



백서 **2018**



+11,000.00

목차

중요 사항

1. 서론.....	6	2) 금융기관.....	19
2. 업계 개요.....	8	3) 사용자 기능.....	19
1) 글로벌 금융기관 결제시스템 - 블루 스카이 시장.....	8	a. 계정 설정 및 관리.....	20
2) 현행 자금이체 방식.....	9	i. 송금인 데이터 검증.....	20
3) 현행 자금이체 과정 내의 정보.....	11	b. 거래 관리.....	20
4) 업계 규제.....	11	c. 아이비코인 구매, 매도 및 이체.....	20
a. 금융기관의 자금세탁방지("AML").....	11	6. 아이비코인 기술 사양.....	22
b. 자금세탁방지법의 파급 효과.....	12	1) 기술적 아키텍처 개요.....	22
c. 추가 정보의 이점.....	12	a. 공용망, ivySend 및 공용 아이비코인 토큰(IVYA).....	24
3. 아이비코인의 기회 - 뛰어난 고도의 와해성 기술.....	13	b. 사설망, ivyReceive 및 사설 아이비코인 토큰(IVYB).....	24
1) 기존 금융시스템과의 비교.....	13	c. 체인 간의 통신 및 아이비코인 오라클(Oracle) 서비스.....	25
2) 경쟁 암호화폐와의 비교.....	15	2) 아이비코인 네트워크상의 신원.....	26
4. 성공적인 실적을 보유한 세계 최고 수준의 팀.....	17	a. 송금인의 신원.....	26
5. 아이비코인 운영 사양.....	18	b. 금융기관 및 중개기관의 신원.....	26
1) 운영 플랫폼 개요.....	18	3) 블록체인 기술 응용.....	26
a. 기본 기능.....	18	4) 아이비코인 데이터 컨테이너.....	28
b. 불변화폐 네트워크에 대한 피어투피어(Peer-to-Peer) 방식 암호화폐.....	18	a. 아이비코인 데이터 컨테이너 생성 및 저장.....	29
c. 소프트웨어 통합.....	18	b. 아이비코인 데이터 컨테이너에 대한 액세스.....	29
d. 캐시어(Cashier) 및 전환 서비스.....	18	7. 토큰 생성 이벤트 이후의 토큰 구조.....	30
e. 공개시장조작을 통한 고정가격 이체.....	19	8. 로드맵.....	32
		a. 토큰.....	32
		b. 운영.....	32
		10. 위험.....	34
		용어해설.....	37

중요 사항

본 문서는 아이비코인 기술의 현재와 미래 개발 동향을 설명하는 기술 백서입니다. 본 문서는 정보공개서가 아닙니다. 본 문서는 Ivy Koin LLC(아이비코인 또는 당사)에서 발행할 프리세일(Pre-Sale) 약정서에 따라 부여되는 토큰(토큰)에 대한 권리(권리)를 통해 토큰(이후에 설명)을 구매할 기회를 검토할 목적으로 수신 당사자(수취인)에게 특별히 제공됩니다.

본 문서에 포함되어 있거나, 추후에 당사 또는 직원, 대리인, 컨설턴트에 의해 또는 이들을 대신하여 구두 또는 서면으로 수취인에게 제공되는 정보는 본 문서에 명시된 조건에 따라 제공됩니다.

본 문서는 대외비이며 당사의 사전 서면 동의 없이는 어떠한 형식으로도 복사 또는 유포할 수 없습니다.

수취인은 본 문서를 보유함으로써 본 문서의 조건을 읽고 이해하였으며 수락한다는 사실을 당사에 대해 인정하게 됩니다. 만일 수취인이 이 조건을 수락하지 않는 경우에는 즉시 본 문서를 당사에 반환해야 합니다.

본 문서는 오직 정보 제공의 목적으로만 작성되었고 수취인이 권리와 토큰의 취득 여부를 결정할 수 있도록 돕기 위한 것이며 해당 용도로만 사용할 수 있습니다. 본 문서는 2018년 1월 16일 기준 작성된 문서이며, 당시 입수 가능한 정보에 기초하여 당사가 작성 및 발행하였습니다.

본 문서의 목적은 투자나 신용 의사결정, 그 밖의 위험 평가를 위해 유일한 또는 주요한 근거를 제공하는 것이 아닙니다. 모든 수취인은 필요하거나 바람직하다고 판단되는 독립적인 조사를 토대로 권리와 토큰 취득에 관한 이해관계를 결정해야 합니다.

비록 당사가 본 문서를 작성하는 동안 충분한 주의를 기울였음에도 불구하고 당사 또는 그 고문은 본 문서에 포함된 정보의 정확성 또는 완전성과 관련하여 어떠한 진술이나 보증도 하지 않습니다. 본 문서 또는 그외 서면이나 구두로 수취인에게 전송되거나 제공된 의사소통상의 정보는 일체 약속이나 진술로서 신뢰하지 아니하며, 본 문서에 기재된 추정치, 예측, 예상의 정확성 또는 달성 가능성과 관련하여 어떠한 진술이나 보증도 하지 않습니다.

이러한 정보, 추정치, 예측, 예상과 관련하여 당사 또는 그 고문은 어떠한 책임도 지지 않습니다.

본 문서는 호주 증권투자위원회(ASIC)에 제출되지 않았으며 향후에도 동 기관에 제출되지 않을 것입니다. 본 문서는 수취인에게 정보를 제공하는 것만을 목적으로 하며, 회사법(Corporations Act 2001)(회사법) 또는 그에 준하는 타 관할지역 법령에 정의되거나 언급된 투자설명서(Prospectus), 약식 투자설명서 또는 기타 정보공개서에 해당하지 않습니다.

권리와 토큰을 구매할 가능성이 있는 사람은 본 문서를 전부 읽어야 합니다. 본 문서를 읽은 후에 궁금한 점이 있는 경우, 본 문서를 제공한 사람에게 문의해야 합니다. 당사는 절대적 제량에 따라 권리나 토큰의 판매 여부를 결정할 권리를 가집니다.

책임 배제

당사는 본 문서에 포함된 정보, 오류나 누락, 본 문서의 정확성 또는 신뢰성을 포함해(이에 국한되지 않음) 어떠한 식으로든 본 문서와 관련하여 수취인, 또는 기타 개인이나 법인에게 발생한 모든 손실 또는 손해에 대하여 일체 책임을 지지 않습니다.

면책조항

본 문서는 오직 정보 전달의 목적으로만 제공됩니다. 본 문서의 정보는 완전하지 않을 수 있고 당사에 의해 언제든지 변경, 수정, 개정될 수 있으며 당사의 진술과 보증에 해당하지 않습니다. 또한, 당사는 권리와 토큰 판매를 통해 조달한 자금을 적절하다고 판단되는 방식으로 사용함에 있어서 어떠한 제약도 받지 않습니다.

당사와 당사의 고문 모두 본 문서를 업데이트할 의도가 없으며 수취인에게 정보 접근을 허용하거나, 추가 정보를 포함시키거나, 본 문서 또는 그외 당사, 권리, 토큰과 관련하여 제공되는 정보의 부정확성을 수정해야 할 의무를 지지 않습니다.

당사의 사업은 최근에야 구축된 스타트업(Start-up) 사업이며 사업 및 전망 또는 토큰 개발 전망의 평가 근거가 될만한 주요 사업 이력을 갖추고 있지 못합니다. 그러므로 본 문서에 포함된 정보는 본질적으로 추측에 해당합니다.

추천 부인

본 문서는 권리 또는 토큰의 매수를 권고하지 않습니다. 권리 또는 토큰을 매수하려는 결정은 매수자 자신의 상황, 조사, 당사의 사업 및 전망에 대한 분석 및 평가, 권리와 토큰에 대한 분석 및 평가를 토대로 해야 합니다. 잠재적 매수자는 권리와 토큰 매수의 장점을 독자적으로 평가해야 하고 각자의 고문에게 자문을 구해야 하며 필요하다고 판단될 경우 추가 조사를 진행해야 합니다. 잠재적 매수자는 권리 또는 토큰의 취득에 높은 수준의 위험이 수반될 수 있다는 점을 주의해야 합니다.

본 문서의 어떠한 내용도 회사법 제766B조 상의 목적으로 개인적이든 일반적이든 금융상품에 관한 자문으로 해석해서는 안됩니다. 본 문서는 금융상품의 매수, 매도, 보유 여부에 관한 권고 또는 의견 진술을 포함하거나 암시하지 않습니다.

과세

권리 또는 토큰을 취득하면 과세 대상이 되며 과세 기준은 각 매수자의 개별 재정상황에 따라 달라집니다. 권리 또는 토큰의 모든 잠재적 매수자는 과세 관점과 일반적인 관점에서 권리·토큰의 취득에 따른 결과에 대하여 독립적인 재정자문을 구할 것을 권합니다. 법이 허용하는 최대한의 한도 내에서 당사, 임원 및 각 고문은 권리 또는 토큰의 매수에 따른 과세와 관련하여 어떠한 책임도 지지 않습니다.

달러

달러 명시하지 않는 한 모든 금액은 미국 달러로 표시됩니다.

한정적 진술

본 문서에서는 ‘예측’, ‘계획된’, ‘목표’, ‘믿음’, ‘잠재적’, ‘추정치’, ‘의도의’, ‘목표로 하다’와 같은 용어가 사용되었습니다. 이러한 진술은 현 시점에서 당사의 사업에 대한 이해와 해당 사업이 기대하는 목표에 근거를 두고 있습니다. 단, 이러한 진술을 하는 것에는 내재적인 위험이 있으며 잠재적 매수자는 해당 목표가 달성되지 못할 수도 있다는 전제 하에 권리 또는 토큰을 매수해야 합니다.

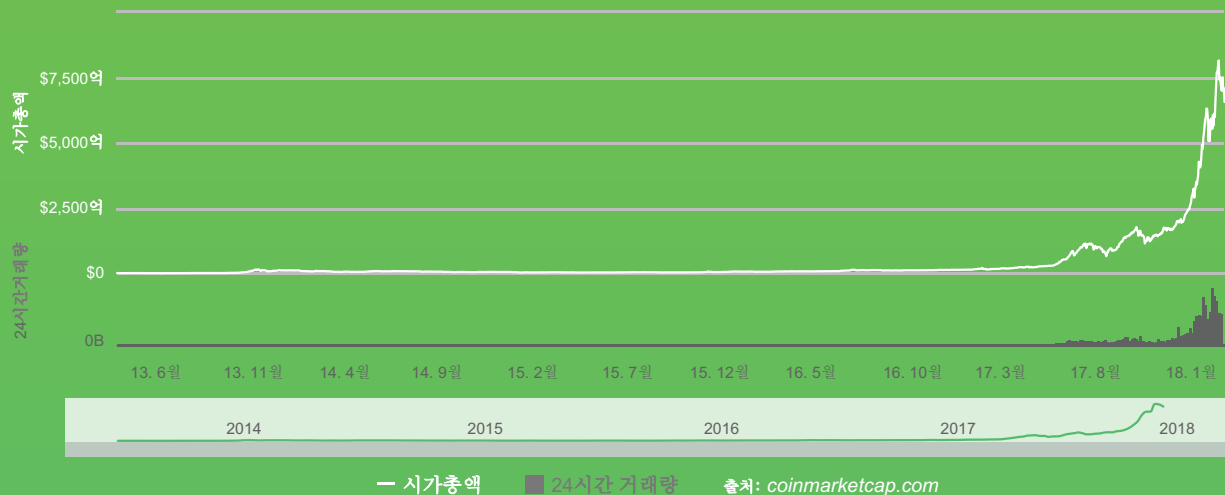
토큰의 유용성

당사는 마찬가지로 당사가 개발을 제안하고 있고 결제를 용이하게 해줄 디지털 플랫폼(아이비코인 네트워크)의 일부로 토큰을 사용할 것을 제안합니다. 구현될 경우, 토큰 보유자는 블록체인 기술의 보안성과 신뢰성을 갖춘 암호화폐 거래를 촉진하고자 금융기관이 만족할 만큼 자발적으로 거래 데이터의 익명성을 해제할 수 있습니다.

서론

1

암호화폐 시장은 급속도로 확장 및 심화되고 있으며, 세계 암호화폐시장 규모는 2018년 기준 7천2백억 달러입니다.¹⁾



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

글로벌 뱅킹·금융산업 내에 암호화폐 지원이 부족한 주된 이유는 현행 규정상 특정 거래 정보가 익명성과 충돌할 수 밖에 없기 때문입니다.

토큰은 금융기관과의 거래가 목적인 블록체인 기반 암호화폐가 될 것이며 이를 통해 스위프트(SWIFT) 프로토콜, 칩스(CHIPS), 페드와이어(Fedwire)와 같은 현행 기본결제시스템을 포함, 기존의 결제 네트워크보다 훨씬 많은 거래확인(Know Your Transaction, KYT) 및 고객확인(Know Your Customer, KYC) 정보가 결제시 포함될 것입니다.

토큰 보유자는 블록체인 기술의 보안성과 신뢰성을 갖춘 암호화폐 거래를 촉진하고자 금융기관이 만족할 만큼 자발적으로 거래 데이터의 익명성을 해제할 수 있습니다.

당사는 토큰이 어마어마한 기회를 가져다 줄 것이라고 전망합니다.

- 블루 스카이(Blue Sky) 시장
 - o 암호화폐 시장의 지속적인 성장 잠재력
 - o 글로벌 금융기관 거래의 보급 잠재력
- 고도의 와해성 기술
 - o 아이비코인 네트워크는 아이비코인에 가장 가까운 가상화폐이자 주요 글로벌 알트코인(Altcoin)인 리플(Ripple)에 비해 아키텍처가 향상될 것으로 기대됩니다. 리플의 현재 시가총액은 최대 1,240억 달러에 달합니다.²
- 실적 기록이 증명하는 세계 최고 수준의 팀 보유

당사는 아래에서 당사의 제안을 상세히 설명하고 토큰 보유자로 여러분을 맞이할 수 있기를 기대합니다.

Ivy Management Group LLC

2018년 1월 16일

1. <https://coinmarketcap.com/> 2018년 1월 9일 기준
2. <https://coinmarketcap.com/> 2018년 1월 7일 기준

2

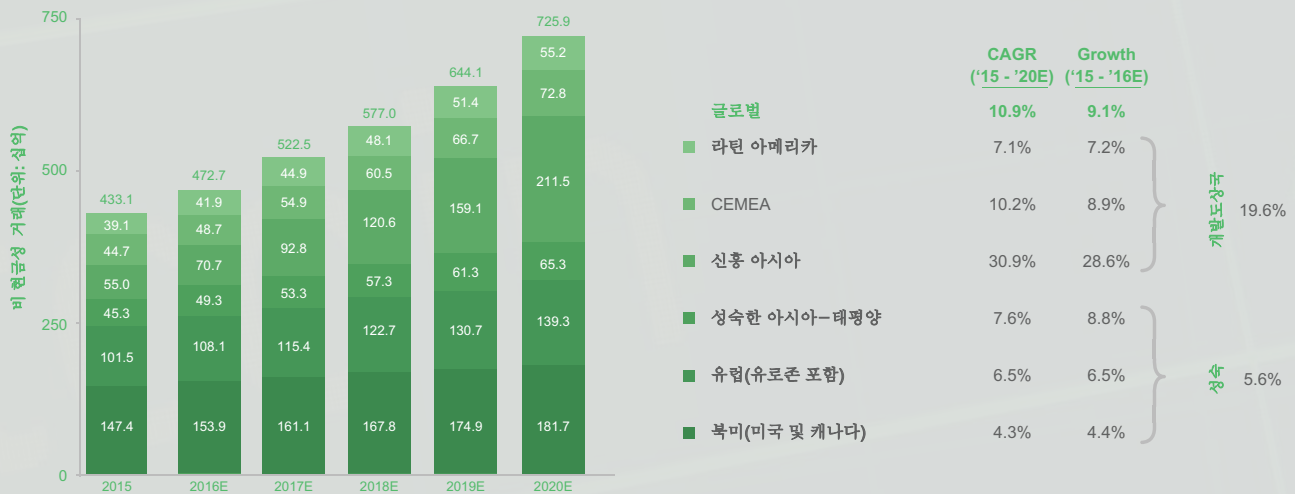
업계 개요

1) 글로벌 금융기관 결제시스템 - 블루 스카이 시장

글로벌 금융기관 결제의 중요성이 대두되고 있습니다. SWIFT라는 플랫폼만 하더라도 일평균 전 세계 거래량은 약 5조 달러, 연간 1,250조 달러에 이릅니다.³

또한 아래 차트는 업계의 전년 대비 성장을 보여줍니다. 신흥시장에서의 결제가 더 높은 성장률을 보이고 있지만 북미 및 유럽과 같이 비교적 확립된 지역에서는 암호화폐 기반 결제 솔루션에 대해 훨씬 크고 즉각적인 시장이 존재합니다.

그림 2 - 2017년 글로벌 결제 시장 보고서⁴



3. https://www.fincen.gov/sites/default/files/shared/Appendix_D.pdf
4. Capgemini & Royal Bank of Scotland 2017

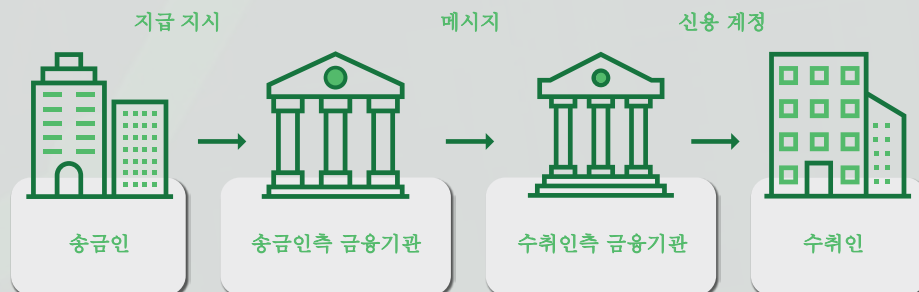
2) 현행 자금이체 방식

전자자금이체(Electronic Fund Transfer, 이하 "EFT")란 금융기관 고객의 요청에 따라 한 금융기관에서 다른 금융기관으로(또는 한 계좌에서 다른 계좌로) 자금이 이동하는 거래를 말합니다. 이를 위해 금융기관은 필수 부기입력(bookkeeping)과 자금 제공을 가능하게 해주는 전자 메시지를 주고받습니다. 전자자금이체는 두 당사자 간의 자금이체를 위해 기업들이 사용하는 기본 메커니즘입니다.

금융기관은 SWIFT와 ISO 20022 등 잘 알려져 있고 충분히 지원받고 있는 표준에 따라 전자 메시지를 송수신함으로써 전자자금이체를 수행합니다. 금융기관간에 전송된 메시지는 송신 은행이 송금인의 계좌에서 자금을 인출하고 수신 은행이 수취인의 계좌에 입금하도록 지시합니다.

이와 같은 이체에 관여하는 주체는 다음과 같습니다.

- 송금인(사업체 또는 개인) - 이체 개시자
- 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



주로 사용되는 지급결제 형식:

SWIFT	<p>세계은행간 금융데이터통신협회(The Society for Worldwide Interbank Financial Telecommunications, 이하“SWIFT”)는 표준화 코드로 자금이체 지시를 할 수 있게 해주는 회원 소유의 메시징 네트워크입니다.</p> <p>SWIFT는 한 국가의 금융기관이 다른 국가의 지사 또는 타 금융기관과 통신할 때 사용할 수 있는 네트워크입니다. SWIFT는 금융결제시스템이라기보다는 자금이체 지시를 위한 메시징 시스템입니다.</p> <p>국제 은행간 메시지 대부분은 SWIFT 네트워크를 사용합니다. SWIFT는 메시지를 ‘메시지 유형’ 이라고 하는 일련의 형식으로 분류합니다. 각 메시지 유형은 거래 또는 메시지의 유형을 나타내며, 이러한 메시지 유형은 10가지 범주로 구분됩니다. (MT0xx – 시스템 메시지, MT1xx – 고객 지불 및 수표, MT2xx – 금융기관 이체, MT3xx – 채권 시장, MT4xx – 추심 및 현금 서신, MT5xx – 증권 시장, MT6xx – 채권 시장 – 금속 및 신디케이션, MT7xx – 신용장 및 보증; MT8xx – 여행자 수표; MT9xx – 현금 관리 및 고객 상태).</p> <p>SWIFT는 일평균 2,840만개의 FIN 메시지를 처리하고 있으며,⁵ 전 세계적으로 매일 약 5조 달러, 연간 1,250조 달러 규모의 이체를 처리합니다.⁶</p>
CHIPS	<p>어음교환소 가맹 은행간 지급결제시스템(Clearing House Interbank Payments System, 이하 “CHIPS”)은 세계 최대의 가장 활발한 일부 은행을 대상으로 지급지시서(미 달러화)를 발송하고 결제하는 자금이체 시스템입니다.</p> <p>CHIPS이 발송하고 결제하는 ‘지급결제 메시지’ 건수는 평균 446,000건 이상이며 그 가치는 1조 5,000억 달러에 달합니다. 하루 20시간 운영되며 실시간으로 은행 간 거래를 처리합니다.⁷</p>
Fedwire	<p>페드와이어 자금서비스(Fedwire Funds Service, 이하 “Fedwire”)는 미국 내 12개 지역 연방준비은행(FRB)이 공동소유한 실시간 총액결제시스템입니다.⁸ 송금인과 수취인 양측은 Fedwire에 참여하는 금융기관의 계좌를 개설해야 하고 이체는 당일 중에 처리되며 취소가 불가능합니다. 참여 금융기관 모두가 미국에 기반을 두고 있지만 Fedwire는 해외송금의 미국측 결제 수단으로 사용 가능합니다.</p> <p>2016년 Fedwire의 일평균 거래량은 590,209건으로 3조 5백억 달러에 달했습니다.⁹</p> <p>Fedwire 서비스는 영업일 전날 오후 9시부터 익일 오후 6시까지 운영됩니다.(동부 표준시 기준)</p>
ACH	<p>전자결제시스템(Automated Clearing House, 이하 “ACH”)은 1만여개 금융기관이 지원하는 비영리 협회 전자결제협회(National Automated Clearing House Association, 이하 “NACHA”)에서 운영하는 전자결제네트워크입니다. ACH 이체로는 직접 예금, 급여 지급, 소비자 결제(예: 보험사, 용자회사로의 결제) 등이 있습니다.</p> <p>ACH 출금이체에는 보험료, 담보대출 및 기타 청구서에 대한 소비자 결제가 포함됩니다. ACH는 미국 전역에 서비스를 제공합니다. ACH에 준하는 유럽측 시스템은 유로단일결제지역(Single Euro Payments Area, 이하 “SEPA”)이며 영국의 경우 BACS, CHAPS, Faster Payments의 세 가지 시스템을 갖추고 있습니다.</p> <p>ACH 네트워크는 매년 43조 달러 상당의 전자금융거래 250억 건을 처리합니다.¹⁰</p>

금융기관은 거래의 성격에 따라 다양한 결제 방식을 사용합니다. 경우에 따라서는 단일 거래에 복수의 결제방법을 사용할 수 있습니다.

5. <https://www.swift.com/about-us/swift-fin-traffic-figures> (2017년 12월 19일 기준)
6. https://www.fincen.gov/sites/default/files/shared/Appendix_D.pdf
7. <https://www.theclearinghouse.org/-/media/tch/pay%20co/chips/reports%20and%20guides/chips%20volume%20through%20november%202017.pdf?la=en> (2017년 12월 19일 기준)
8. https://frbserve.org/serviceofferings/fedwire/fedwire_funds_service.html
9. https://www.federalreserve.gov/paymentsystems/fedfunds_ann.htm
10. <https://www.nacha.org/ach-network/timeline> (2017년 12월 19일 기준)

3) 현행 자금이체 과정 내의 정보

두 당사자 간의 거래는 일반적으로 금융 업계 내에서 제3자 결제라고 일컫습니다. 즉, 금융기관이 아닌 당사자(개인 또는 단체)를 대신하여 금융기관이 처리하는 거래를 말합니다. 몇몇 예외를 제외하고는 이러한 제3자 결제 거래는 일반적으로 크게 두 가지 유형으로 나눌 수 있습니다.

- 하나 이상의 금융기관이 신용장, 보증 및/또는 기타 정보(선하 증권 및 기타 선적 정보)에 접근할 수 있는 무역 금융의 경우처럼 금융기관의 접근이 허용된 문서에 따라 처리되는 거래.
- 위와 같은 문서를 보유하지 않은 상황에서 처리되는 거래가 두 번째 제3자 결제 유형이며 이러한 거래를 흔히 ‘정산(clean payments)’ 이라고 합니다. 처리되는 제3자 결제의 대부분이 이 유형에 속하며 이때 해당 결제를 처리하는 금융기관은 기초 거래의 성격을 파악하기가 비교적 어렵습니다. 무역 금융 분야에 있어서 이러한 거래를 ‘신용조건부거래(open account trade)’ 라고 합니다.

금융거래에 포함될 수 있는 정보는 다음 두 가지 범주로 나뉩니다.

- **고객확인제도(Know Your Customer, KYC):** KYC 정보에는 일반적으로 고객 이름, 주소, 계좌번호 등과 같은 기본 신상정보가 포함됩니다.
- **거래확인제도(Know Your Transaction, KYT):** KYT 정보에는 거래 유형(예: 현금, 해외 전신 지급 또는 수표 관련 거래), 자금 수취인(송금인이 신고한 주소 포함) 등의 세부사항, 거래 메모에 포함된 세부사항이 포함됩니다.

4) 업계 규제 및 아이비코인의 관련성

지난 50년 간 자금이체의 전자화 확대에 따른 거래량 증가로 인하여 금융기관과 법집행기관, 규제기관은 금융범죄 퇴치에 있어 다양하고 복잡한 도전과제에 직면해 있습니다. 전 세계의 국가들은 자금세탁(Anti-money laundering, 이하 “AML”) 방지법을 지속적으로 강화하고 있습니다. 대부분의 국가들이 이러한 법률을 제정하고 그 이행을 촉구하기 위해 많은 재원을 투입하고 있어 소비자 및 기업은 신규 금융계좌 개설 시 또는 대규모 자금이체 시 금융기관이 고객의 신원 확인을 위해 KYC 정보를 요청하는 것에 익숙해져 있습니다.

a. 금융기관의 자금세탁방지

미국의 경우 금융기관은 은행비밀법(Bank Secrecy Act, 이하 “BSA”)¹¹ 및 기타 규제 요구 사항에 따라 의심스러운 거래의 탐지와 조사 및 보고를 하기에 충분한 정책과 절차 및 통제를 시행하고 준수해야 합니다. 의심스러운 거래에는 자금세탁(AML), 탈세, 기타 범죄행위에 해당될 수 있는 거래가 포함됩니다. 전 세계 선진국들도 이와 유사한 요건을 갖추고 있습니다.

의심스러운 거래를 탐지하는 방법에는 일반적으로 규칙에 기반하여 의심스러운 거래를 자동으로 감시하는 플랫폼이 수반되는데 이 플랫폼은 최근의 고객 활동을 일괄 처리하여 검토합니다. 이러한 규칙이나 시나리오는 추가 분석을 위해 특정 거래 또는 거래군에 표시를 합니다. 추가 분석은 일반적으로 금융기관 직원이 직접 검토하는 과정을 거치며 표시된 활동을 ‘의심스럽지 않은 거래’로 표시하거나 추가 검토, 나아가 법 집행기관으로의 보고를 위해 해당 거래를 상부에 보고하게 됩니다.

또한 위험도가 높은 특정 고객은 주기적으로 진행되는 실사 검토의 대상이 되곤 하는데 가령 최근 6개월 또는 12개월의 기간 동안 해당 고객이 수행한 거래를 심층 분석하게 됩니다. 이러한 실사 검토는 자동화된 거래 감시·탐지 방법과 비슷한 목적을 갖습니다. 그것은 바로 해당 활동의 본질을 이해함으로써 금융기관이 고객관계 유지의 위험 및 수용가능성과 관련하여 결정을 내리고, 확인된 당사자의 계좌에 적절한 통제를 적용하며, 필요에 따라 의심스러운 활동을 보고하는 것입니다.

규제측면에서는 고객 활동이 의심스럽지 않다는 확신을 줄 수 있도록 금융기관이 충분한 실사와 분석을 수행하도록 제하고, 고객 활동이 의심스러운 경우에는 더 자세히 분석하여 법 집행기관에 보고하도록 하는 금융기관에 대한 규제강화가 마련되기를 기대합니다. 금융기관은 이용 가능한 모든 정보를 바탕으로 이러한 평가를 수행해야 합니다. 추가 정보가 도움이 될 경우 금융기관은 이를 수집하고 고객 또는 관련 당사자를 포함한 그 누구에게라도 현재 조사가 진행 중이거나 진행될 수 있다는 사실을 알리지 않아야 합니다.

11. <https://www.occ.treas.gov/topics/compliance-bsa/bsa/index-bsa.html>

b. 자금세탁방지법의 파급 효과

은행들이 자금세탁방지법을 준수하기 위해서는 이상탐지 프로그램을 구현, 실행, 지원할 수 있는 충분한 정보가 필요합니다. 그러나 암호화폐 거래는 본질적으로 은행이 사기 또는 위법 활동을 식별하기 위해 수행하는 과정에서 필요한 정보가 수반되지 않아 은행들은 이러한 암호화폐와 그에 내재된 익명성으로 인해 곤경에 처하게 됩니다. 은행들은 보통 자기방어 차원에서 암호화폐 관련 거래에서 발생한 불환(fiat) 예금 포함 계좌를 일시 정지하고 암호화폐를 통한 이득 또는 정산을 합법적인 교환의 매개로서 수락하지 않습니다. 이 결정이 시사하는 한 가지는 암호화폐는 수익금을 저축할 수 없기 때문에 합법적인 기업이 암호화폐 관련된 거래를 수행할 수 없다는 것입니다.

c. 추가 정보의 이점

자동화된 거래감시시스템의 경고를 조사하거나 진행중인 실사의 일환으로 거래 활동을 검토하는 동안 추가 정보를 쉽게 확보함에는 분명한 이점이 있습니다. 추가 정보는 조사관 또는 검토자로 하여금 관련 당사자를 포함한 거래 활동의 본질이 그 적합성 또는 적법성에 관한 의심을 초래하는지 여부를 더욱 효과적이고 효율적으로 판단할 수 있도록 해주기 때문입니다.

또한 추가 정보는 금융기관으로 하여금 해당 고객이 고위험 고객으로 분류되어야 하는지, 또는 금융기관이 자금세탁방지법의 의무를 위반하고 있는지 여부를 판단할 수 있도록 해줍니다. 일상적인 정상활동의 경우, 추가 정보는 은행의 조사 재원이 더욱 효과적으로 다른 고객 및 이들의 고위험 활동에 집중될 수 있게 해줍니다.

비록 전통적인 결제방법은 일반적으로 제한적인 정보가 내장되어 있지만, 금융기관의 고객신상(KYC) 기록 또는 고객의 직접적인 거래 지시를 통해 추가 정보를 쉽게 입수할 수 있습니다.

전자의 경우 고객 비즈니스의 성격, 지리적 초점, 계정에 발생할 것으로 예상되는 활동, 수익적 소유자 및 서명인 등과 같은 계정 관련 당사자의 정보가 포함될 수 있습니다. 거래 자체(KYT)에는 송장, 신용장, 선적 서류 등의 증빙서류 관련 정보와 거래 당사자 식별정보(발송자와 수취인 외에도 해운업체와 같은 당사자가 포함될 수 있음)가 포함될 수 있습니다. 또한 미 재무부 산하 해외자산통제국(OFAC) 또는 미 상무부 산하 산업안보국(BIS)에서 발급한 면허와 같이 거래의 법적 허용가능성을 입증하는 문서 또는 증거 서류도 포함될 수 있습니다.

추가 정보를 지원 프로토콜의 측면에서 지급지시서 메커니즘에 포함시키는 경우, 금융기관의 검토자가 거래 활동의 성격을 더욱 포괄적으로 명확하게 파악하는 데 큰 도움이 될 수 있습니다. KYC 및 KYT 정보를 더욱 쉽게 확보하고 지식격차를 해소함으로써 금융기관은 면밀한 조사가 필요한 다른 사례의 조사에 집중할 수 있습니다. 불행하게도, 금융 기술의 수많은 프로토콜 개발은 상호 운용성과 속도에 크게 초점을 맞춘 나머지 규제 준수를 배포 이후의 어느 시점에 해결할 수 있는 불편한 것으로 간주합니다. 이는 포괄적 솔루션의 가능성은 좀처럼 실현되지 않는다는 것을 의미합니다.

3

아이비코인의 기회 뛰어난 고도의 와해성 기술

기존 금융시스템 대비 암호화폐의 이점은 충분히 이해되고 있습니다.



신속성



사용 용이성



가격 경쟁성



추적 가능성



적시성



데이터 방대성



보안성

그러나 현재 대부분의 암호화폐에 내재된 익명성은 오늘날 금융시스템과의 호환성을 저해합니다.

아이비코인 네트워크는 블록체인 기반 암호화폐를 사용하여 KYC, KYT, AML 데이터 지원 거래를 가능하게 해줍니다. 기존 결제 네트워크에 비해 훨씬 많은 준법감시 및 거래 감사 정보를 담고 있어 금융기관과의 거래에 최적화될 것입니다. 금융기관과 중개기관의 엄격한 요건을 충족시킬 수 있는 거래 데이터가 제공될 것입니다. 따라서 아이비코인 네트워크가 구현된다면 기존 금융시스템과 경쟁 암호화폐에 비해 확연한 우위를 점할 것입니다.

아이비코인은 현재의 글로벌 금융시스템과 새롭게 등장하는 암호화폐 사이의 격차를 해소하여 글로벌 결제의 미래로 자리매김 하고자 합니다.

1) 기존 금융시스템과의 비교

최종 개발완료시 아이비코인 네트워크와 전통적인 지불 네트워크 간의 주요 차이점은 다음과 같습니다.

- 아이비코인은 신뢰할 수 있고 분산된 아이비코인 네트워크를 통해 KYC와 KYT 데이터를 연계시키면서 암호화폐 결제 이체를 안전하게 진행합니다.
- 아이비코인은 근거 거래 데이터에 대한 변경 불가능한 참조를 퍼블릭 블록체인 내에 안전하게 저장합니다.
- 아이비코인은 기존 결제방법에 비해 더 많은 KYT 정보를 이체에 포함시킵니다.
- 아이비코인은 기존 결제방법에 비해 더 많은 KYC 정보를 이체에 포함시킵니다.
- 아이비코인은 기존 बैं킹 소프트웨어에 통합될 수 있습니다.
- 아이비코인은 부기(bookkeeping) 효율성 향상을 위해 회계 소프트웨어에 쉽게 통합될 수 있습니다.
- 아이비코인은 금융기관, 회계사, 경영진 및 기타 사용자가 필요로 하는 정보에 따라 KYC/KYT 데이터에 대하여 취소가능 액세스를 제공합니다.



KYC 및 KYT와 관련하여 자주 사용되는 기존 결제 형식은 비교적 적은 데이터 포인트 수집을 지원하는 것이 일반적입니다. 아래 표는 전형적인 거래에 포함된 KYC/KYT 데이터 포인트의 대략적인 값을 나타냅니다.

	SWIFT	Fedwire	Chips	ACH
KYC 및 AML 데이터 포인트	10	17	9	10






참고: 당사는 SWIFT, CHIPS, ACH, Fedwire와 제휴하지 않습니다. 모든 정보는 일반적인 기준에 따라 제공되며 당사의 조사 시점에 입수 가능한 정보 기준입니다.

아이비코인 네트워크가 구현된다면 기존 시스템 및 프로세스 대비 훨씬 더 많은 정보를 기술하게 될 것입니다. 수행되는 금융거래 유형에 따라 아이비코인 네트워크는 120개 이상의 다양한 KYT 데이터 포인트와 70개 이상의 다양한 KYC 데이터 포인트를 거래 메시지에 포함시킬 수 있을 것으로 예상됩니다. 이들 데이터 포인트를 분류하는 편리한 방법은 이들이 생성되는 출처 문서에 따라 결정됩니다.

거래 유형	데이터
	
핵심 거래 정보	74
추가 당사자 정보	13
제재 연계	7
수출 통제 연계	7
선적 정보	21
상업 송장	12
상업 계약	17
검사 증명서	3
대변표(Credit Note)	10
차변표(Debit Note)	10
발송 지시	6
계정 명세서	7
발주서	11

2) 경쟁 암호화폐와의 비교

최종 개발완료시 아이비코인의 토큰은 기존 경쟁 암호화폐와는 차별된 여러가지 기능 및 이점을 제공할 것입니다.

기능	설명	이점
 확인 가능	아이비코인 네트워크 및 관련 거래를 통해 암호화폐 거래의 흐름에 KYC/KYT/AML 데이터를 명확하게 통합할 수 있습니다.	당사자들과 거래 목적의 정당성을 쉽게 이해할 수 있으며 지불 및 예금에 관한 결정을 내릴때 사용할 수 있습니다.
 양도 가능	토큰은 기존 금융기관 및 중개기관이 제공한 KYC/KYT/AML 정보 필요없이 공용 블록체인 상에서 자유롭게 거래 가능한 암호화폐가 될 것입니다.	당사자는 토큰가치를 투명하게 반영하고, 암호화폐의 가치를 결정하는 독립적인 결정인자인 ivyKoin.com 및 암호화폐 교환소를 제거함으로써 토큰의 유용성에 따라 쉽게 사용 • 교환할 수 있습니다.
 위조 불능	아이비코인 네트워크 거래 및 증빙 데이터는 블록체인 아키텍처 사용을 가능하게 해줄 것이며 이에 따라 할당 및 거래 데이터의 변경불가능성은 더욱 강해집니다.	아이비코인 네트워크 사용자는 현금 이동 관련 결정을 지원하는 거래 및 데이터의 내구성을 보장하는 거래 무결성 및 정보 보안성에 대한 확신을 받게될 것입니다.
 제한적 공급	토큰은 향후 공개될 확정 수량만큼 발행될 예정이며 최초 분배 및 할당량도 공개될 것입니다.	공개 거래는 코인의 희소성과 관련된 경제원리의 수혜를 누립니다. 사실 네트워크 움직임은 네트워크 내 자금의 유동성과 속도를 정확히 반영합니다.
 요청 시 익명 해제	수집된 모든 데이터는 금융기관과 중개기관으로 구성된 사적 결제 네트워크 상에서 지속적으로 보호, 전송, 추적됩니다.	적격 당사자는 KYC/KYT/AML 기능에 필요한 정보를 보유하고 있습니다. 데이터의 기본 보안성을 훼손하지 않고도 당사자를 추가하거나 제거할 수 있습니다.



인식 가능



양도 가능



위조 불능



제한적 공급



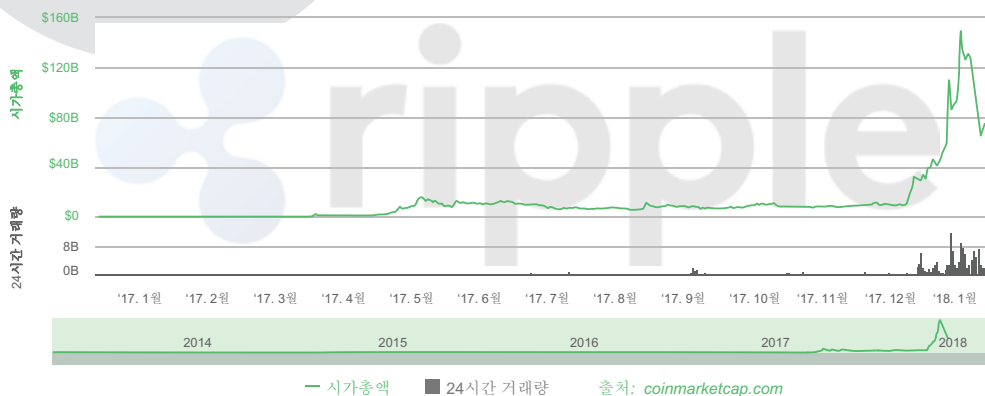
요청 시 익명 해제

최종 개발완료시 아이비코인 네트워크는 경쟁 암호화폐이자 선두주자인 리플(Ripple 또는 XRP)에 비해 백한 장점을 갖을 것으로 예상됩니다.

아이비코인	VS	리플
<ul style="list-style-type: none"> 가상화폐와 기존 금융시스템 사이의 KYC/KYT/AML 장벽을 허물 수 있도록 설계 거래 당 최대 74 이상의 KYC, 120 이상의 KYT 데이터 포인트 및 고객 파일 분산적 거래 검증 시스템 공개 장부 상의 유틸리티 거래 규모에 의해 움직이는 공공 코인 경제 		<ul style="list-style-type: none"> 핵심 디자인에 KYC/KYT/AML을 포함하지 않음 암호화폐와 관련이 없는 KYC/ KYT 데이터 중앙집중식 거래 검증 시스템 투명하지 않은 공공 코인 경제, 사적으로 보유하는 대규모 준비금

특히 리플과 관련하여, 아이비코인 네트워크는 네트워크 상에서 KYC/KYT/AML 데이터 통신 및 잔액 정산을 목적으로 토큰을 사용하는 검증인(금융기관과 중개기관으로 구성)을 위한 분산형 네트워크가 될 것입니다. 규정 준수 및 감사는 아이비코인 네트워크가 가장 중요시 하는 우려사항입니다. 토큰을 이용한 거래는 송금 수취인이 자신의 금융기관에서 불환화폐(fiat currency) 형태로 쉽게 지급받을 수 있도록 토큰을 사용하여 공공 이더리움(Ethereum) 네트워크상에 올라온 계약을 대상으로 시작됩니다. 이는 리플의 핵심 화폐이자 교환매체로서의 수단 외에는 공개적으로 거의 사용되지 않는 리플과는 큰 차이를 보입니다.

시장 잠재력은 잘 알려져 있습니다. 리플은 암호화폐 중 비트코인 다음으로 가장 큰 규모를 가지고 있습니다.¹²



2017년 1개년 간 리플 토큰의 가치는 28,000% 이상 증가했습니다.

<http://fortune.com/2017/12/29/ripple-cryptocurrency-surge/>

* 2018년 1월 14일 기준

**미화 1,500만 달러 조달을 전제로

12. <https://coinmarketcap.com/> 2018년 1월 14일 기준

4

성공적인 실적을 보유한 세계 최고 수준의 팀

당사는 성공적인 실적을 보유한 세계적 수준의 팀이 이끌고 있습니다. 고도로 숙련된 당사 경영진은 프로젝트 성공을 위해 필요한 모든 단계에서 업계 최고의 지식과 네트워크를 갖춘 글로벌 자문위원회의 지원을 받고 있습니다.

팀에 대한 자세한 정보는 웹사이트(www.ivykoin.com)에서 확인하시기 바랍니다.



5

아이비코인 운영 사양

1) 운영 플랫폼 개요

a. 기본 기능

아이비코인 네트워크는 최종 사용자에게 다음의 기능을 제공할 계획입니다. 이 기능은 데스크탑/웹 및 모바일을 통해 해당 구성요소에 제공될 것입니다.

송금인 및 수취인

- 토큰의 구매 및 판매
- 가상화폐 거래가능성 및 일반적인 가상화폐 환율 확인
- 네트워크 요금 추산 및 토큰 사용에 대한 건적 수령
- 금융기관 및 금융 중개기관의 평균 결제 시간 확인
- 개인 식별 정보(송금인측)에 대한 KYC 데이터의 액세스 로그 확인

금융기관 및 금융중개기관

- 기업 계정(enterprise account) 유지 및 정보 식별
- 조직 구성원의 계정 액세스 설정 관리
- 토큰 데이터 컨테이너 콘텐츠 및 액세스 이력 관리

당사는 위에서 설명된 기본 기능 외에도 적절한 시기에 다음과 같은 특징, 기능 및 솔루션을 아이비코인 네트워크에 통합시킬 계획입니다.

b. 불환화폐 네트워크에 대한 P2P(Peer-to-Peer) 방식 암호화폐

아이비코인 네트워크는 애초에 주로 B2B 거래를 위해 제공되었지만 개인이 손쉽게 암호화폐를 주고받고 관리할 수 있고 이를 불환화폐로 쉽게 전환할 수 있도록 해주는 간소화된 결제 네트워크에 대한 수요 또한 높습니다.

c. 소프트웨어 통합

당사는 KYT와 KYC가 해당 은행 시스템 내의 올바른 위치에 자동적으로 배포할 수 있도록 기존 은행 소프트웨어와의 통합을 모색할 것입니다.

또 당사는 주요 회계 소프트웨어 시스템과 통합을 생각하고 있습니다. 청구서 세부내용을 포함, 고객의 지불 및 수취 정보를 간단히 통합함으로써 거래 내역을 회계 소프트웨어에 직접 로딩하여 고객의 관리 부담을 줄일 계획입니다.

d. 캐시어(Cashier) 및 전환 서비스

당사는 캐시어 서비스와 전환 서비스를 개발하려고 합니다. 캐시어 서비스는 다음을 가능하게 해줍니다.

- 불환화폐를 은행계좌에서 인출 후 암호화폐로의 전환
- 암호화폐를 다시 불환화폐로 전환 후 은행계좌로 입금



교환 서비스는 고객으로 하여금 토큰을 일련의 다양한 암호화폐로 상호 전환할 수 있게 해줍니다.

당사는 캐시어 서비스와 교환 서비스를 모두 제공함으로써 아이비코인 네트워크가 특히 대규모 이체를 하는 기업들에게 E2E(End-to-End) 솔루션이 되도록 할 것입니다. 당사가 추구하는 바는 다음과 같습니다.

- 불환화폐에서 암호화폐로의 용이한 전환
- 전 세계 어디에서든 용이한 암호화폐의 이체
- 수취인이 자신의 은행 계좌 상에서 암호화폐를 다시 불환화폐로 전환할 수 있도록 지원

가장 중요한 점은 아이비코인 네트워크는 송금 또는 수취 금융기관과 문제를 일으키지 않으며 이러한 작업을 수행할 계획입니다.

e. 공개시장조작(open market operation)을 통한 고정가격 이체

암호화폐 이체 과정에서 발생하는 잠재적 화폐 손실은 상인들이 가상화폐를 주류로 채택하지 못하도록 하는 가장 큰 요인 중 하나입니다. 따라서 당사는 암호화폐의 가격 변동성에 따른 화폐 손실을 없애기 위해 고정가격 솔루션을 개발하려고 합니다.

고정가격 솔루션에는 특히 두 개의 은행 계좌가 관여하는 미 달러화 불환화폐간 거래용 기금 코인(treasury coins) 풀이 사용됩니다. 불환화폐를 최초 예치 금융기관(Originating Deposit Taking Financial Institution, 이하 "ODFI")을 이용하여 송금인의 은행 계좌에서 송금한 후 아이비코인 네트워크는 이러한 목적으로 특별히 설계된 장외 토큰 기금을 사용하여 불환화폐를 토큰으로 전환하게 됩니다(섹션 7 참조).

2) 금융기관

금융기관 지원이 강화됨에 따라 아이비코인 네트워크는 다음과 같은 거래 외에도 상당수 거래에 사용될 가능성이 높습니다.

- 국내외 상품 구매
- B2B 서비스
- 금융기관 내에서 불환화폐가 되는 가치의 일반적 이전
- 소프트웨어 라이선스 구매
- 부동산 구매
- 글로벌 투자
- 대규모 개인 이체
- 소규모 개인 이체

3) 사용자 기능

아이비코인 네트워크는 (1) 송금 당사자가 수령 당사자에게 거래의 암호화폐를 송금하려고 하고 (2) 수령 당사자가 은행 계좌에 해당 암호화폐 잔고를 불환화폐로 수령하는 경우, 거래 당사자 간에 가치 교환을 제공할 것입니다.

송금인과 수취인 모두 ivyKoin.com와 주요 교환소에서 구매 가능한 토큰을 사용하여 아이비코인 네트워크를 통해 금융기관으로 암호화폐를 이동시킬 수 있을 것입니다. 아이비코인 네트워크를 통해 다른 암호화폐를 이동시키려는 계정 보유자는 우선 제3자 암호화폐를 토큰으로 교환해야 합니다.

ivyKoin.com은 사용자가 전화나 모바일 기기를 통해 접속 가능할 것이며, 송금인의 관점에서 다음과 같은 핵심 기능을 제공하게 됩니다.

- 계정 설정 및 관리
- 거래 관리
- 토큰의 구매, 판매 및 이전

a. 계정 설정 및 관리

송금인과 수취인은 각각 ivyKoin.com에서 아이비코인 네트워크 계정을 생성하고, 등록 프로세스를 거친 후 송금인의 고유식별정보를 받아볼 수 있습니다. 아이비코인 네트워크는 이후의 이체를 위해 동일한 정보를 제공할 필요가 없도록 송금인의 모든 계정 정보를 저장합니다. 이 KYC 정보는 이름, 전자메일, 전화번호, 주소, 신분증과 같이 사용자의 신원을 나타내는 다양한 데이터 필드 및 파일로 구성됩니다.

완전히 개발될 경우, 계정은 ivyKoin.com의 온라인 대시보드를 통해 관리될 수 있습니다(KYC 및 반복적인 거래 데이터 업데이트 포함). 계정 보유자는 다른 아이비코인 네트워크 계정 보유자와의 연결을 요청하고, 알려지고 확인된 암호화폐 결제 계정 명단을 추가할 수 있습니다. 이는 동일한 수취인에게 자주 송금하거나 새로운 수취인에게 신속하고 효율적으로 송금할 때 도움이 됩니다. 계정 보유자들은 전 세계적으로 아이비코인 네트워크 상에서 자신이 공개되도록 할 수 있으며 자신의 명부에 다른 계정 보유자를 추가할 수 있도록 요청할 수도 있습니다. 또한 이들은 아이비코인 네트워크 서비스를 이용하여 토큰을 전환하고 금융기관에 있는 자신의 불환계좌로 송금할 수 있습니다.

i. 송금인 데이터 검증

아이비코인 네트워크는 계정 개설 프로세스의 일환으로 은행 계좌의 기본 송금인 데이터와 정당성을 검증합니다. 아이비코인 네트워크는 다양한 제3자 서비스를 사용하여 초기 신분증명서 검증을 제공합니다. 여권, 운전면허증과 같은 신분증명서는 수분 내로 검증이 끝나는 반면, 신분증명서가 인식되지 않는 경우에는 추가 조사를 위해 해당 계정을 보류상태로 분류합니다. 마찬가지로 사업허가 및 기타 등록된 회사 서류도 신속하게 확인할 수 있습니다.

마찬가지로, 계정 보유자의 은행 계좌 정보는 소액 예수금이 계정 보유자의 은행 계좌로 입금되는 절차를 통해 검증되며, 해당 입금액은 아이비코인 네트워크와 은행 계좌 간의 성공적인 연결상태를 독립적으로 검증하는 데 사용됩니다.

이 같은 노력에도 불구하고 당사는 실령 해당 실무가 기존 네트워크 상의 실무와 매우 유사하다 할지라도 결제의 정당성 여부에 대하여 책임을 지지 않습니다.

a. 거래 관리

아이비코인 네트워크 계정이 개설되면 송금인은 수취인에게 토큰 이체를 개시할 수 있게 됩니다. 송금인은 거래에 앞서 특정 거래정보를 계정에 입력합니다. 아이비코인 네트워크는 모든 이체에 대하여 기초 정보를 요청하지만, 추가로 요청된 세부사항은 적용 법률 및 규정에 따라 달라지므로 아이비코인 네트워크는 송금인에게 거래에 관한 추가 세부정보를 제공하도록 요청합니다. 예를 들어 송금인이 상품에 대한 대가로 결제를 하는 경우, 아이비코인 네트워크가 이체에 포함시키는 정보에는 원산지, 최종 목적지, 수입 관세 납부 증명 또는 기타 식별 정보가 포함될 수 있습니다. 또한 송금인은 이체에 관한 추가 세부정보(예: 해당 결제의 송장 사본)를 제공하기로 선택할 수 있습니다. 또한 만약 수취인이 신뢰하는 출처가 아님을 송금인이 알고 있다면, 품질확인서, 배치(batch) 정보, 정관 및 기타 광범위한 자발적 KYT 정보 등이 포함될 수 있습니다.

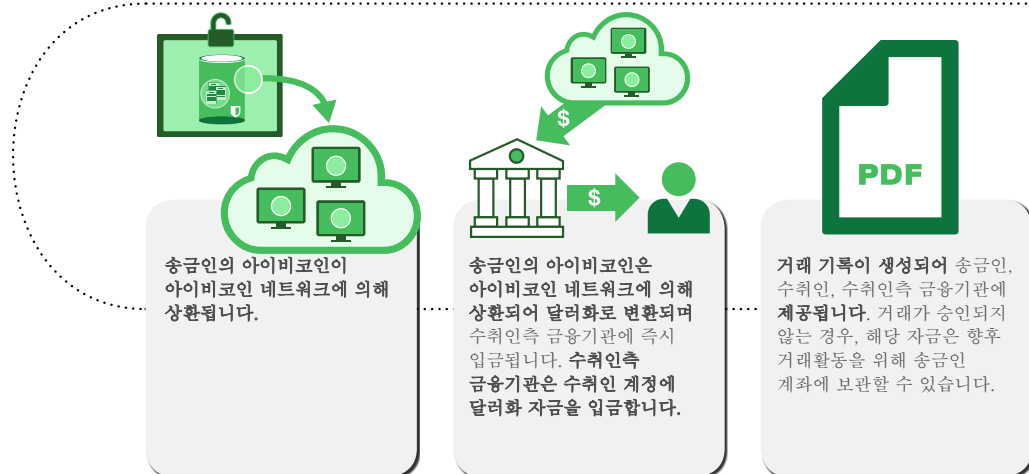
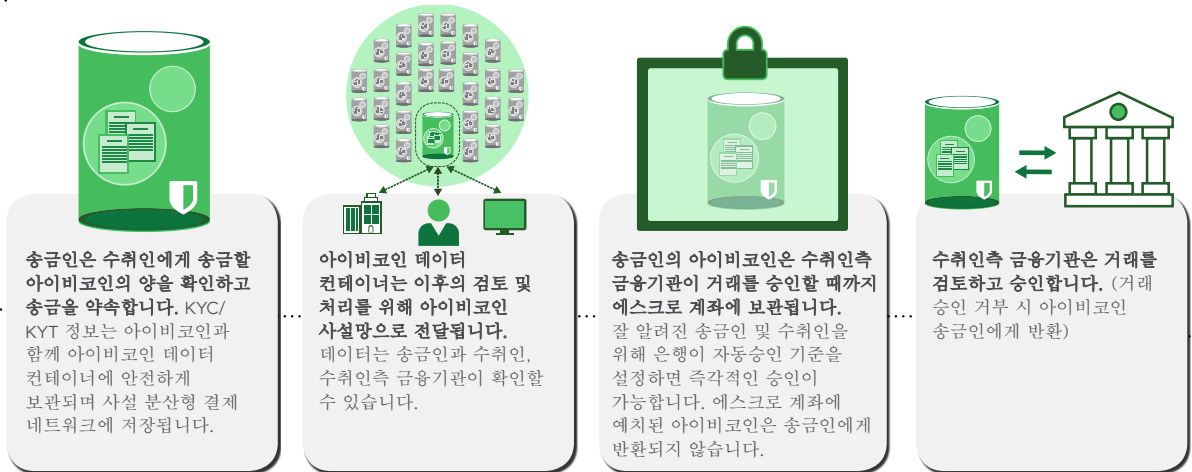
b. 아이비코인 구매, 매도 및 이체

아이비코인 네트워크는 송금인과 금융기관 모두를 위해 자금과 데이터의 안전한 전송을 가능하게 해줄 것으로 기대됩니다. 은행이 의심스러운 활동을 찾기 위해 거래를 심사하고 있다면, 레거시 결제 네트워크나 결제 이체에 사용되는 보다 현대적인 대안들에 비해 검토에 도움이 되는 훨씬 많은 데이터 포인트가 제공될 것입니다.

결제 금액은 블록체인 내에서 일반인이 확인할 수 있으며 삭제가 불가능합니다. KYT 및 KYC 데이터는 암호화되어 송금인이 아이비코인 네트워크로 보낸 토큰과 합쳐지게 되며 이후 수신 기관 및 수취인이 액세스 할 수 있습니다. KYC/KYT/AML 데이터는 오직 거래 관련 당사자만 확인할 수 있습니다.

아래 도표는 송금인과 수취인, 금융기관의 관점에서 예상되는 토큰의 흐름을 보여줍니다. 사용자 인터페이스는 간단하며 직관적입니다.

아이비코인-미 달러화 전환의 기능적 프로세스 개요



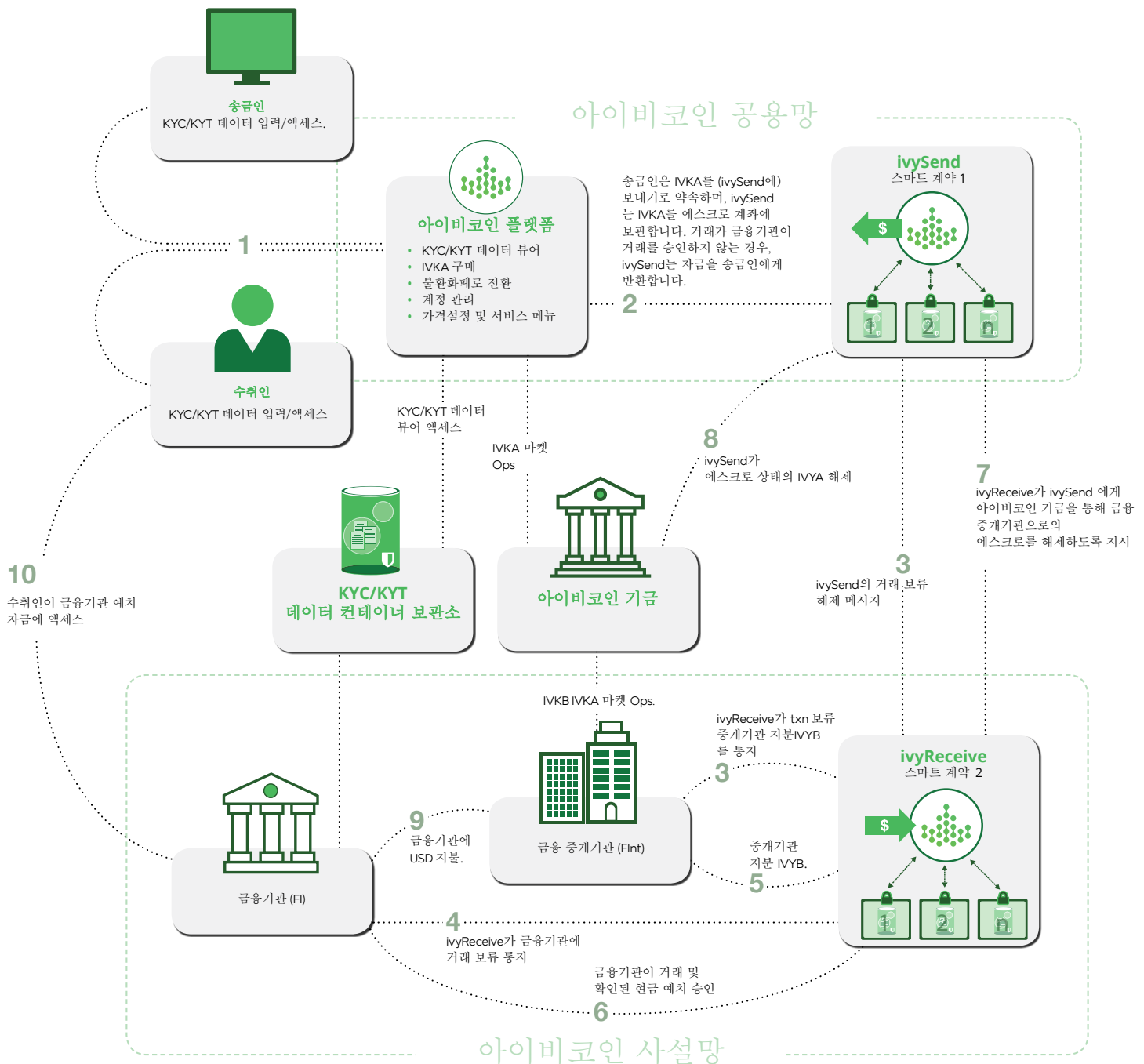
6

아이비코인 기술 사양

1) 기술적 아키텍처 개요

아이비코인 네트워크는 이중 네트워크 아키텍처를 사용하여 작동하여 토큰의 발송자는 공용망 (아이비코인 공용망) 을, 불환화폐로 금융결제를 제공하는 당사자는 사설망 (아이비코인 사설망)을 사용할 것입니다. 거래를 증빙하는 KYC/KYT/AML 데이터는 아이비코인 공용망과 아이비코인 네트워크 스마트 계약의 상호작용을 통해 생성되어 아이비코인 사설망 참여자들의 결제를 지원하는 암호화 컨테이너에 캡처될 것입니다. 해당 데이터는 불환 잔고 수취인측 금융기관과 규제 당국이 저장하고 액세스 할 수 있을 것입니다. 다음의 기술 사양은 완전히 개발될 경우 각각 아이비코인 네트워크에 포함될 것으로 예상됩니다.





a. 공용망, ivySend 및 공용 아이비코인 토큰(IVYA)

아이비코인 네트워크가 가동되면, 해당 수취인의 계정으로 제3자 암호화폐를 송금하려는 공공 당사자는 보유한 암호화폐를 공공 교환소에서 토큰으로 교환하거나 아이비코인 네트워크로부터 직접 토큰을 구매해야 합니다. 아이비코인 공용망 토큰(IVYA)은 이더리움 네트워크에서 사용 가능한 ERC20 사양에 맞춰 준비됩니다. 토큰은 이더리움 네트워크상에서 아이비코인 네트워크 계약(ivySend 계약)에 제출되며 이후 에스스로 계좌에 예치되며, 에스스로 상태는 다음 두 조건 충족 시 종료됩니다. 첫째, 이체가 성공적으로 완료된 경우, 이때 토큰은 아이비코인 네트워크로 이체되어 2차 시장이나 당사 웹사이트에서 현금 또는 제3자 암호화폐로 판매되거나 그렇지 않으면 소각됩니다. 둘째, 이체가 실패한 경우, 이때 아이비코인 네트워크에 제출된 토큰은 전량 환불됩니다.

ivySend 계약은 공개 이더리움 네트워크로부터의 호출에 관심 있는 당사자가 다룰 수 있는 스마트 계약이 될 것으로 기대됩니다. 초기 구현 중인 ivySend 계약은 ivyKoin.com의 인터페이스, 웹 사이트와 이더리움 네트워크의 직접적인 통합을 통해 사용 가능할 것입니다. 또한 다른 당사자들은 본 계약을 결제 인터페이스로 유사하게 포함시킬 것으로 예상됩니다. ivySend 계약은 이더리움 네트워크 가스 인센티브(gas incentive)를 사용하여 운영될 계획이며 이때 송금인이 반드시 계약 호출비용을 부담하고 이를 통해 이더리움 네트워크 상에서 계약이 진행될 수 있습니다. 제출된 가스가 공용 인센티브 채굴에 충분하지 않은 것으로 드러나는 경우, 에스스로 계약은 송금인의 아이비코인 네트워크 계정 잔액을 확보할 수 없으며 그 결과 거래의 나머지 부분도 계속 진행될 수 없습니다. 또한 아이비코인 네트워크 수수료는 ivySend 계약 프로세스의 비용에 포함됩니다(기존 금융기관에서 수행하는 전신송금과 유사).

아이비코인 네트워크를 사용하려는 당사자는 당사의 웹 사이트를 통해 a) 다양한 공통 암호화폐 교환소의 일반 암호화폐-토큰 환율, b) ivySend 계약 성사를 위한 예상 이더리움 가스 수수료, c) 대상 수취인 계좌로 이체하려는 불환화폐 잔액에 대한 토큰 수수료 총액(해당 불환화폐 잔액 + 가스 수수료 + 수수료) 등을 쉽게 확인할 수 있습니다. 이들 구성요소 상당수는 전반적인 가격결정 시 변동을 보입니다. 그러한 이유로 당사의 웹사이트를 이용하여 ivySend 계약 사용자는 10분 동안의 가격 견적을 받을 수 있으며 이 견적은 가격 견적이 주어진 시점에 아이비코인 네트워크에 표시된 변동성의 상한선과 하한선 내에서 주어진 견적 매개변수의 ivySend 계약 거래를 위한 실행 견적값으로 고정됩니다.

그리하여 완전히 개발될 경우, IVYA는 보유자에게 완전한 유틸리티 기능을 제공하고 계약에 불리하게 작용되는 변동성으로부터 이들을 보호할 것으로 기대됩니다.

b. 사설망, ivyReceive 및 사설 아이비코인 토큰(IVYB)

아이비코인 사설망은 사설 ivyNetwork 계약(ivyReceive 계약)을 사용하여 특정 수취인의 은행 계좌에 자금을 배분할 목적으로 만들어졌습니다. 아이비코인 사설망은 이더리움 블록체인에 특화된 금융기관-중개기관 공조의 허가된 사설 버전을 사용하여 운영하도록 제안되었습니다.

ivyReceive 계약은 아이비코인 사설망 상에서 호스팅 될 것으로 예상됩니다. 이는 참여 금융기관 및 중개기관의 정산 원장이 아이비코인 사설망에서 운영되며 이더리움과 호환 가능한 ERC20 토큰인 사설 토큰(IVYB)을 사용하여 자신의 몫을 투자하는 수단으로서의 메커니즘이 됩니다. ivyReceive 계약은 아이비코인 네트워크가 IVYB를 수신인 계좌의 잔액을 직접 정산하는 데 사용하는 방법이 될 것입니다.

완전히 개발될 경우, IVYB는 아이비코인 사설망 계좌 보유자를 반영하는 자산 연동 토큰이 될 것으로 기대됩니다. 아이비코인 사설망 계좌 보유자는 아이비코인 네트워크 거래의 정산이 가능한 불환 준비금을 보유하고 있습니다. IVYB는 당사가 사전 채굴할 것이고, 당사에 의해서만 IVYA로 전환 가능하며, 아이비코인 네트워크 내의 보유 준비금에 비례하여 아이비코인 네트워크 계정 보유자에게 제공될 것입니다. 당사가 IVYB를 사용하는 경우, 네트워크상의 달러 예금이 에스스로나 예치 여부와 상관없이 보유한 토큰 보유액과 항상 동일함을 입증하기 위해 IVYB 자산 및 부채에 대한 공공회계를 제공하고자 합니다.

거래 보류 메시지가 아이비코인 사설망에 도착하면 계정 보유자는 해당 잔고를 수령할 기회를 위해 IVYB에 표시해야 합니다. 이는 아이비코인 사설망 계정 보유자가 최소한 거래액과 동일한 IVYB의 잔액을 보유하고 있어야 함을 의미합니다. 이러한 상호작용 가운데 토큰을 표시하는 과정은 KYC/KYT/AML 정보를 해당 금융기관 또는 중개기관에 제공하며, 이때 이들은 자금을 수락하거나 거절해야 합니다(수동으로, 또는 사전 승인된 경우 자동으로). 이 토큰은 ivyReceive 계약에 제출됩니다. ivyReceive 계약에는 토큰의 릴리즈에 적용되는 두 가지 필수 조건이 있습니다.

- a) 거래 승인 증명 - 해당 KYC/KYT/AML 정보의 검토가 끝나면 해당 금융기관의 대리인은 ivyReceive 계약에 승인 또는 거부 응답을 보냅니다. 여기에는, 두 가지 잠재적 결과가 있습니다. a) 거래가 성공적으로 진행되는 경우, 아이비코인 사설망 계정 보유자에 의해 예치된 IVYB 금액이 수취인측 금융기관에 입금됩니다. b) 거래가 실패하는 경우, IVYB는 금융기관으로 환불됩니다.

- b) 현금 입금 증명 - 아이비코인 사설망 계좌 보유자의 은행 계좌 상태에 대한 모니터링은 금융기관이 수취인의 계좌로 현금을 입금했다는 사실을 증명하는 메커니즘이 됩니다. 계좌상태를 주시하기 위한 목적으로 Yodlee¹³, Xignite¹⁴, 또는 Plaid¹⁵와 같은 공급업체의 계정 액세스 서비스를 사용하여 맞춤형 또는 유사한 통합을 해야 할 수 있습니다. 어느 쪽이든, 아이비코인 네트워크와 금융기관 간의 B2B 계약은 계정 간 자금 릴리스의 타이밍 제약을 명시할 것입니다.

‘거래 승인 증명’과 ‘현금 입금 증명’이 모두 사실로 확인된 경우, 아이비코인 사설망에서 IVYB를 선택한 당사자는 아이비코인 공용망의 잠금 해제된 ivySend 계약으로부터의 지급 자격을 갖습니다. 두 조건이 모두 거짓이거나 사실이 될 때까지 아이비코인 공용망의 ivySend 계약은 송금인이 보완할 수 있습니다. 거래 승인은 아이비코인 데이터 컨테이너와 함께 제출된 KYC/KYT/AML 데이터를 사용하여 식별된 준수 요건을 충족하려 하는 금융기관에 의해 보류될 수 있습니다. 거래 및 컨테이너 관련 메타데이터를 사용하면 상거래에서 교환되는 상품의 원산지과 성격, 또는 그 외 금융기관이나 중개기관이 원하는 설정가능한 규칙을 기준으로 자동 정산을 어느 정도 용이하게 할 수 있습니다. 마찬가지로, 수동 작업 흐름은 에스스로 거래를 장기간 유지해야 할 수 있습니다. 제출의 기본 동작은 송금인 에스스로가 아이비코인 사설망의 결과에 의해 결정되도록 하는 것입니다. 하지만 은행 KYC/KYT/AML 프로세스의 지연 및 송금인과 수취인 간의 의사소통의 결과로 어느 정도의 합의가 필요할 수 있으며, 그에 따라 일정 기간의 지연 후 송금인은 에스스로 계좌에서 토큰 예금을 회수하는 방식으로 프로세스를 풀 수 있습니다.

ivyReceive 계약은 계류중인 모든 거래의 식별 가능한 잔액을 유지합니다. 아이비코인 사설망에 대한 허가는 개인 잔고와, 각 수취인측 금융기관 및 금융 중개기관에서 계류중인 결제의 작업 흐름 상태를 분리합니다. 이러한 방법으로, ivyReceive 계약에 고정된 개인 소유의 토큰은 a) 금융기관 또는 중개기관이 잔고 전송의 타당성을 고려하는 검토 과정에 가시성을 제공하고, b) 금융기관 운영을 위한 조질장치를 제공하여 만족스러운 수준의 정산 없이 불균형한 거래를 진행하지 않도록 합니다. 물론 이는 금융기관이나 중개기관으로 하여금 필요에 따라 예치를 하도록 하는 것은 도대체 무엇인지에 대한 질문을 제기합니다. 이러한 이유로 아이비코인 네트워크는 네트워크상의 각 금융기관과 중개기관의 서비스 수준을 보고할 수 있을 것입니다. 분명한 점이지만, 한 금융기관이 고객의 니즈를 충족시키지 못한다면 고객은 이체가 더욱 신속하게 이루어지거나 신뢰할 수 있는 아이비코인 네트워크의 다른 참가자들 중에서 다른 선택권이나 기회를 고려할 수 있어야 합니다.

c. 체인 간의 통신 및 아이비코인 오라클(Oracle) 서비스

아이비코인 네트워크는 위에서 설명한 아이비코인 사설망과 아이비코인 공용망 간의 기능적 중개자 역할을 하며 ivySend 계약 및 ivyReceive 계약 관련 이벤트에 귀 기울이고 응답합니다.

ivySend 계약의 상태 변화는 공용 이더리움 네트워크에 참여하는 공인 아이비코인 검증인이 예의주시할 것으로 예상됩니다. 마찬가지로, ivyReceive 계약의 상태 변화는 아이비코인 사설망에 참여하는 아이비코인 네트워크 검증인이 예의주시합니다. 이들 두 검증인 모두 각 에스스로 계약의 상태에 대한 증명을 제공하고, 각각의 기능을 가능하게 해주는 아이비코인 오라클 서비스에 알릴 수 있습니다.

특히 흥미로운 점은 아이비코인 공용망 원장 잔고에서 아이비코인 사설망 원장 잔고로 가치가 이동하는 방식입니다. 이는 IVYA에서 IVYB 로의 가치 이동을 연관지으려는 것이며, ivyReceive 계약에 대한 승인 메시지를 수령하고 수취인의 은행 계좌에 게시된 잔액을 증명할 때 수행됩니다. 이 두 사건이 모두 발생하는 시점에 IVYB가 해제되고 에스스로 계약의 IVYA가 아이비코인 네트워크에 의해 청구됩니다. IVYA는 아이비코인 오라클 서비스 및 아이비코인 사설망에 대한 구성요소 검증인을 통해 아이비코인 사설망 원장에서의 IVYB 거래에 관한 결정을 수령합니다. IVYB가 ivyReceive 계약에 위탁될 때, IVYB에 대한 송금인의 공용 주소가 기록됩니다. 이 공용 주소는 KYC/AML 데이터의 아이비코인 거래 컨테이너

13. <https://www.yodlee.com/>

14. <https://www.xignite.com/>

15. <https://www.plaid.com/>

를 전송하는 데 사용되었습니다. 이후 공용 주소는 네트워크에 대한 자체 거래를 사적으로 정산하기 위한 아이비코인 네트워크의 결제 계정 주소로 사용됩니다.

2) 아이비코인 네트워크상의 당사자 신원

개발 완료 시, 당사는 아이비코인 네트워크에서 두 가지 유형의 신원, 즉 송금인의 신원과 금융기관 및 중개기관의 신원을 관리할 계획입니다.

a. 송금인의 신원

아이비코인 네트워크는 송금인이 화폐를 송금하기 전에 네트워크에 등록할 것을 요구합니다. 아이비코인 네트워크에서는 계정 설정의 일환으로 수취인이 각자의 금융기관 및 중개기관에 의해 식별된다고 가정합니다.

아이비코인 네트워크 상에서 송금인 계정을 설정하려면 자주적 신원(self-sovereign identity)으로 충분합니다. 그러나 아이비코인 네트워크에 대한 승인은 추가적인 거래 정보가 필요할 수 있습니다. 이러한 정보는 계정을 설정할 목적으로 아이비코인 네트워크 상의 송금인이 제출 및 저장하며, 당사로서 하여금 증빙 정보가 필요한 특정 거래 유형에 대하여 증명을 제시할 수 있게 해줍니다. 송금인의 자주적 신원정보 사본은 대상 잔고 수취인의 금융기관 및 기타 중개기관에 거래를 제출하는 과정에서 아이비코인 데이터 컨테이너에 포함되어 제공됩니다. 이러한 자격은 각각의 목적에 특별히 한정되어 있지만 거래의 범위를 벗어나 오랜 시간 동안 액세스가 가능하며 관련성을 갖습니다. 당사 웹사이트를 통해 이러한 자격에 누가, 언제 지속적으로 액세스하는지를 모니터링할 수 있습니다.

b. 금융기관 및 중개기관의 신원

아이비코인은 데이터를 교환하는 금융기관 및 중개기관의 모범 고용사례와 철저한 정보보안 관행에 의존할 것입니다. 당사가 모든 고용 이벤트, 기업 • 인사 관련 활동을 추적하기란 대체로 비현실적인 일이므로 아이비코인 네트워크는 KYC/AML 데이터의 분산 컨테이너에 대한 액세스를 활성화/비활성화하고자 금융기관, 중개기관 및 이해관계 기관의 관련 준법감시 직원의 신원을 아이비코인 네트워크에 등록하도록 할 것입니다. 아이비코인 네트워크는 금융 중개기관의 관련 고용 조치를 적시에 업데이트할 것입니다.

금융기관 관리자는 ivyReceive 계약 기능과 컨테이너 데이터에 대한 관련 직원의 액세스 및 권한을 관리하기 위해 아이비코인 네트워크에 로그인할 수 있습니다. 식별된 사용자의 모든 활동을 중앙에서 추적 • 관리할 수 있고 개별 거래의 컨테이너 이력을 조회할 수 있습니다.

3) 블록체인 기술 응용

분산 원장에 대하여 모두가 합의하는 부분은, 네트워크에 제출된 거래를 고려했을 때 채굴자(miner)라고도 불리는 검증인이 올바른 원장 잔액을 반영하기에 적절하도록 데이터를 정확하게 나타내는 기능입니다. 네트워크 및 시스템 중단 가능성은 고려해보면 예상치 못한 부재 발생 시 일부 당사자의 연결이 끊어지고 중요한 데이터가 누락될 가능성이 있음을 쉽게 예측할 수 있습니다.

마찬가지로, 공유의 관점이 존재하는 네트워크에는 진실이라고 하는 단 하나의 안정적인 결과를 도출하는 확립된 메커니즘이 필요합니다. 비트코인과 이더리움과 같은 네트워크에서는 현재 메커니즘을 ‘작업증명(proof of work, POW)’ 이라고 합니다. 작업 증명은 네트워크에 제출된 거래의 유효성을 확인하기 위해 검증인으로 하여금 연산능력 및 전력에 근거하여 서로 경쟁하도록 장려합니다. 연산능력을 높임으로써 검증인은 암호화된 난제를 해결할 수 있으며 이는 이후 캡처된 거래를 블록으로 네트워크에 첨부할 권리를 위해 네트워크에 제출됩니다(단, 이러한 거래 블록은 이전에 제출된 다른 블록의 예측을 기반으로 검증되며 결과적으로 하나의 체인이 생성되는데 여기서 ‘블록체인’ 이라는 용어가 나왔습니다). 블록체인이 커짐에 따라 새로운 블록의 추가가 어려워집니다. 그리고 검증인은 각자의 네트워크 내에서 캡처하고 재배포하고자 하는 검증 인센티브와 블록 보상의 가치를 모두 확보하기 위해 큰 비용을 들여가며 경쟁합니다. 비잔틴 장애 허용(byzantine fault tolerance) 개념에 대비하기 위한 이 프로세스는 사설망의 경우 비용이 많이 들고 속도도 느립니다. 결과적으로, 비트코인과 이더리움의 초당 거래 처리건수가 20건에 못미치는 이유가 여기에 있습니다.¹⁶ 그 대신에, 텐더민트(Tendermint)에서 구현하고 이더리움의 업그레이드 버전 ‘캐스퍼(Casper)’ 로 제안된 ‘지분 증명(proof of stake, POS)’ 메커니즘에 힘입어 원장 거래 블록을 추가할 권리의 획득 비용은 연산능력 및 전력에 대한 투자에서 암호화폐 자체에 대한 투자로 옮겨갔습니다.¹⁷ 지분증명의 경우, 상대적으로 더 많은 암호화폐를

16. <http://www.altcointoday.com/bitcoin-ethereum-vs-visa-paypal-transactions-per-second/>

17. CIT

보유한 당사자는 그만큼 다음 거래 블록을 추가할 가능성이 높습니다. 각 검증인이 네트워크 내에 ‘투입’ 되어 있기 때문에 네트워크는 거짓 트랜잭션 블록을 생성하여 나머지 네트워크가 후속 수정에 나설 수 밖에 없는 악의적 행위에 대하여 네트워크의 지분을 회수하는 방식으로 검증인을 처벌할 수 있습니다. 하지만 이 접근법 역시 다음 두 가지 이유에서 어려움이 있습니다. 첫째, 네트워크 가치의 51%를 지닌 단일 또는 복수의 당사자가 합의를 이끌어 낼 가능성이 훨씬 높습니다. 둘째, 악의적인 다수의 의견은 작업증명(POW)이 허용하는 연산능력 투자를 통해 뒤집을 수 없습니다. 더욱이, 작업증명이 검증인의 거래 포착을 위해 블록 보상의 형태로 검증 인센티브를 요구하는 것과 마찬가지로 지분증명 또한 네트워크상의 상응하는 재정적 가치 없이도 작업을 창출하는 거래(예: 스팸)가 제출되지 않도록 인센티브(예: ‘가스’)를 사용합니다.¹⁸

금융결제 네트워크에서 특히 사설의 허가형 네트워크는 공용의 익명 네트워크에 비해 공동이익에 의해 더욱 쉽게 조직되고 관리됩니다. 따라서 의심스러운 행위를 방지하기 위한 인센티브 조정 문제는 정확하고 규정을 준수하는 결제를 촉진하는 조정 기능의 회복력과 실질적인 처리량과 관련하여 우려를 제기합니다. 스텔라(Stellar)와 리플(Ripple)을 포함한 여러 네트워크들은 자체 검증인을 사용하거나, 네트워크 결과에 대한 직접 입력을 보호하고자 검증인을 공유함으로써¹⁹ 외부의 악의적인 참가자가 개입할 가능성을 낮춥니다. 여기에서 그들의 합의는 네트워크를 통한 분산 원장의 회복력과 가용성에 초점을 맞추고 있습니다. 결과적으로 처리량은 더욱 높습니다.²⁰

당사는 아이비코인 사설망이 자신 이외의 다른 회사들이 후원하는 유효성 검증 노드로 구성되어 있다고 봅니다. 아이비코인 사설망은 독립적이지만 조율된 금융기관 및 중개기관이 직접 검증하게 됩니다. 이러한 환경 속에서 권한이 부여된 네트워크 참여자의 스팸 메시지는 매우 가능성이 낮고, 애초에 아이비코인 네트워크 참여라는 이들의 공통의 목표에 유해한 것으로도 보입니다. 네트워크 스팸과 인센티브 조정의 가능성이 크게 줄어들며 따라 일반적으로 퍼블릭 블록체인 네트워크를 장려하는 블록 보상이 불필요해집니다. 합의를 위해서는, 이스탄불 BFT와 같이 예정된 비잔틴 장애 허용 알고리즘을 사용하는 것이 가장 합당합니다.²¹ 이 합의된 알고리즘의 각 참여자는 예정된 라운드 로빈 방식으로 블록을 생성하여 그 결과를 나머지 네트워크에 제출합니다. 리더의 블록 계산을 승인하려면 나머지 네트워크의 2/3가 찬성해야 합니다. 이 접근방법에 따르면 네트워크의 검증인 약 1/3이 악의적인 것으로 드러나는 중에도 네트워크는 회복력을 보여줍니다. 이스탄불 BFT의 구체적인 벤치마크는 초당 최대 1000건의 거래를 처리할 수 있음을 보여 주는데,²² 이는 현재 FedWire, SWIFT 및 ACH간에 발생하는 기관간 거래의 전체 예상 네트워크를 반영하고 있습니다.²³

아이비코인 사설망은 그 목적에 부합하여 초기에 이스탄불 BFT 컨센서스 알고리즘을 사용하는 JP모건의 이더리움 네트워크, 퀴럼(Quorum)의 사용을 채택할 것입니다.²⁴ 이 같은 이더리움의 구현은 아이비코인 네트워크 입장에서 많은 잠재적 이점을 갖습니다. 첫째, 글로벌 금융기관의 맥락에서 검증되고 개선된 이더리움 블록체인의 이점을 제공합니다. 둘째, 스마트 계약 개발 및 투자와의 상호운용성을 제공합니다. 이러한 개발 및 투자는 프로토타입화될 수 있고 다른 어떠한 이더리움 가상머신(EVM) 지원환경(Ethermint, Qtum, 심지어 공용 이더리움 블록체인까지도 포함)으로도 이식 가능합니다.^{25, 26} 셋째, 금융 커뮤니티 내에서 대체 블록체인의으로서의 익숙함을 고려할 때, 퀴럼을 채택하고 사용하는 것은 당사가 네트워크 기능을 지원하려 하는 바로 그 금융기관 및 중개기관에 반영될 가능성이 가장 높은 커뮤니티와 지원의 기준이 됩니다. 게다가 높은 거래 처리량이 요구되고 네트워크 참여자의 의도 안정성으로 블록 검증 오버헤드가 감소할 경우, 퀴럼은 선도적인 검증인의 권한을 기반으로 한 대체 합의(consensus) 알고리즘을 지원합니다.

18. 공개 설정에서, 스팸 거래는 합법적인 거래를 밀어내고, 서비스 거부 공격 설정에 존재하는 것과 유사한 환경을 만들 수 있습니다. 검증인이 무의미한 거래에 소모적인 노력을 기울이게 된다면, 가치 있는 거래의 처리가 더 힘들어 집니다.

19. CIT - 스텔라 샤딩 (Stellar sharding)

20. CIT

21. 비잔틴 장애 허용(BFT)은 일반적으로 비잔틴 장군 문제라고 하는 분산 시스템 네트워크 내의 조정 문제를 해결하는 컴퓨터 과학 문제에 대한 레퍼런스입니다. 이에 의해, 자신의 장치에 남겨져 있는 단일 시스템 행위자는 네트워크의 정직한 이익 대신 자신의 이익을 위해 작업하도록 인센티브를 받습니다.

22. CIT

24. <https://github.com/jpmorganchase/quorum>

25. CIT [Ethermint 백서]

26. CIT [Qtum 백서]

사설망 노드는 가용성과 데이터 무결성을 보장하기 위해 IPFS와 BigchainDB를 사용하여 데이터 교환을 조율합니다.^{27,28} 사설망 노드의 논리적 표현은 아래 그림과 같습니다:



개념적 아이비코인 사설망 노드

4) 아이비코인 데이터 컨테이너

개념적 아이비코인 사설망 노드

아이비코인 네트워크는 dxChain 암호화 컨테이너를 사용하여 낱짜 컨테이너(아이비코인 데이터 컨테이너)에 KYT/KYC/AML 데이터를 저장할 것으로 예상됩니다. 데이터는 사용자가 이체 신청을 제출하는 시점에 아이비코인 애플리케이션의 인터페이스를 통해 수집됩니다. 아이비코인 데이터 컨테이너 특유의 컨테이너 형식은 아래 그림과 같습니다:



아이비코인 데이터 컨테이너

아이비코인 데이터 컨테이너에 포함될 내용은 다음과 같습니다.

- 컨테이너 메타데이터
- 거래 메타데이터
- 제출된 거래 세부내역
- 송금인 신원정보(해당되는 경우)
- 증빙서류 및 첨부파일

27. <https://ipfs.io>

28. <https://www.bigchaindb.com>

39. https://en.wikipedia.org/wiki/Grover's_algorithm

근거 데이터의 각 구성요소는 유희 시나 교환 중 액세스를 확보하기 위해 위의 형식을 사용하여 독립적 • 영구적으로 암호화됩니다. 이때 표준 AES-256 대칭 암호화 방법과 4096비트 RSA 비대칭 암호화 방법, SHA-384 메시지 요약(message digests)이 사용됩니다. RSA 비대칭 키 기반의 디지털 서명은 블랙박스 함수 입력 결정과 큰 수의 인수분해에 양자컴퓨팅을 적용하는 것과 관련하여 Grover²⁹ 및 Schor의³⁰ 알고리즘 모두에 대해 취약할 것으로 예상되며,

업계의 이해도와 지원이 향상됨에 따라 이러한 알고리즘은 각각 양자 방지 알고리즘의 유효성을 반영하도록 업그레이드 될 것입니다.³¹

암호 컨테이너는 아이비코인 네트워크에 다음의 몇 가지 주요 기능을 제공한다는 목적을 갖고 있습니다.

- 전달된 모든 정보를 지속적으로 통제하고 보호합니다.
- 최초 수령 후 아이비코인 네트워크가 컨테이너에 당사자를 추가하거나 제거할 수 있도록 해줍니다.
- 수취인과의 거래내역이 기밀정보라는 보증을 발송자에게 제공합니다.

아이비코인 데이터 컨테이너를 사용하여 네트워크에 대한 개별 행위를 추적하고 확인할 수 있습니다.

아이비코인 데이터 컨테이너는 ivySend 계약의 제출 과정에서 취합된 구조화 및 비구조화 콘텐츠 모두를 저장하게 됩니다. 해당하는 경우, 아이비코인은 메시지 표준 ISO 20022의 데이터 세트, 코드 및 형식을 준수하기 위해 아이비코인 데이터 컨테이너 내의 데이터 컬렉션을 표준화합니다.³²

a. 아이비코인 데이터 컨테이너 생성 및 저장

개발 완료 시 아이비코인 네트워크 계약에 콘텐츠가 제출되는 즉시 관련 데이터의 컨테이너를 생성하라는 요청이 아이비코인 네트워크에 대해 전달됩니다. 애플리케이션은 제출된 KYT/KYC/AML 데이터를 아이비코인 네트워크로 보내고 컨테이너 식별자를 발송자에게 돌려보냅니다. 발송자는 자신의 아이비코인 예치금과 생성된 컨테이너 식별자를 ivySend Network 계약에 제출합니다.

생성된 아이비코인 데이터 컨테이너는 아이비코인 사설망의 영역 내에 호스팅되는 IPFS 파일 시스템에 상주하게 됩니다. 아이비코인 사설망의 파일 시스템은 네트워크 내에서 관련 내용을 공유할 수 있게 해줍니다.³³ 요청 시 로컬 사본만 보장되므로 파일 중복을 위해 아이비코인 사설망으로 아이비코인 데이터 컨테이너를 따로 세 차례 기록합니다. 컨테이너 식별자 매핑과 아이비코인 사설망 상의 객체식별 포인트는 아이비코인 사설망의 노드간에 공유되는 BigchainDB 네트워크에 저장됩니다.³⁴

아이비코인 데이터 컨테이너 검색은 관련 컨테이너 검색을 목적으로 관련 객체 식별자를 수신하기 위해 생성 컨테이너의 컨테이너 식별자가 BigchainDB 네트워크에 질의하는 과정입니다. 아이비코인 네트워크 내에서 이 기능은 허가형 네트워크 상의 호스팅된 서비스에 의해 추출 및 유지관리됩니다. 아이비코인 데이터 컨테이너는 기초 보안모델에 위배되지 않으면서 자유롭게 복사 및 저장 가능합니다.

b. 아이비코인 데이터 컨테이너에 대한 액세스

아이비코인 데이터 컨테이너에 대한 액세스는 네트워크 기반(network-bound) 액세스 관리 서비스에 의해 관리됩니다. 이 액세스 관리 서비스는 아이비코인 데이터 컨테이너 내용의 특정 부분에 대한 요청을 처리하고 다음 기준에 따라 필요한 액세스를 제공합니다(편의상 사용자, 시스템 및 시스템 프로세스를 사용자 요청으로 처리합니다).

- 요청 사용자의 조직 – KYC 데이터가 요청하는 사용자 조직에서 발생한 거래와 관련이 있는지 또는 요청한 사용자의 조직이 규제 기구인지 여부의 판단,
- 요청 사용자가 제출한 자격증명 – 요청한 사용자의 자격 증명이 아이비코인 사설망 계정 보유자와 아이비코인 신원 관리 환경 사이의 통신마다 최신의 것인지 여부의 판단,
- 요청 사용자가 제출한 자격 증명에 대한 특정 행정적 제약 및 요청된 신원정보의 특정 유형. 예를 들어 개인식별정보로 식별된 특정 정보는 모든 요청 사용자에게 제공되지 않을 수 있습니다. 이러한 제약은 해당 금융기관의 관리자와 아이비코인 네트워크간의 조율을 거칩니다.

아이비코인 데이터 컨테이너에 대한 권한이 부여되면 요청된 내용이 요청 사용자 또는 프로세스에 제공됩니다.

30. https://en.wikipedia.org/wiki/Shor's_algorithm

31. <http://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.8105.pdf>

32. <https://www.iso20022.org/>

33. <https://ipfs.io/>

34. <https://www.bigchaindb.com>

7

토큰 생성 이벤트 이후의 토큰 구조

아이비코인은 예정된 토큰 생성 이벤트(Token Generation Event; TGE)에 앞서 아이비코인 토큰 사전판매를 실시합니다.

핵심 세부사항

사전판매 청약 공개

보증된 배정 기간¹

사전판매 종료²

사전판매 토큰 물량

사전판매 토큰 가격

사전판매 조달 금액

토큰 생성 이벤트³

토큰 총 발행량

총 공급 토큰 시가총액

2018년 1월 16일

2018년 1월 29일

2018년 2월 9일

1억5천만³

0.10 달러

1,500만 달러³

2018년 1분기 예상

약 15억

8,400만 달러⁴

* 외환 상장 수수료 및 청약 비용 제외

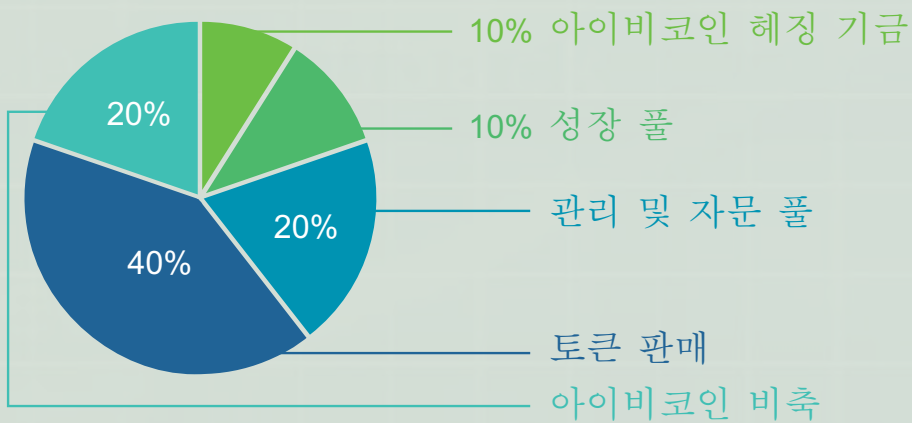


1. 리드 매니저가 응찰을 승낙한 적격 투자자의 경우.
2. 아이비코인은 절대적 재량에 따라 사전판매를 조기에 종료하거나 연장할 권리를 갖습니다.
3. 아이비코인은 절대적 재량에 따라 최대 15억의 아이비코인 총 공급량 내에서 조달 금액을 변경할 권리를 갖습니다. 이 수치는 추정치에 불과하며 당사는 이 수치가 실현될 것이라고 보장하지 않습니다.
4. 이 수치는 추정치에 불과하며 당사는 이 수치가 실현될 것이라고 보장하지 않습니다. TGE에서 조달·발행하는 1,500만 달러 기준, 비순환 공급에는 글로벌 금융 파트너십 구축, 제도적 파트너십, 불환화폐-불환화폐 헤징 및 미래 토큰 판매를 위해 비축해둔 토큰이 포함됩니다.

수익금의 사용⁵



발행 이후 보유 - 총 토큰



범례

- 토큰 판매 - 이전의 모든 토큰 판매 및 관련 토큰 수수료 등 TGE에 앞서 판매된 모든 토큰이 포함됩니다.
- 아이비코인 비축(Ivy Koin Reserve) - 필요한 경우 추가적인 개발 및 운영 자금으로만 사용됩니다.
- 성장 풀 - 금융기관을 포함한 파트너가 아이비코인을 테스트 및 도입하도록 하기 위한 인센티브로 사용됩니다.
- 아이비코인 기금 - ivySend 거래 및 기타 재무기능 촉진에 사용됩니다.
- 관리 및 자문 풀 - 현직 고문 및 미래 경영진이 당사에 합류하도록 하기 위한 인센티브로 사용됩니다.

5. 이 분석은 단지 추정이며, 당사는 모든 수익금을 절대적인 재량에 따라 적합하다고 판단하는 방식에 따라 사용할 권리를 보유합니다.

8

로드맵

다음의 일정 및 이벤트는 각각 예상과 기대에 해당합니다.

단기 계획

2018년 상반기:

- 토큰 생성 이벤트 (2018년 1분기)
- 공개적으로 IVYA 제공
- 스마트 계약과의 테스트 네트워크 라이브
- KYC/KYT 거래 컨테이너
- 아이비코인 공개 인터페이스 라이브
- 금융기관과의 파트너십 구축 미국 규제당국과의 협의

2018년 하반기:

- 공용망 라이브
- 기존 은행간 시스템과의 ivySend 라이브
- 아이비코인이 IVYA 매도 및 시장조작 라이브 지시
- IVBY 은행간 자금이체와의 ivyReceive 라이브
- 금융기관 파트너십 가속화

a. 토큰

사모투자가 완료되는대로 당사는 가능한 한 신속하게 토큰 생성 이벤트를 진행하려고 합니다. 더 자세한 정보는 당사가 제공하는 토큰 생성 이벤트 약관을 참조하십시오.

b. 운영

토큰 출범에는 두 단계가 있습니다.

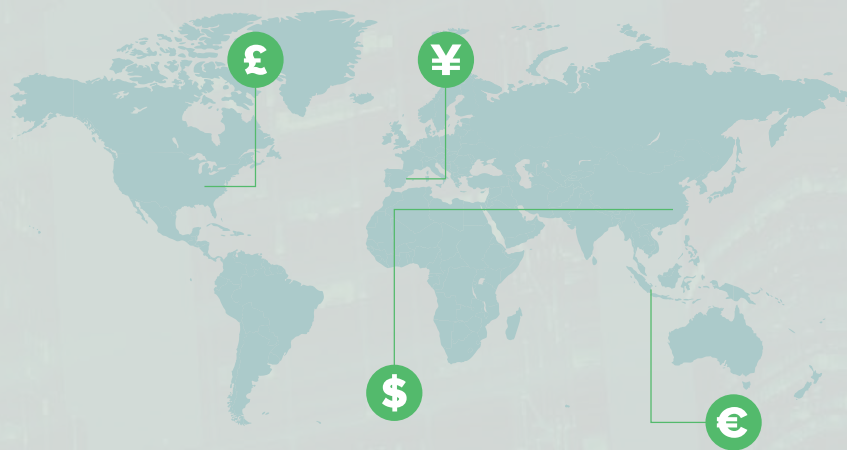
- **토큰 생성 이벤트:** 최초 토큰은 이더리움 기반 토큰으로 채굴됩니다.
- **전면적 출시 및 전환:** 모든 기능을 갖춘 토큰이 이더리움 상에서 사용 가능해집니다.



중장기 계획

2019년

- 모든 불환/암호화폐 전환 라이브
- 컨테이너에 대한 기업 승인
- 최초 금융 중개기관



아이비코인 네트워크 개발은 2018년에 두 단계에 걸쳐 진행될 예정입니다. 아이비코인 네트워크 개발 제 1단계에서는 ACH 또는 전신송금과 같은 기존의 은행간 결제방법을 통해 당사로부터 직접 지급을 받습니다. 제 2단계에서는 은행이 네트워크상의 사설 IVYB 이체를 촉진하는 아이비코인 네트워크 검증인로부터 지급을 받으며 회원 금융기관이 보유한 계정을 통해 해당 기관에 대하여 즉시 • 직접 지급을 됩니다. 향후 당사는 다음과 같이 진행할 계획입니다.

- 전세계 금융기관이 참여하는 네트워크 구축
- 더 많은 불환화폐와 디지털 자산을 포함하도록 변환역량 확장
- 아이비코인 네트워크의 수혜를 입을 수 있는 조직과의 파트너십 개발
- KYT/KYC/AML 데이터 검증을 위한 개선된 방법 개발

위험

권리와 토큰은 투기성이 높은 것으로 간주되며, 권리와 토큰의 구매에는 상당한 위험이 따릅니다. 이사들은 구매 희망자들이 아래에서 설명하는 위험요소와 더불어 본 백서상의 다른 정보를 고려하고, 권리와 토큰의 취득 여부를 결정하기에 앞서 전문가의 자문을 구할 것을 강력히 권고합니다.

다음 위험요소 중 하나라도 잠재적 구매자가 수용할 수 없는 경우에는 권리나 토큰을 구매해서는 안됩니다.

아래에 명시된 위험의 순서는 해당 위험이 발생할 가능성 또는 특정 구매자에 대한 해당 위험의 중요성에 일체 영향을 미칠 의도가 없습니다.

권리 및 토큰 구매는 비트코인, 에테르(Ether) 및 기타 블록체인 기반 소프트웨어 시스템과 같은 암호화 토큰의 사용 및 복잡성과 관련하여 풍부한 경험과 이해를 지닌 개인 또는 단체만이 수행해야 합니다. 구매자는 기타 암호화 토큰과 관련한 저장·전송 메커니즘의 기능을 이해해야 합니다. 당사는 조언을 제공하지 않으며 당사는 구매자가 행하거나 행하지 않은 행동으로 인한 자금, 권리, 토큰의 손실에 대해 일체 책임을 지지 않습니다.

액세스 권한 상실

토큰은 지갑(wallet)에 저장될 수 있고 (그 중에서도) 주요 서명을 통해 액세스할 수 있습니다. 구매자의 디지털 지갑과 관련된 필수 암호기를 상실하면 저장된 토큰도 상실하게 됩니다. 구매자가 암호키 또는 암호키 액세스에 필요한 패스워드의 정확한 기록을 관리하지 못하면 토큰에 대한 액세스를 영구적으로 상실할 수 있습니다. 구매자는 기본 위치에서 제대로 분리된 하나 이상의 백업 위치에 패스워드를 안전하게 보관해야 합니다. 구매자의 암호키에 액세스할 수 있는 모든 제3자는 구매자의 토큰에 액세스할 수 있습니다. 잠재적 구매자가 그러한 경험이나 전문지식을 갖고 있지 않은 경우에는 권리 또는 토큰을 구매해서는 안됩니다.

암호화폐 프로토콜 관련 위험

토큰은 암호화폐 프로토콜을 기반으로 합니다. 아이비코인 프로토콜의 오작동, 예상치 못한 작동, 분기, 고장 또는 폐기는 토큰에 중대한 악영향을 미칠 수 있습니다. 예를 들어, 구매자가 토큰을 이체하지 못하거나 안전하게 보유하지 못하게 될 수 있습니다. 또한, 암호화의 발전 또는 양자 컴퓨팅의 개발은 아이비코인 프로토콜의 근간이 되는 암호화 합의 메커니즘을 무효화할 수 있습니다. 그와 같은 영향은 토큰의 가치에 악영향을 미칠 수 있습니다.



채굴 공격

토큰은 이중 지출 공격, 다수 채굴력 공격(majority mining power attacks), 이기적 채굴 공격, 경쟁 조건 공격을 포함하여(이에 국한하지 않음) 아이비코인 블록체인상의 토큰 거래를 검증하는 과정에서 채굴자로부터 공격을 받기 쉽습니다. 공격이 성공하는 경우, 정확한 실행, 토큰 관련 거래 기록, 예상되는 적절한 지불 활동을 포함하여(이에 국한되지 않음) 토큰에 대한 위험이 따릅니다.

해킹, 사이버 위협, 보안 취약점

해커, 개인, 기타 악의적인 무리 또는 조직은 맬웨어 공격, 서비스 거부 공격, 합의 기반 공격, 시빌 공격(Sybil attack), 스머핑(smurfing), 스푸핑(spoofing)을 포함해(이에 국한되지 않음) 다양한 방식으로 토큰이 거래되는 플랫폼과 토큰 그 자체에 간섭하려는 시도를 할 수 있습니다.

코드 크래킹의 진보, 또는 양자 컴퓨터 개발과 같은 기술적 진보로 인해 토큰에 위험이 제기되고 토큰이 도난 당하거나 손실되는 결과가 초래될 수 있습니다.

시장 위험

당사는 모든 토큰 구매자의 행동을 완전히 통제할 수 없습니다. 제3자 교환소에 의해 토큰의 2차 거래가 진행된다 하더라도 이러한 거래는 비교적 새로운 거래이다 보니 적용 가능한 규제감시가 거의 없고 결국 사기나 조작에 더 취약할 수 밖에 없습니다. 또한 제3자가 외부적 교환가치를 토큰에 귀속시키는 경우(예: 불환화폐로 금액 표시) 그 가치는 극도로 변동성이 심할 수 있고 감소하여 결국에는 사라질 수 있습니다. 구매자가 교환소에서 토큰을 사용하기로 결정하면 구매자 자신이 위험을 감수해야 합니다. 이러한 교환소들은 당사와는 무관하며 당사가 운영하거나 통제하지 않습니다.

교환소의 위험

토큰을 거래할 수 있는 암호화폐 교환소는 상대적으로 새로운 교환소일 것이며 대체로 규제를 받지 않을 가능성이 높기 때문에 충분히 자리를 잡은 정규 거래소에 비해 사기와 실패에 더 많이 노출될 수 있습니다. 토큰 거래량의 상당 부분을 차지하는 암호화폐 교환소가 사기에 연루되거나 보안 침해 또는 기타 운영상의 문제를 겪게 되는 경우, 암호화폐 교환소의 실패는 토큰 가격과 가치의 하락을 초래할 수 있습니다.

무보험 및 거래 손실

은행이나 다른 금융기관의 계좌에 보관하는 자금과는 달리, 토큰은 구매자가 별도로 사보험에 가입하지 않는 한 보험 적용을 받지 않는 것이 일반적입니다. 토큰을 상실하거나 토큰을 사용할 능력을 상실하는 경우, 토큰과 관련하여 적용되는 공보험 또는 사보험은 존재하지 않습니다.

토큰이 도난 당하거나 잘못 이체된 경우, 토큰은 되찾지 못할 수 있으며 당사는 이에 대해 책임을 지지 않습니다. 결과적으로 잘못 실행된 토큰 거래는 토큰의 가치에 악영향을 미칠 수 있습니다. 암호화 토큰 거래는 해당 거래 수취인의 동의 및 적극적인 참여, 또는 이론적으로 호스트 블록체인 플랫폼 상의 연산능력 대부분의 제어나 동의 없이는 되돌릴 수 없습니다. 일단 거래가 검증되어 블록체인에 추가된 데이터 블록에 기록되면, 잘못 실행된 토큰 이체 또는 토큰의 도난은 일반적으로 되돌릴 수 없으며 해당 이체나 도난과 관련한 어떠한 배상이나 법적 또는 기타 상환 수단도 존재하지 않을 수 있습니다. 이러한 손실은 일반적으로 토큰의 가치에 악영향을 미칠 수 있습니다.

불확실한 규제, 집행 조치, 지정학적 사건

상당수 관할지역 내 암호화 토큰, 블록체인, 분산 원장 기술(Distributed ledger technology, DLT)의 규제 상태는 불명확하거나 불안정합니다. 규제 기관이 토큰을 포함하여 위의 기술 및 그 응용과 관련하여 기존 규제를 적용할 수 있는지의 여부 또는 적용 방법을 예측하기란 어렵습니다. 마찬가지로, 입법부나 규제 기관이 토큰을 포함하여 블록체인, 분산 원장 기술(DLT) 및 그 응용에 영향을 미치는 법률과 규정을 변경할지의 여부 또는 변경 방법을 예측하기도 어렵습니다.

규제 조치는, 예를 들어 토큰이 공개, 등록, 라이선스 요건을 유인하는 하나 이상의 관할지역에서 규제되는 금융 상품이라는 결정, 또는 토큰의 사용이나 거래에 대한 전면적 금지를 포함해, 다양한 방식으로 토큰에 악영향을 미칠 수 있습니다.

당사는 규제 조치, 법이나 규정 변경으로 인해 해당 관할지역에서 운영이 불법이 되는 경우, 또는 해당 지역에서의 운영에 필요한 규제상의 승인을 얻거나 관련 규제요건을 충족하는 것이 상업적으로 바람직하지 않은 경우에는 해당 지역에서의 운영을 중단할 수 있습니다.

정치·경제 위기는 토큰의 대규모 매각을 촉발할 수 있으며, 이로 인해 토큰 가격이 하락하고 토큰 가치에 악영향이 미칠 수 있습니다. 본 토큰과 같은 암호화 토큰에는 대안적·분산적 거래 수단에 대한 희망을 기반으로 수요와 공급의 힘이 작용하며, 이러한 수요와 공급이 지정학적 사건으로부터 어떠한 영향을 받을지는 알 수 없습니다. 대규모 토큰 매각은 해당 토큰의 유동성이 감소하는 결과를 초래합니다.

세금

상당수 관할지역 내 권리와 토큰의 조세 특성 및 권리와 토큰 보유에 따른 조세 영향은 분명하지 않습니다. 구매자는 권리와 토큰 구매시 스스로 세금 관련 자문을 구해야 하며, 이는 원천 징수세, 소득세, 세금 신고 요건을 포함해(이에 국한하지 않음) 구매자에게 세금 차원의 불이익을 초래할 수 있습니다. 구매자는 토큰 구매, 사용, 보유시 일체의 과세 요건에 대해 전적으로 책임을 집니다.

불리한 화폐 변동

당사는 권리 매각 수익금을 토큰의 유지관리 및 개발을 위한 자금 조달에 사용할 계획입니다. 해당 청약의 수익금은 액면이 미 달러화로 표기됩니다. 본 행사기간 중이나 이후에 미 달러화 가치가 불리하게 변동하는 경우, 당사는 토큰 개발에 자금을 지원하지 못할 수도 있습니다.

극한의 변동성

토큰은 공식적 또는 법적 구속력 있는 투자에 해당하지 않으며 일단 개발이 되고 나면 반드시 공개시장에서 거래가 되어야 할 필요가 없습니다. 또한 공개시장에서 가치를 지니는 암호화 토큰은 단기간에 걸쳐 정기적으로 극단적인 가격 변동을 보였습니다. 이러한 가격 변동은 시장의 힘이 작용한 결과이며 수요와 공급의 균형이 변화하고 있음을 의미합니다. 교환소 및 공개시장은 당사와는 무관하며 당사가 운영하지 않습니다. 교환소 또는 공개시장에서의 거래는 매수자 본인이 위험을 감수해야 하며 당사는 시장 유동성이나 토큰의 매매 가능성을 보증할 수 없으며 보증하지도 않습니다.

또한 다양한 관할지역의 다양한 규제요건, 전 세계에 위치한 교환소에서 특정 관할지역의 시민이 계정을 개설하지 못할 가능성으로 인해 토큰의 유동성은 관할지역별로 큰 차이가 날 수 있습니다. 이는 시장간의 상당한 가격 차이로 드러날 가능성이 높습니다. 또한 향후 토큰의 가치가 크게 떨어질 수도 있습니다. 이처럼 토큰의 가치가 하락하게 되면 토큰 개발을 포함하여 지속적인 운영을 위한 당사의 자금조달 능력에 악영향을 미칠 수 있습니다.

경쟁 암호화폐가 대부분의 암호화 토큰 사용자층에게 본 토큰보다 더 바람직한 기능을 갖추게 되거나, 기술에 대한 전반적인 신뢰 감소 때문에 암호화 토큰 사용이 전반적으로 위축될 가능성이 있습니다. 실제로 이러한 일이 발생하는 경우, 토큰의 수요와 사용이 감소하여 토큰 가격 전반에 악영향을 미칠 수 있습니다.

또한 암호화폐 교환소의 안정성 결여, 그리고 사기, 사업실패, 해커나 악성코드, 정부 규제에 따른 암호화폐 교환소의 폐쇄 또는 일시적 거래 중단은 토큰 가격의 변동성이 더욱 커지는 결과를 초래할 수 있습니다.

지적재산권 주장

제3자는 권리나 토큰, 소스 코드 또는 그 밖의 기초 지적재산과 관련하여 지적재산권을 주장할 수 있습니다. 지적재산권 주장 또는 기타 법적조치의 가치와 상관없이 해당 조치가 취해졌다는 사실만으로도 토큰 가치에 악영향을 미칠 수 있습니다.

예상하지 못한 위험

권리 및 개발될 토큰은 상대적으로 검증되지 않은 신기술에 해당합니다.

위에서 언급한 위험 외에도, 당사가 예상하지 못한 위험을 비롯해 권리나 토큰의 구매, 보유, 사용과 관련된 위험이 존재합니다.

예상치 못한 위험은 앞서 명시한 위험이 변형되거나 조합된 방식으로 나타날 수 있습니다.

G

용어해설

이더리움(ETHEREUM)

이더리움은 스마트 계약을 위한 주요 분산형 플랫폼으로, 솔리디티(Solidity) 프로그래밍 언어를 사용합니다. 오픈 소스, 퍼블릭 블록체인 기반의 분산 컴퓨팅 플랫폼입니다.

에테르(ETHER)

이더리움 블록체인 플랫폼의 가치 토큰을 ‘에테르’라고 합니다.

스마트 계약

스마트 계약은 당사자간 교환관계의 정확한 조건을 명시적으로 기술한 프로그래밍 추상개념입니다. 스마트 계약 조건은 거래의 기록과 실행에 앞서 ‘사실’임이 만족되고 확인되어야 합니다. 스마트 계약은 솔리디티(Solidity)라는 프로그래밍 언어로 작성됩니다. 모든 스마트 계약은 모든 블록체인 노드에 공개적으로 저장됩니다.

IPFS

영구적으로 문서를 생성, 저장, 공유할 방법을 제공하는 오픈 소스, 분산형 파일시스템 프로토콜입니다. IPFS 노드는 분산형 파일공유 네트워크의 근간이 됩니다. 블록 스토리지 모델을 기반으로 하는 높은 처리량입니다. 파일 식별을 위해 해시를 사용함으로써 변경 불가능한 데이터를 저장할 수 있는 견고한 환경을 조성할 수 있습니다.

SOLIDITY

블록체인을 위한 스마트 계약은 솔리디티(Solidity)라는 프로그래밍 언어로 작성됩니다.

X509

공개키 인증서 정의를 위한 암호화 표준. 보안 통신의 핵심 구성요소이며 전자거래시 ‘디지털 서명’ 검증에 사용될 수 있습니다. X.509는 전기 통신 • 표준의 국제적 조율을 담당하는 유엔 산하 국제전기통신연합(ITU)에서 규정합니다.

PKI

공개키 인프라(PKI)는 디지털 인증서의 작성, 관리, 배포, 사용, 저장, 취소에 필요한 일련의 역할, 정책, 절차이며 공개키 기반 암호화 시스템의 핵심 구성요소입니다.

신뢰 체인

신뢰 체인은 하드웨어와 소프트웨어의 각 구성요소를 상향식으로 검증함으로써 구축합니다. 이는 체인 내의 각 하드웨어 및 소프트웨어 구성요소를 검증함으로써 오직 신뢰할 수 있는 소프트웨어 및 하드웨어만 사용될 수 있도록 해줍니다.

데이터 필드

거래에서 전송되는 데이터의 양은 당사자가 정의내린 요구사항과, 거래를 관장하는 스마트 계약의 요구사항에 따라 달라집니다. 아이비코인은 (간단한 계정 개설 프로세스 이외에) 고객 데이터를 검증하는 것이 아니라, 오히려 검증을 용이하게 해줍니다.



ivyKoin

Ivy Koin LLC
Ivy Management Group LLC

468 N. Camden Drive, Suite 200,
Beverly Hills, CA 90210

www.ivyKoin.com