[52페이지: 아래서 3행]

비유할 수 있다. 이 주소에는 암호키에 대한 정보가 들어 있기 때문에 거래 당사자의 주소만 있으면 별도의 추가 정보가 없어도 해당 키를 가진 사람이 이를 통제할 수 있게 된다.

→

비유할 수 있다. 그러나 금융기관이 발급하는 계좌번호와 달리 이 주소는 각 개인이 임의로 만들어 사용하므로 절대 익명의 거래가 가능하다. 이 주소에는 암호키에 대한 정보가 들어 있기 때문에 거래 당사자의 주소만 있으면 별도의 추가 정보가 없어도 해당 키를 가진 사람이 이를 통제할 수 있게 된다. 그 자세한 기술적 메커니즘을 알고 싶다면 부록 4를

[13페이지: 아래서 3행]

벽이 낮기 때문이다. 한마디로 쉽게 돈벌이가 되며 별다른 기술이 필요 없기 때문이다.

→

장벽이 낮기 때문이다. 한마디로 쉽게 돈벌이가 되는 것에 비해 별다른 기술이 필요 없기 때문이다.

[42페이지: 아래서 8행]

는 통상 법화(법정통화)만을 일컫는다. 따라서 암호화폐는 법화가 아니기 때문에 질문 자체가 성립하지 않는다. 이 질문은 순전히 그 이름 때문에 생긴 것이다. 비트코인이 화폐

→

통상 법화(법정통화)만을 일컫는다. 따라서 암호화폐는 법화가 아니기 때문에 질문 자체가 성립되지 못한다. 이 질문은 순전히 그 이름 때문에 생긴 것이다. 비트코인이 화폐인가 하

[50페이지: 메모 박스 6행]

2. 2017년 7월 대니 라이언(Danny Ryan)이라는 사람은 재미있는 실험을 하나 하고, 그 결과를 해커눈(Hacker Noon) 사이트에 소개했다. 라이언은 단순 덧셈을 100만

→

2. 2017년 7월 대니 라이언(Danny Ryan)이라는 사람은 재미있는 실험을 하고, 그 결과를 해커눈(Hacker Noon) 사이트에 소개했다. 라이언은 단순 덧셈을 100만 번 할

[50페이지: 각주 1번]

1 이더리움은러시아 개발자 비탈릭 부테린(Vitalik Buterin)이 비트코인을 흉내 내 2015년에 만든 새로운 암호화폐다.

→

1 이더리움은 러시아 개발자 비탈릭 부테린(Vitalik Buterin)이 비트코인을 흉내 내 2015년에 만든 새로운 암호화폐다.

[63페이지: 4행]

BTC를 보내기 위해 실제로 0.0035 BTC가 필요한 것이다.

→

있는데, 2018년 초 기점으로 약 0.003 BTC에 육박한다. 즉, 0.0005 BTC를 보내기 위해 실제로 0.0065 BTC가 필요한 것이다.

[64페이지: 3행]

된 정의조차 존재하지 않는다. 심지어 비트코인 논문에는 '블록체인'이라는 단어가 단 한 차례로 언급되지 않는다. 원 논문에는 오로지 블록과 체인이라는 일반명사만 개별적으로

→

된 정의조차 존재하지 않는다. 심지어 비트코인 논문에는 '블록체인'이라는 단어가 단 한 차례도 언급되지 않는다. 원 논문에는 오로지 블록과 체인이라는 일반명사만 개별적으로

[85페이지: 아래서 7행]

를 자신의 개인키로 암호화한 뒤 배부한다. 이 메시지를 전달받은 사람들은 투자자가 제공한 공개키를 사용해 메시지를 검증한다. 투자자가 개인키로 암호화한 메시지는 오로지

→

신의 개인키로 암호화한 뒤 배부한다. 이 메시지를 전달받은 사람들은 투자 전문가가 제공한 공개키를 사용해 메시지를 검증한다. 투자 전문가가 개인키로 암호화한 메시지는

[85페이지: 아래서 6행]

공한 공개키를 사용해 메시지를 검증한다. 투자자가 개인키로 암호화한 메시지는 오로지 짝이 되는 공개키로만 복호화 할 수 있으므로 이 메시지가 공개키로 복호화된다는 사실

→

공한 공개키를 사용해 메시지를 검증한다. 투자 전문가가 개인키로 암호화한 메시지는 오로지 짝이 되는 공개키로만 복호화 할 수 있으므로 이 메시지가 공개키로 복호화된다

[85페이지: 아래서 4행]

은 메시지가 분석가의 개인키로 암호화됐다는 사실과 투자 전문가가 작성한 것이 확실함을 증명해준다.

→

는 사실은 메시지가 투자 전문가의 개인키로 암호화됐다는 사실과 그가 작성한 것이 확실함을 증명해준다.

[101페이지: 1행]

이제 블록체인의 작동 원리를 이해하기 위해 알아야 할 기본 기술을 모두 살펴봤다. 이제

→

지금까지 블록체인의 작동 원리를 이해하기 위해 알아야 할 기본 기술을 모두 살펴봤다.

[119페이지: 팁박스 추가]

TIP

놀랍게도 앞서 설명한 탈중앙화 합의라는 성질로 인해 블록체인의 모든 거래는 영원히 확정되지 않는다. 확률은 극히 낮지만 이론적으로는 2009년에 최초로 채굴된 블록조차 퇴출될 수 있기 때문이다. 따라서 즉시 거래가 확정되는 중앙 시스템과 달리 블록체인은 영원히 거래가 확정되지 않는 불안정한 시스템으로 볼 수 있다.

[187페이지: 팁박스 추가]

TIP

폭등하는 비트코인을 보고 "투자할 걸"이라고 생각했다면 큰 오산이다. 오르는 종목을 사는 것과 수익을 얻는 것의 상관관계는 의외로 낮다. 예컨대 2020년 S제약을 샀다면 이론적으로 최대 16배 가까이 벌 수 있었지만, 반대로 -70%의 손실을 볼 수도 있었다. 워렌 버핏은 "주식이 오른다고 사는 것은 매우 바보 같은 짓이다."라는 말을 남겼다.

비트코인의 현 가격이 '적절한가?'에 대한 확실한 분석을 할 수 없다면 쳐다보지 않는 것이 현명하다. 모든 비트코인 주소 중 단 2%가 전체 물량의 95%이상을 가지고 있다는 점을 항상 명심하라.

[188페이지: 메모박스 추가]

Memo

2020년 페이팔(Paypal)은 자사 고객을 상대로 암호화폐 중개 서비스를 개시한다고 밝혔다. 비슷한 시기에 싱가포르 최대 상업은행인 DBS도 암호화폐 거래 관련 서비스를 개시한다고 발표했다. 페이팔은 한발 더 나아가 암호화폐를 물품 구매에 즉시 활용할 수 있게 서비스하겠다고 선언했다. 이 때문에 암호화폐에 대한 중대 전환점이 생긴 것처럼 떠드는 언론도 등장했다.

삼성전자가 카지노를 운영하면 포커가 도박이 아닌 기술로 바뀌는가? 결제 분야 세계 최고 기업과 거대 상업은행이 암호화폐를 중개한다고 해서 비트코인의 투기 속성과 자금세탁 위험이 사라지지는 않는다. 이 두 기업은 단지 중개 수수료가 돈이 되리라 판단한 것뿐이다.

한편, 페이팔은 물품 구매에 암호화폐를 쓸 수 있게 한다고 주장하지만, 정작 물품 판매자는 법화를 절대적으로 더 선호한다. 이 때문에 페이팔은 매번 중간 환전이라는 비정상적인 절차로 비용을 낭비하며 변동성 큰 구매자의 암호화폐를 법화로 바꾼 뒤 판매자에게 지급해야 할 것이다.

원래 기업이란 돈이 되면 뭐든 하려고 한다. 이 때문에 영리 추구만을 목적으로 하지 않는 사회적 기업에 대한 갈망이 더 커지고 있다. 암호화폐 중개 수수료 시장은 분명히 크다. 그러나 모두가 그 시장에 뛰어들지 않는 이유는 '사회적 기여'에 대한 기업들의 판단 기준이 다르기 때문일 뿐이다. 기업의 존재 이유를 '주주 이익의 극대화'로 주장하는 미국식 주주자본주의는 돈만 되면 대량해고를 비롯해 뭐든 다하는 몰염치한 기업들을 양산했다. 최근 테슬라의 일론 머스크는 비트코인을 사면서 다른 사람들도 사라고 부추겼다. 카지노의 승자는 주인뿐이다. 코인 시장이 활성화되면 유일한 승자는 중개소일 뿐, 참여자 대다수는 돈을 잃고 극소수만 돈을 딴다. 이는 아무런 사회적 가치가 없다. 일론 머스크도 결국 남의 돈을 땄거나 잃었겠지만 그 과정에 아무런 사회적 기여를 못할 것은 분명하다.

[216페이지: 소제목]

8.1.1② 기형적 숫자 놀음의 끝판왕 – 비트코인 골드

→

8.1.1① 기형적 숫자 놀음의 끝판왕 - 비트코인 골드

[227페이지: 아래서 3행]

익만 적절히 감춰 두면 형을 마친 후 편하게 살 수 있다고 생각하기 때문이다. 2011년에는 인터넷 도박으로 부당 이득을 취한 범인이 110억 원에 가까운 돈을 자신의 마늘 밭에 5만 원권으로 숨겨 뒀다가 적발된 사건이 있었다. 당시 비트코인의 존재를 알았다면 범

→

익만 적절히 감춰 두면 형을 마친 후 편하게 살 수 있다고 생각하기 때문이다. 2011년에는 인터넷 도박으로 부당 이득을 취한 범인이 110억 원에 가까운 돈을 매형의 마늘 밭에 5만 원권으로 숨겨 뒀다가 적발된 사건이 있었다. 당시 비트코인의 존재를 알았다면 범인

[238페이지: 8.6.2 1행]

프랑스는 유럽연합EU 회원국 중 가상자산에 가장 우호적인 것으로 알려져 있다. 진작에 ICO Initial Coin Offering를 전면 금지한 중국이나 명시적으로 금지하지는 않았지만 법률 집행을 통해 간접적으로 ICO를 금지[15]하고 있는 우리나라와는 달리 토큰을 자유롭게 발행하고 유통할 수 있다. 스위스 역시 가상자산에 대해 대단히 우호적인 것으로 유명하다. 특히 한때 ICO의 메카로 알려진 스위스 추크Zug시는 자국의 규제를 피해 각국의 코인 업체들이 ICO만을 위해 몰려들었고 받아쓰기 언론들은 인구가 고작 3만 명인 추크시의 알자리가 블록체인 덕분에 10만여 개 만들어졌다는 가짜 뉴스도 여과없이 퍼트려 빈축을 사기도 했다. 2020년 현재 추크시는 파산 직전에 있고 스위스 연방정부에 1,300억 원에 달하는 구제 금융 지원을 요청했으나 거부당한 상태다. 스위스 연방정부는 코로나 바이러스 사태로 인해 유사한 구제 금융신청을 24건 접수했는데, 유일하게 추크시의 신청만 거부했다. 그 배경에 추크시가 내세운 가상자산 관련 사업의 허황됨이 있음은 자명한 일일 것이다. 스위스의 블록체인 협회 설문에 따르면 스위스 내 가상자산 관련 기업의 80% 이상이 파산 직전으로 파악되기도 했다.[x]

한편 일본은 화이트 리스트를 사용하는 대표적인 국가다. 우리나라를 포함한 대다수의 국가에서는 중개소에서 취급하는 코인은 중개소 스스로가 임의로 결정한다. 그러나 일본에서는 정부에서 허가한 소수의 코인만 취급할 수 있고 화이트 리스트에 없는 새로운 코인을 취급하려면 금융청에 그 이유를 설명할 수 있는 자료를 제출해 별도 허가를 받아야 한다. 일본은 진작에 가상자산으로 얻은 수익에 최대 50%의 양도세를 부과하는 것으로도 유명하다. 현재 우리나라도 20% 수준에서 가상자산의 차익에 대한 양도세를 준비하고 있으나, 일본에 비하면 매우 약한 수준이다. 또 비상장 주식에 대한 양도세율이 최대 30%이고 부동산과다보유법인 등의 경우는 양도세율이 최대 40%까지 과세되는 점을 감안하면 가상자산에 부과하는 20%는 상대적으로 아주 작은 편이다.

가상자산에 대한 각국 정부의 세부적인 대응은 천차만별이지만, 두 가지 공통적인 부분이 있다. 이 두 가지를 살펴보면 우리나라 정부의 향후 방향도 예측해볼 수 있을 것이며, 그에 따라 가상자산에 대한 각국 정부의 대응도 예상할 수 있을 것이다.

첫째, 투자자 보호 측면이 강화되고 있다. 중개소가 취급할 수 있는 종목을 정부에서 지정해주는 국가부터 소비자 보호를 위해 중개소에 부과한 각종 의무 사항이 갈수록 강화되고 있다.

둘째, ML/TF 위험 요소를 줄이기 위한 CDD[16]가 빠르게 도입되고 있다.

→

미국은 가장 적극적으로 가상자산을 규제하는 국가 중 하나이며 그 발행과 관련해서는 연방법이 적용되고 증권거래 위원회SEC, U.S. Securities and Exchange Commission가 관장한다. 즉, 발행되는 자산이 증권으로 제공 또는 거래되거나 집합투자를 통해 행해지면 증권법으로 규제한다는 입장이다. 2017 ICO 형태로 진행됐던 이더리움 재단의 The DAO 사태도 증권법과 거래소법의 위반 소지가 있다고 보는 것이 SEC의 판단이다.

한편 가상자산의 거래에 관해서는 개별 주마다 다른 법령을 적용하는데 뉴욕주의 경우에는 새로운 법령을 제정한 반면, 워싱턴주는 기존의 법령을 그대로 적용한다. 전체적으로 보면 미국은 가상자산의 거래에 있어서 기존 핀센FinCen이 발효한 트래블 룰을 가상자산에도 그대로 적용한다는 원칙을 갖고 있다.

한편, 가상자산에 대해 대단히 우호적인 국가로는 스위스와 싱가포르가 있다. 페이스북의 리브라 어소시에이션을 비롯해 900여 개가 넘는 블록체인 혹은 암호화폐 관련 단체들이 모두 스위스로 몰려드는 것도 이러한 우호적인 환경 때문이다. 스위스는 일반적으로 암호화폐의 개발과 유통을 규제하지 않지만 미국과 마찬가지로 자산형 토큰이나 유틸리티 토큰 등의 경우 해당 자산이 증권에 해당하는지 별도로 판단하고 있다.프랑스 역시 가상자산이 증권발행과 유통에 관한 기존 법령에 상충하지 않는 한 토큰의 발행과 유통은 가능하다는 입장이나 2016년을 기점으로 블록체인과 암호화폐는 엄격히 분리해 취급하고 있다.

일본은 암호화폐에 대한 규제 플랫폼을 구축한 최초의 국가에 속한다. 초기부터 중개소에 대한 등록과 함께 투자자들에 대한 보호와 자금 세탁 방지 대책을 수립해왔고 2018년 중개소 해킹으로 6천억 원이 도난당하는 사건을 기점으로 본격적인 규제를 제정하기 시작했다. 일본은 실질적으로 화이트 리스트를 통해 매매 가능한 코인 종류를 통제해오고 있으며 리스트에 없는 코인을 거래하려면 금융청의 심사를 받아야 한다. 이 때문에 일본은 일찍부터 대시나 z 캐시 등 자금 세탁 기능이 강화된 코인을 시장에서 퇴출시켜 버렸다. 한편 일본은 암호화폐 매매로 인한 연간 시세차액에 과세하며 20만 엔을 넘을 경우부터 최소 15%에서 최대 55%까지 세금을 부과하고 있다.

홍콩은 ICO를 전면 금지한 중국과는 다른 법령을 적용하고 있으며 증권선물법(SFO)를 통해 규제하고 있다. 대체로 지급결제수단으로서의 가상자산에 대해서는 별도의 규정을 마련하고 있지 않지만 증권형 토큰의 경우 SFO의 규제를 받을 수 있으며 성격에 따라 다른 면허를 취득해야만 한다.

[239페이지: 2행]

두고 있다. 그러나, 특정금융법의 시행령의 마련과 동시에 가상자산사업자에 의무를 부과해 소비자 보호 측면을 강화할 가능성이 높아진다. 이 경우 지금까지 중개소 스스로 운

→

두고 있다. 그러나, 특정금융법의 시행령의 마련과 동시에 가상자산사업자에 의무를 부과해 간접적으로 소비자 보호 측면이 강화되는 효과도 생길 것이다. 이 경우 지금까지 중개

[239페이지: 2행]

두고 있다. 그러나, 특정금융법의 시행령의 마련과 동시에 가상자산사업자에 의무를 부과해 소비자 보호 측면을 강화할 가능성이 높아진다. 이 경우 지금까지 중개소 스스로 운

→

두고 있다. 그러나, 특정금융법의 시행령의 마련과 동시에 가상자산사업자에 의무를 부과해 간접적으로 소비자 보호 측면이 강화되는 효과도 생길 것이다. 이 경우 지금까지 중개

[240페이지: 마지막 문단 추가]

가상자산에 대한 각국의 법 규정 제정 방향을 살펴보면 큰 맥락에서의 공통점은 사적 자치는 어느 정도 보장해주되, 자금세탁과 관련한 것은 철저히 규제한다는 것을 알 수 있다. 또 일본 등의 예외 경우를 제외하면 투자자 보호를 위한 법률 규정은 명시적으로 보이지 않는다.

[246페이지: 메모박스 1행]

현재 특정금융법상에서는 가상자산에서 게임 아이템, 선불카드, 전자등록주식 등을 제외하도록 일일이 열거하고 있다. 이 경우 새로운 형태의 디지털화 자산 또는 디지털 자산

→

현재 특정금융정보법상에서는 가상자산에서 게임 아이템, 선불카드, 전자등록주식 등을 제외하도록 일일이 열거하고 있다. 이 경우 새로운 형태의 디지털화 자산 또는 디지털 자

[275페이지: 아래서 3행]

기 저장된 모든 트랜잭션의 정보로부터 추출된 해시 값은 0에서 설명한 머클트리 루트에 저장된다. 따라서 여기에 사소한 변화라도 생기면 머클트리 루트 값을 통해 바로 감지할

→

저장된 모든 트랜잭션의 정보로부터 추출된 해시 값은 앞서 설명한 머클트리 루트에 저장된다. 따라서 여기에 사소한 변화라도 생기면 머클트리 루트 값을 통해 바로 감지할 수

[282페이지: 1행]

이는 앞서 유사 코드로 살펴본 절차와 완전히 일치한다. ❶에서 블록이라 쓰인 박스 내의 오른쪽 아래 그림 A2-2에서 점선 박스에 있는 난스 부분이다.

→

앞서 유사 코드로 살펴본 절차와 완전히 일치한다. ❶에서 블록헤더라고 쓰인 박스 내의 오른쪽 아래 그림 A2-2에서 점선 박스에 있는 난스 부분이다.

[293페이지: 팁박스 1행]

그림 A4-3이나 A4-3에 있는 asm과 hex는 동일한 내용이다. 편의상 asm은 스크립트 형태, hex는 16진수로 중복해 표현한 것일 뿐, 실상은 같다.

→

그림 A4-2나 A4-3에 있는 asm과 hex는 동일한 내용이다. 편의상 asm은 스크립트 형태, hex는 16진수로 중복해 표현한 것일 뿐, 실상은 같다.