국민의 평생 금융파트너

디지털자산 보고서 시리즈 제3편

가상자산거래소를 바라보는 금융의 시선

2022. 11

연구위원 권세환

■ 누구도 알려주지 않는 가상자산거래소 이야기

■ 가상자산 지갑에 대한 이해

■ 신문 헤드라인으로 살펴본 가상자산거래소

[참고] FTX 거래소에 무슨 일이 있었나?

KB금융지주 경영연구소
www.kbfng.com/kbresearch

※ 해당 보고서는 디지털자산 보고서 시리즈 중 제3편으로,
가상자산의 기본적 개념 등 기존에 소개된 내용은 중복해서 설명하지 않았음을 참고 부탁드립니다

[Executive Summary]

■ 가상자산거래소는 증권거래소와 비슷해 보이지만 세부적으로 살펴보면 차이점이 존재

➔ 주식시장은 금융투자회사(채널) – 한국거래소(거래 체결) – 한국예탁결제원(실물 보관)으로 권한이 분산되는 구조인데 반해, 가상자산시장은 가상자산거래소가 중개를 비롯해 상장, 예탁, 매매, 결제 등 거의 모든 기능을 단독으로 수행

■ 한때 국내 가상자산거래소에는 공급이 급격히 증가한 시장 수요를 받쳐주지 못하면서 해외 거래소 대비 5%~20% 코인 가격이 높은 '김치프리미엄'이 발생

➔ 국내는 코인 채산성이 낮아 채굴을 통한 공급이 부족했고, 해외는 중국 등의 투기 세력 자금 유입으로 수요가 급증하면서 김치프리미엄이 가속화

➔ 시장 간 가격 차이가 발생하면 보통 재정거래를 통해 가격 안정화가 이뤄지지만, 가격이 낮은 해외 거래소에서 코인을 구매하는 것 자체가 제한되면서 사실상 재정거래가 어려워짐

■ 가상자산거래소에서 자산 매매는 실제로 실물이 거래되는 것이 아니라 단순히 장부에 숫자만 바뀌는 일종의 '장부거래'

➔ 가상자산은 거래소에서 개인 지갑으로 자산이 출금(이체)될 때 비로소 실질적인 이동이 발생

➔ 거래 편의성을 고려할 때 장부거래 자체가 잘못된 것은 아니지만, 고객이 보유한 잔액만큼 거래소가 실제 코인을 가지고 있느냐에 대한 검증이 어렵다는 우려가 존재

➔ 거래소는 고객의 급작스러운 출금 요청에 대비해 충분한 유동성 확보가 매우 중요한데 고객 입장에서는 이에 대한 객관적 검증이 불가능

■ 가상자산 지갑이란 블록체인 네트워크에서 본인이 소유한 자산을 인증할 수 있는 개인키를 관리하는 도구로 지갑 주소는 계좌번호, 개인키는 비밀번호와 유사

➔ 가상자산이 실제로 지갑에 들어 있는 것은 아니며, 실질적인 가상자산은 블록체인 네트워크 내 존재하고 이에 대한 접근권(소유권)만 패스워드(개인키) 형태로 지갑에 보관(개인키를 분실할 경우 코인을 모두 잃어버리는 것이므로 개인키 자체를 코인이라 봐도 무방)

■ 글로벌 3 대 암호화폐거래소 FTX 가 지난 11 월 11 일 파산을 신청하면서 시장에 큰 파장

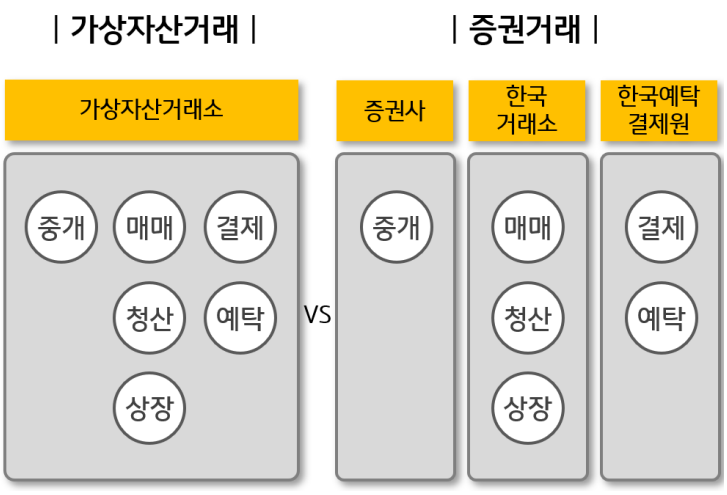
➔ FTX 계열사 알라메다리서치가 과도한 FTT 담보 레버리지 투자를 감행했고, 여기에 FTX 의 부실 경영과 고객 자금 유용 등의 의혹이 불거지면서 유동성 위기가 발생

■ 누구도 알려주지 않는 가상자산거래소 이야기

○ 가상자산거래소[1]는 비트코인, 이더리움 등의 가상자산을 다른 자산과 교환할 수 있는 거래소를 뜻함

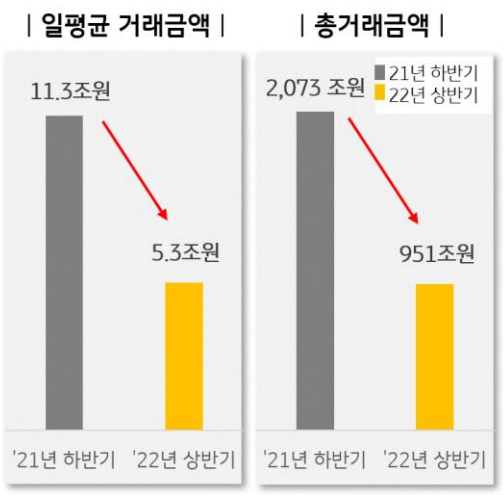
- 가상자산거래소는 증권거래소와 비슷해 보이지만 세부적으로 살펴보면 차이점이 존재
  - 가상자산거래소는 개장 시간과 폐장 시간이 없는 매일 24시간 1년 365일 운영
  - 증권거래소는 모든 유가증권이 한국거래소(KRX) 한곳에서 유통되는 구조인데 반해, 가상자산거래소는 서로 독립적으로 운영됨에 따라 거래소별 코인 가격이 다름
  - 주식시장은 금융투자회사(채널) - 한국거래소(거래 체결) - 한국예탁결제원(실물 보관)으로 권한이 분산되는 구조인데 반해, 가상자산시장은 가상자산거래소가 중개를 비롯해 상장, 예탁, 매매, 결제 등 거의 모든 기능을 단독으로 수행
- 2022년 상반기 가상자산시장은 거래 금액과 가치 모두 전년 대비 상당한 하락세를 보임
  - 2022년 상반기 금융위원회에서 실시한 가상자산 사업자 실태 조사에 따르면 국내 가상자산 일평균 거래금액은 5조 3천억 원으로 작년 하반기 11조 3천억 원에서 53% 하락
  - 국내 가상자산 시장가치[2]는 2022년 6월 말 기준 23조 원으로 2021년 하반기 55조 2천억 원 대비 32조 2천억 원이 감소

[그림 1] 가상자산 거래 vs 증권 거래



자료: 연구자 작성

[그림 2] 가상자산 거래금액 변화



자료: 2022년 상반기 가상자산 사업자 실태 조사

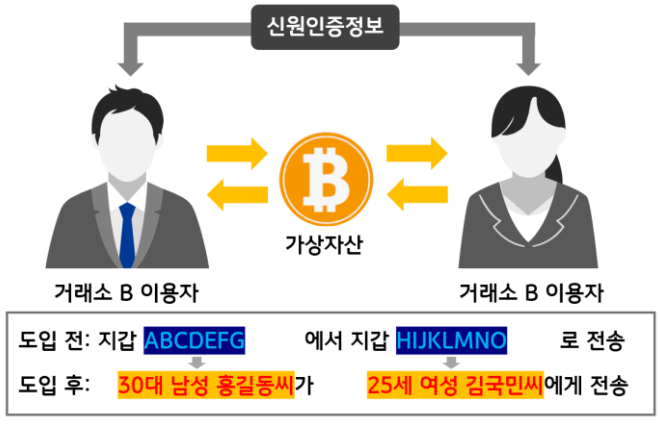
[1] 해외에서는 암호화폐거래소(Cryptocurrency Exchange)라는 이름을 사용

2 Σ사업자별 보유 거래 지원 가상자산 수량 * 해당 가상자산의 시장가격

- 국내에서는 특정금융정보법(특금법)에 따라 세계 최초로 트래블룰(Travel Rule)[3]을 도입하면서 자금 추적에 대한 투명성을 강화
  - 국제자금세탁방지기구(FATF)는 가상자산이 자금 세탁이나 테러자금 조달 행위 등에 활용되는 것을 막기 위해 고객 정보 수집 의무를 부과하는 트래블룰 지침을 발표했고, 한국은 특금법 시행령 개정안에 이 내용을 포함시킴
  - 원화마켓을 운영 중인 가상자산거래소들은 ISMS(정보보호관리체계) 인증 취득과 시중은행 실명계좌 발급 의무화를 수용하면서 제도권 진입에 첫발을 내딛음

- 한때 국내 거래소에는 공급이 급격히 증가한 시장 수요를 받쳐주지 못하면서 해외 거래소 대비 5%~20% 코인 가격이 높은 '김치프리미엄'이 발생
  - 국내는 코인 채산성이 낮아 채굴을 통한 공급이 부족했고, 해외는 중국 등의 투기 세력 자금 유입으로 수요가 급상승하면서 김치프리미엄이 가속화
  - 시장 간 가격 차이가 발생하면 보통 재정거래(Arbitrage)[4]를 통해 가격 안정화가 이뤄지지만, 가격이 낮은 해외 거래소에서 코인을 구매하는 것 자체가 제한되면서 사실상 재정거래가 어려워짐[5]
  - 현재는 가상자산 가격이 급락하면서 시장 수요가 줄었기 때문에 김치프리미엄이 크지 않은 수준

[그림 3] 트래블룰 도입 후 변화



자료: <매일경제>

[그림 4] 김치프리미엄 확인 사이트

Upbit 기준거래소 / Binance 비교거래소

코인	binance($)	upbit(₩)	김치프리미엄(₩)
BTC	20,530.42	28,807,000	-479,644 (-1.64%)
ETH	1,587.74	2,226,000	-38,911 (-1.72%)
BCH	115.60	162,250	-2,653 (-1.61%)
LINK	7.936	11,130	-190.7 (-1.68%)
DOT	6.690	9,395	-148.3 (-1.55%)
XRP	0.4609	646.0	-11.5 (-1.75%)
ADA	0.4017	563.0	-10.0 (-1.75%)

자료: cryprice.com

[3] 자금 세탁 방지를 위해 시행되는 제도로서, 디지털 자산을 주고받을 때 가상자산 사업자가 송수신자의 정보를 확인하는 규칙
[4] 가격이 저렴한 시장에서 매입하고 비싼 시장에 매도함으로써 매매차익을 얻는 거래 행위
[5] 해외 거래소에서 직접 코인을 구매하기 위해서는 현지 계좌를 가지고 있어야 하며, 만약 해외은행 계좌가 있더라도 국내에서 해외로 송금 가능한 한도는 연간 5만 달러에 불과

○ 국내 원화마켓 5대 가상자산거래소는 업비트, 빗썸, 코인원, 코빗, 고팍스이며 이들 중 상위 3대 거래소가 시장 대부분을 점유

- **[업비트]** 카카오가 지분 투자한 두나무에서 운영 중인 국내 최대 가상자산거래소
  - 오프라인 중심 타 제휴 은행 대비 비대면 계좌 개설이 용이한 K뱅크와 제휴하여 코로나 시기 신규 고객 유입을 극대화했고, 로그인과 입출금 시 카카오 서비스를 연동해 UI/UX(사용자 인터페이스/사용자 경험) 최적화에도 많은 노력을 기울임
  - 반면 고객센터 연결이 어렵고 상담 대응이 느리다는 평가

History 업비트 시기별 이슈 정리

시기	내용	기타
2018.01	기업은행 실명계좌 발급 계약 체결	
2018.05	보유하지 않은 암호화폐를 판매한 혐의로 압수수색	회계법인 실사 후 사기 혐의에서 벗어남
2018.12	자전거래를 통해 1,492억 가량의 부당이익을 챙긴 혐의	1심 무죄, 2심 진행중
2019.11	580억원 상당의 이더리움 해킹	북한 해킹조직 연류 추측
2020.06	케이뱅크와 실명계좌 발급 계약 체결	앞선 이더리움 해킹으로 기업은행 실명계좌 재계약 불발

- **[빗썸]** 한때 국내 1위 가상자산거래소였으나 현재는 업비트에 이어 2위. 가상자산 종합정보 사이트 코인마켓캡(Coinmarketcap)의 거래소 평가점수[6]가 6.2로 국내 거래소 중 가장 높음
  - 24시간 고객 상담이 가능하고, 원화 출금 한도가 최대 보안등급 인증 시 1일 20억 원으로 타 거래소 대비 높음
  - 수수료가 0.25%로 경쟁사 대비 비싸며, 2017년과 2018년 두 차례 해킹 사건이 발생하는 등 보안에 대한 신뢰가 부족

- **[코인원]** 설립 후 8년간 무사고를 기록하는 가장 안정적인 거래소 중 하나로 국내 거래소 최초로 다중서명(Multisig) 지갑[7]을 적용
  - 스테이킹 등 새로운 서비스 도입에 적극적이고 시스템 보안을 매우 강조. 실명확인 입출금 계좌 은행을 NH농협은행에서 카카오뱅크로 변경할 예정
  - 거래량이 상대적으로 적고, 본인 인증을 위한 앱(코인원 PASS)의 잦은 에러는 단점

[6] 웹 트래픽, 평균 유동성, 거래량, 신뢰도 등을 기준으로 판단한 코인마켓캡의 자체 평가 기준
[7] 보통의 지갑과는 달리 복수의 키를 동시에 서명해야 거래가 이뤄지는 방식으로 보안성을 강화한 기술

○ 가상자산거래소의 규제 필요성은 과거부터 꾸준히 제기되어 왔으며, 최근 테라·루나 사태로 가상자산 관련 법적 기반 마련이 시급하다는 분위기가 조성

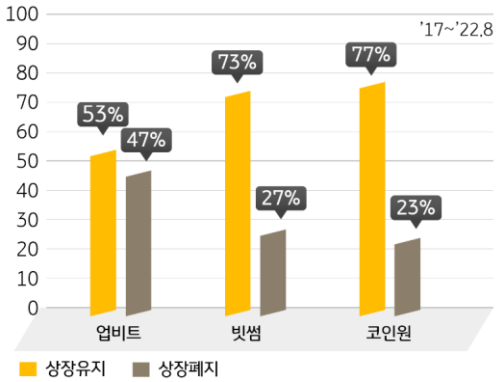
- 테라·루나 사태 당시 국내 거래소들은 투자자 보호보다 거래 수수료 수익에 집중하면서 많은 사람의 공분을 사기도 함
  - 가상자산거래소들은 루나를 유의 종목으로 지정하고 몇 주가 지난 후 거래를 종료했는데, 이때 상위 3대 거래소가 벌어들인 수수료의 합계 금액은 총 86억 원을 초과[8]
- 가상자산거래소 내 코인 상장 및 폐지와 관련해 구체적인 요건과 절차가 투자자에게 공개되지 않는 등 정보의 비대칭도 심화
  - 실제로 업비트의 경우 2017년부터 2022년 8월까지 총 334개의 코인을 상장하고 이 중 절반 가까운 157개(47%)를 폐지하는 등 코인 상장과 폐지를 결정하는 거래소의 기준이 명확하지 않음
  - 현재는 발행사가 제공하는 정보를 단순 공시하는 수준에 그치고 있지만, 이에 대한 폐해가 증가하면서 상장 제도에 대한 구체적인 법적 규제를 통한 투자자 보호가 시급
  - 한글 백서를 의무화하고 백서에 포함되어야 할 필수적인 내용과 형식을 구체적으로 명시해야 할 필요도 있음
- 가상자산거래소의 불공정 거래 행위는 명확한 근거의 부재로 여전히 규제의 사각지대
  - 고객 예탁금을 횡령하거나, 가상자산 가격을 임의로 조작하는 펌프 앤 덤프(Pump-and-dump), 자전거래(Cross Trading)를 통한 시세 조정, 내부자거래 등의 논란이 계속됨
  - 특금법 시행령 개정을 통해 특수관계인 발행 가상자산 취급 금지, 내부 직원의 가상자산 거래 금지 등이 추가되었으나 불공정 거래 행위를 제재하기에는 역부족

[표 1] 루나 유의 종목 지정일 및 거래 종료일

	업비트	빗썸	코인원
유의종목 지정일	2022.05.11	2022.05.11	2022.05.11
거래 종료일	2022.05.20	2022.05.27	2022.06.01
수수료 수익	62억 8천만 원	19억 7천만 원	3억 7천만 원

자료: 윤영덕 국회의원

[그림 5] 가상자산거래소 상장 유지 및 폐지 비율



자료: 금융감독원, 윤창현 국회의원

[8] 국내 5대 가상자산거래소로 구성된 디지털자산거래소 공동협의체가 더불어민주당 윤영덕 의원에게 제출한 자료

○ 가상자산거래소에서 자산 매매는 실제로 실물이 거래되는 것이 아니라 단순히 장부에 숫자만 바뀌는 일종의 '장부거래'

- 비트코인과 이더리움 같은 주요 가상자산은 이체 후 거래 완료까지 오랜 시간이 걸리지만[9], 거래소 입장에서는 실제 블록체인 네트워크를 이용하지 않는 장부거래이기 때문에 주식처럼 빠른 매매가 가능
  - 거래 편의성을 고려할 때 장부거래 자체가 잘못된 것은 아니지만, 고객이 보유한 잔액만큼 거래소가 실제 코인을 가지고 있느냐에 대한 검증이 어렵다[10]는 우려가 존재
  - 과거 '코인네스트'라는 국내 가상자산거래소는 장부상 고객이 보유한 코인보다 실물 코인이 적어 압수수색을 당하기도 함[11]

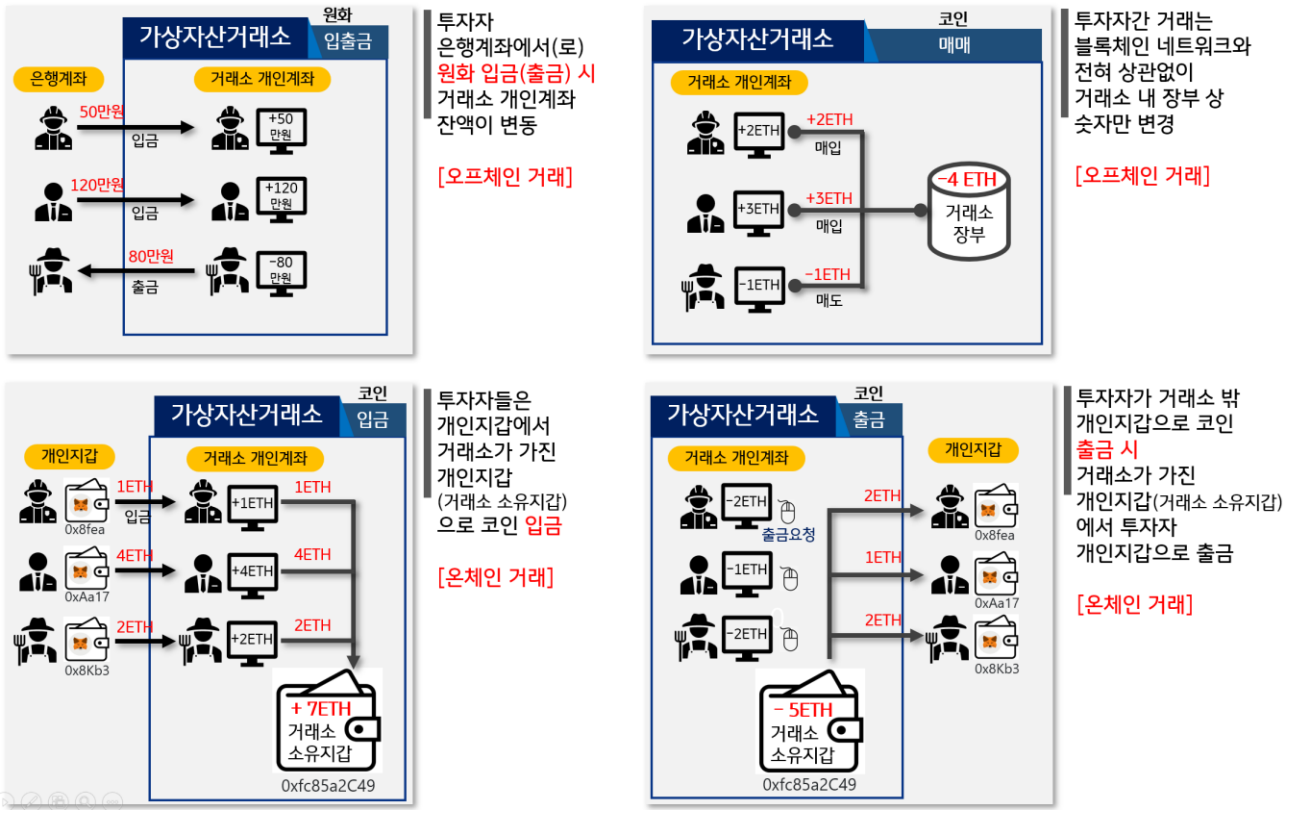
- 가상자산은 거래소에서 개인지갑으로 자산이 출금(이체)될 때 비로소 실질적인 이동이 발생
  - 거래소 내 거래는 실물이 아니라 숫자상으로 주고받는 것이며, 실제 실물과 연동되는 시점은 외부의 개인 지갑과의 입금 혹은 출금 시에만 발생
  - 거래소는 고객의 급작스러운 출금 요청에 대비해 충분한 유동성 확보가 매우 중요한데 고객 입장에서는 이에 대한 객관적 검증이 불가능
  - 은행의 경우 대량 인출 사태에 대비하기 위해 지급준비금제도에 가입하는 등의 소비자 보호 체계가 마련하는데 비해 가상자산거래소는 이에 대한 대비책이 전혀 없음

○ 전통 금융사에게 가상자산거래소는 디지털자산시장의 입구(Entry Point)인 동시에 게이트웨이 역할을 수행한다는 점에서 눈여겨볼 만한 주요 비즈니스 중 하나

- 지난 11월 11일 FTX 사태[12]와 같이 현재 가상자산거래소들이 보여주는 낮은 신뢰성과 투명성, 고객확인제도(KYC)의 복잡성 등은 소비자의 주요한 불만 사항으로 이를 해소할 수 있다면 또 다른 기회로 작용 가능
  - 특히 거래소는 상장과 폐지 기능을 포함하고 있기에 평가 기준을 투명하게 공유하고 지속적으로 점검하여 소비자의 신뢰를 얻는 것이 중요
  - 향후 시장이 더욱 확대되어 가상자산이 새로운 투자자산으로 완전히 자리매김한다면, 금융 소비자에게 더 나은 가치를 제공하기 위한 목적으로 전통 금융사의 가상자산거래소 비즈니스 진출도 예상 가능

[9] 비트코인의 블록 생성 시간은 10분에 1개씩, 이더리움은 15초마다 1개씩 처리
[10] 검증을 위해서는 누군가에게 개인키를 공개하여 실질 대사를 해야 하는데, 이는 패스워드를 알려주는 것과 같기 때문에 불가능
[11] 실제 코인은 보유하지 않은 채 장부거래로 고객의 거래 수수료만 취득했다는 의혹이 있었음. 결국 2019년 4월 서비스 종료
[12] 상세 내용은 [참고] 페이지를 참고

[그림 6] 가상자산거래소 내 온체인/오프체인 거래



자료: 연구자 작성

■ 가상자산 지갑에 대한 이해

○ 가상자산 지갑이란 블록체인 네트워크에서 본인이 소유한 자산을 인증할 수 있는 개인키를 관리하는 도구로 지갑 주소는 계좌번호, 개인키는 비밀번호와 유사

- 가상자산이 실제로 지갑에 들어 있는 것은 아니며, 실질적인 가상자산은 블록체인 네트워크 내 존재하고 이에 대한 접근권(소유권)만 개인키(패스워드) 형태로 지갑에 보관(개인키를 분실할 경우 코인을 모두 잃어버리는 것이므로 개인키 자체를 코인이라 봐도 무방)
  - 지갑 생성은 가상자산 생태계 진입을 위해 가장 기본적인 과정이지만, 코인별로 각각 만들어야 하고 사용해야 하는 프로그램도 각양각색이라 초보 투자자에겐 진입장벽으로 작용하기도 함

○ 가상자산거래소는 가상자산 입출금을 위해 투자자별로 개별 계좌를 제공하는데, 개인이 거래소 외부에서 자체적으로 만든 개인지갑(예를 들어 메타마스크)과는 목적과 용도에서 차이가 존재

- 둘 다 가상자산 거래에 사용한다는 점에서는 동일하지만 개인지갑은 가상자산을 보다 안전하게 보관하고 데 집중하고, 거래소지갑은 거래소 내 거래 편의성을 높이는 데 초점을 맞춤
  - 거래소 개인 계좌는 블록체인 네트워크에 연결되지 않은 채 거래소 내 코인 매매에만 활용(거래소 내 코인 매매는 블록체인 네트워크와 무관한 장부거래이기 때문)
  - 개인 계좌는 거래소가 관리하기 때문에 패스워드 분실을 걱정할 필요가 없으나 거래소 해킹 가능성이 존재. 이에 반해 개인지갑은 개인키 관리만 잘 한다면 해킹 가능성이 낮지만, 개인지갑 간 코인 이체 시 많은 비용과 시간이 소모

○ 가상자산거래소들은 올해 3월 트래블룰 시행으로 지갑 소유자의 신원 확인 절차가 필수가 되자 소비자 편의를 도모하기 위해 거래소 외 다른 지갑들(예를 들어 해외 거래소지갑, 개인지갑)까지 신원 확인 절차를 적용하기 시작

- 그러나 고객의 해외 거래소지갑 혹은 개인지갑 주소를 수기로 사전 등록하는 절차가 복잡하여 오히려 불편함을 가중시킴
  - 빗썸의 경우 동일한 트래블룰 소프트웨어를 사용하는 거래소[13]와 시스템 연동이 가능하지만, 그 외 해외 거래소지갑와 개인지갑의 경우 '거래소 주소가 보이는 모니터 화면 위에 신분증을 올리고 사진 촬영하여 증빙'([그림 7] 참조)하는 수기 작업이 필요(개인지갑으로의 이체는 본인 계좌에 한해서만 가능)

[13] 현재 트래블룰은 국제 표준이 마련되지 않고 베리파이바스프(VerifyVASP)와 코드(CODE)라는 두 가지 솔루션이 각각 존재하며, 동일 솔루션 간 거래는 원활하지만, 서로 다른 솔루션 간 시스템 연계를 위해서는 추가적인 개발이 필요한 상황

[표 2] 트래블룰 적용 후 거래소 입출금 가능 경로

경로 / 거래소	거래소→개인지갑	개인지갑→거래소	거래소→해외 거래소	해외 거래소→거래소
업비트 (실명계좌:케이뱅크)	메타마스크(Ethereum) 카이카스(Klaytn) 팬텀(Solana)	메타마스크(Ethereum) 카이카스(Klaytn) 팬텀(Solana)	바이낸스, FTX, 후오비 등	바이낸스, 후오비, FTX, 코인베이스 등
빗썸 (실명계좌:NH농협은행)	메타마스크(Ethereum) 카카오클립(Klaytn)	별도 제한 없음	바이낸스, FTX, 코인베이스 등	별도 제한 없음
코인원 (실명계좌:NH농협은행 →카카오뱅크 예정)	메타마스크(Ethereum) 카이카스(Klaytn) 카카오클립(Klaytn) 등	별도 제한 없음	바이낸스, FTX, 코인베이스 등	별도 제한 없음
코빗 (실명계좌:신한은행)	메타마스크(Ethereum) 카이카스(Klaytn) 카카오클립(Klaytn) 등	별도 제한 없음	바이낸스, FTX, 코인베이스 등	별도 제한 없음

자료: 팔라(Pala), 연구자 재작성(2022년 10월 7일 기준)

○ 가상자산 지갑은 세부적으로 인터넷 연결 유무에 따라 핫월렛(Hot Wallet)과 콜드월렛(Cold Wallet)으로 구분할 수 있음

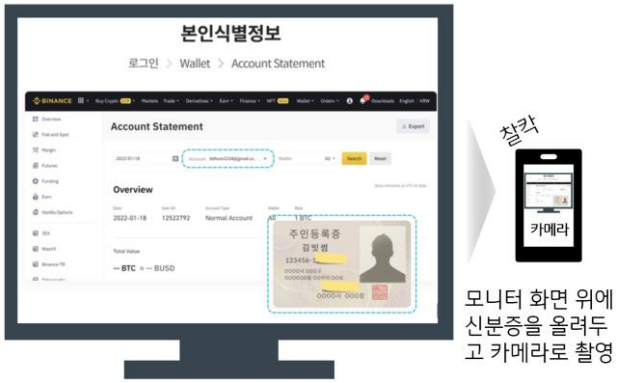
- **[핫월렛]** 온라인으로 연결된 지갑을 핫월렛이라 하며, 개인 투자자 대부분이 사용
  - 언제 어디서나 실시간 거래가 가능하다는 점에서 편리하지만, 비밀번호에 해당하는 개인키가 온라인상에 연결되어 있으므로 해킹 위험이 있음

- **[콜드월렛]** 오프라인 상태로 보관되는 지갑으로 주로 거래 편의성보다 안전성을 선호하는 고액 투자자나 기업이 사용
  - 인터넷이 차단된 하드웨어 장치에 개인키를 보관하고, 거래가 필요한 경우 오프라인에서 개인키 서명을 한 뒤 생성된 트랜잭션 코드만 온라인으로 전송하는 방식

개념정리 가상자산 지갑에 들어있는 정보는?

가상자산 지갑에는 비밀번호 역할을 하는 '개인키'가 저장되어 있음. 흔히 지갑에 코인이 들어 있다고 생각하는데, 코인 자체는 네트워크상에 존재하고 지갑에는 본인의 코인을 이동시킬 수 있는 권한(개인키)만을 보유하는 구조. 이런 관점에서 보면 콜드월렛 디바이스 역시 개인키가 저장된 일종의 USB 같은 저장매체라 할 수 있음

[그림 7] 해외 거래소지갑을 등록 과정



자료: 빗썸

[그림 8] 콜드월렛 디바이스 예시

자료: 디센트

◯ 가상자산 지갑은 지원하는 가상자산 코인에 따라 각각 만들어야 하며, 가이드가 부실하고 생성하는 과정도 복잡

- 특히 가상자산 지갑 서비스 자체가 트래블룰 적용을 고려하지 않은 채 설계되었기 때문에 고객확인제도 적용을 위한 불편함을 고객에게 전가하고 있는 상황
  - 자금세탁방지(AML)와 고객확인제도 절차를 이미 적용한 전통 금융사에서 가상자산 지갑 시장에 진출한다면, 고객에게 더 나은 사용자 경험을 제공 가능
  - 다양한 코인을 하나의 지갑에서 서비스할 수 있도록 설계 가능하다면, 지금처럼 코인별로 지갑 솔루션을 설치하는 번거로움을 덜 수 있음

■ 신문 헤드라인으로 살펴본 가상자산거래소

○ **"日 가상자산거래소에서 1260억 빼내간 해킹범, 알고 보니 북한 소행"**

-<머니투데이>(2022년 8월 11일)

Q) 블록체인 네트워크는 해킹이 불가능하다고 말하던데 어떻게 해킹이 발생했나요?

A) 비트코인과 이더리움 같은 블록체인 네트워크는 해킹이 불가능한 것이 사실이지만 블록체인 네트워크 밖에 존재하는 서비스들은 상대적으로 해킹에 취약. 예를 들어 패스워드를 보관하는 개인지갑과 중개 서비스를 제공하는 가상자산거래소 등은 블록체인 기술과는 무관하기 때문에 항상 유의할 필요가 있음

해킹이 발생할 수 있는 곳은 [그림 9]에서 붉은색 표시가 된 부분으로 개인지갑(특히 인터넷이 연결된 핫월렛), 거래소 서버와 서버 내 개인 계정 등을 들 수 있음

○ **"머스크의 뼈 있는 한마디 '콜드월렛에 넣어야지'[FTX 사태 정리]"**

-<이데일리>(2022년 11월 16일)

Q) 콜드월렛은 무엇이며 어떤 점이 안전한가요?

A) 블록체인 네트워크에 보관된 코인을 거래하기 위해서는 개인키(패스워드)가 필요한데, 이것을 보관하는 서비스를 개인지갑이라 함. 콜드월렛은 개인지갑의 한 형태로, 인터넷이 단절되어 있다는 특성 때문에 외부 해킹에 대한 위험 요소가 거의 없음. 콜드월렛은 오프라인에서 개인키 서명을 한 뒤 트랜젝션 코드만 온라인으로 전송하기 때문에 개인지갑을 인터넷에 연결하지 않아도 거래 가능한 구조. 하지만 그 과정이 매우 복잡하여 한 번의 거래를 위해 많은 시간이 소요되고 불편함이 따른다는 단점도 존재

인터넷에 연결되지 않은 콜드월렛과 인터넷에 연결되어 있는 핫월렛을 구분하는 방법은 [그림 9]를 참조. 거래소 역시 여러 개의 개인지갑을 콜드월렛과 핫월렛 형태로 소유[14]

○ **"美 정부, 4조 7천억 원 도난 암호화폐 회수, 팝콘 통까지 샅샅이 수색"**

-<뉴시스>(2022년 11월 8일)

Q) 기사 내용을 보면 화장실 벽장에 있는 팝콘 통에서 암호화폐를 발견했다고 하는데?

A) 암호화폐 자체는 현실 세계에 존재하지 않기 때문에 팝콘 통에서 발견할 수 없음. 정황상 팝콘 통에서 콜드월렛 디바이스 혹은 개인키(패스워드)를 적어놓은 종이를 발견했을 가능성이 높음. 크게 보면 개인키가 곧 소유자산 자체라고 볼 수 있기 때문에 기사 내용이 어느 정도 옳다고 말할 수 있음

[14] 보통 해킹에 대한 노출을 이유로 거래소 소유 지갑 주소를 공개하지 않음

○ “[업비트 쇼크] 발단은 ‘코인 이동 없는 장부거래’”

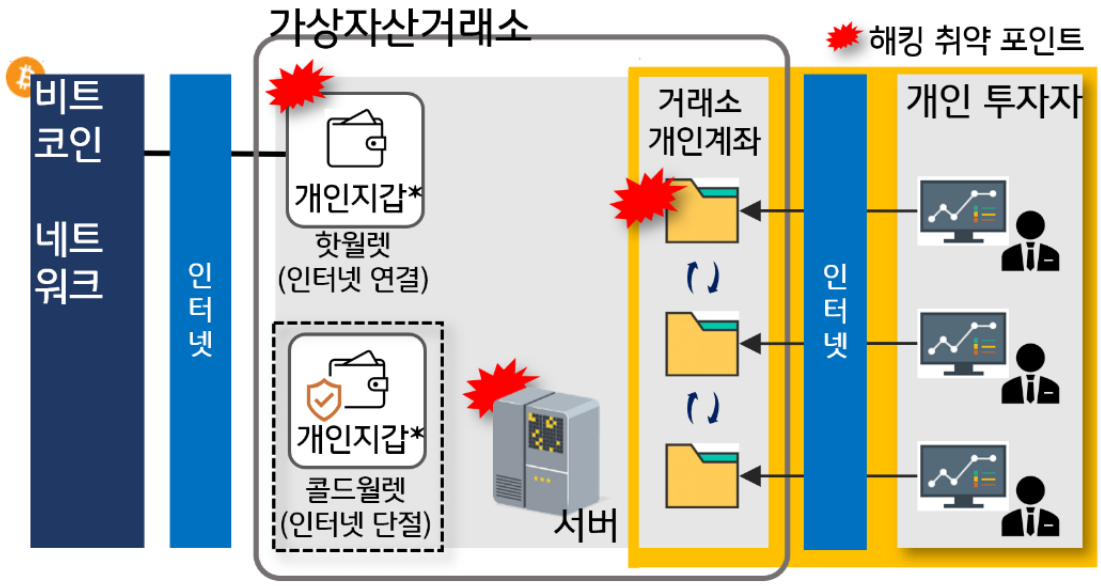
-<비즈니스와치>(2018년 5월 14일)

Q) 코인 이동 없는 장부거래가 무슨 말인가요? 그리고 장부거래는 불법인가요?

A) 만약 거래소 내에서 A라는 투자자가 B에게 이더리움 1개를 샀다면, 거래소 장부 A계정에는 이더리움 1개를 추가하고 B계정에는 이더리움 1개를 차감. 이때 실제 이더리움 네트워크에서는 전혀 매매 거래가 발생하지 않음. 즉 거래소 서버 내 개인 계정의 잔액 숫자만 바뀌는 것으로 투자자가 거래소 밖 개인지갑으로 코인을 출금(이체)하기 전까지 거래소 서버 내에만 존재하는 일종의 ‘사이버 머니’에 불과. 장부거래 자체는 불법으로 볼 수 없지만, 거래소에 실제 코인이 존재하지 않는 채 매매를 진행했다면 이는 불법으로 볼 수 있음

장부거래가 발행하는 구간은 [그림 9]에서 노란 음영색 부분

[그림 9] 가상자산거래소 내 해킹 취약 포인트 및 개인지갑 구조



주1)*거래소의 개인지갑은 ‘거래소 소유지갑’으로도 불림
주2) ■영역: 개인투자자들의 자산 조회 및 거래가 이뤄지는 구간
(실제 네트워크와 연결되지 않은 채 서버내에서만 거래가 이뤄짐)
주3)개인지갑은 블록체인 네트워크 별로 각각 생성되어야 함

자료: 연구자 작성

<연구위원 권세환(pursue312@kbfg.com, 02-2073-5764>

[참고] FTX 거래소에 무슨 일이 있었나?

사전지식 **FTX 사태를 이해하기 위한 몇 가지 배경 지식**

1. 미국 기업가 샘 뱅크먼 프리드(Sam Bankman-Fried)는 2017년 '알라메다리서치(Alameda Research)'라는 암호화폐 투자회사를 세운 뒤, 이 회사를 통해 조달한 자금으로 2019년 'FTX' 암호화폐거래소를 설립. 즉 두 회사의 CEO가 동일한 인물
2. FTX가 자체적으로 발행한 토큰 FTT를 알라메다리서치가 초기에 매입하면서 FTT 가격이 상승. FTT 가격 상승으로 알라메다리서치의 장부상 이익이 폭증하면서 이를 근거로 투자를 받아 또 다른 코인에 투자하는 순환구조를 형성
3. 글로벌 최대 암호화폐거래소 '바이낸스'는 FTX 초기 투자를 통해 최소 2천3백만 개 이상의 FTT를 소유(약 $583M 규모)

○ FTX는 샘 뱅크먼 프리드(주로 SBF로 불리우며, 국내에서는 뽀글이[15]란 별칭으로 유명)가 설립한 글로벌 3대 암호화폐거래소로, 11월 11일 파산을 신청하며 가상자산 시장에 큰 파장을 초래

- 사건 발단은 암호화폐 전문 매체 <코인데스크>가 FTX 계열사 알라메다리서치의 재무 건전성에 의혹을 제기한 일에서 시작(알라메다리서치의 대차대조표에 FTT 토큰이 40% 상당으로 과도하게 큰 비중을 차지하고 있음을 지적[16])
  - 바이낸스 CEO 자오창펑(趙長鵬)은 <코인데스크> 기사를 이유로 바이낸스가 보유 중인 5억 8천3백만 달러 규모의 FTT 토큰을 전량 매각하겠다는 트윗을 올림
  - 알라메다리서치 CEO 캐롤라인 엘리슨은 자오창펑의 발언에 "시장 충격을 최소화하기를 원한다면 오늘이라도 당장 1개당 22달러[17]에 매입하겠다"고 제안했지만, 시장은 이미 걷잡을 수 없을 만큼 큰 패닉 상태에 빠짐
  - 불안감을 느낀 개인과 기관은 앞다퉈 FTX에 예치한 자금을 인출하기 시작했고, 이로 인해 FTX의 유동성 위기가 가속화
  - 바이낸스는 FTX 인수 의사를 타진하며 검토 절차를 진행했지만 최종적으로 인수를 철회. 결국 FTX는 파산을 신청했고, 이후 6억 6천2백만 달러 상당의 코인 유출 소식과 함께 해킹 가능성이 제기됨[18]

---

15 항상 파마를 한 헤어 스타일로 인해 생긴 별칭
16 전체 자산 146억 달러 중 58억 달러가 FTT로 구성
17 시장에서는 알라메다리서치가 FTT를 담보로 잡혀 있고 청산가격이 22달러 근처가 아니냐는 의문을 품음
18 시장에서는 해킹이 내부 자작극일 것이라는 추측도 나돌고 있음

- FTX를 파산으로 이끄는 데 가장 큰 역할을 한 자오창펑이 'FTT 전량 매각' 트윗을 올린 의도를 추측해보면 다음과 같음
  - 최근 FTX가 자체 스테이블코인 발행을 예고하면서, 스테이블코인시장을 두고 바이낸스와 다툴 수밖에 없는 상황(바이낸스는 이미 자체 스테이블코인을 발행하고 있었으며, 스테이블코인시장을 확장하기 위해 다양한 노력을 시도 중이었음)
  - 자오창펑은 샘 뱅크먼 프리드의 미국 내 적극적인 로비 활동이 바이낸스에 불리한 내용을 담은 법안으로 돌아올 것을 우려(샘 뱅크먼 프리드는 지난해 민주당에 4천만 달러 가까이 기부)
  - 테라·루나 사태 이후 FTX는 무너지는 기업에 자금을 투입하며 암호화폐시장에서 명망을 쌓았는데, 자오창펑은 이러한 FTX의 행보에 대해 "업계 보호도 중요하지만 쓸데없는 곳에 유동성을 낭비해서는 안 된다"는 입장을 보이며 샘 뱅크먼 프리드의 시장 내 영향력이 커지는 것을 견제

◯ 시장에서는 테라·루나 사태 이후 또 한 번의 신뢰가 무너졌다는 반응

- 알라메다리서치가 과도한 FTT 담보 레버리지 투자를 감행했고, 여기에 FTX의 부실 경영과 고객 자금 유용 등의 의혹이 불거지면서 유동성 위기가 발생
  - 내부 통제와 감시의 부재 역시 이번 사태를 막지 못한 결정적 요인이라는 지적도 이어지는 가운데, 샘 뱅크먼 프리드는 이번 사태의 진원지인 알라메다리서치의 부채를 상환하기 위해 FTX에 예치된 약 100억 달러에 달하는 고객 자금을 임의 사용한 혐의까지 받고 있음
  - FTX가 제출한 파산신청서에 따르면 FTX 부채는 100~500억 달러, 채권자는 10만 명에 이르는 등 사상 최대 규모이고 개인 투자자는 물론 블랙록과 소프트뱅크, 세쿼이아캐피털, 타이거글로벌매니지먼트와 같은 기관 투자자도 손실. 캐나다에서 세 번째로 큰 연기금 온타리오교사연기금도 FTX 펀딩에 두 차례 참여한 것으로 알려졌고, 싱가포르 국부펀드도 투자자 명단에 포함(손실 예상액은 세쿼이아캐피털 2억 1,350달러, 소프트뱅크 1억 달러가량)

- FTX처럼 자체 발행한 코인을 담보로 대출을 받아 이를 레버리지로 규모를 확장하는 비즈니스 모델은 일종의 관행으로 가상자산시장에서 흔히 볼 수 있는데, 이러한 모델은 투명성이 보장되지 않기 때문에 발생사가 임의 거래가 가능하다는 점에서 상당한 리스크가 따름
  - 이러한 구조는 시장에 충격을 가하여 담보가격이 급락하면 담보가 강제 청산되면서 연쇄적으로 문제를 일으킬 수 있음

– 국내 위믹스재단 역시 위믹스를 담보로 대출받아 기업 인수 등에 활용하는 과정에서 정확한 유통량 정보를 기재하지 않으면서 국내 가상자산거래소에서 투자 유의 종목으로 지정받기도 함

○ FTX 파산 신청에 따른 국내외 영향을 살펴볼 때 직간접적 피해 규모는 상당할 것으로 예측

• FTX는 국내 거래소에서 보기 힘든 레버리지와 선물 등 다양한 고위험 상품을 거래하다 보니 '고위험 고수익(High Risk, High Return)'을 추구하는 일명 '고인물' 투자자 중심으로 큰 인기

– FTX 사용자 비율은 2022년 7월 현재 미국을 제외하고 한국 6.21%, 싱가포르 5.26%, 독일 4.2%, 러시아 3.66%, 일본 3.56%를 기록[19]

– 앱 분석 서비스 모바일인덱스에 따르면 기준 지난달 FTX 앱의 월간활성이용자수(MAU)는 1만 140명 정도

– FTX가 대리인으로 지명한 구조조정 전문 컨설팅회사 크롤의 법원 제출 문서에 따르면 뱅크오브아메리카(BoA), JP모건, 웰스파고 등 미국 대형 은행뿐 아니라 미쓰비시UFG 등 일본 대형 은행까지 총 41개 금융사가 '잠재적 이해관계자'로 분류

– 국내 일부 거래소(코인원, 코빗, 코팍스)에서도 FTT를 취급했는데, 이 거래소들을 통해 FTT를 보유한 투자자 수는 지난 11월 9일 기준 약 6천 명, 보유 수량은 11만 개로 집계. 현재 FTX는 가상자산 출금을 모두 막은 상태이며, 만약 FTT가 상장 폐지될 경우 국내 투자자가 입을 피해는 최대 23억 원 정도로 추산[20]

• 개인 투자자뿐 아니라 기업 역시 국내 거래소에서는 법인 계정 등록이 불가능하다 보니 바이낸스, FTX 등의 해외 거래소를 주로 이용

– 국내 게임 업체 컴투스는 FTX에서 자체 코인 C2X를 발행한 만큼 상당량의 코인이 FTX 내에 묶여 있을 가능성이 높고, 2018년 블록체인 관련 사업을 목적으로 설립된 '한남그룹'도 FTX 소유로 알려짐(한남그룹은 알라메다리서치의 한국 내 투자 활동을 위해 설립한 법인으로 추측)

• 가상자산시장에서 FTX의 파산은 파급력이 상당할 것으로 보이며, 실물 금융시장에까지 연쇄적으로 영향을 미칠 수 있음

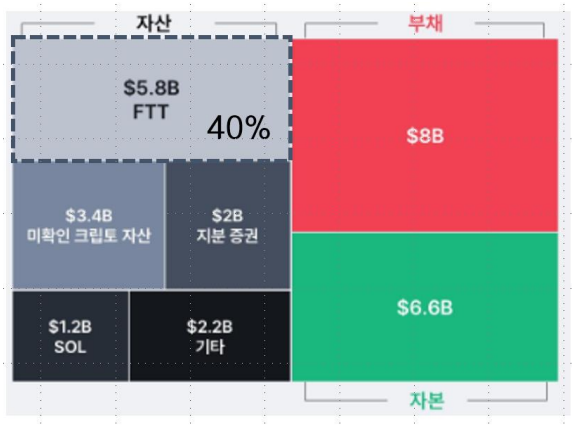
– 국내 가상자산 투자자는 주로 국내 거래소를 사용한다는 점에서 FTX 파산과 관련하여 직접적 피해보다 그 여파로 인한 국내 거래소의 유동성 문제, 가상자산 폭락 가능성 등

[19] 「How many people use FTX in 2022」(Earthweb, 2022, 8.2)
[20] 「'파산 위기' FTX 발생 코인, 국내서도 6000명 샀다」(조선Biz, 2022.11.11)

시장 전체가 흔들리는 간접적 피해가 클 것으로 예상

– 가상자산거래소는 파산할 경우 소비자 보호장치가 전무하기 때문에 이번 사태의 피해는 단순히 FTX 하나로 끝나지 않을 가능성도 존재

[그림 10] 알라메다리서치 대차대조표 현황



자료: Xangle, Coindesk, Twitter@cz_binance

[그림 11] FTT 가격 차트

자료: Coinmarketcap.com

[그림 12] FTX와 라메다리서치 뱅크런 타임라인

11월 2일 9AM	알라메다 대차대조표에 대한 코인데스크의 기사
11월 6일 9AM	알라메다 CEO: 코인데스크 기사에 반영되지 않은 자산이 있다고 정정
11월 6일 10AM	바이낸스 CEO: $500M 이상의 FTT를 청산하겠다고 발표
11월 6일 11AM	알라메다 CEO: 바이낸스가 보유한 FTT를 $22에 OTC 제안
11월 6일 4AM	바이낸스 CEO: FTT 청산 의지 밝힘
11월 7일 7AM	FTX CEO: FTX는 괜찮다고 반복
11월 7일 9AM	FTT 가격이 $22 아래로 하락
11월 8일 6~7AM	이더리움, 솔라나, 트론 네트워크의 FTX 주소에서 마지막으로 출금이 이루어짐
11월 8일 11AM	FTX CEO: 바이낸스와의 전략적 거래 발표
11월 8일 11AM	바이낸스 CEO: FTX 인수 검토 발표
11월 10일 6AM	바이낸스 FTX 인수 철회
11월 11일 11PM	FTX 파산 선언

자료: Xangle, The Block, 연구자 재구성