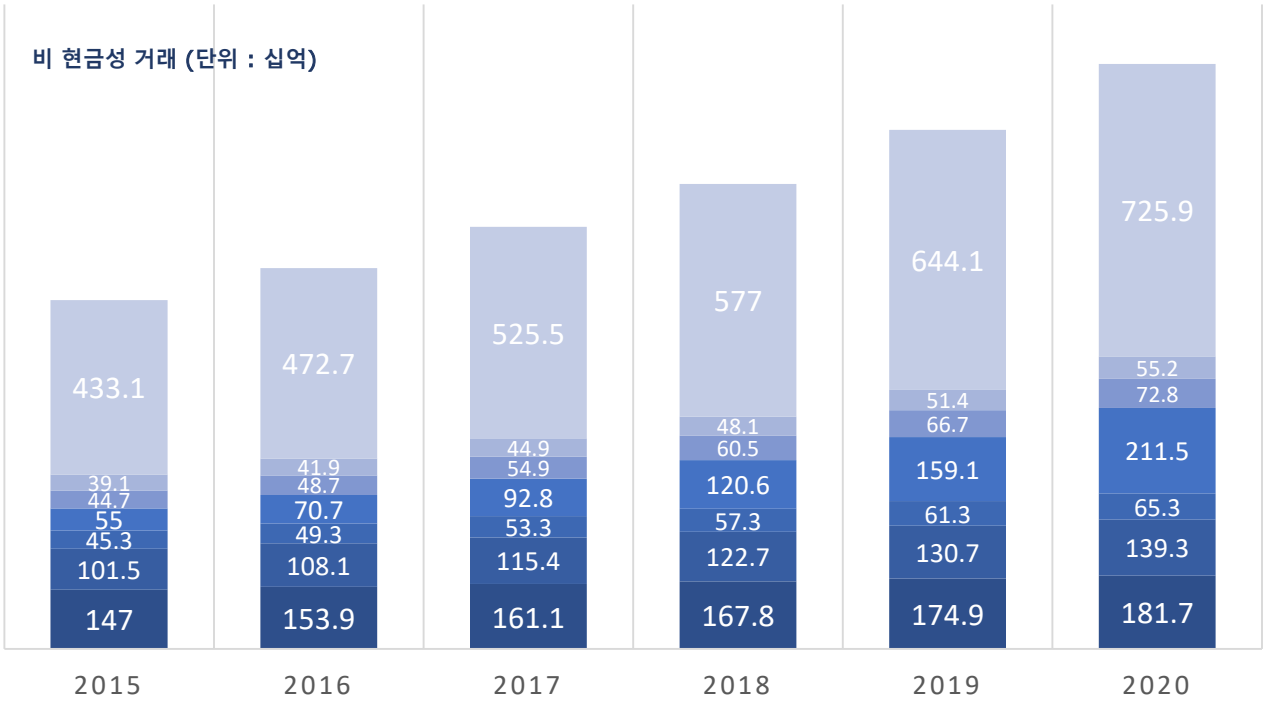
모바일 간편 결제 장소

(단위 : %)



02 시장현황

2-3 온·오프라인 결제 시장



	CAGR 15-20E	Growth 15-16E	
글로벌	10.9%	9.1%	
라틴 아메리카	7.1%	7.2%	개발도상국 19.6%
CEMEA	10.2%	8.9%	
신흥 아시아	30.9%	28.6%	
성숙한 아시아-태평양	7.6%	8.8%	
유럽 (유로존 포함)	6.5%	6.5%	성숙 5.6%
북미 (미국 및 캐나다)	4.3%	4.4%	

글로벌 금융기관 결제의 중요성이 대두되고 있다. SWIFT라는 플랫폼의 경우 일평균 전 세계 거래량은 약 5조 달러,
연간 1,250조 달러에 이른다.

또한 차트상 업계의 전년 대비 성장을 보여준다. 신흥시장에서의 결제가 더 높은 성장률을 보이지만 북미 및 유럽 등의 비교적 확립된 지역에서는 암호화폐 기반 결제 솔루션에 대해 훨씬 크고 즉각적인 시장이 존재한다.

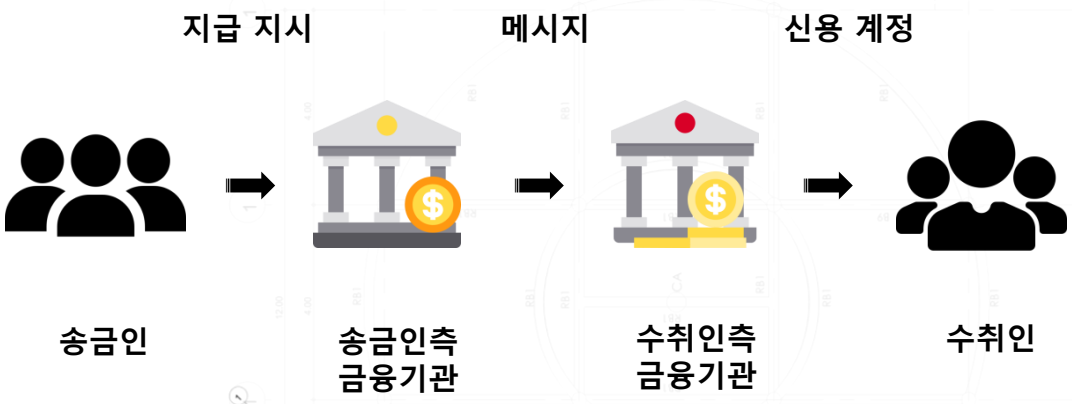
02 시장현황

2-4 현행 자금 이체

전자자금이체(Electronic Fund Transfer, 이하 EFT)란 금융기관 고객의 요청에 따라 한 금융기관에서 다른 금융기관으로 (또한 한 계좌에서 다른 계좌로) 자금이 이동하는 거래를 말한다.
이를 위해 금융기관은 필수 부기입력(Book Keeping)과 자금 제공을 가능하게 해주는 전자 메시지를 주고받는다.
전자 자금 이체는 두 사람 간의 자금 이체를 위해 기업에서 사용하는 기본 메커니즘이다.
금융기관은 SWIFT와 ISO 20022 등 사람들에게 알려져 있고, 충분히 지원받고 있는 표준에 따라 전자 메시지를 송수신 함으로써 전자 자금 이체를 수행한다.

금융기관 간에 전송된 메시지는 송신 은행이 송금인의 계좌에서 자금을 인출하고,
수신은행이 수취인의 계좌에 입금하도록 지시한다. 이와 같은 이체에 관여하는 주체는 다음과 같다.

- 송금인(사업체or개인) – 이체 게시자
- 수취인 – 이체의 최종 수취 당사자
- 송금인측 금융기관 – 송금인의 이체 지시를 받아 자금을 수취인측 금융기관에 송금하는 금융기관
- 수취인측 금융기관 – 자금을 수령하여 계좌에 보관하는 금융기관
- 추가 / 중개 금융기관 – 거래 수행에 필요한 기타 금융기관

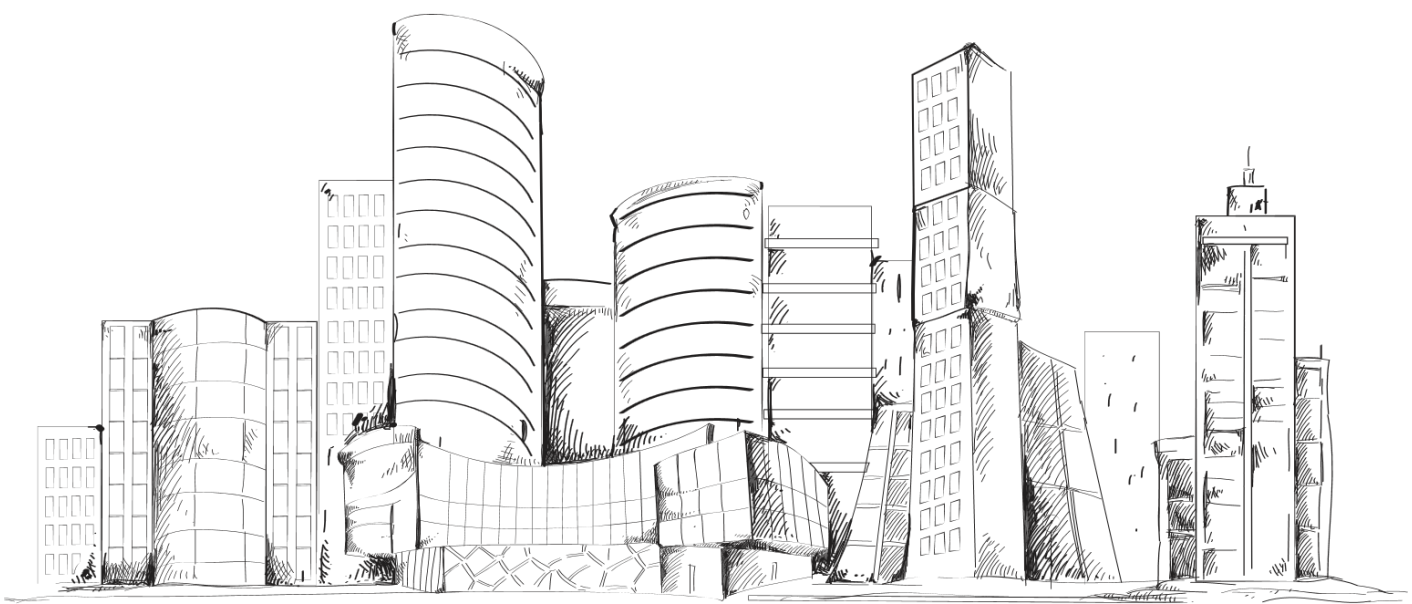


03 Our Mission

3-1 타겟에 맞춘 시장(Target Market)

3-2 온·오프라인 결제

3-3 글로벌 Exchange And Remittance



03 Our Mission

3-1 타겟에 맞춘 시장(Target Market)

시가총액 수십, 수백 조원에 달하는 수 많은 암호화폐가 투자, 투기의 목적으로 활발히 거래가 되고 있으나, 실제 각종 지불과 결제로서의 사용은 미미한 것이 현실이다.
여타의 암호화폐와는 달리 RUEDA코인은 지불, 결제 능력을 가장 중요시하며,
실제 사용이 가능한 화폐 기능에 목표를 두고 있다.

건설 / 산업현장에서는 자재, 장비 대여, 노임 등의 결제가 월별 / 주별 / 일별 등으로 이루어지며 이러한 결제의 종류는 다양하고 복잡한 체계로 이루어져 있다. 이뿐만 아니라 지급 방법의 경우 현금, 수표, 어음 등으로 다양하다.

RUEDA는 이러한 수 많은 결제를 편리한 방법으로 진행할 수 있는 방법이 없을까 하는 생각에서 시작되었다.
어려운 산업의 현장 속에서 결제 지연, 어음 및 수표결제의 늦은 현금 회전율은 부도, 인건비 연체 등으로 이어져 참여 회사와 산업 종사자를 더욱 어렵게 만들고 곤경에 빠지게 한다.

우리는 이러한 문제점을 RUEDA 코인의 개발과 사용을 통해 극복하고자 한다.

03 Our Mission

3-1 온·오프라인 PAYMENT

RUEDA COIN은 웹-기반 및 네이티브를 지원하는 소프트웨어 솔루션 세트이며, 대부분의 주요 운영 체제 및 상용 하드웨어와 호환된다. 본질적으로 Payment의 RUEDA COIN 시스템은 다음과 같다.

1 RUEDA COIN Payment 코어

데이터베이스를 운영하는 처리 서버 및 데이터베이스를 판매 업체 또는 암호화폐 핵심 팀과 같은 다양한 외부 사용자와 연결하는 API의 조합으로 이루어진다.

2 결제 처리 게이트웨이 세트

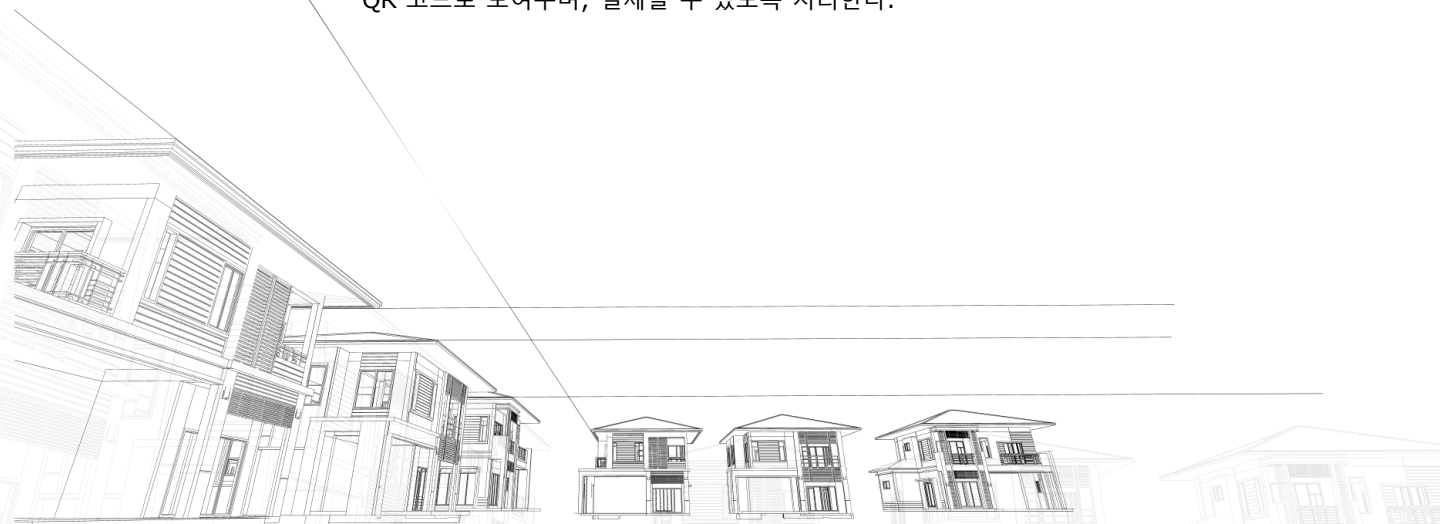
게이트웨이는 본사의 결제 파트너의 비즈니스 로직을 코어에 적용하여 커뮤니케이션 유니폼을 생성한다.

3 RUEDA COIN의 올인원 다중 암호화폐지갑

RUEDA COIN Payment 시스템 내에서 사용 가능한 암호화폐를 송금 및 수령이 가능하다.

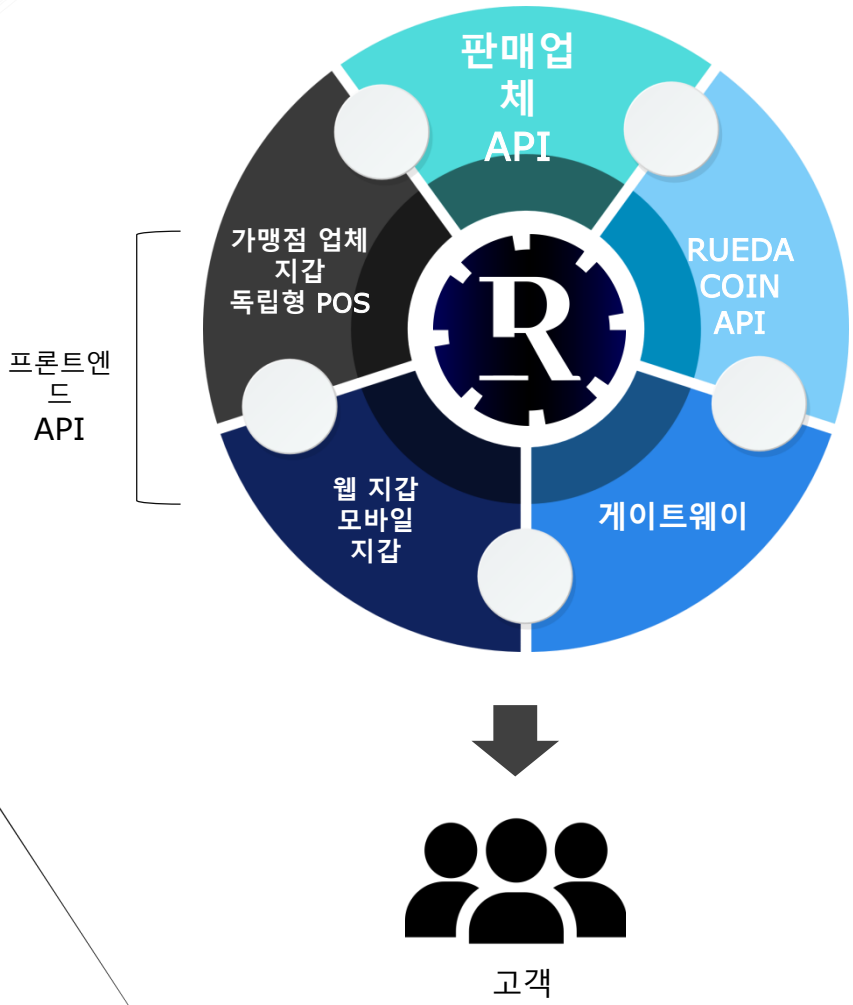
4 독립형 POS 시스템

RUEDA COIN Payment 시스템 내에서 가맹점용으로 사용하며, 상품 등록 및 가격 등을 QR 코드로 보여주며, 결제할 수 있도록 처리한다.



03 Our Mission

3-1 온·오프라인 PAYMENT



게이트웨이는 노드에 연결되며 각 노드는 RUEDA COIN 시스템 내에서 결제 수단으로 사용할 수 있는 암호화폐를 나타낸다. 또한 게이트웨이는 거래소에 직접 연결되어 RUEDA COIN 코어와 통화 간의 원활한 변환이 가능하다. 그리고 제휴 은행에 연결할 수 있기 때문에 암호화폐를 직접 현금으로 변환 가능하다.

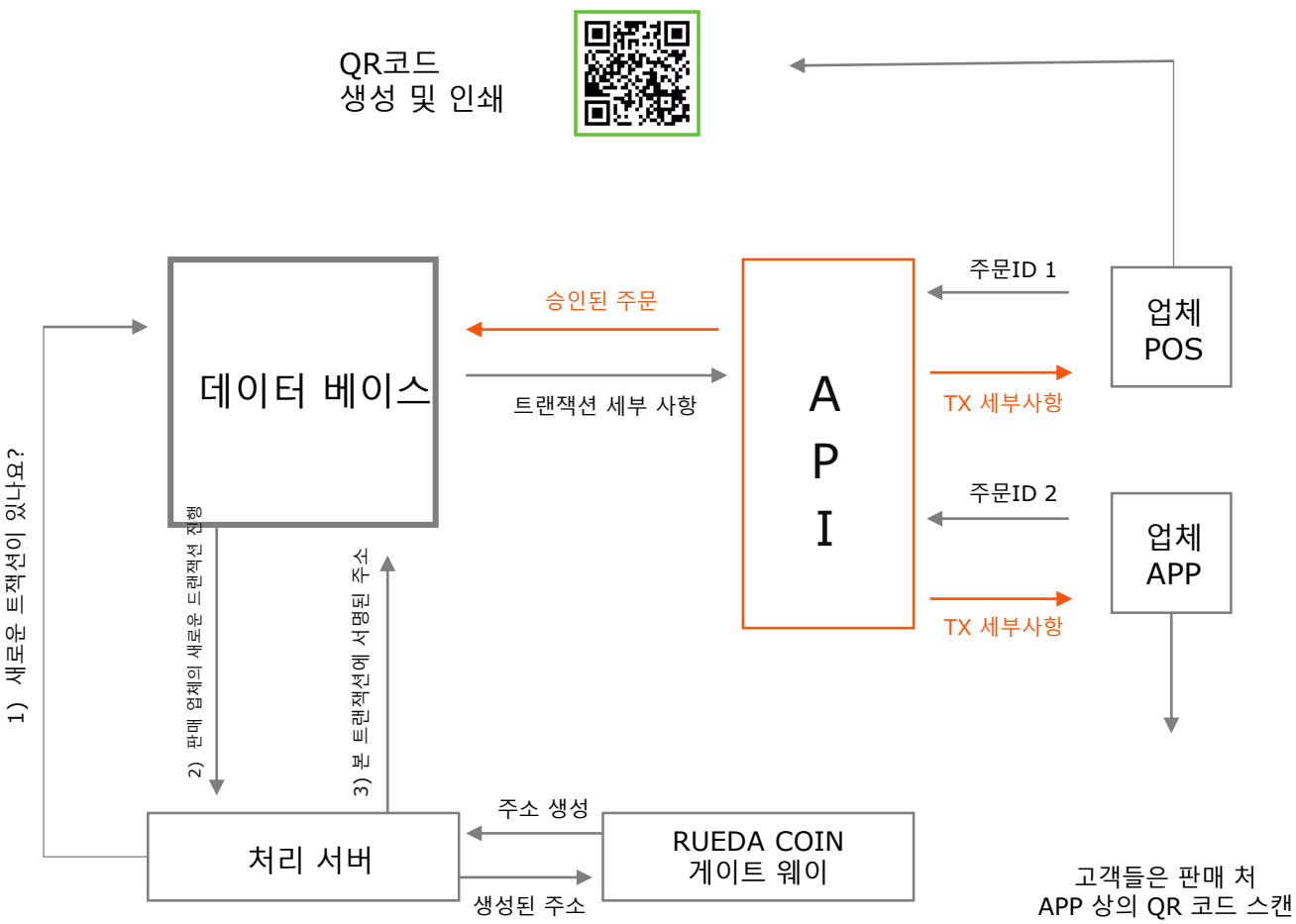
마지막으로 게이트웨이는 기타 결제 시스템들과 RUEDA COIN간의 상호 운용성 인터페이스 기능을 수행할 수 있다.

03 Our Mission

3-1 온·오프라인 PAYMENT

POS통합, QR 코드 생성

RUEDA COIN은 기존 POS 솔루션, 결제 처리 및 게스트 관리 소프트웨어,
플러그인 작성 및 API 통합 수행을 통해 RUEDA COIN을 통한 결제를 처리할 수 있다.



03 Our Mission

3-1 온·오프라인 PAYMENT

판매 업체가 RUEDA COIN으로 결제하길 원할 때마다 먼저 고객에게 청구서를 제출해야 한다.
청구서 세부 내용은 추적되지 않으며 총액만 추적된다.
POS 소프트웨어 또는 독립형 POS 판매 업체 APP로 청구서 생성을 시작하려면
판매 업체가 먼저 주문을 생성해야 합니다.
주문에는 주문 ID(판매 업체 POS 소프트웨어가 생성하는 고유 ID)가 존재하며 결제에 사용될
루에다코인 및 지불 금액이 포함된다.
판매 업체가 주문을 생성하여 루에다코인 판매 업체 API로 전송한 후
루에다코인 API는 다음 내역을 확인한다.

1. 주문 ID 중복
2. 결제 자격
3. 루에다코인 사용 가맹점 유무
4. 고객이 결제에 사용하는 루에다코인의 진위 여부
5. 결제 금액 – 본 결제를 적절하게 처리하기에는 너무 낮거나 높을 수 있다.
6. 기타 판매 업체의 특수 사항

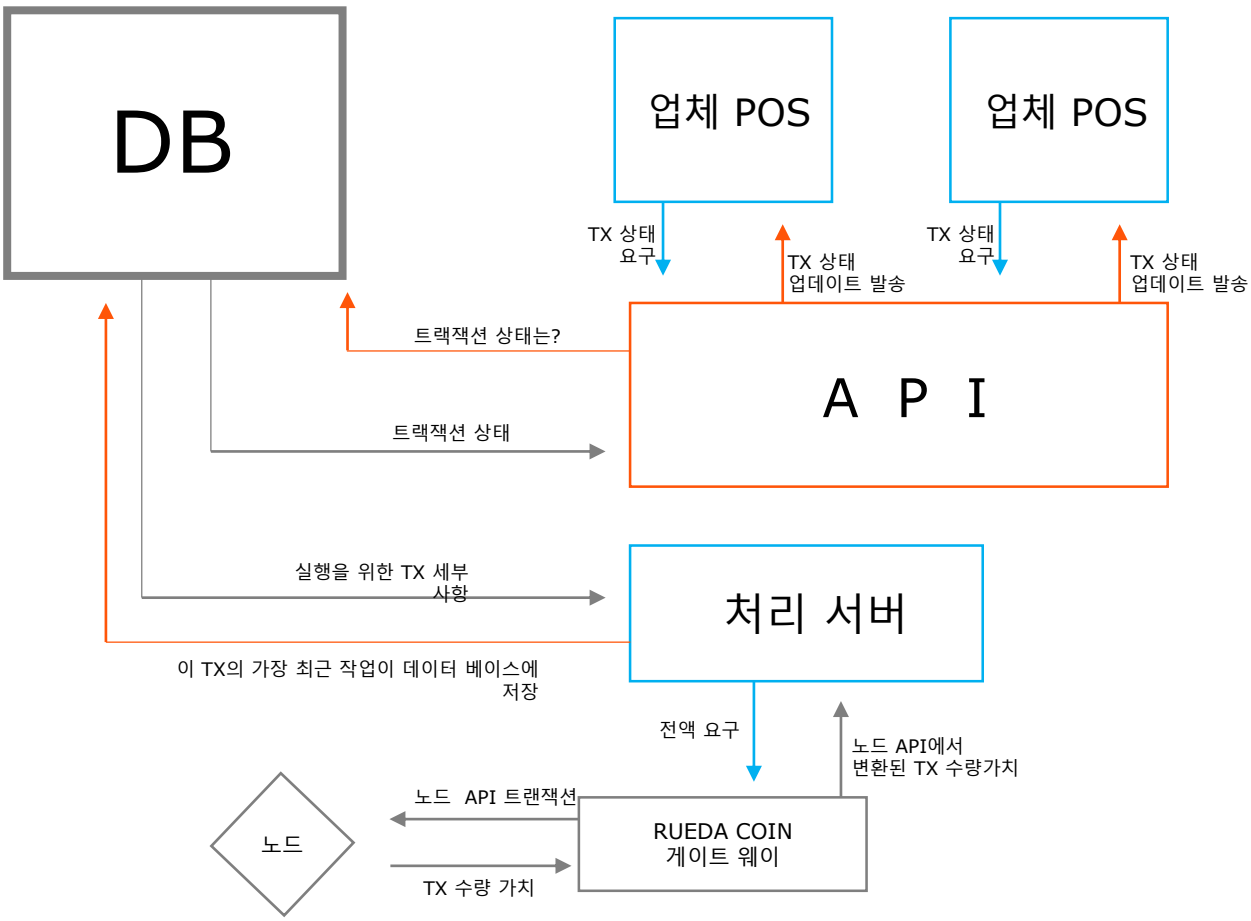
유효성 검사가 성공적이라면 유효성 검사가 완료된 주문은 데이터베이스에 전송되어
시스템 내부에서 트랜잭션 ID를 받는다.
데이터베이스는 고객, 트랜잭션, 화폐 및 게이트웨이에 대한 정보를 저장한다.
처리 서버는 게이트웨이 및 다양한 API에서 이 데이터를 폴링하고
이를 데이터베이스 내부에서 처리하는 서버 애플리케이션이다.
게이트웨이가 무엇인지에 대해서는 이미 RUEDA COIN 시스템 섹션에서 간략하게 설명하였다.
게이트웨이가 RUEDA COIN POS 통합에 참여하는 방법을 이해하는데
중요한 사안은 각 트랜잭션마다 블록체인 주소를 생성한다는 것이다.
이 방법으로 시스템 내에서 사용 가능한 모든 루에다코인에 대해 블록체인에서 발생하는
트랜잭션을 기존의 회계 및 결제 처리 기술과 연결한다.

03 Our Mission

3-1 온·오프라인 PAYMENT

POS통합, 트랜잭션 상태폴링

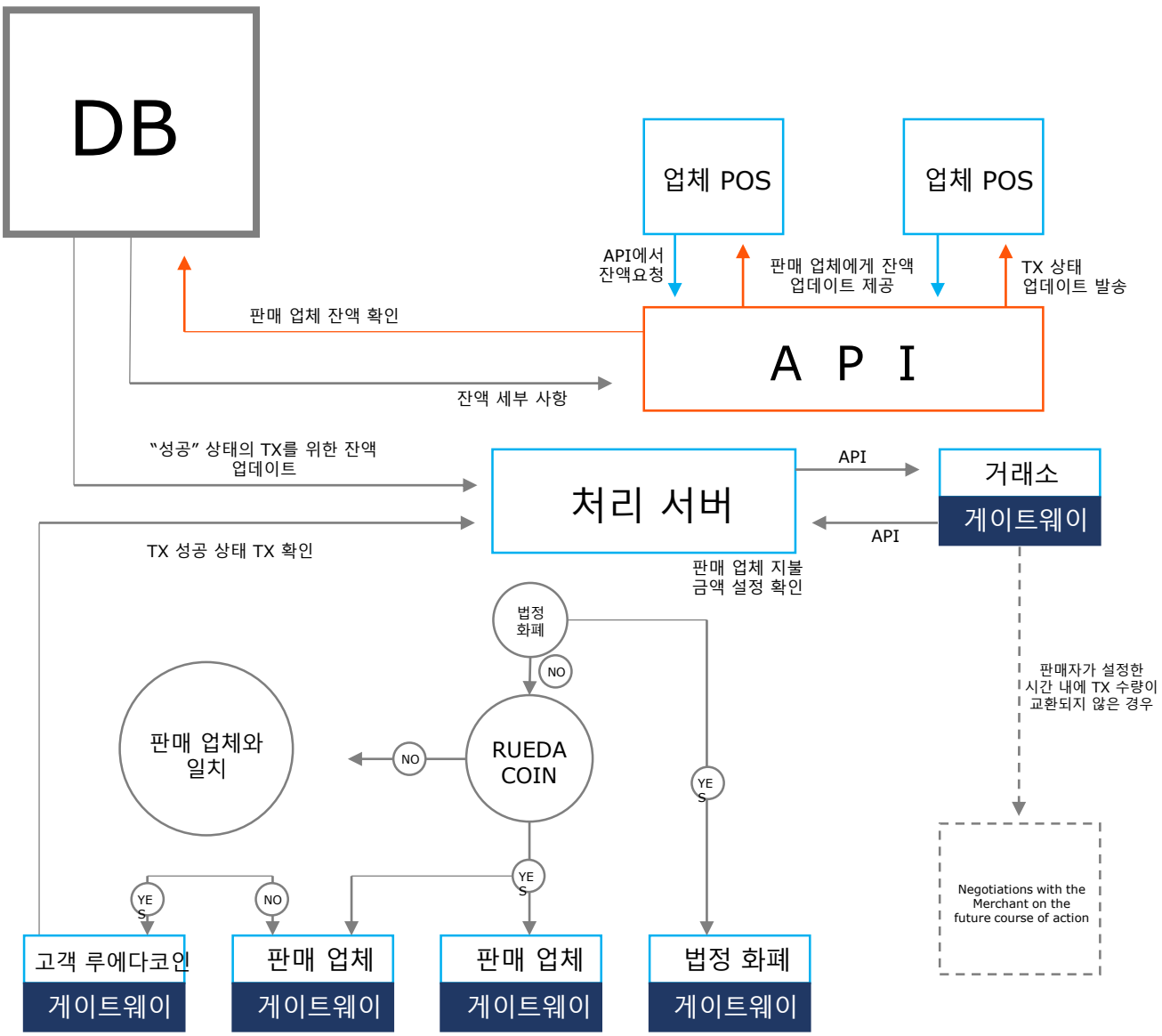
판매 업체는 고객에게 QR 코드가 들어있는 청구서를 제시한다.
고객은 암호화폐로 결제를 시작한다.
그 후 루에다 코인 코어는 관련 게이트웨이를 통해
고객의 루에다 코인 블록체인을 주기적으로 폴링하여결제 상태를 확인한다.



03 Our Mission

3-1 온·오프라인 PAYMENT

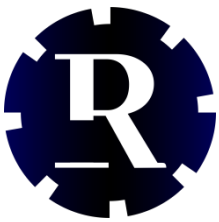
POS통합, 트랜잭션 성공 및 잔액 업데이트



03 Our Mission

3-2 온·오프라인 결제

온라인 결제 대체서비스



RUEDA COIN 이용

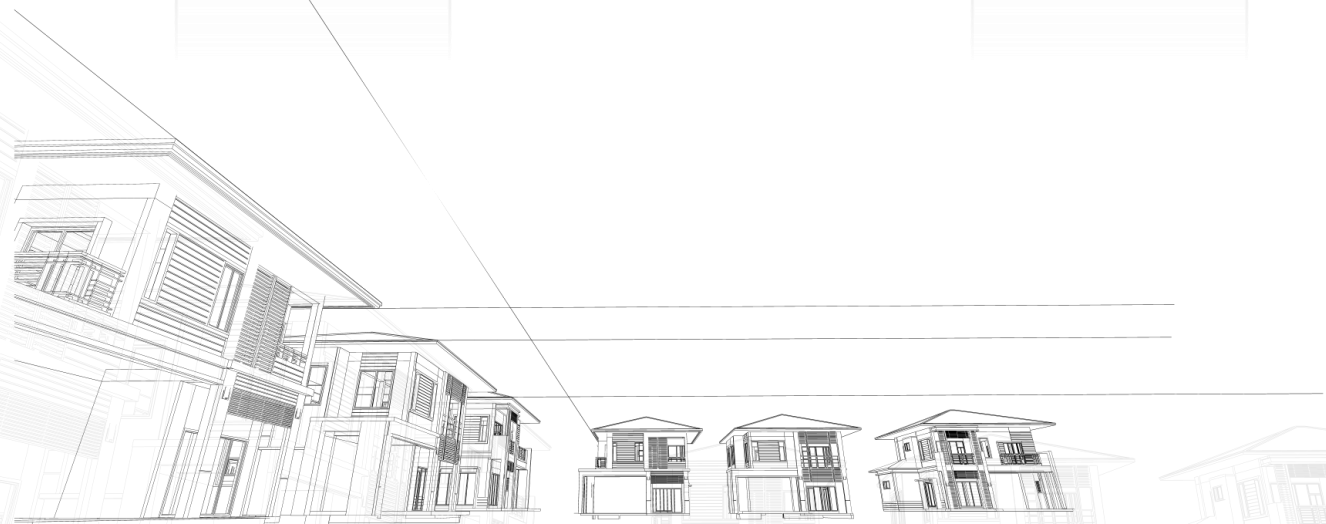
송신자
상품 또는 서비스 구매

PG 시스템 이용

YES

NO

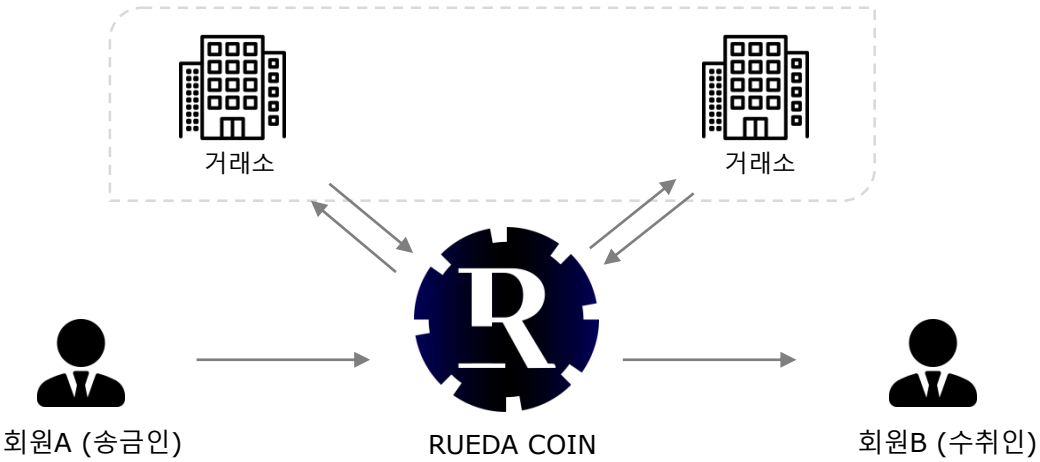
즉시 전송	금융회사 수수료 1.5 ~ 4%
안전한 거래	PG사 수수료 0.15 ~ 0.5%
빠른 자금 회수	7~14일 소요



03 Our Mission

3-3 글로벌 Exchange And Remittance

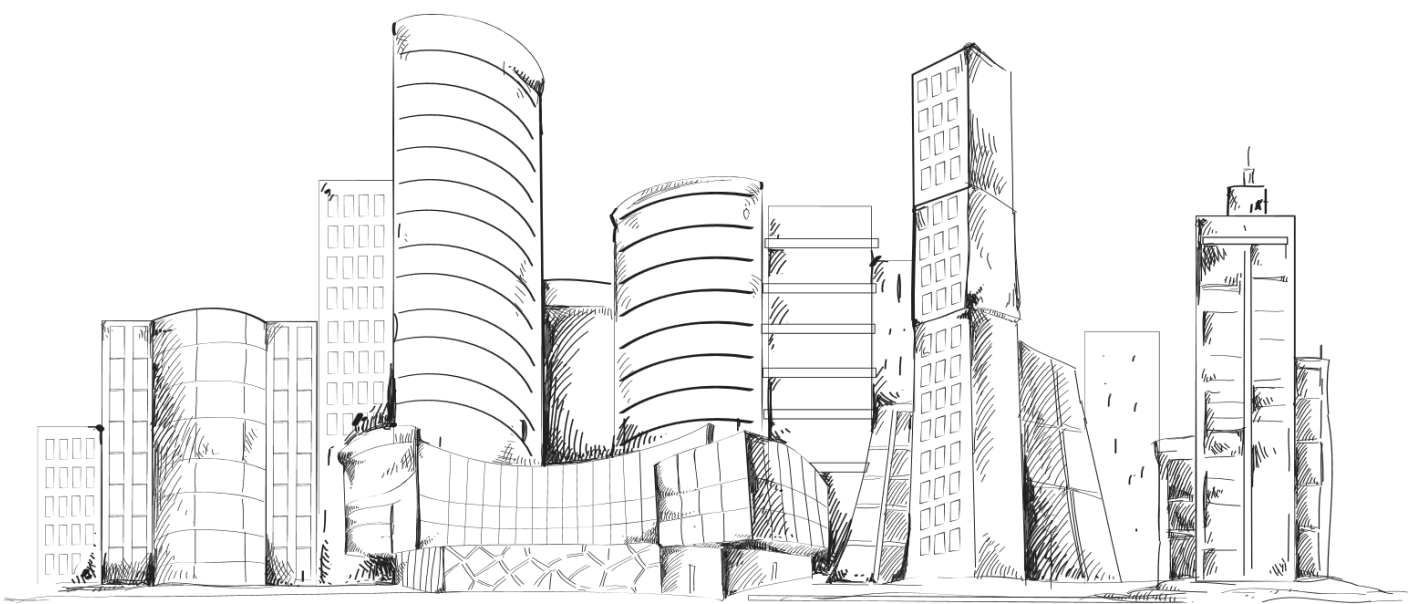
- 세계 각 지의 코인 거래소 인프라(API)를 활용하는 구조
- 코인을 활용하여 각 나라별 통화의 환율에 대한 적용을 받지 않는다.



- 송금 요청부터 수락 후 완료까지 걸리는 시간은 최대 1분 정도로 거의 실시간에 가까운 송금 시간을 장점으로 한다.

04 해결 책

4-1 RUEDA COIN 블록체인 TECHNOLOGY
4-2 APP 전자 지갑 / POS 시스템

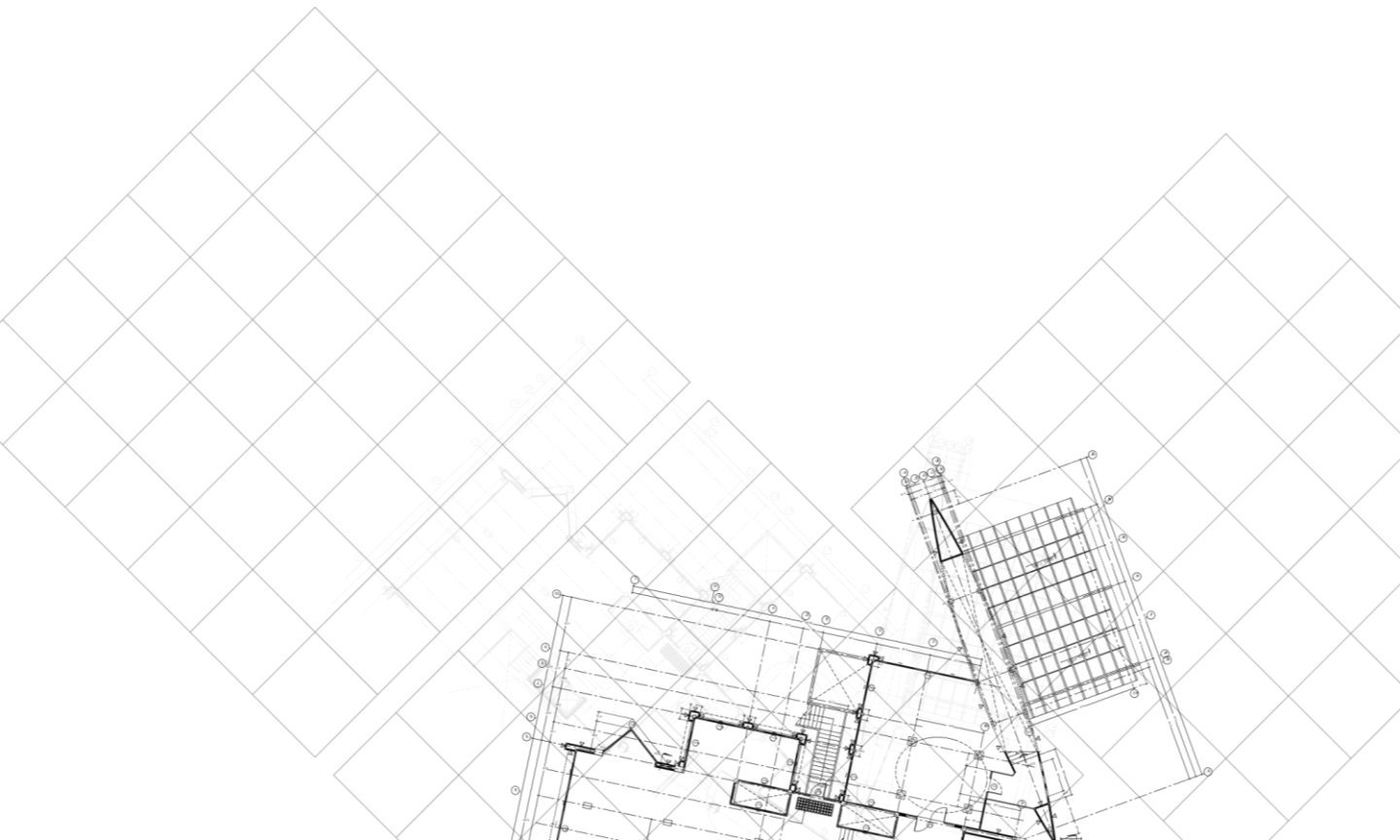


04 해결책

4-1 RUEDA COIN 블록체인 TECHNOLOGY

제3자의 개입 없이 이루어지는 결제 시스템의 블록체인 기술

완전한 P2P 방식의 루에다 코인을 이용하면 금융기관을 통하지 않고 한쪽에서 다른 쪽으로 온라인 송금이 가능하다. 전자 서명이 일반적인 해결책이지만, 이중지불(Double – Spending)을 방지하기 위해 신뢰받는 제 3자의 개입을 필요로 한다면 우리가 원하는 바에서 벗어나게 된다. 이 문서는 P2P 네트워크를 이용하여
이중지불을 막는 해결책을 제시하고자 한다. 이 네트워크는 암호화 함수를 실행하는
해싱(Hashing) 작업을 통해 해시 기반 작업증명(Proof-of-work) 체인(Chain)에
타임스탬프(Time Stamp)를 통해 시간을 기록하는데, 이를 통해 작업증명을 다시 수행하지 않고서는 변경할 수 없는 안전한 기록을 생성한다.
가장 긴 체인은 네트워크에 의해 검증된 거래의 연속적인 기록일 뿐만 아니라 가장 큰
연산능력(CPU Power)의 결과물이기도 하다. 다수의 연산능력이 네트워크를 공격하는데 동조하지 않는 한, 가장 긴 체인을 만들면 공격자는 무력화된다. 또한, 네트워크는 최소한의 구조만을 필요로 한다. 메시지는 최선의 노력을 다하는 것을 근간으로 삼아 네트워크에 전파되고, 노드는
네트워크에서 언제든 이탈했다가 재접속할 수 있으며,
이탈한 기간 동안에는 가장 긴 작업증명 체인을 받아들이면 된다.



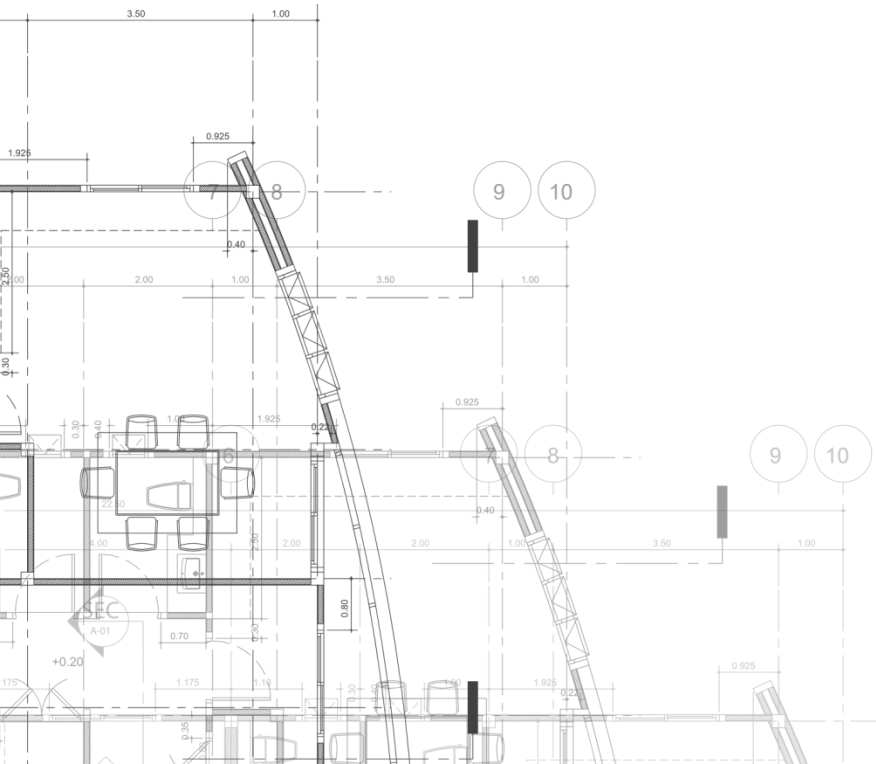
04 해결책

4-1 RUEDA COIN 블록체인 TECHNOLOGY

제3자의 개입 없이 이루어지는 결제 시스템의 블록체인 기술

온·오프라인 상의 거래는 대부분 금융기관을 신뢰받는 제3자의 역할로 사용하는 지불 방식에 의존하고 있다. 이러한 시스템은 일상 대부분의 거래에 무리 없이 작동하지만, “신뢰를 기반”으로 한 구조라는 약점을
가지고 있다. 금융기관의 형태는 중재를 위한 분쟁을 피할 수 없어 완벽하게 취소가 불가능한 거래를
보장하기 어렵다. 게다가 중재에 사용되는 비용은 거래 비용의 상승, 최소 거래량의 제한, 작고 간단한 거래의 원천적인 봉쇄와 같은 문제를 야기하게 된다. 결국 취소가 불가능한 서비스를 필요로 하는 지불 방식을 만들지 못해 더 많은 비용을 소진하게 된다. 거래 취소가 가능한 구조는 일반적으로 더 많은 신뢰를 필요로 하게 된다. 판매자는 고객을 더 경계하게 되어 더 많은 정보들도 요구하게 될 것이다.
그렇기 때문에 거래 내 사기가 발생하게 되면 이 모든 부담을 고객이 안고 갈 수 밖에 없다. 이러한 비용의 증가와 지불의 불확실성 증가는 실물 화폐를 사용하여 거래를 한다면 해결될 문제이지만, 이렇게 처리하게 되면 신뢰기간 없이 통신 채널만을 통해 지불하는 방법이 없다는 것과 같다.

신용 기반이 아닌 암호화 기술에 기반한 전자 지불 시스템을 이용하면, 신뢰받는 제3자 없이 당사자간의 직접 거래가 가능해진다. 전산을 통해 취소가 불가능한 거래는 판매자를 사기로부터 보호할 수 있으며, 에스크로 방식을 통해 구매자도 보호할 수 있다.



04 해결책

4-1 RUEDA COIN 블록체인 TECHNOLOGY

거래

전자 화폐를 디지털 서명이 연결된 것으로 정의해 보면, 소유자들은 이전 거래와 다음 소유자의 공개키를 해시하여 전자 서명하고 이를 코인 뒤에 붙이는 형태로 전송한다. 수취인은 체인의 소유권을 확인하는 것으로 서명을 검증할 수 있다.

문제는 수취인의 입장에서 원 소유주가 이중지급을 하였는가, 하지 않았는가 검증하지 못한다는 것이다. 보편적인 해결책은 거래가 이중지급 되었는지 확인하는 신뢰할 수 있는 중앙기관 혹은 조폐국을 두는 것이다. 거래가 발생하면 모든 코인은 조폐국으로 들어가 새 코인이 발행되도록 하고, 조폐국을 거친 거래만을 유효한 것으로 인정하면 이중지급의 위험에서 벗어날 수 있다. 이 방식의 문제는 전체 시스템의 운명이 모든 거래에 개입하는 조폐국을 운영하는 주체에 달려있다는 점이다.

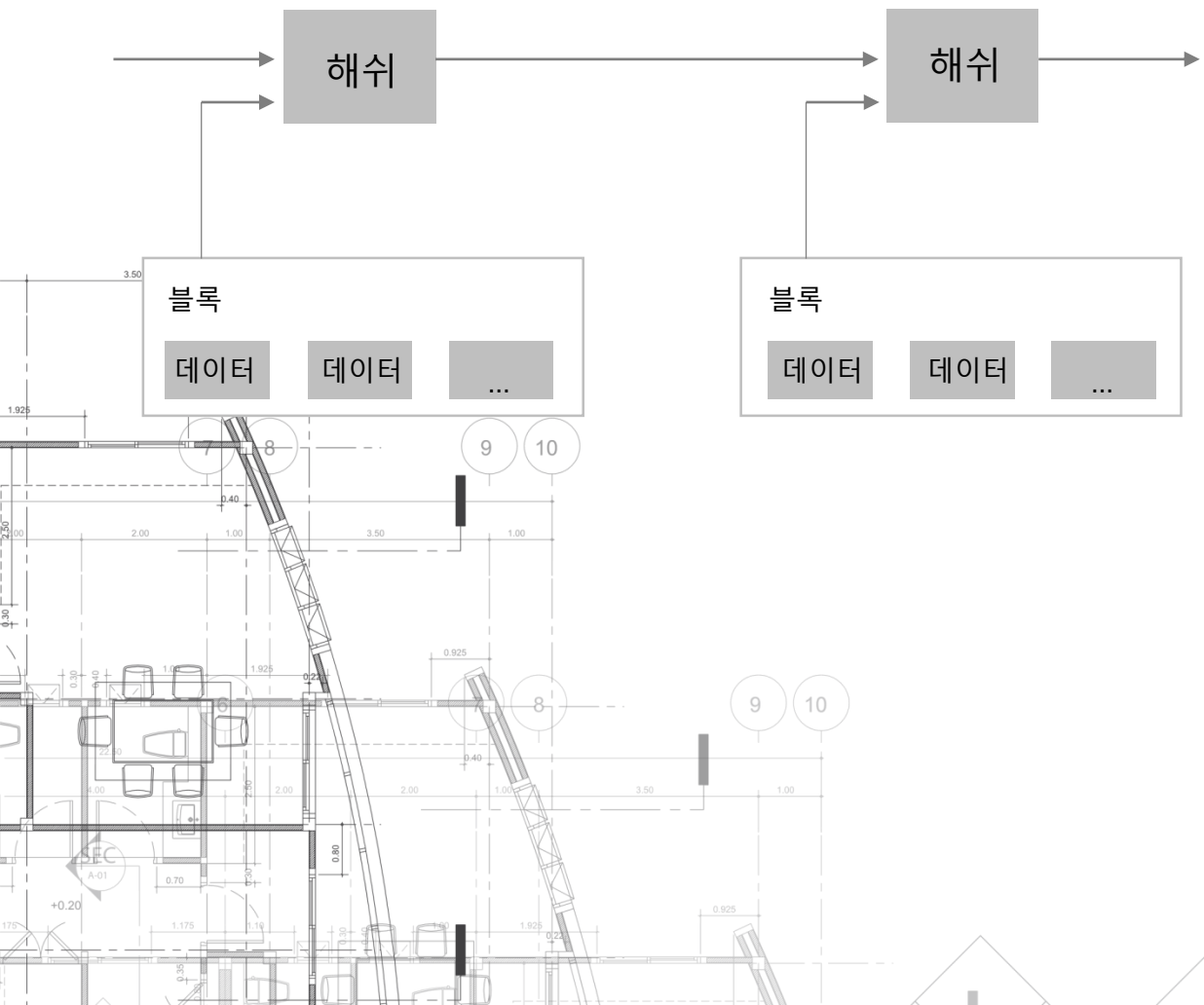
수취인의 입장에서 이전 소유자가 어떤 거래에도 서명을 사용하지 않았다는 것을 확인할 방법이 필요하다.
이를 위해서는 해당 서명을 사용한 가장 최초의 거래만 계산하면 뒤이어 이어지는 거래에 이중지급이 있는가를 굳이 확인할 필요가 없다. 또한 누락된 거래가 있는가를 확인하는 유일한 방법은 모든 거래를 확인하는 것이다. 조폐국을 기반으로 한 모델에서는 조폐국이 모든 거래를 확인하여 어떤 거래가 먼저 이루어진 것인지 결정해주면 된다. 이를 조폐국처럼 신뢰받는 주체가 없는 상태에서 해결하고자 한다면, 거래는 공개적으로 알려져야 하며, 참가자들이 받는 것을 순서대로 정리한 단일한 이력을 사용하는 시스템이 필요하다. 수취인은 거래가 발생하면 노드의 대다수가 이중 수취가 아닌 최초의 수취라고 인정하는 증명을 필요로 한다.

04 해결책

4-1 RUEDA COIN 블록체인 TECHNOLOGY

타임스탬프 서버 (Time StampServer)

제시하려는 해결책은 타임스탬프 서버에서 시작 된다. 타임스탬프 서버는 시간 순으로 기록된 블록들의 해시를 취하고, 신문이나 유즈넷 포스트[2-5]처럼 해시를 발행하는 역할을 한다. 타임스탬프는 해시의 형태로 취합되기 위해 해당 시간에 그 데이터가 존재했음을 증명해야 한다. 각각의 타임스탬프는 이전 타임스탬프 해시의 형태로 포함하는 구조로 결국, 각 타임스탬프는 이전 타임스탬프를 강화하는 형태로 체인을 형성한다.



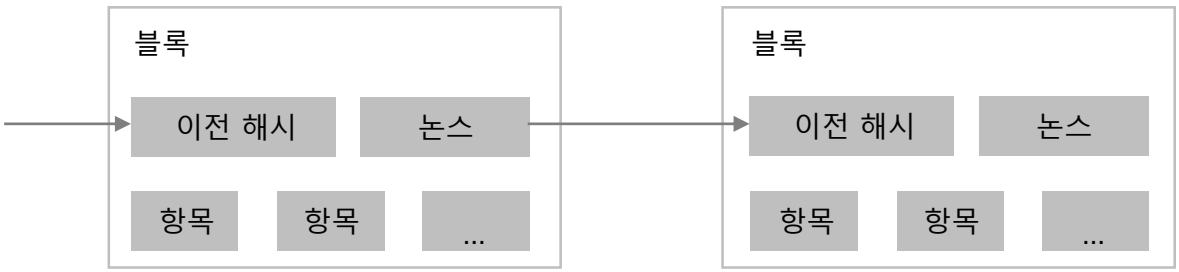
04 해결책

4-1 RUEDA COIN 블록체인 TECHNOLOGY

작업 증명 (Proof – of – work)

P2P를 기반으로 한 분산형 타임스탬프 서버를 실현하기 위해서는 유즈넷이나 신문 등의 방식이 아니라,
Adam Back의 Hashcash[6]와 유사한 작업증명 시스템을 이용해야 한다. 작업증명 방식은 SHA-256 같은 알고리즘을 통해 해시 되었을 때 0(Zero)으로 시작되는 값들을 찾는 과정을 수반한다. 해시를 한번 수행하는 것으로 확인하는 이 작업의 소요 시간은 어떠한 평균치에 수렴하며, 요구하는 0의 숫자가 많을수록 소요 시간이 지수의 형태로 늘어나는 특성을 가진다.

타임스탬프 네트워크는 블록 해시를 수행한 결과 만족하는 0 Bit를 가질 때까지 임의의 값인 논스(Nonce)를 증가시키는 방식으로 작업증명을 구현한다. CPU가 노력한 결과가 작업증명 조건을 충족하게 되면,
이 블록은 수행한 작업증명과 같은 노력의 일을 반복하지 않는 한 변경할 수 없다. 하나의 블록을 변경하려면 해당 블록에 연결된 모든 블록에 작업증명을 다시 진행해야 한다.



또한, 작업증명 방식은 다수결 의사결정에서 대의(代議)의 문제를 해결한다. 만약, IP 주소당 하나의 투표권을
부여하게 되면 누구나 IP 주소를 많이 확보하는 것만으로 시스템을 전복시킬 수 있다. 이에 반해, 작업증명은 연산 능력에 비례하여 투표권을 주는 것이다. 가장 긴 체인은 가장 많은 연산능력(작업증명)을 포함하고 있으므로 이것이 곧 다수의 결정이 된다. 정직한 노드들이 연산능력의 대부분을 차지하고 있다면, 정직한 체인이 가장 빠르게 늘어나 여타 경쟁 체인을 압도할 것이다. 과거의 블록 한 개를 수정하려면 공격자는 해당 블록과 이후의 모든 블록에 작업증명 과정을 수행하여 정직한 노드의 블록 길이를 추월해야 한다. 느린 공격자가 블록을 따라잡을 가능성은 뒤에 추가로 언급하겠다.

증가하는 하드웨어 속도와 노드를 실행하는 동기를 보상하기 위해 작업증명의 난이도는 시간당 생성되는 블록의 이동평균을 통해 정해진다. 만약 블록이 빠르게 생성되면, 난이도는 증가한다.

04 해결책

4-1 RUEDA COIN 블록체인 TECHNOLOGY

네트워크 (Network)

네트워크는 아래와 같은 과정으로 동작한다.

1. 새로운 거래들이 전체 노드들에게 전파된다.
2. 각 노드들은 새 거래들을 블록에 취합한다.
3. 각 노드들은 블록에 가장 어려운 난이도로 행해진 작업증명을 찾는다.
4. 노드가 새로운 작업증명을 발견하면 해당 블록을 전체 노드에 전파한다.
5. 노드들은 모든 거래가 유효하고, 이미 사용되지 않은 경우에만 블록을 받아들인다.
6. 노드들은 체인 위의 다음 블록에 이전 블록을 해시 형태로 추가하는 것으로 해당 블록을 받아들였다는 의사를 표현한다.

노드들은 항상 가장 긴 체인을 옳은 것으로 간주하고 인증된 체인을 이어간다. 만일 두 개의 노드가 각기 다른 버전의 다음 블록을 동시에 전파하는 경우, 다른 버전의 블록을 전달받는 노드들이 발생한다. 이 경우, 먼저 전달받은 블록을 기준으로 작업을 수행하지만, 다른 갈래의 블록도 저장하여 해당 블록이 더 길어질 것에 대비한다. 다음 작업증명이 완료되어 둘 중 하나가 더 긴 체인이 되는 경우 더 이상 두 블록은 대등하지 않고 긴 체인을 형성한 블록을 기준으로 작업한다. 새로운 거래는 꼭 모든 노드에 전파될 필요는 없다. 최대한 많은 노드에 도달한다면 이 거래는 블록이 길어지기 전에 포함될 것이다. 블록의 전파가 누락되는 경우에도 크게 걱정할 필요가 없다. 만약 노드가 중간 블록을 전달받지 못하더라도, 이를 요청하여 받게 되면 정상적인 체인을 만들 수 있다.

보상 (Incentive)

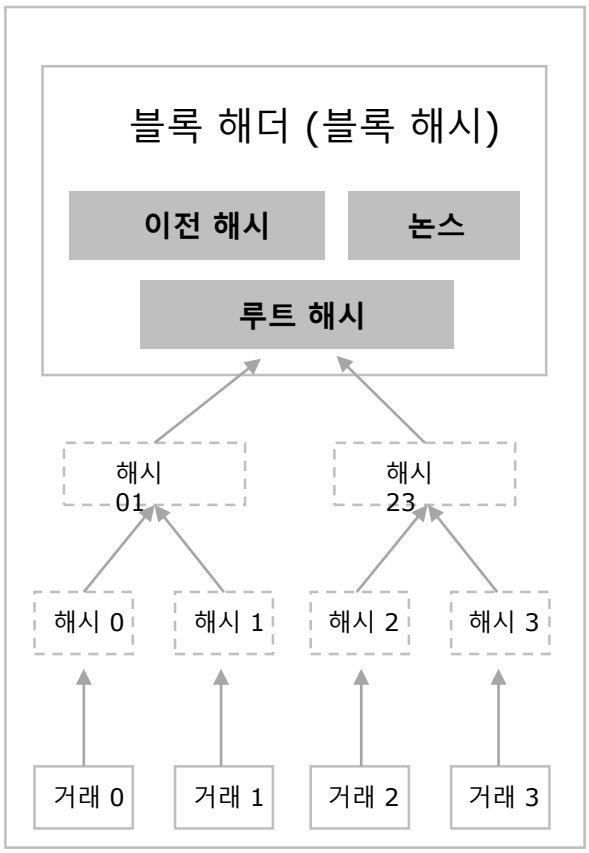
블록의 첫 거래는 블록의 생성자에게 새로운 코인을 보내는 특별한 거래가 된다. 이는 네트워크를 유지하는 노드들에게 보상이 되고, 중앙관리기구 없이 분산된 형태로 유통되는 구조를 만들 수 있다. 새로운 코인이 지속적으로 공급되는 것은 흡사 금광을 캐는 광부들이 자원을 소진하여 금의 순환구조를 만드는 것과 비슷하다. CPU 사용 시간과 전력이 소비되는 자원에 해당한다.
거래 수수료도 보상 중 하나이다. 거래에서 출력되는 돈보다 입력되는 금액이 작다면 그 차이는 거래 수수료의 형태로 블록을 생성하는 보상으로 추가된다. 초기 예상 발행량의 전부가 발행된 이후에는 거래 수수료만 보상으로 주어지며, 인플레이션에서 벗어날 수 있다.
이러한 보상 체계는 노드들이 선의의 행동을 하도록 독려해야 한다. 만약 이기적인 공격자가 선의의 노드보다 많은 연산능력을 끌어모을 수 있다면, 다른 이의 지불을 갈취하거나, 새로운 코인을 생성하여 사적인 이익을 취하려 할 것이다. 하지만 이러한 방법보다 정해진 규칙에 순응하는 것이 더 많은 코인을 가져다주기 때문에 공격자가 굳이 공격해야 할 이유는 없다.

04 해결책

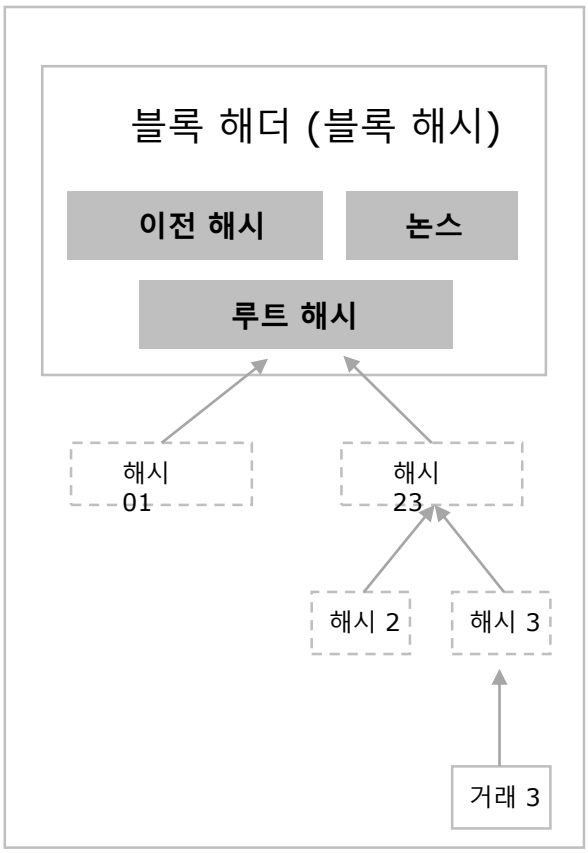
4-1 RUEDA COIN 블록체인 TECHNOLOGY

저장 공간의 재 사용 (Reclaiming Disk

코인을 기준으로 충분히 많은 블록이 이어지게 되면 지난 거래 내역은 저장 공간의 확보를 위해 폐기해도 된다. 블록 해시를 깨지않고 이를 가능하게 하려면 거래가 머클 트리(Merkle Tree) [7] [2] [5] 안에 해시되고, 머클트리의 루트 부분만 블록 해시에 포함되면 된다. 오래된 블록은 나무의 가지를 친 것처럼 최소화할 수 있다. 내부의 해시는 저장될 필요가 없다.



머클트리 형태로 해시된 거래



블록에서 거래0, 거래1, 거래2를 제거한 경우

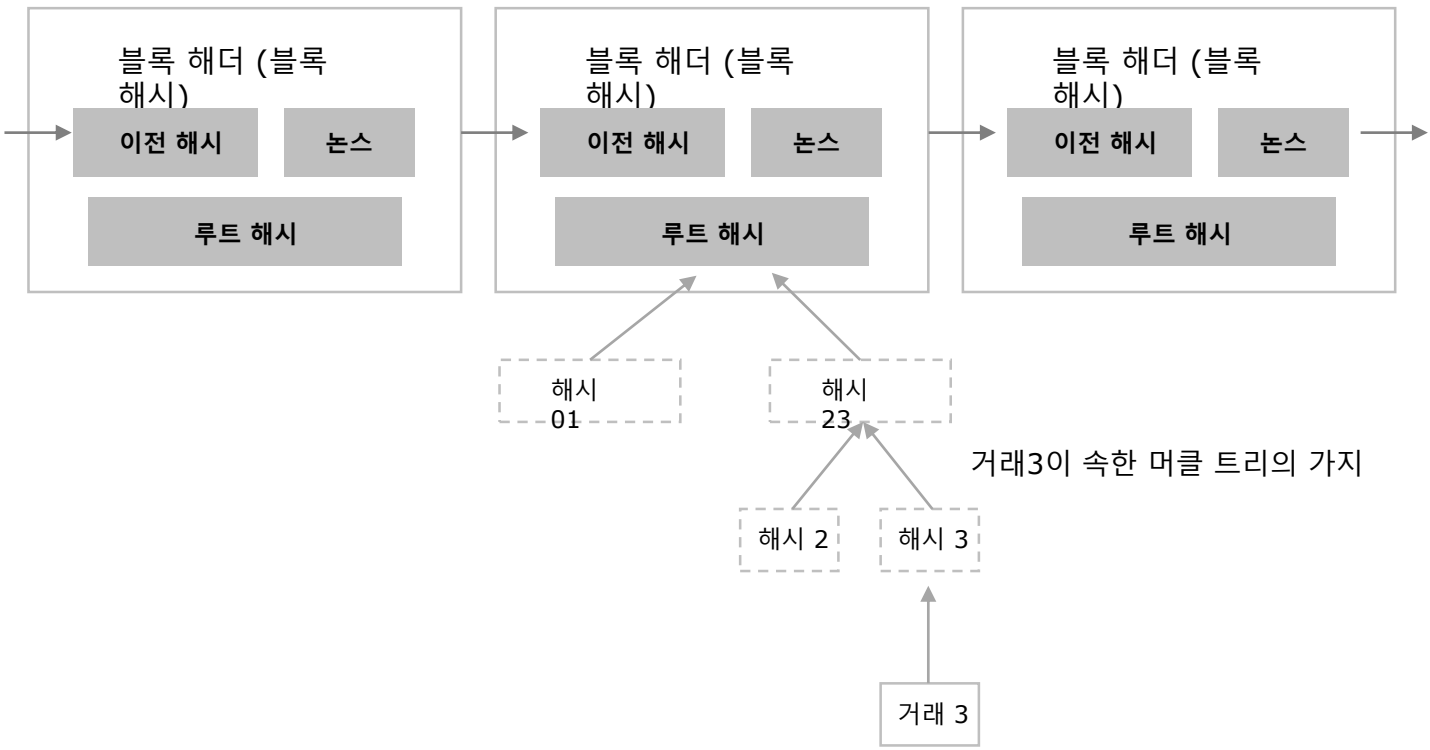
거래가 하나도 포함되지 않은 블록의 헤더는 80바이트(Byte)이다. 만약 블록이 매 10분마다 생성된다고 가정하면, 연간 소요되는 데이터는 80 Bytes x 6 x 24 x 365 = 42MB가 된다. 2008년에 보편적인 컴퓨터가 2GB 램(RAM)을 장착하고 있으며, 무어의 법칙에 따라 현재 기준으로 1.2GB가 1년에 증가하므로, 블록 헤더가 메모리에 저장되더라도 큰 문제가 되지 않는다.

04 해결책

4-1 RUEDA COIN 블록체인 TECHNOLOGY

지불 검증의 간소화 (Simplified Payment

풀 노드(Full Network Node)를 운용하지 않더라도 지불을 검증하는 것은 가능하다. 사용자가 자신이 가장 긴 체인임을 확인할 수 있을 때까지 네트워크 노드들에게 요청하여 가장 긴 작업증명 체인의 블록 헤더의 사본(Copy)을 가지고 있으면 해당 거래가 포함된 블록의 머클트리의 가지(Branch)를 얻어올 수 있다. 사용자 스스로 거래의 유효성을 체크할 수 없으나, 체인에 연결된 것을 확인하고, 네트워크 노드들이 이를 받아들이는지 확인한 뒤, 블록이 뒤에 연결되는지 확인하면 할 수록 네트워크가 이를 유효한 것으로 인식하는지 확신할 수 있다.



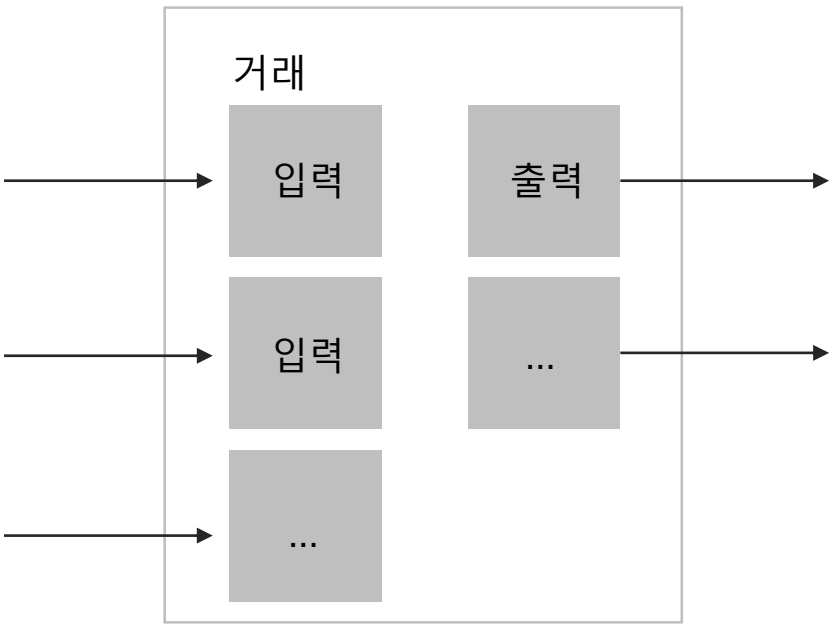
정직한 노드들이 네트워크를 제어하는 상태에서 이루어지는 검증 작업은 신뢰할 수 있으나, 공격자의 힘이 강한 네트워크에서는 신뢰가 어렵다. 네트워크 노드들이 검증 절차를 가지고 있다하더라도, 공격자가 지속적으로 네트워크에서 힘을 유지하고 기록을 날조하여 잘못된 거래 내역을 퍼뜨리면 속을 수 밖에 없다. 이러한 문제를 막기 위한 하나의 방편은, 사용자의 소프트웨어가 블록 전체를 다운로드 받아 모순점이 있는지 확인할 수 있도록 하고, 유효하지 않은 블록을 발견했을 때 네트워크 노드들에 경고성 알림을 보내는 것이다. 이런 면에서, 잦은 거래를 필요로 하는 사업분야에서는 빠른 검증과 독립적인 보안체계를 유지하기 위해 자신의 노드를 직접 운용하는 것을 원할 것이다.

04 해결책

4-1 RUEDA COIN 블록체인 TECHNOLOGY

가치의 병합과 분할 (Combining And Splitting

코인을 중심으로 개별적 관리를 하는 것도 가능하지만, 이는 작은 단위의 거래를 하기에는 불편하다. 가치가 나누고 합쳐질 수 있도록 하기 위해 다수의 입력과 다수의 출력을 허용한다. 보통, 큰 규모의 단일 입력이거나 다수의 소액을 합친 입력일 것이며, 출력은 지불을 위한 것 하나와 남는 잔액을 송금자에게 돌려주는
출력 두 개일 것이다.



하나의 거래가 여러 거래로 부터 비롯되고, 이 거래들은 더 많은 거래로 부터 비롯되는 팬아웃(Fan-Out) 형태는 여기서 문제가 되지 않는다. 거래 기록의 완전한 독립 사본을 추출할 필요가 없기 때문이다.

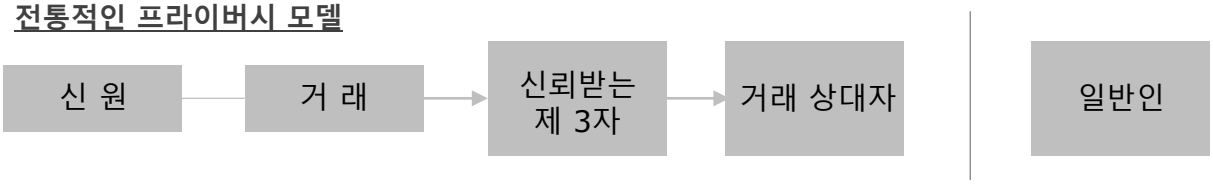
04 해결책

4-1 RUEDA COIN 블록체인 TECHNOLOGY

프라이버시

기존의 은행 구조는 담당하는 그룹과 신뢰받는 제3자의 정보 접근 권한을 제한하는 방식으로 프라이버시를 보호한다. 모든 거래를 공개하는 방식에서 은행 형태의 모델을 차용할 수는 없지만 프라이버시를 유지하면서 모든 거래를 공유하는 것이 불가능한 것은 아니다. 공개 키들을 익명으로 사용하면 된다. 참여자 누구나 어떤 이가 다른 이에게 얼마를 보냈는지 확인할 수 있지만, 정작 거래가 누구에게 귀속되는 지에 대한 정보는 공개하지 않는 방식이다. 이는 증권 거래소에서 정보를 공개하는 것과 비슷하다. 시간과 거래량은 공개되지만 누구의 거래인지 알 수 없는 것처럼.

전통적인 프라이버시 모델



새로운 프라이버시 모델

추가적인 방화벽으로서, 매 거래 마다 새로운 키를 사용하도록 하여 소유자 분별이 어렵도록 한다. 다수의 입력이 존재하는 거래일 경우 입력들이 동일한 소유자에서 온 것이 밝혀질 수도 있다. 만약 소유자의 키가 공개되면, 다른 거래의 것도 동일한 소유자라는 것이 밝혀질 수 있다는 위험성이 있으므로 새로운 거래를 수행 시 매번 새로운 키를 사용하도록 권장한다.

04 해결책

4-1 RUEDA COIN 블록체인 TECHNOLOGY

계산 (Calculations)

공격자가 정직한 체인보다 빠르게 체인을 이어가려는 경우를 생각해보자.
이 공격이 성공한다 해도 시스템에 없던 돈을 새로 만들어내거나 하는 식의 제멋대로인 상태로 망가뜨릴 수는 없다. 노드들은 유효하지 않은 거래는 받아들이지 않을 것이고, 정직한 노드는 아예 해당 내용을 블록에 포함하는 것조차 허용하지 않는다. 공격자는 오직 자신이 행한 거래의 돈을 되찾는 공격만 가능하다.
정직한 체인과 공격자 체인의 경쟁은 이항무작위행보(Binomial Random Walk)의 특성을 지닌다. 정직한 체인이 블록 한 개를 성공적으로 생성하는 사건에 +1을 부여하고, 공격자 체인이 블록 한 개를 성공적으로 생성하는 사건에 -1을 부여한다고 생각해보자.

공격자가 적자의 상태에서 시작하여 선의의 체인을 따라잡을 가능성은 도박사의 파산 문제(Gambler's Ruin Problem)와 유사하다. 적자 상태의 도박사가 무제한의 신용을 바탕으로 무한대로 게임을 시도하여 손익분기점에 도달했다고 생각했을 때, 손익분기점에 도달할 확률, 혹은 공격자가 정직한 체인을 따라잡을 확률은 다음과 같이 계산할 수 있다.

p = 정직한 노드가 다음 블록을 찾을 확률

q = 공격자가 다음 블록을 찾을 확률

q_z = 공격자가z 개의 블록이 뒤떨어진 상태에서 따라잡을 확률

$$q_z = \begin{cases} 1 & if \ p \leq q \\ [\, q/p \,]^z & if \ p > q \end{cases}$$

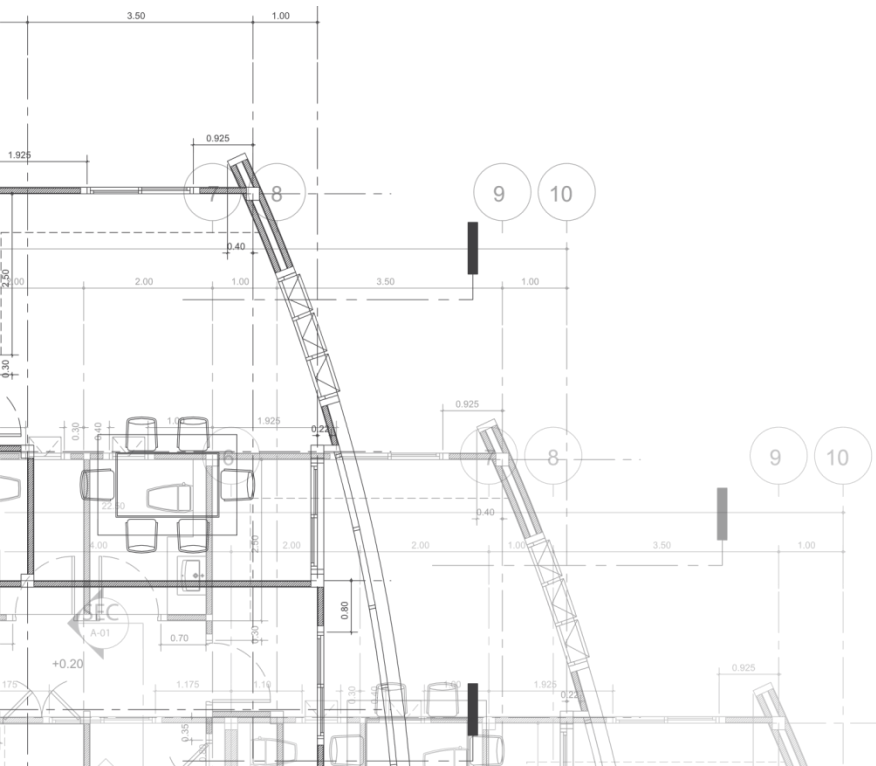
p>q 라 가정한다면, 공격자가 블록을 따라잡을 확률은 블록 수의 증가분에 지수로 감소 한다. 공격자가 가능한 빨리 시도하여 운 좋게 성공하지 못한다면, 가능성은 뒤로 갈수록 희박해 진다. 수신자의 입장에서 송금자가 수신자로 하여금 일정 기간동안 자신은 돈을 받았다고 믿도록 하다가 다시 돈을 자신에게 되돌리는 시도를 할 것이다. 수신자는 이에 대한 경고를 받겠지만 공격자는 이미 늦은 상태에서 알림을 받게 하길 원한다.

04 해결책

4-1 RUEDA COIN 블록체인 TECHNOLOGY

결론

지금까지 신뢰에 기반하지 않은 전자 거래 시스템을 제안하였다. 전자 서명으로 이루어진 일반적인 형태는 소유권에 대한 강한 통제권을 제공하지만, 이중지급을 막지 못하면 불완전할 수밖에 없다. 이를 해결하기 위해 작업증명을 이용하여 공개적으로 거래를 기록하는 P2P 네트워크를 제안하였다.
이 방식은 정직한 노드들이 다수의 연산능력을 확보하고 있다면 공격자가 쉽게 조작하는 것이 불가능하다.
이 네트워크는 간결함을 기반으로 함에도 견고하다. 노드들은 약간의 협력만으로 합일이 가능하다. 특정한 위치까지 메시지가 전달되지 않더라도 최선을 다하는 것을 기반으로 전달되기만 하면 되기 때문에, 신원을 밝힐 필요도 없다. 노드들은 언제든지 네트워크에서 이탈했다가 재접속 할 수 있으며, 그들이 이탈한 동안 이루어진 작업증명의 체인을 받아들이기만 하면 된다. 유효한 블록의 뒤에는 블록을 연장하고, 유효하지 않은 블록은 거부하는 행위를 통해 작업증명 연산 능력은 참여자들의 의사 표현의 수단이 된다.
이러한 합의 구조는 규칙이나 보상과 함께 제시된다.



04 해결책

4-2 APP 전자 지갑 / POS 시스템

APP 전자 지갑

루에다 코인 지갑은 메신저 플랫폼 기반으로 동작한다. 루에다 코인 지갑은 보안성이 뛰어난 P2P 기반 메신저로, 사용자가 친숙한 메신저 인터페이스를 가지고 있다. 친구와 대화하듯이 편리하기 코인을 주고 받으며, 지불결제 수단으로 활용할 수 있다.
또한 루에다 코인의 기본 설계 사상인 개인 간의 대화는 개인 만이 확인할 수 있어야 한다는 것이 암호화폐의 기본 사상과 일치되는 바, 전자지갑 APP를 코인 지갑의 기본 어플리케이션으로 이용하는 것이 암호화폐 거래의 익명성을 보장하고 거래의 안정성을 담보할 수 있는 기본 어플리케이션으로 손색없다.

P2P 메신저 플랫폼

루에다 코인의 메신저 플랫폼은 서버에 메시지를 저장하지 않는 P2P 기반의 메신저 플랫폼이다. 이 플랫폼은 서버에 사용자의 대화내용을 저장하지 않고, 단순하게 중계만 하는 P2P 기반 플랫폼이다. 루에다 코인 메신저는 디바이스와 디바이스 간에 직접 통신을 하는 방식이며, 모든 사용자의 대화는 사용자의 개인키를 이용하여 암/복호화 되므로 통신 구간 감청 및 서버에서 대화의 내용을 확인하는 것이 불가능하다.

루에다 코인 APP 전자 지갑 기능

루에다 코인은 사용자에게 친숙한 메신저 플랫폼이다.
전화번호만으로 간편 가입이 가능하고, 1:1 대화하기, 그룹대화 등이 가능하다. 또한 소액 해외 송금을 위한 트랜스퍼와 연계하여 저렴하고 신속한 해외 송금이 가능하다.

04 해결책

4-2 APP 전자 지갑 / POS 시스템

루에다 코인 APP 전자 지갑 주요 특징

◆ 보안성

루에다 코인은 보안에 완벽한 P2P 메신저이다. 서버는 단순 중계만 할 뿐 모든 사용자 간의 대화는 디바이스 간에 P2P 방식으로 이루어진다.

- 암 / 복호화 알고리즘
- 개인키는 루에다 어플리케이션 내에 안전하게 암호화 되어 저장된다.
- 모든 대화는 AES256으로 암호화 되어 송수신 되고, 최종 단말 단에서 암/복호화가 이루어지기 때문에 통신 구간에서 감청이 안전하다.
- 어떠한 경우에도 서버에 사용자간 대화가 저장되지 않는다.

◆ 간편성

- 사용자의 핸드폰 번호만으로 간편가입이 가능하다.
- 핸드폰 번호 이외에 어떠한 정보도 사용자에게 요구하지 않는다.
- 일반적인 메신저의 인터페이스를 가지고 있어, 사용자가 쉽게 사용할 수 있다.

◆확장성

- 루에다 코인은 메신저 플랫폼으로 다양하게 확장이 가능하다.
- 루에다 코인 지갑 뿐만 아니라, 해외 소액 송금, 쇼핑몰, 지불 시스템 연계 등이 가능하도록 개방형 아키텍처로 되어있다.

04 해결책

4-2 APP 전자 지갑 / POS 시스템

POS 시스템

가맹점 코드로 로그인	루에다 코인 가맹점 등록. 가맹점 코드 발급
내 스마트폰이 POS 단말기	별도의 POS 단말기 설치가 필요 없이 루에다 코인 POS APP 하나로 OK
간편 결제	P2P 방식의 결제로 QR 코드 스캔 한 번으로 결제 완료
상품 등록 및 관리	판매 상품 등록은 물론 기존 등록 상품의 관리도 간편하게 가능
매출 관리 및 재고 관리	요일, 시간 대 별 매출 파악으로 효율적인 점포 운영 가능
고객 관리	효율적인 고객 관리를 통해 효과적인 마케팅

05 ROAD MAP

루에다 코인

2019

- 시장 및 자료 조사
- 백서 컨셉 및 백서 작성
- 백서 및 토큰 컨셉 확정

2020 1Q

- 토큰 연구 개발 및 블록체인 생성
- 국내 메이저 거래소 상장 진행

2020 3Q

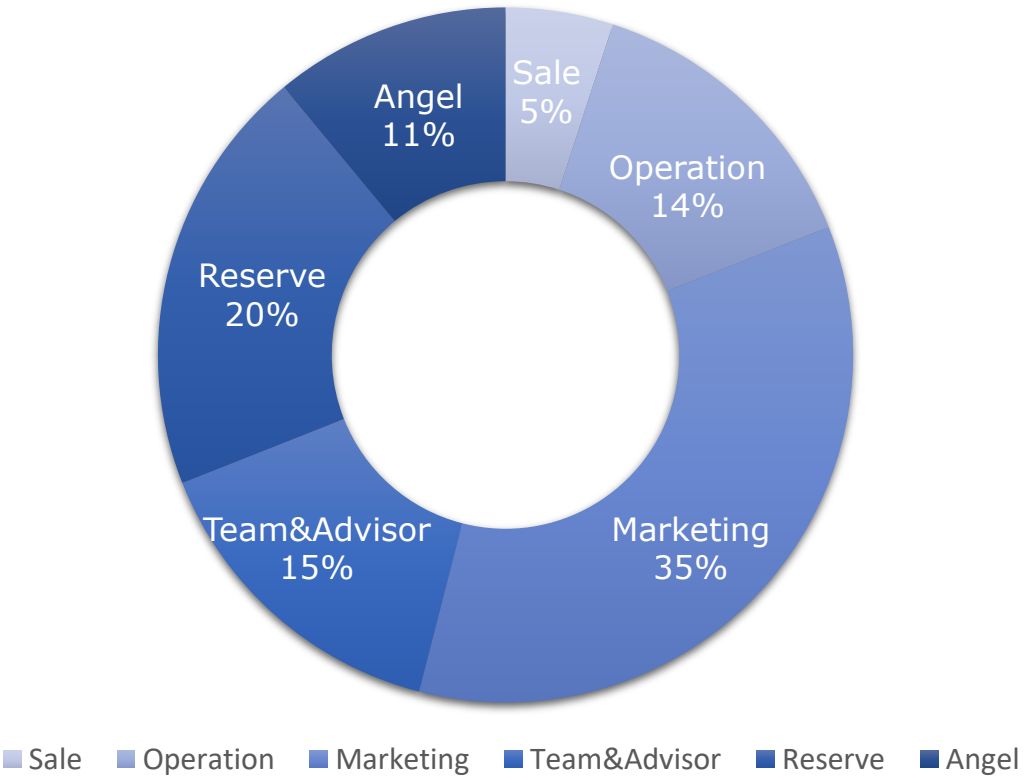
- 해외 거래소 상장 제안

실적

- 구로 항동 우남아파트 부대토목공사 (우남건설 ㈜)
- 마곡 넥센타이어연구소 부대토목공사 (쌍용건설 ㈜)
- 일산 차병원 신축공사 부대토목공사 (쌍용건설 ㈜)
- 수인선 인천 논현역 부속시설 증축공사 (한길종합건설 ㈜)
- 광명 15R구역 재정비 주택재개발 정비사업 (대우건설 ㈜)
- 구로항동 택지조성사업 (서울시)
- 원종동 오건아파트 재건축사업 (한길종합건설 ㈜)

06 TOKEN Allocation

토큰 분배 기간동안 계약서를 통해 루에다 코인이 발행될 계획이다. 발행되는 전체 코인의 80% 정도의 코인은 6개월~1년 동안 락업 형태로 소유되며, 락업 기간동안 코인 보유자는 코인을 팔 수 없게 된다. **<u>이는 모두 예상치이며 변동 가능성이 있다</u>**.



총 발행 수량: 20억개

RUEDA