Dong-A 2022 INFOSEC

2022 동아 인포섹- 정보보호 콘퍼런스

Dong-A InfoSec 2022-
Information Security & Privacy Conference

2022년 2월 23일(수) 오후 2시 ~ 5시 15분
은행회관 2층 국제회의실

디지털 자산과 금융보안

동아일보 CHANNEL A

Dong-A 2022 INFOSEC

2022 동아 인포섹- 정보보호 콘퍼런스

Dong-A InfoSec 2022-
Information Security & Privacy Conference

2022년 2월 23일(수) 오후 2시 ~ 5시 15분
은행회관 2층 국제회의실

디지털 자산과 금융보안

동아일보 CHANNEL A

INDEX

콘퍼런스 개요 03

프로그램 04

기조강연 05

특정금융정보법과 가상자산
전요섭 금융위원회 금융정보분석원 제도운영기획관

주제발표 1 18

2022년 디지털자산과 보안위협
이상록 금융보안원 보안연구부장

주제발표 2 38

금융시장 NFT(Non-Fungible Token)활용과 보안 이슈
김승주 고려대 정보보호대학원 교수

주제발표 3 57

디지털화폐(CBDC) 도입이 가져올 금융보안의 변화와 새로운 보안 과제
강민석 KAIST 전산학부/정보보호대학원 교수

주제발표 4 67

한국은행 CBDC 발행에 대응한 멀티에셋 디지털지갑 핵심기술과 정보보호
박형주 KB국민은행 디지털신사업본부장

주제발표 5 77

디지털자산거래소의 보안 차별화 전략
차종현 두나무 최고정보보호책임자(CISO)

주제발표 6 89

NFT가 불러올 금융 플랫폼의 미래 변화
유태현 신한카드 디지털First본부장(상무)

2022 동아 인포섹-정보보호 콘퍼런스

Dong-A InfoSec 2022-Information Security & Privacy Conference

비트코인 같은 가상자산 시장이 급성장하고 블록체인과 메타버스를 기반으로 한 대체불가토큰(NFT), 중앙은행디지털화폐(CBDC) 등 새로운 디지털 자산이 빠르게 영역을 넓히고 있습니다. 디지털 자산 생태계가 커지는 만큼 새로운 보안 위협도 도사리고 있습니다.

동아일보와 채널A는 '디지털 자산과 금융보안'을 주제로 '2022 동아 인포섹-정보보호 콘퍼런스'를 개최합니다. 신종 코로나바이러스 감염증(코로나19) 방역을 위해 현장 참석 인원을 최소화하고 온라인으로 실시간 중계할 예정입니다. 많은 성원 바랍니다.

콘퍼런스 개요

일시 | 2022년 2월 23일(수) 오후 2시 ~ 5시 15분

장소 | 서울시 중구 명동 은행회관 2층 국제회의실

주제 | 디지털 자산과 금융보안

온라인 생중계_ www.dongainsight.com

주최 | 동아일보 CHANNEL A

초청 연사

축사 1

윤재옥

국회정무위원회 위원장
(국민의힘 국회의원)

축사 2

이찬우

금융감독원
수석부원장

기조강연

전요섭

금융위원회
금융정보분석원 제도운영기획관

주제발표 1

이상록

금융보안원
보안연구부장

주제발표 2

김승주

고려대
정보보호대학원 교수

주제발표 3

강민석

KAIST
전산학부/정보보호대학원 교수

주제발표 4

박형주

KB국민은행
디지털신사업본부장

주제발표 5

차종현

두나무
최고정보보호책임자(CISO)

주제발표 6

유태현

신한카드
디지털First본부장(상무)

프로그램

시간(오후)	프로그램	주제	발표자
2:00~2:05 (05′)		개회사	**박제균** 동아일보 논설주간
2:05~2:10 (05′)		축사 1	**윤재옥** 국회정무위원회 위원장 (국민의힘 국회의원)
2:10~2:15 (05′)		축사 2	**이찬우** 금융감독원 수석부원장
2:15~2:35 (20′)	기조강연	특정금융정보법과 가상자산	**전요섭** 금융위원회 금융정보분석원 제도운영기획관
2:35~3:00 (25′)	주제발표 1	2022년 디지털자산과 보안위협	**이상록** 금융보안원 보안연구부장
3:00~3:25 (25′)	주제발표 2	금융시장 NFT(Non-Fungible Token)활용과 보안 이슈	**김승주** 고려대 정보보호대학원 교수
3:25~3:50 (25′)	주제발표 3	디지털화폐(CBDC) 도입이 가져올 금융보안의 변화와 새로운 보안 과제	**강민석** KAIST 전산학부/정보보호대학원 교수
3:50~4:00 (10′)		휴식	
4:00~4:25 (25′)	주제발표 4	한국은행 CBDC 발행에 대응한 멀티에셋 디지털지갑 핵심기술과 정보보호	**박형주** KB국민은행 디지털신사업본부장
4:25~4:50 (25′)	주제발표 5	디지털자산거래소의 보안 차별화 전략	**차종현** 두나무 최고정보보호책임자(CISO)
4:50~5:15 (25′)	주제발표 6	NFT가 불러올 금융 플랫폼의 미래 변화	**유태현** 신한카드 디지털First본부장(상무)

Dong-A 2022 INFOSEC

기조강연

특정금융정보법과 가상자산

전요섭

금융위원회 금융정보분석원 제도운영기획관

2022 동아 인포섹-정보보호 콘퍼런스

Dong-A InfoSec 2022-Information Security & Privacy Conference

기조강연

특정금융정보법과 가상자산

전요섭
금융위원회 금융정보분석원 제도운영기획관

키워드 #가상자산 #가상자산사업자 #자금세탁방지

주요경력

- 금융정보분석원 기획행정실장
- 금융분쟁대응단장
- 은행과장
- 구조개선정책과장

전요섭 금융위원회 금융정보분석원 제도운영기획관

특정금융정보법과 가상자산

금융정보분석원
제도운영기획관 전요섭

Ⅰ 가상자산사업자 현황

1. 해외

☞ **CoinMarketCap, 스팟시장, 2022.2.19일 기준**

- 가상자산거래업자 460개, 코인수 17,644개,
- 시가총액 2094조원, 1일 거래량 74.5조원

연번	사업자명	거래량(1일)	코인수
1	Binance	11조7310억원	405
2	Mandala Exchange	7조793억원	330
3	CoinFLEX	6조2923억원	19
4	OKX	3조3027억원	322
5	Upbit	3조1426억원	159
6	HitBTC	3조1072억원	417
7	IndoEX	2조7286억원	95
8	Coinbase Exchange	2조4105억원	159
9	FMFW.io	2조2332억원	127
10	TOKENCAN	2조1975억원	38

1

전요섭 금융위원회 금융정보분석원 제도운영기획관

Ⅰ 가상자산사업자 현황

2. 국내

▣ 2022.2월 현재, 신고 접수한 42개 사업자 중 33개사가 특금법에 따른 신고수리를 받고 영업을 개시

구 분		신고접수 (21.9.14)	수리결정	철회/유보
거래업자	원화마켓	4	4	0
	코인마켓	25	22	3
기타업자		13	7	6
합 계		42	33	9

2

Ⅱ 가상자산 관련 리스크

❖ 레이 달리오, Bridgewater Associates 창립자

- "비트코인의 리스크는 ① 더 좋은 가상화폐가 나와서 비트코인을 대체할 수 있는 점(대체가능성), ② 사이버 공격, ③ 정부규제"

❖ 제롬 파월, 前 미국 연방준비제도 의장

- "가상화폐는 본질적 가치가 없다 … 가상화폐들은 매우 변동성이 크기 때문에 유용한 가치저장 수단이 아니다" → ④ 높은 가격변동성(초고위험자산)

3

전요섭 금융위원회 금융정보분석원 제도운영기획관

II 가상자산 관련 리스크

❖ 이주열, 한국은행 총재

- "비트코인 등 암호화폐는 높은 가격 변동성으로 인해 지급·가치저장수단으로서 기능하는데 제약이 있다 … 향후 CBDC(중앙은행 디지털화폐)가 도입되면 지급수단으로서의 암호화폐 수요는 감소할 것이다" → ④ 높은 가격변동성(초고위험자산), ① 대체가능성

❖ 라가르드, 유럽중앙은행(ECB) 총재

- "비트코인은 매우 투기적인 자산이며 이것은 불법활동과 흥미롭고 완전히 이상한 자금세탁활동에 연루되어 왔다. … 규제의 허점이 있으면 비트코인이 범죄에 활용될 수 있다 … 세계 각국이 동일한 규제에 합의해야 한다" → ③ 정부규제

4

III 가상자산 관련 정보보안사고

1. 가상자산 관련 정보보안사고 유형

❖ 가상자산시장 규모가 확대됨에 따라 자금세탁, 해킹 위험이 증가

❖ 가상자산 관련 정보보안사고의 유형은

➢ ① 가상자산사업자가 보유한 가상자산을 직접 해킹하여 탈취하는 형태,
➢ ② 정부, 기업에 대한 해킹 공격 후 댓가로 가상자산을 요구하는 형태(랜섬웨어)로 분류 가능

☞ ① 유형의 공격에 대하여는 해킹 방지대책이 필요
①② 유형의 공격 모두에 대하여는 자금세탁 방지 대책이 필요

5

전요섭 금융위원회 금융정보분석원 제도운영기획관

III 가상자산 관련 정보보안사고

2. 가상자산사업자 자체에 대한 해킹 사례

가상자산사업자 해킹으로 인한 코인 탈취 → 코인 세탁 → 가상자산거래소를 통해 현금화

❖ 2014.2월, 일본의 가상자산거래소 Mt.Gox는 해킹 사고를 당하여 470억엔 상당의 85만 비트코인(Bitcoin)을 도난당함

❖ 2018.1월, 일본의 가상자산거래소 Coincheck는 해킹으로 580억엔(5,600억원) 상당의 NEM 코인을 도난당함

6

III 가상자산 관련 정보보안사고

2. 가상자산사업자 자체에 대한 해킹 사례

❖ 2021.8월, 해커조직 Lockbit은 IT 컨설팅업체인 액센츄어를 공격하여 데이터를 탈취

❖ 2021.8월, DeFi 플랫폼 사업자인 Poly Network는 6.1억 달러 상당의 코인을 해킹당함

❖ 우리나라 거래소 해킹 사례(출처 : 언론보도)

- 2017년, 코인빈(유빗) 170억원 상당
- 2018년, 코인레일 450억원 상당
- 2018년, 빗썸 190억원, 2019년 220억원 상당
- 2019년, 업비트 580억원 상당

7

전요섭 금융위원회 금융정보분석원 제도운영기획관

III 가상자산 관련 정보보안사고

3. 랜섬웨어 공격 사례

랜섬워어 공격 후 코인 요구 → 코인 세탁 → 가상자산거래소를 통해 현금화

❖ 2021.8월, 해커조직 Revil은 미국 기업 200여 곳을 공격하여 7천만 달러 상당의 비트코인을 랜섬으로 요구

❖ 미국의 사이버크라임 誌, 랜섬웨어에 의한 피해금액

- 2015년 3,800억원, 2021년 23조 6,000억원이었고,
- 2031년에는 312조원에 달할 것으로 예측

8

III 가상자산 관련 정보보안사고

4. 대응 방향

❖ 현행 제도

➢ (특금법) 자금세탁 방지를 목적으로 하므로 사업자에 대한 CDD, CTR, STR 의무를 부과

- 특금법은 가상자산에 대한 규율을 하고 있는 유일한 법률로서 정보보안과 관련해서 담당자들의 비밀유지 의무를 규율하고 있긴 하지만, 물리적, 전산적 보안규정은 두지 않음
- 2021.3월부터 가상자산사업자에 대해서도 자금세탁방지 의무를 부과하고 있으나, 새로운 기술이 적용된 분야이므로 트래블룰 적용의 불완전성 등 아직 미흡한 부분 존재

➢ (전자금융거래법) 금융회사에 대해 금융거래의 안전성 확보의무를 부과하고 있으나, 가상자산사업자에게는 적용되지 않음

9

전요섭 금융위원회 금융정보분석원 제도운영기획관

III 가상자산 관련 정보보안사고

4. 대응 방향

① 안전성 확보의무 부과 및 위반시 제재

- 정부, 기업 스스로 사이버 공격에 대한 방어 노력이 필요하나, 가상자산사업자에 대해서는 법률에 의한 안전성 확보의무를 부과할 필요
- 가상자산사업자가 보유한 가상자산을 직접 해킹하여 탈취하는 유형의 사이버 공격에 대하여는 가상자산사업자에 대한 직접적인 해킹방지의무 부과 필요
- 가상자산사업자에 대해서는 이용자 보호 차원에서 현재 논의 중인 가상자산업법에서 전금법 상 보안규정을 준용하는 형태의 규율의 필요성을 검토
- 가상자산사업자에게 ISMS 인증 확보를 신고 요건으로 하고 있으나, 보안사고 발생시 피해의 규모나 영향을 고려할 때 당국이 보다 직접적으로 감독하고 위반에 따른 제재를 부과할 수 있는 제도를 구축할 필요

10

III 가상자산 관련 정보보안사고

4. 대응 방향

② 가상자산 관련 자금세탁방지 체계의 고도화

- 2021.3월, 특금법 개정안 시행으로 가상자산사업자에게 자금세탁방지 규율이 적용되고 있음 (→ IV. 가상자산 관련 AML/CFT 제도)
- 2021.10월, FATF는 가상자산 관련 지침서를 개정하여 트래블룰 적용을 비사업자에까지 확대하였으므로, 이의 국내 제도화를 위하여 특금법 개정 추진
- 2021.10월, 30여 개국이 랜섬웨어 피해 대응을 위해 공동협력하여 가상자산을 활용한 자금세탁을 차단하기 위하여 강력히 대응하기로 결의

11

전요섭 금융위원회 금융정보분석원 제도운영기획관

Ⅳ 가상자산 관련 AML/CFT 제도

- **가상자산사업자 신고 제도** (법 §7)
- **신규 사업자 신고 / 변경 신고 / 갱신 신고** (법 §7①②③⑥)
- **가상자산사업자의 조치의무** (법 §8)
- **가상자산 이전시 트래블룰** (법 §6③, 영 §10의10)
- **가상자산사업자에 대한 감독 및 검사** (법 §7⑤, §15)

12

Ⅳ 가상자산 관련 AML/CFT 제도

1. 신고 수리요건 (특금법 제7조제3항: 불수리 요건)

- **정보보호 관리체계(ISMS) 인증**
- **실명확인 입출금 계정 획득**
  - ✓ 예외 : 가상자산과 금전의 교환행위가 없는 경우 (감독규정 제27조제1항)
- **특금법, 범수법, 테러자금금지법, 외국환거래법, 금융관련법률 등에 따른 벌금 이상의 형 선고/집행면제로부터 5년 경과**
  - ✓ 법 시행 후 최초로 법률 위반행위를 한 경우부터 적용 (법 부칙 제4조)
- **신고/변경신고 말소 후 5년 경과**

☞ **신규사업자 ISMS 획득 관련 이슈**

13

전요섭 금융위원회 금융정보분석원 제도운영기획관

IV 가상자산 관련 AML/CFT 제도

2. 가상자산사업자의 의무

가상자산사업자의 의무

- **FIU 신고의무** (법 제7조)
- **자금세탁방지의무** (공통)
  - 고객확인(CDD, EDD), 의심거래보고, 내부통제지침 마련
  - 가상자산 이전시 정보제공(Travel Rule) ➡ 2022.3.25일부터 시행
- **가상자산사업자의 조치** (법 제8조 및 영 제10조의20)
  - 고객별로 거래내역을 분리하여 관리
  - 고객 예치금을 고유재산과 구분하여 관리
  - 다크코인 취급 제한
  - 오더북 공유시 상대방 가상자산사업자 및 고객 확인 등
  - 추가(2021.11.6일 시행) : 자신 및 특수관계인 발행 코인 취급 제한, 거래소 임직원 거래 제한 등

14

V 가상자산 트래블룰 제도 개선

1. 현행 트래블룰

시행시기

- FATF의 가상자산 관련 지침서(2019.6월)에 따라 가상자산사업자에 대한 트래블룰 준수의무를 부과하는 특금법령이 개정되어 2021.3.25. 시행
- 다만, 가상자산사업자의 트래블룰 준수여부에 대한 검사. 감독은 정보공유시스템 구축 및 도입 기간을 고려하여 2022.3.25.부터 시행

적용범위

- 가상자산 이전시 기준금액 : 1백만원 상당 이상

15

전요섭 금융위원회 금융정보분석원 제도운영기획관

V 가상자산 트래블룰 제도 개선

1. 현행 트래블룰

제공정보

- **송신인의 성명 및 가상자산지갑주소, 수신인의 성명 및 가상자산지갑주소**를 송신 사업자가 수신 사업자에게 제공해야 함
- 수신 사업자 또는 FIU가 송신인 실명번호를 요청하는 경우에는 요청받은 날로부터 3영업일 이내에 제공해야 함

정보보관의무

- 송신 사업자는 거래 등 관계가 종료된 때로부터 5년간 정보 보관

비밀보장의무

- 사업자는 제공받은 정보를 다른 사람에게 제공. 누설하거나 목적 외 사용 금지
  (☞ 위반시 5년 이하 징역 또는 5천만원 이하 벌금)

16

V 가상자산 트래블룰 제도 개선

2. FATF 지침서 개정 (2021.10.)

적용범위

- **가상자산사업자 사이**에만 적용 → **사업자와 비사업자 간** 거래까지 적용
  - 일방이 비사업자인 경우 사업자가 자신의 고객으로부터 송수신인에 대한 필수정보를 획득 수집하여야 하며, 사업자가 비사업자에게 정보를 전송할 의무는 없음

- **기준금액(1천 달러/유로) 이상**의 거래에 대하여 적용 가능
- **기준금액 미만의 거래**에 대하여도 송수신인의 성명, 가상자산 지갑주소에 대한 수집의무를 부과

17

전요섭 금융위원회 금융정보분석원 제도운영기획관

V 가상자산 트래블룰 제도 개선

2. FATF 지침서 개정 (2021.10.)

제공정보

- 송신인의 성명 및 가상자산지갑주소, 수신인의 성명 및 가상자산지갑주소, **송금인의 식별정보**(주소, 주민번호, 생년월일과 출생지 중 하나)

상대방 식별의무

- 가상자산사업자가 상대 사업자에게 정보를 전송하기 위해서는 상대 사업자를 식별하고 확인(due diligence)하는 작업을 실시하여야 함
- 상대 사업자의 AML/CFT 관리수준을 평가하고, 상대방이 정보를 적절히 보호할 수 있는지 신뢰하기 위한 합당한 근거를 고려해야 함

18

V 가상자산 트래블룰 제도 개선

3. 향후 일정

- 업계, 금융권, 전문가로 구성된 제도개선TF를 구성하여 트래블룰의 국내 적용을 위한 제도 개선안을 마련
- 상반기 중 개선안 마련, 하반기 중 법령 개정 일정으로 추진

19

특정금융정보법과 가상자산

전요섭 금융위원회 금융정보분석원 제도운영기획관

감사합니다.

Dong-A 2022 INFOSEC

주제발표 1

2022년 디지털자산과 보안위협

이상록

금융보안원 보안연구부장

2022 동아 인포섹-정보보호 콘퍼런스

Dong-A InfoSec 2022-Information Security & Privacy Conference

주제발표 1

2022년 디지털자산과 보안위협

이상록
금융보안원 보안연구부장

키워드	#디지털자산 #가상자산 #보안위협
핵심문장	디지털자산 관련 보안위협 이슈 및 국내·외 규제 동향을 살펴봄

주요경력

- 금융보안원 침해대응부장, 감사실장
- 금융보안연구원 본부장

이상록 금융보안원 보안연구부장

Contents

01 **디지털자산** 동향 ---- 3
02 디지털자산 **보안위협 사례** ---- 9
03 디지털자산 **보안위협 전망** ---- 20
04 디지털자산 **보안** 관련 **국내·외 규제** ---- 27
05 **안전한 디지털자산 활용**을 위한 **대응** ---- 31

2022년 디지털자산과 보안위협

이상록 금융보안원 보안연구부장

01. 디지털자산 동향

01 디지털자산 동향

금융보안원은 '21.11월에 발표한 「2022년 디지털금융 및 사이버보안 이슈 전망」에서 디지털자산 보안위협 이슈에 대해 전망

이상록 금융보안원 보안연구부장

01 디지털자산 동향

참고 「2022년 디지털금융 및 사이버보안 이슈 전망」 중 "디지털자산 확산에 대한 기대와 우려"

1 이슈 분석

- **디지털자산[26]의 형태와 용도는 다양한 양상으로 확대되는 추세**

지급·결제[27], 투자뿐만 아니라 자산의 소유권 보장 및 거래(예 : NFT[28]) 등 디지털자산의 용도가 점차 다양화되는 추세

이와 함께 탈중앙화 금융, 즉 중개기관 없이 블록체인상의 스마트 계약을 통해 디지털자산 간 교환, 대출, 파생상품 등의 서비스를 제공하는 디파이(DeFi)[29]가 등장

* '21.11.8. 기준 약 1,057억 달러가 디파이에 예치되어 있으며, 이는 전년 동기 대비 약 4.9배 증가한 수치 (DEFI PULSE, '21.11월)

한편, 세계 각국의 중앙은행은 디지털 전환의 흐름에 발맞추어 물리적 법정화폐를 대체 또는 보완하기 위한 수단으로 CBDC 도입을 추진[30]

- **디지털자산 관련 보안위협[31] 등 해결해야 할 과제 존재**

디지털자산 거래소 또는 CBDC 발행·참여기관에 대한 사이버공격, 디파이의 스마트 계약 관련 취약점을 이용한 공격 등 디지털자산과 관련하여 다양한 보안위협이 존재

디지털자산 및 디파이 관련 보안위협(예시)[32]

- 디지털자산 거래소 또는 CBDC 발행·참여기관 대상 DDoS, 해킹 등의 사이버 공격
- 거래소 사칭 사기 또는 거래소에 의한 금융사기*
  * 시세조작, 거래소 영업 중단 후 이용자의 디지털자산 인출 차단 등
- 이용자의 관리 부실 등으로 인한 디지털자산 전자지갑 개인키 탈취
- 블록체인 기술의 취약점을 악용한 공격(예 : 더스팅 공격[33], 51%공격[34] 등)
- 신규 디파이 서비스를 미끼로 디지털자산 발행 및 투자금 모집 후, 의도적으로 스마트계약에 취약점을 심어 디지털자산을 탈취

※ 디지털자산 및 디파이 서비스와 관련하여 발생 가능한 보안위협의 예시로, 설계·운영방식 등에 따라 위협이 상이할 수 있음

디지털자산의 익명성 보장 정도에 따른 범죄 악용 가능성, CBDC의 프라이버시 이슈 등도 살펴보아야 할 과제

01 디지털자산 동향

디지털자산의 형태와 용도가 다양한 양상으로 확대

지급·결제	투자	자산 소유권 보장 및 거래	디파이(DeFi)
VISA PayPal mastercard 디지털자산 **결제서비스** 제공	MZ세대의 **40.5%**가 디지털자산 투자 경험 보유 (700명 대상, 전경연, '21.11월)	디지털 화가 '비플'의 작품이 **6930만 달러**(약 830억원)에, 트위터 창업자가 작성한 첫 트윗이 **290만달러**(약 35억원)에 판매 (동아일보, 대체불가토큰(NFT) 일상을 넘보다, '22.2.19.)	중개기관 없이 블록체인 상의 **스마트 계약**을 통해 디지털자산 간 **교환, 대출** 등의 서비스 제공

* [참고] 관련 언론보도

※ [본 발표자료 내 모든 아이콘 출처] flaticon.com

이상록 금융보안원 보안연구부장

01 디지털자산 동향

국내 금융권의 디지털자산 관련 사업 진출도 활발

수탁 (커스터디)	디지털자산을 안전하게 보관·관리하는 서비스 제공 ※ 은행권에서 주로 합작 또는 투자 형태로 진출
전자지갑	디지털자산 보관, 송금, 결제 등이 가능한 전자지갑 개발 (예) OO은행 - NFT 등을 보관하는 전자지갑 시험 개발 완료(21.12월)
NFT 발행	디지털자산 플랫폼을 구축하여 NFT 발행 (예) OO카드 - 자체 디지털자산 플랫폼을 구축하여 NFT 발행 서비스 출시('22.1월)
기타	디지털자산 시세 분석, 매도 시점 추천 등 자산관리·평가서비스 제공 NFT 펀드 출시, NFT 기반 담보대출 등

*[참고] 관련 언론보도

01 디지털자산 동향

가상자산 총 시가총액 및 거래량

※ [출처] CoinMarketCap(coinmarketcap.com/charts)

이상록 금융보안원 보안연구부장

02. 디지털자산 **보안위협 사례**

02 디지털자산 **보안위협 사례** – 침해 대상 및 유형

침해 대상

블록체인, 거래소, 전자지갑, 디파이, NFT . . .

침해 유형

블록체인 – 51% 공격, 스팸공격, 취약점 악용 . . .
거래소 – 피싱, 사기, DDoS 공격, 해킹, 내부데이터 접근 . . .
전자지갑 – 탈취, 취약점 악용 . . .
디파이 – 스마트계약 취약점 악용, 가상자산 소각/플래시 론 공격 . . .
NFT – 사기, 저작권침해, 개인정보 유출 . . .

이상록 금융보안원 보안연구부장

02 디지털자산 **보안위협 사례** – (1) 블록체인 대상

거래 과부하 발생으로 블록체인 네트워크 중단('21.9월)

일부 노드에 권한 집중 → 노드 장애 시 서비스 중단 발생

파이낸셜뉴스

솔라나, 거래 과부하에 18시간 먹통..."노드 중앙화 문제"

기사입력 2021-09-15 17:42

[파이낸셜뉴스] '이더리움 킬러'라는 별명으로 올해 글로벌 블록체인·가상자산 시장의 스포트라이트를 받은 솔라나 블록체인이 18시간이나 먹통이 되는 사고가 발생하며 논란이 되고 있다.

솔라나가 타 블록체인 네트워크와 차별화된 높은 거래 처리 속도를 내세우며 등장했지만, 이를 실현하기 위해선 블록체인의 탈중앙성은 어느정도 포기할 수밖에 없다. 즉, 블록체인 네트워크에서 거래 유효성 검증 역할을 하는 노드 수가 적다는 뜻인데, 이같이 노드의 분산이 미흡한 상태에서 만약 트랜잭션 부화가 발생하게 된다면 노드가 모두 멈춰버리는 문제가 발생하기 쉽다는 것이다.

※ [출처] 파이낸셜뉴스, 솔라나 거래 과부하에 18시간 먹통… 노드 중앙화 문제, '21.9.15.

02 디지털자산 **보안위협 사례** – (2) 거래소 대상

가상자산 거래소 사칭 → 피싱 또는 허위 투자 유도

Digital Today

HOME > 블록체인

가상자상 거래소 사칭 금융사기 기승...한달에 한번꼴 주의보

ㅅ 강진규 기자 | ⏲ 승인 2021.12.31 07:30

빗썸은 고객 공지를 통해 "최근 빗썸을 사칭한 이메일 발송 및 공공기관을 사칭한 보이스피싱 시도가 이뤄지고 있어 피해가 발생하지 않도록 각별한 주의를 부탁한다"고 밝혔다.

이어 2월 업비트는 트위터, 페이스북 등을 통해 특정 회사의 최고경영자(CEO)를 사칭해 접근한 후 가상자산을 입금할 경우 수배로 돌려준다는 사례가 있었다고 밝혔다.

코인원의 경우는 올해 4월 고객 공지를 통해 코인원 고객센터를 사칭해 일회용비밀번호(OTP) 번호를 불러달라고 하는 사례가 있다고 경고했다. 또 코인원은 자사 임직원을 사칭해 상장을 미끼로 사기 행각을 벌이거나 코인원을 사칭해 피싱사이트 유도하는 경우도 있다고 지적했다.

코빗은 올해 3월 코빗을 사칭해 투자를 유도하는 피싱사이트가 발견됐다고 주의를 당부했다.

※ [출처] 디지털투데이, 가상자상 거래소 사칭 금융사기 기승...한달에 한번꼴 주의보, '21.12.31.

이상록 금융보안원 보안연구부장

02 디지털자산 **보안위협 사례** – (3) **전자지갑** 대상

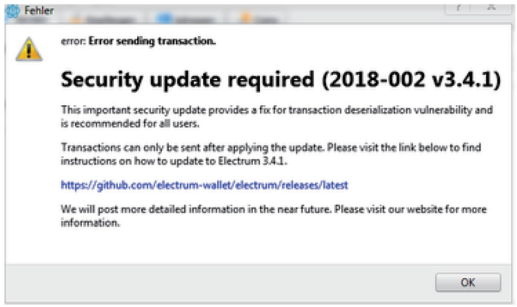
전자지갑 S/W의 허위 업데이트를 유도하여 가상자산 탈취

1) **(악성 서버 추가)** 공격자는 블록체인에 악성 서버 등록

2) **(허위 업데이트)** 전자지갑 거래 요청이 악성 서버로 전달
→ 허위 오류 메시지를 띄워 업데이트 유도

3) **(멀웨어 설치)** 허위 업데이트로 멀웨어 설치

4) **(가상자산 탈취)** 사용자의 코인을 공격자의 전자지갑으로 송금



※ [출처] ZDNet, Bitcoin wallet update trick has netted criminals more than $22 million, '20.10.12.

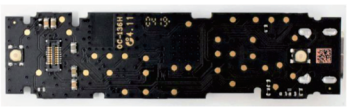
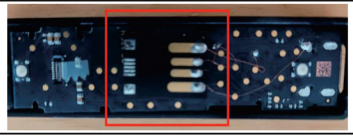
02 디지털자산 **보안위협 사례** – (3) **전자지갑** 대상

H/W 전자지갑에 스파이 칩을 부착한 후 판매

해외 직구, 저가 제품, 중고 거래 등으로 이를 구매한 사용자의 전자지갑 내 데이터 탈취

가짜 홀로그램 부착

H/W 전자지갑에 스파이 칩 부착

진품	
가품 (스파이 칩 부착)	

※ [출처] SatoshiLabs, [PSA] Non-genuine Trezor One devices spotted. Be careful, buy only from Trezor Shop or authorized resellers, '18.11.20.
Cointelegraph, Scammers mail out fake hardware wallets to victims of Ledger data breach, '21.6.17.

이상록 금융보안원 보안연구부장

02 디지털자산 **보안위협 사례** – (3) 전자지갑 대상

전자지갑 개설 시 신원확인을 우회하여 지원금 편취

타인 명의로 전자지갑이 개설되므로 대포통장처럼 사용될 위험 존재

서울경제

엘살바도르, 공식 비트코인 지갑 '치보' 해킹 피해자 속출

기사입력 2021-11-01 17:42

타인 개인정보 도용해 '치보' 가입
정부서 무상 지급하는 30달러 상당 비트코인 노린 수법
가입 시 신분 인증 절차 엉터리 작동

현지 인권단체 크리스토살에 따르면 지난 10월 9일부터 14일까지 5일간 치보 지갑에서 정보를 도용당했다는 신고가 755건이나 접수됐다.

외신에 따르면 치보 앱에 가입하는 과정에서 신분 인증 절차가 제대로 작동하지 않은 것으로 드러났다. 치보에 가입하려면 신분증 확인과 안면 인식 절차를 거쳐야 한다. 그러나 실험 결과 신분증 사본만으로도 가입이 가능했다. 안면 인식 역시 영화 포스터 속 인물로도 가입이 승인된 것으로 드러났다. 가짜 신분 인증으로도 30달러(약 3만 5,000원) 상당의 비트코인을 챙길 수 있는 것이다.

※ [출처] 서울경제, 엘살바도르 공식 비트코인 지갑 '치보' 해킹 피해자 속출, '21.11.01.

02 디지털자산 **보안위협 사례** – (4) 디파이(DeFi) 대상

코드 수정 중 오류로 인한 이자 과잉 지급 발생('22.1월)

ZDNet Korea

위메이드 디파이 '클레바', 이자 과지급 사고…"피해액 회수중"

기사입력 2022-01-28 11:26 최종수정 2022-01-28 17:25

600억 원 상당의 이자 과잉 지급… 이중 200억 원 상당의 KUSDT 1700만 개는 출금

위메이드가 만든 탈중앙금융서비스(DeFi) 클레바에서 200억 원 상당의 암호화폐가 비정상적으로 사라지는 사고가 발생했다. 사고가 알려진 직후 해킹 의혹이 제기되기도 했지만, 원인분석 결과 서비스 업데이트를 위해 코드를 수정하는 과정에서 이자율 계산 코드가 영향을 받아 이자가 과잉지급된 것으로 확인됐다.

※ [출처] ZDNet Korea, 위메이드 디파이 '클레바' 이자 과지급 사고… 피해액 회수중, '22.1.28.

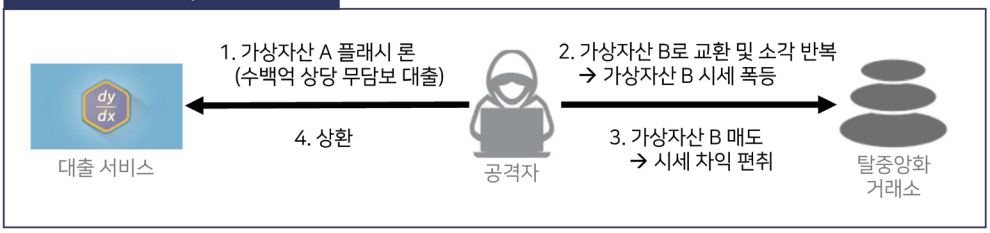
이상록 금융보안원 보안연구부장

02 디지털자산 **보안위협 사례** – (4) 디파이(DeFi) 대상

플래시 론으로 거액을 무담보 대출받아 시세 조작 자금으로 악용

플래시 론(Flash Loan) : 블록체인의 블록 생성 시간(이더리움 : 약 13초) 내
대출·상환이 이루어지는 무담보 대출 서비스

가상자산 소각(Depletion) 공격



※ [출처] PeckShield, Balancer Hacks: Root Cause and Loss Analysis, '20.6.30.

02 디지털자산 **보안위협 사례** – (5) 기타(NFT)

NFT 대상 사기 속출

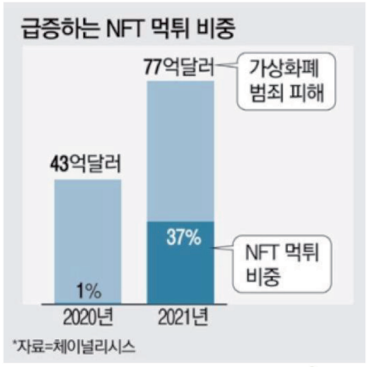
매일경제

[단독] NFT 개발자 돌연 사라졌다...투자금 들고 '먹튀' 속출

기사입력 2022-02-13 18:34 최종수정 2022-02-13 20:49

NFT 신종 사기주의보 발령

가상화폐 먹튀 '러그풀'사례
국내서도 잇달아 피해 발생
캣슬 등 투자자 유치후 잠적



※ [출처] 매일경제, NFT 개발자 돌연 사라졌다…투자금 들고 '먹튀' 속출, '22.2.13.

이상록 금융보안원 보안연구부장

02 디지털자산 **보안위협 사례** – (5) 기타(NFT)

저작권 침해 등 가짜 NFT 발행 기승

연합뉴스

"가짜·표절 NFT 기승"...미국 유명 거래소 NFT 거래중단

기사입력 2022-02-14 12:07

헤자지는 3가지 큰 문제를 꼽았다. 다른 NFT를 허락 없이 복제해 판매하거나, 자신이 소유하지 않은 콘텐츠로 NFT를 만드는 것, 마치 증권처럼 NFT 묶음을 파는 행위 등이다.

이밖에 가격을 올리기 위해 NFT를 자신에게 파는 자전거래도 성행하고 있다는 보고서도 최근 나왔다.

위조나 불법 콘텐츠 문제가 NFT 산업 전반에 퍼져 있다고 헤자지는 말했다.

최대 규모의 NFT 거래소로 기업가치가 133억달러(약 16조원)에 이르는 오픈시(OpenSea)는 자사 플랫폼에서 공짜로 만들어진 NFT의 80%는 표절이거나 위조, 사기라고 지난달 밝혔다.

※ [출처] 연합뉴스, 가짜·표절 NFT 기승…미국 유명 거래소 NFT 거래중단, '22.2.14.

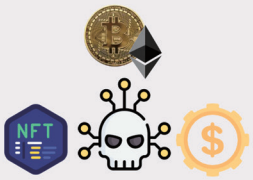
03. 디지털자산 **보안위협 전망**

이상록 금융보안원 보안연구부장

03 디지털자산 **보안위협 전망**

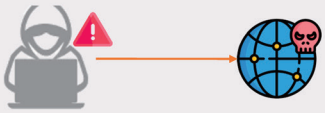
기존 보안위협 진화

- 기존 공격을 타 디지털자산에 적용



새로운 유형의 보안위협 등장

- 디지털자산을 노린 새로운 유형의 공격



03 디지털자산 **보안위협 전망** – 진화 및 새로운 유형 위협 등장

가상자산 대상 공격 → 디지털자산 대상 공격으로 확대

가상자산 생태계에서의 전자지갑, DApp, 거래소 등 대상 공격이 블록체인 기반 디지털자산 금융서비스에도 발생 가능

- CBDC 설계 방식에 따라 가상자산 환경과 유사한 기술이 도입될 수 있음
  → 가상자산 침해 사례가 CBDC에서도 발생될 수 있으니 유의

이상록 금융보안원 보안연구부장

03 디지털자산 **보안위협 전망** – 진화 및 새로운 유형 위협 등장

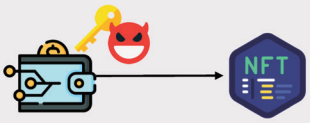
가상자산 대상 공격 → NFT 대상 공격에 적용

NFT 피싱

- NFT 서비스 피싱 사이트 접속
  → 서비스 로그인 정보 탈취

NFT 탈취

- NFT 관리용 개인키 해킹
  → 보관 중인 NFT 탈취



03 디지털자산 **보안위협 전망** – 진화 및 새로운 유형 위협 등장

NFT에 특화된 보안위협 등장

저작권 침해

- NFT 생성 시
  → 타인의 자산을 무단 사용

개인정보 유출

- 개인정보를 NFT에 포함
  → 서비스 사용자 누구나 조회 가능

부정확한 데이터

- NFT에 실물자산 반영 시
  → 실수·고의적으로 잘못된 데이터 입력

원본 유실

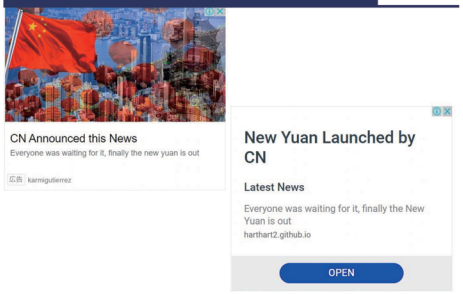
- NFT 원본 파일은 블록체인 외부에 기록
  → 해킹 등에 의해 삭제될 수 있음

이상록 금융보안원 보안연구부장

03 디지털자산 **보안위협 전망** – 진화 및 새로운 유형 위협 등장

인터넷 광고 악용 등 새로운 유형의 사기 등장 전망

구글 배너 광고 → 디지털 위안 사칭



FBI - 검색 광고로 인한 피싱 경고

Catalin Cimpanu | May 12, 2021 — The Record. BY RECORDED FUTURE

FBI warns of cybercriminals abusing search ads to promote phishing sites

The Federal Bureau of Investigation says that cybercrime gangs are using search results and search engine ads to lure victims on phishing sites for financial institutions in order to collect their login credentials.

Scheme has become very popular since at least last year

※ [출처] zzkt, Don't' click on Google Ads - coindaq.io is a fraud organization, '21년
The Record, FBI warns of cybercriminals abusing search ads to promote phishing sites, '21.5.12.

03 디지털자산 **보안위협 전망** – 진화 및 새로운 유형 위협 등장

디지털자산 수탁서비스 활성화 전망(신규 수탁 법인 설립, 서비스 제휴 등)
→ 관리체계미흡/해킹 등에 의한 디지털자산 침해 위협 유의

수탁업체에서 개인키를 분실하여 고객이 맡긴 가상자산에 접근 불가 발생

MARTIN YOUNG — COINTELEGRAPH — JUN 23, 2021

Fireblocks faces lawsuit over deleted keys to $72M Ether wallet

Crypto-custody firm Fireblocks is facing legal action by a firm that claims it was locked out of its wallet containing a substantial amount in crypto assets.

The court was told that a Fireblocks employee allegedly failed to protect or backup the private keys to the wallet, which were subsequently deleted preventing StakeHound from accessing its assets. In a statement, StakeHound claimed:

※ [출처] Cointelegraph, Fireblocks faces lawsuit over deleted keys to $72M Ether wallet, '21.6.23.

이상록 금융보안원 보안연구부장

04. 디지털자산 **보안** 관련 **국내·외 규제**

04 디지털자산 **보안** 관련 **국내·외 규제** – (1) FATF(국제자금세탁방지기구)

FATF는『가상자산·가상자산사업자 위험기반 접근법 지침서』를 발표('21.10월)

거래상대방에 대한 평가 방법을 3단계로 제안하며, 특히 거래 적격성 평가 시 보안성도 고려할 것을 제시

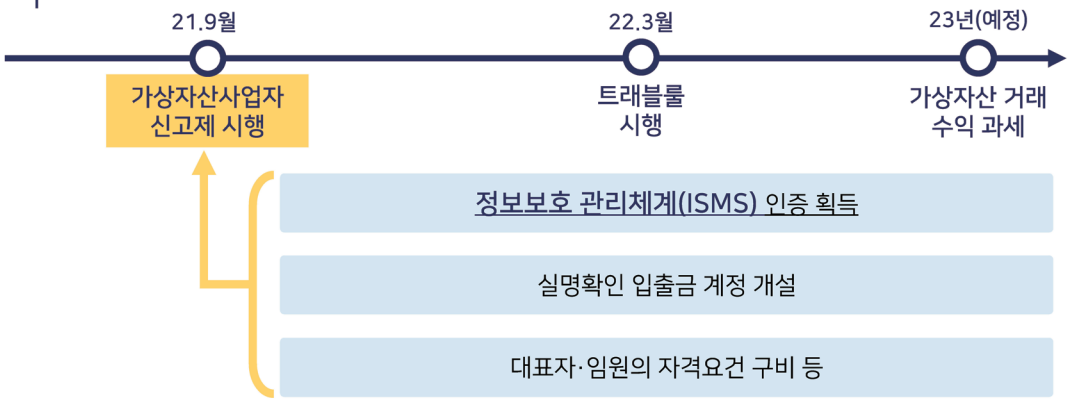
1단계	거래상대방이 가상자산거래소인지 판단
2단계	거래상대방 가상자산거래소의 신원을 확인
3단계	거래상대방 가상자산거래소의 거래 적격성을 평가

각 가상자산사업자는
AML/CFT 관점의 위험기반 분석,
데이터 저장 및 보안 등을 고려
↓
상대 거래소가 고객 데이터 송신 및
비즈니스 관계 형성에 적절한지 평가

이상록 금융보안원 보안연구부장

04 디지털자산 **보안** 관련 **국내·외 규제** – (2) 국내

국내의 경우 가상자산사업자 신고 시 요건으로 ISMS 인증 등을 포함



※ [참고] 금융위원회 보도자료 「자금세탁방지 의무의 신규적용 대상인 가상자산사업자의 신고 매뉴얼을 배포합니다」('21.2.17.) 등

04 디지털자산 **보안** 관련 **국내·외 규제** – (3) EU

EU는 「가상자산 시장 규제(MiCA)」에서 보안 관련 가상자산사업자의 의무를 규정

* 「가상자산 시장 규제(Regulation on Markets in Crypto Assets, MiCA)」는 '20.9월 발표된 후 현재 입법 추진 중

가상자산사업자 의무

건전성	기관 요건
건전성 보호장치 **자금**: (i) 최소 자본 요건 (ii) 전년도 고정간접비 25% 이상 **보험**: 기밀유지 의무 위반, 시스템 중단 또는 장애로 인한 손실 등 보장	■ 탄력적이고 안전한 ICT 시스템 구축 → 서비스 연속성 확보 ■ 비즈니스 연속성 정책 수립 (ICT업무 연속성, 재해복구계획수립 등) → 데이터·기능 보호 및 서비스 유지 ■ 정보의 보안성·무결성·기밀성 보호를 위한 시스템 및 절차 구축 ■ 위험평가를 위한 내부 통제 메커니즘 및 절차를 구축하고, 주기적으로 점검 (ICT시스템 통제·보호조치 등) ■ 거래 관련 모든 기록을 보관 ■ 시장질서교란행위를 모니터링·탐지하는 시스템 및 절차 마련

이상록 금융보안원 보안연구부장

05. 안전한 디지털자산 활용을 위한 대응

05 안전한 디지털자산 활용을 위한 대응

디지털자산 활성화에 따른 금융생태계 변화에 유의

디지털자산

- 비트코인, 이더리움 등
- 스테이블코인
- NFT (대체불가토큰)
- CBDC (중앙은행 디지털화폐)

디지털전환 가속

금융회사 역할, 금융인프라·서비스 등을 대대적으로 변화시킬 수 있는 가능성
→ 비즈니스 모델 다변화 뿐만 아니라 보안위협 대응에 선제적이고 적극적인 준비 필요

이상록 금융보안원 보안연구부장

05 안전한 디지털자산 활용을 위한 대응

디지털자산에 대한 보안성 확보는 선택 아닌 필수

디지털자산은 금전적 이득을 노리는 공격자에게 매력적인 공격 대상

기존 보안위협 진화

기존 가상자산 대상 공격 (사칭, 피싱, 탈취, 취약점 악용, 거래소 사이버공격 등) ➤ NFT, CBDC 등 공격 대상 확대

새로운 유형의 보안위협 등장

- NFT에 특화된 보안위협
- 수탁서비스 대상 공격
- 새로운 유형의 사기 등장 등

디지털자산 관련 정책·제도 수립 시 보안 관련 사항을 면밀히 검토할 필요

05 안전한 디지털자산 활용을 위한 대응

사이버리스크가 금융안정을 위협하지 않도록 안전하고 건전한 디지털자산 서비스 제공을 위해 노력

위협대응체계 확립

가상자산사업자도 금융회사와 유사한 수준의 위험관리정책 및 관리적·물리적·기술적 위협대응체계 확립 필요

제3자 리스크 관리

제휴·연계기관의 미흡한 보안 체계로 인한 제3자 리스크가 발생하지 않도록 유의

- 제3자 관계 목록화 및 제3자 의존성 파악
- 계약서 내 보안성 확보 사항 명시 등

서비스 보안성 확보

서비스 계획수립부터 개발, 운영 등 각 단계마다 보안에 대한 고려 및 보안성 검증이 필수

- 사전 보안성 검토
- 위협대응훈련
- 개발보안 및 취약점 점검
- 상시 모니터링

금융보안원은 지속적 정책·기술 조사·분석·연구 등을 통해 디지털자산 활용에 따른 보안리스크 대응을 적극 지원할 예정

2022년 디지털자산과 보안위협

이상록 금융보안원 보안연구부장

Dong-A 2022 INFOSEC

주제발표 2

금융시장 NFT(Non-Fungible Token) 활용과 보안 이슈

김승주
고려대 정보보호대학원 교수

2022 동아 인포섹-정보보호 콘퍼런스
Dong-A InfoSec 2022-Information Security & Privacy Conference

주제발표 2

금융시장 NFT(Non-Fungible Token)활용과 보안 이슈

김승주
고려대 정보보호대학원 교수

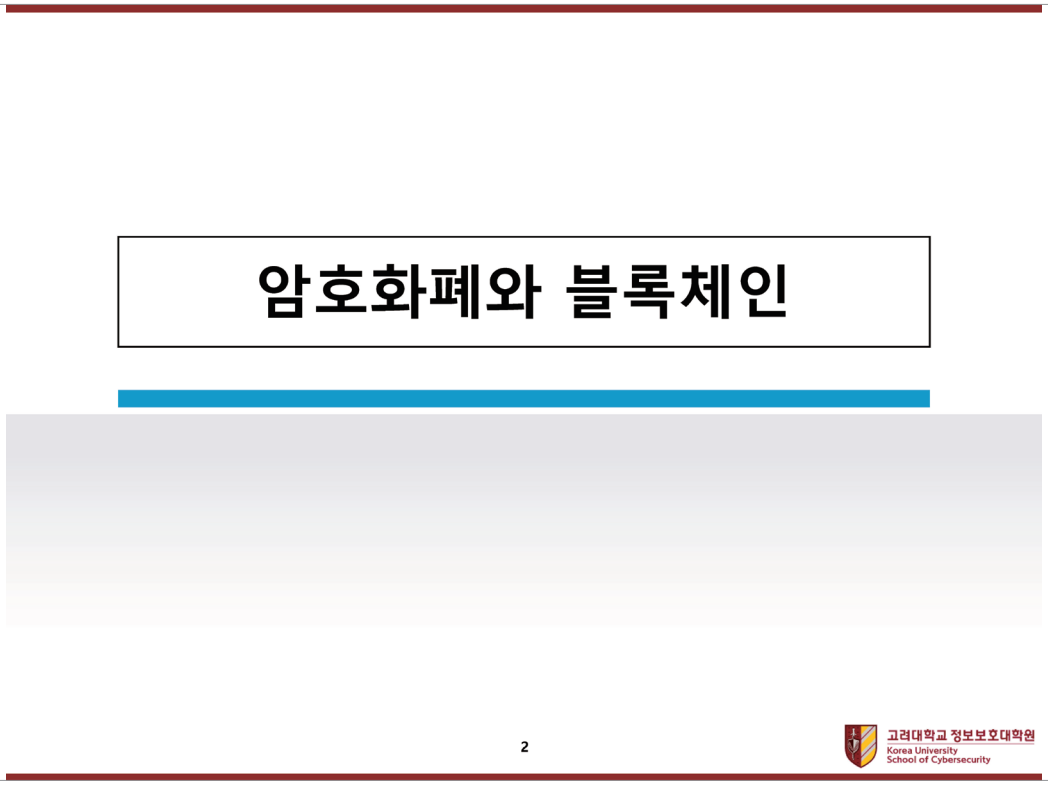
키워드	#블록체인 #암호화폐 #가상자산 #대체불가능토큰 #NFT
핵심문장	NFT의 실체와 올바른 이용방법

주요경력

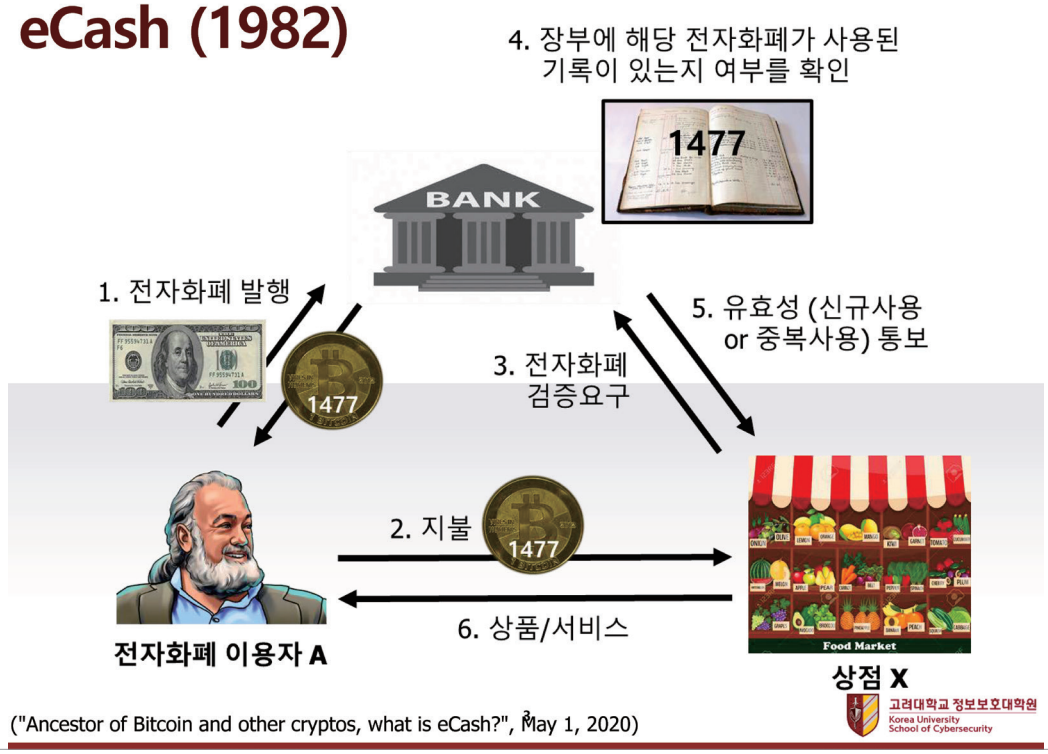
- 대통령직속 4차산업혁명위원회 위원
- 육군사관학교 초빙교수
- 한국인터넷진흥원(KISA) 팀장

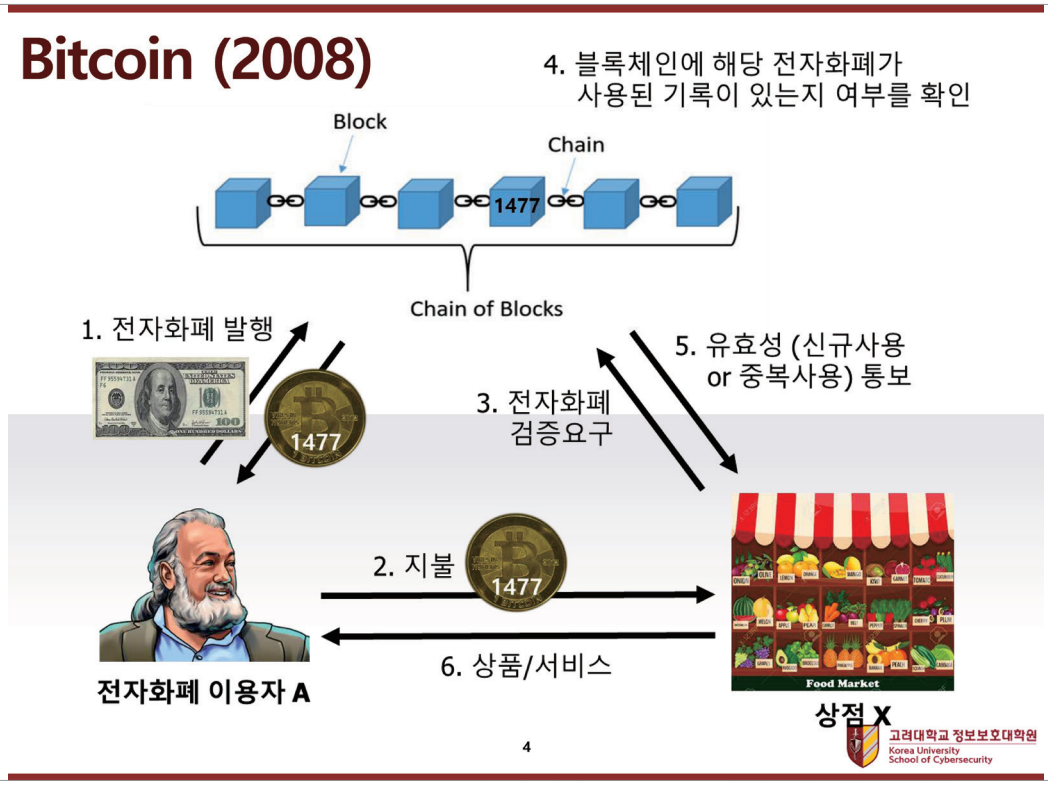
금융시장 NFT(Non-Fungible Token)활용과 보안 이슈

김승주 고려대 정보보호대학원 교수



김승주 고려대 정보보호대학원 교수





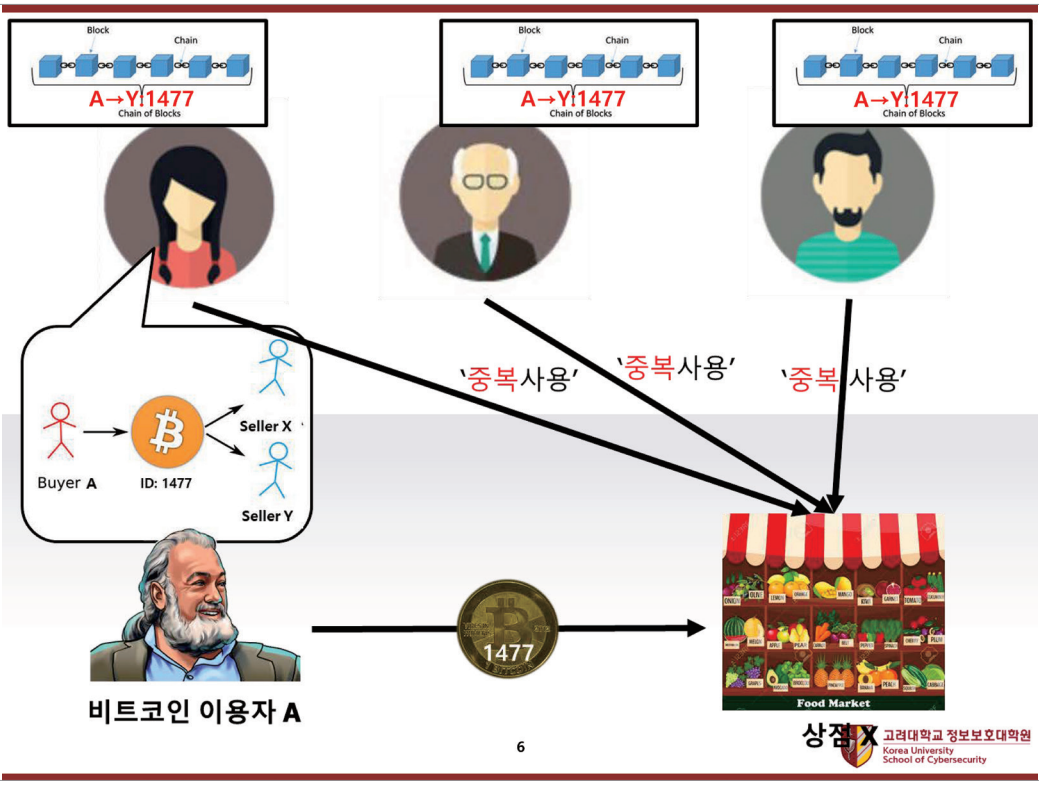
김승주 고려대 정보보호대학원 교수

블록체인(Blockchain)이란?

- 5호(五戶)담당제
  - "서로 감시하고 신고하라"

5

고려대학교 정보보호대학원
Korea University
School of Cybersecurity



6

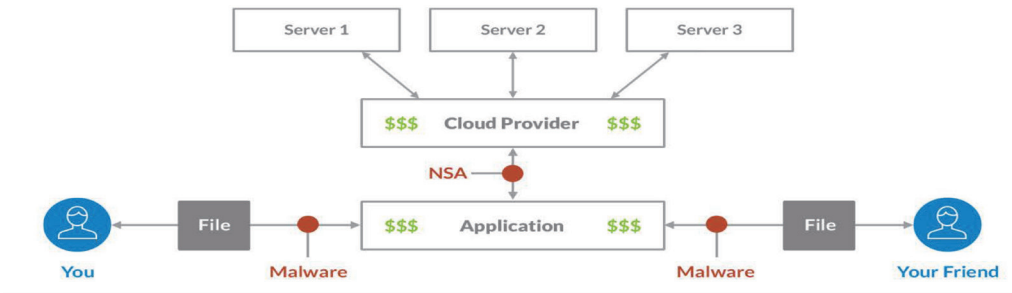
고려대학교 정보보호대학원
Korea University
School of Cybersecurity

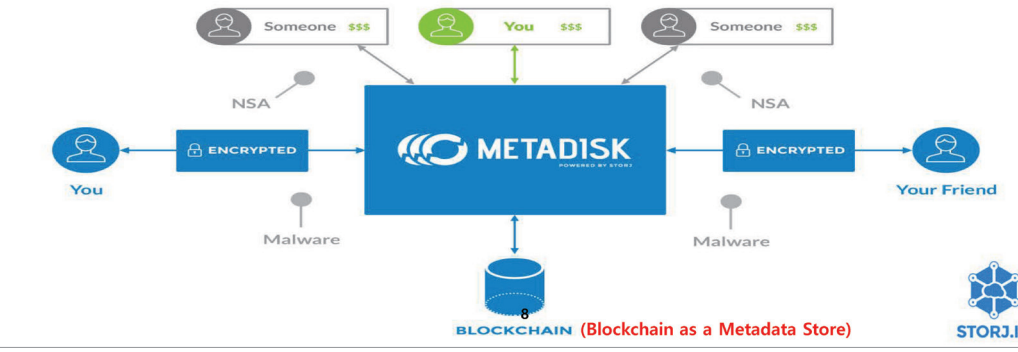
김승주 고려대 정보보호대학원 교수

블록체인의 장점

탈중앙화	투명성	불변성	가용성
중앙 관리자의 역할을 참여자가 분담해 협동조합형 경제 모델을 구축하는데 용이하다.	참여자 간 모든 정보가 공유돼 정보의 비대칭성을 해소한다.	참여자 간의 합의 이후에는 원저작자라 할지라도 기록된 내용을 수정하거나 삭제하는 것이 불가능하다.	데이터가 여러 곳에 중복 저장되므로, 데이터 파괴로 인한 시스템 마비에 효과적으로 대응할 수 있다.

STORJ : Decentralized Cloud Storage





김승주 고려대 정보보호대학원 교수

Blockstack : DNS without SPOF

BLOCKSTACK

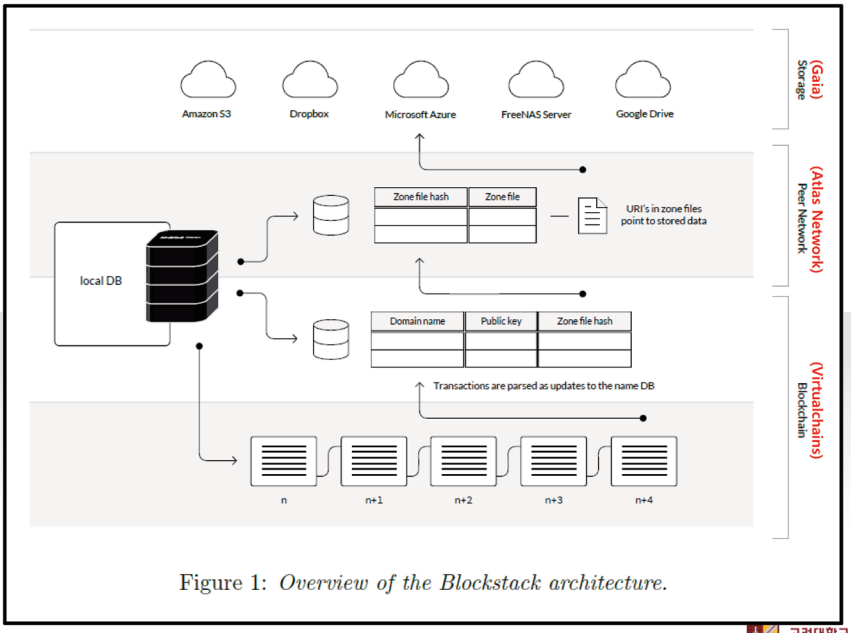


Figure 1: *Overview of the Blockstack architecture.*

(Muneeb Ali et al., "Blockstack Technical Whitepaper", Oct 12, 2017)

9

고려대학교 정보보호대학원 Korea University School of Cybersecurity

CertCoin : CA without SPOF

CertCoin:
A NameCoin Based Decentralized Authentication System
6.857 Class Project

Conner Fromknecht (conner@mit.edu), Dragos Velicanu (velicanu@mit.edu),
Sophia Yakoubov (sonka89@mit.edu)

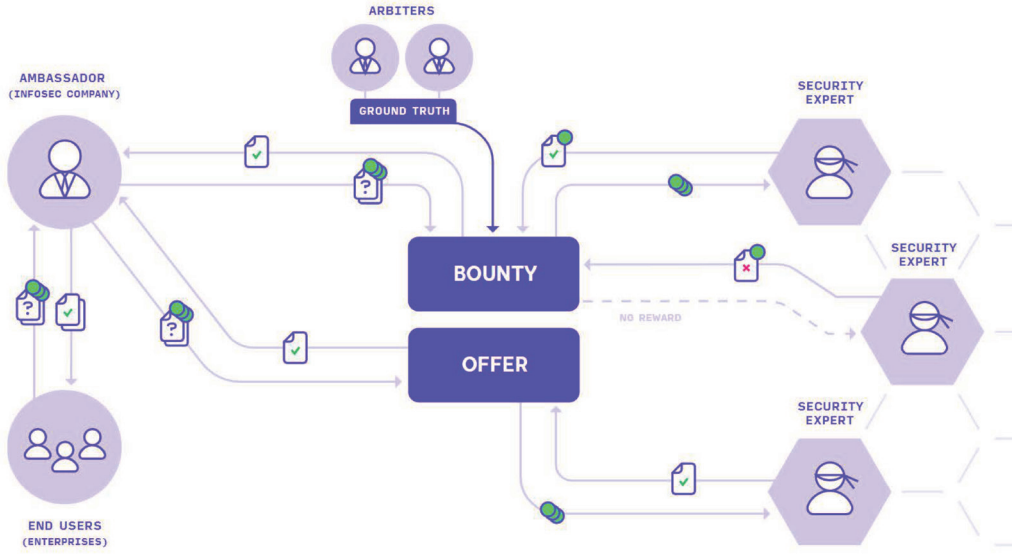
May 14, 2014

10

Korea University School of Cybersecurity

김승주 고려대 정보보호대학원 교수

PolySwarm : Decentralized Virus Total



11

고려대학교 정보보호대학원
Korea University
School of Cybersecurity

대체불가능토큰, NFT

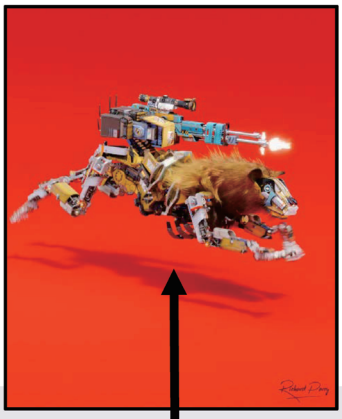
12

고려대학교 정보보호대학원
Korea University
School of Cybersecurity

금융시장 NFT(Non-Fungible Token)활용과 보안 이슈

김승주 고려대 정보보호대학원 교수

김승주 고려대 정보보호대학원 교수



확 인 서 면

등기할 부동산의 표시

건물이나, 토지의 표시(주소, 구조, 면적, 대지권 비율 등) 기재

	성 명	소유자의 성명	등 기 의 목 적
등 기 의무자	주 소	해당 물건의 주소	소유권이전 및 근저당설정 기재
	주민등록번호	소유자의 주민번호	
첨부 서류	주민등록증사본, 여권사본, 자동차운전면허증사본		
특기 사항	신장, 체중, 얼굴 생김새, 머리 스타일 등 신체적 특성 및 특이사항을 상세히 기재		
우 무 인	소유자의 오른손 엄지손가락 지문 날인		

위 첨부서면의 원본에 의하여 등기의무자의 본인임을 확인하고 부동산 등기법 제49조 제3항의 규정에 의하여 이 서면을 작성하였습니다.

20**년 **월 **일

NFT (등기권리증)

{"name":"C.L.A.W Fast-Attack Lion","description":"W"Whoever said that the pen is mightier than the sword has obviously never encountered the C.L.A.W Fast-Attack LionW" - Douglas MacArthurWnWnRichard Parry, 2021Wn1600x1250pix, 30fps","image":"ipfs://Qmeq6cHo4TFHAHve7LbbcBJxpUsZmKEPrAz7uzTTieuwKA/nft.mp4"}

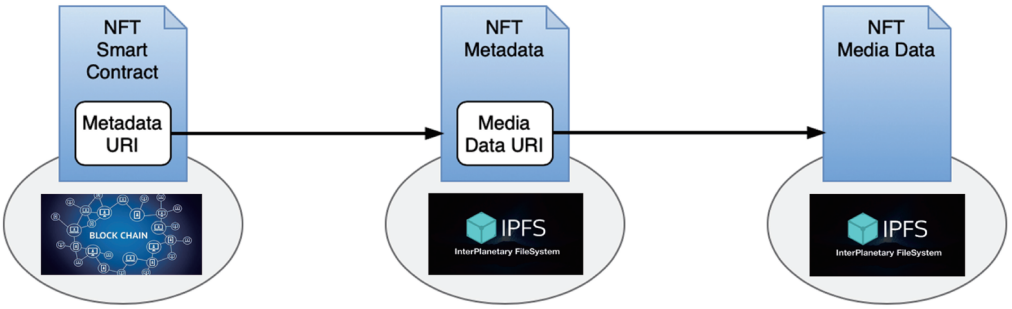
블록체인에 저장

15

고려대학교 정보보호대학원 Korea University School of Cybersecurity

NFT의 세부 구조

NFT 소유권 확인 / 양도 / 로열티 지급 등의 거래를 중앙 신뢰기관의 도움 없이도 개인간(P2P) 가능하게 하는 스마트 컨트랙트



{"name":"C.L.A.W Fast-Attack Lion","description":"W"Whoever said that the pen is mightier than the sword has obviously never encountered the C.L.A.W Fast-Attack LionW" - Douglas MacArthurWnWnRichard Parry, 2021Wn1600x1250pix, 30fps","image":"ipfs://Qmeq6cHo4TFHAHve7LbbcBJxpUsZmKEPrAz7uzTTieuwKA/nft.mp4"}

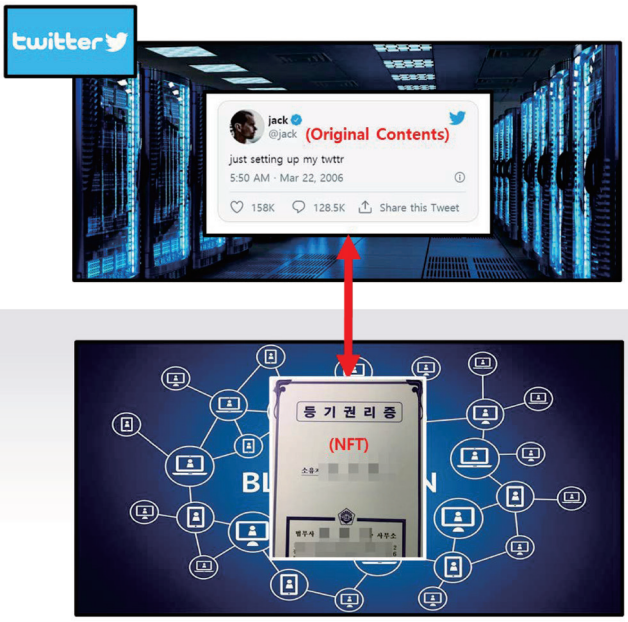
16

고려대학교 정보보호대학원 Korea University School of Cybersecurity

금융시장 NFT(Non-Fungible Token)활용과 보안 이슈

김승주 고려대 정보보호대학원 교수

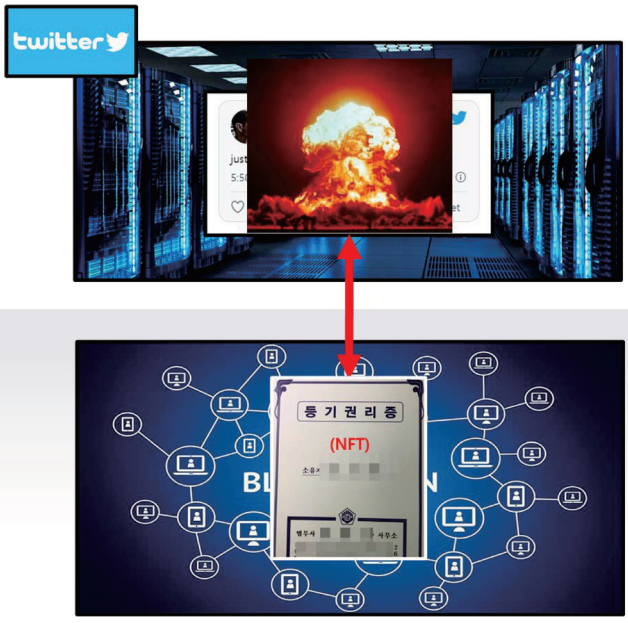
NFT의 단점 – 원본 소실 위험



17

고려대학교 정보보호대학원
Korea University
School of Cybersecurity

NFT의 단점 – 원본 소실 위험

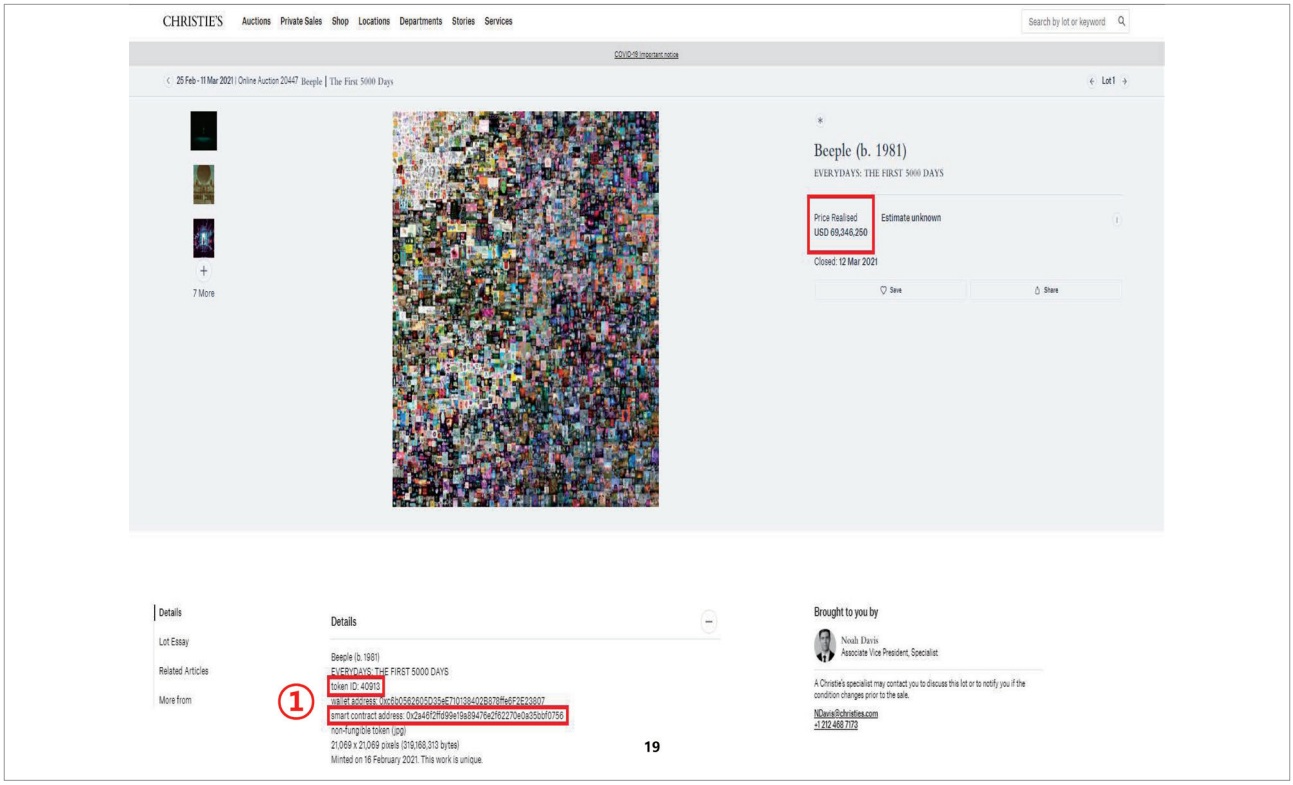


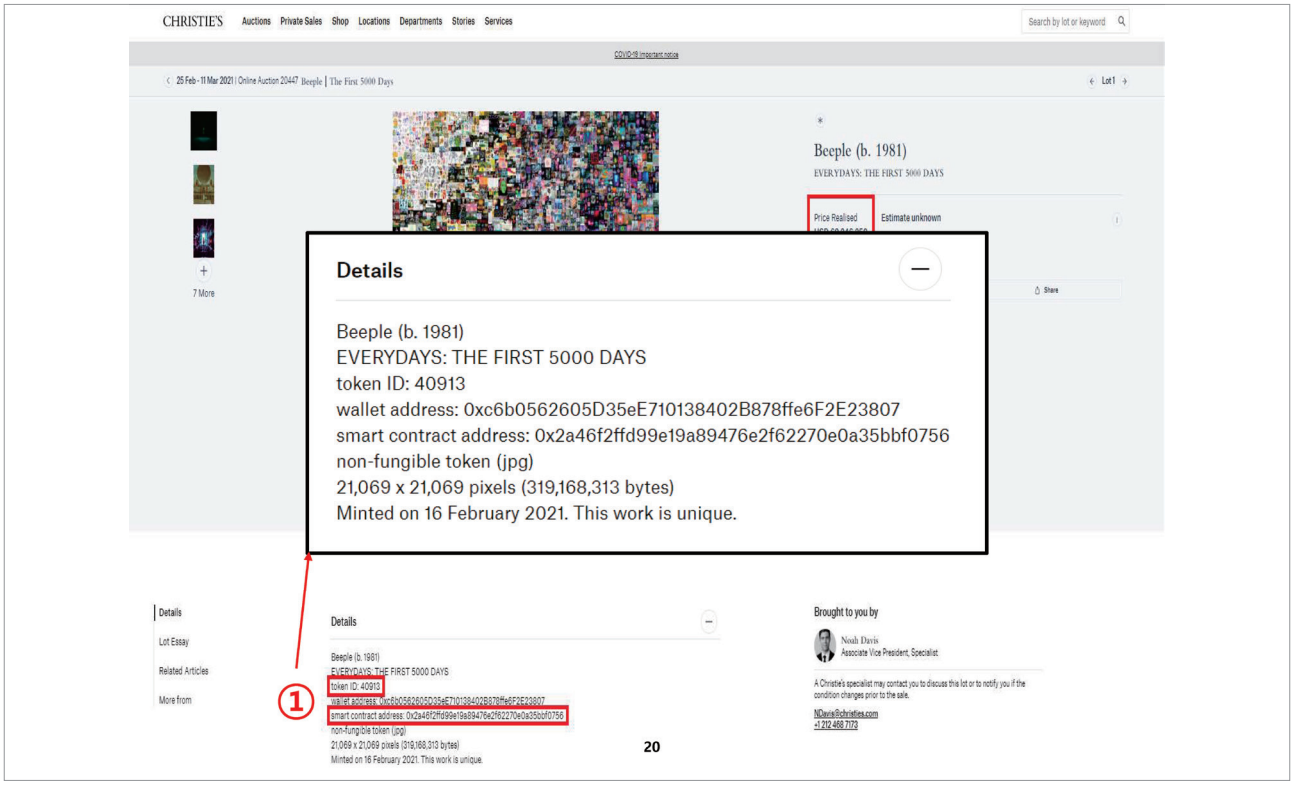
18

고려대학교 정보보호대학원
Korea University
School of Cybersecurity

금융시장 NFT(Non-Fungible Token)활용과 보안 이슈

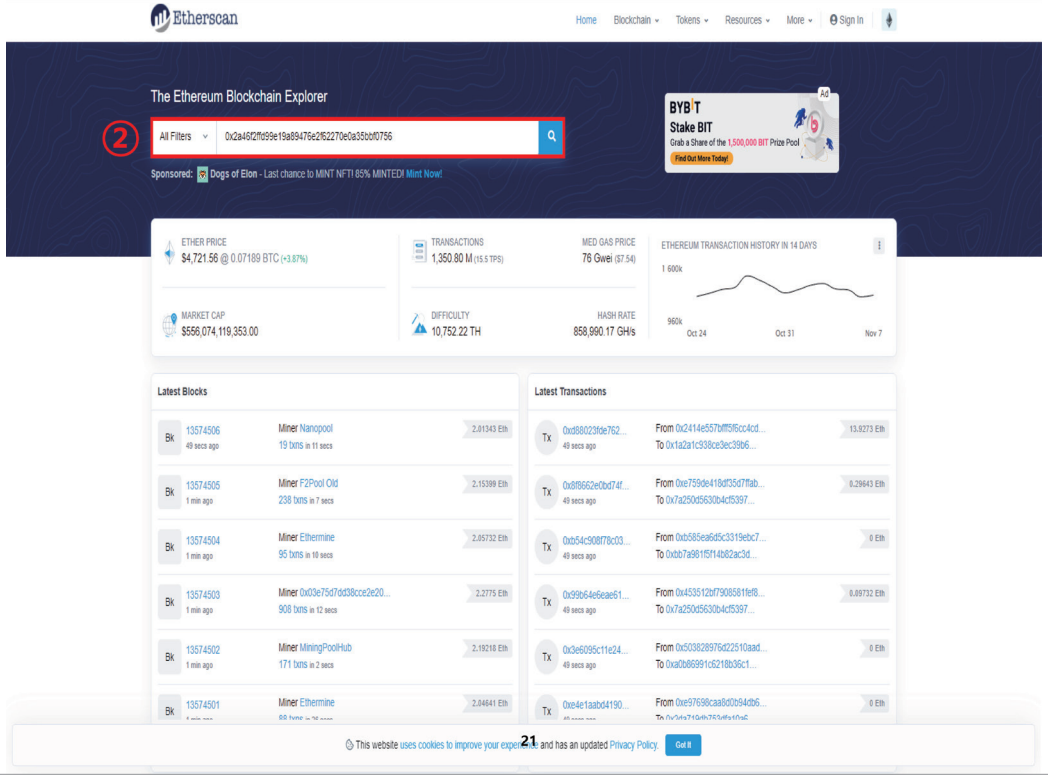
김승주 고려대 정보보호대학원 교수





금융시장 NFT(Non-Fungible Token)활용과 보안 이슈

김승주 고려대 정보보호대학원 교수



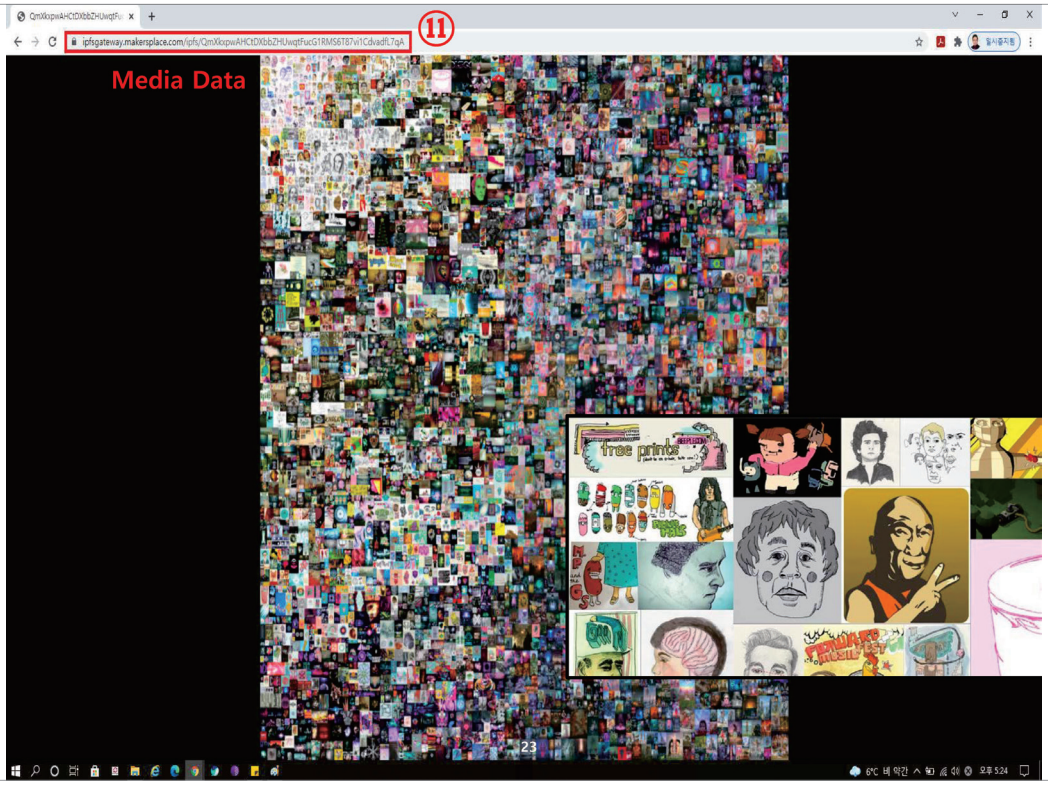

```
{
  "title": "EVERYDAYS: THE FIRST 5000 DAYS",
  "name": "EVERYDAYS: THE FIRST 5000 DAYS",
  "type": "object",
  "imageUrl": "https://ipfsgateway.makersplace.com/ipfs/QmZ15eQX8FPjfrtdX3QYbrhZxJpbLpvDpsgb2p3VEH8Bqq",
  "description": "I made a picture from start to finish every single day from May 1st, 2007 - January 7th, 2021.  This is every motherfucking one of those pictures.",
  "attributes": [
    {
      "trait_type": "Creator",
      "value": "beeple"
    }
  ],
  "properties": {
    "name": {
      "type": "string",
      "description": "EVERYDAYS: THE FIRST 5000 DAYS"
    },
    "description": {
      "type": "string",
      "description": "I made a picture from start to finish every single day from May 1st, 2007 - January 7th, 2021.  This is every motherfucking one of those pictures."
    },
    "preview_media_file": {
      "type": "string",
      "description": "https://ipfsgateway.makersplace.com/ipfs/QmZ15eQX8FPjfrtdX3QYbrhZxJpbLpvDpsgb2p3VEH8Bqq"
    },
    "preview_media_file_type": {
      "type": "string",
      "description": "jpg"
    },
    "created_at": {
      "type": "datetime",
      "description": "2021-02-16T00:07:31.674688+00:00"
    },
    "total_supply": {
      "type": "int",
      "description": 1
    },
    "digital_media_signature_type": {
      "type": "string",
      "description": "SHA-256"
    },
    "digital_media_signature": {
      "type": "string",
      "description": "6314b55cc6ff34f67a18e1ccc977234b803f7a5497b94f1f994ac9d1b896a017"
    }
    "raw_media_file": {
      "type": "string",
      "description": "https://ipfsgateway.makersplace.com/ipfs/QmXkxpwAHCtDXbbZHUwqtFucG1RMS6T87vi1CdvadfL7qA"
    }
  }
}
```

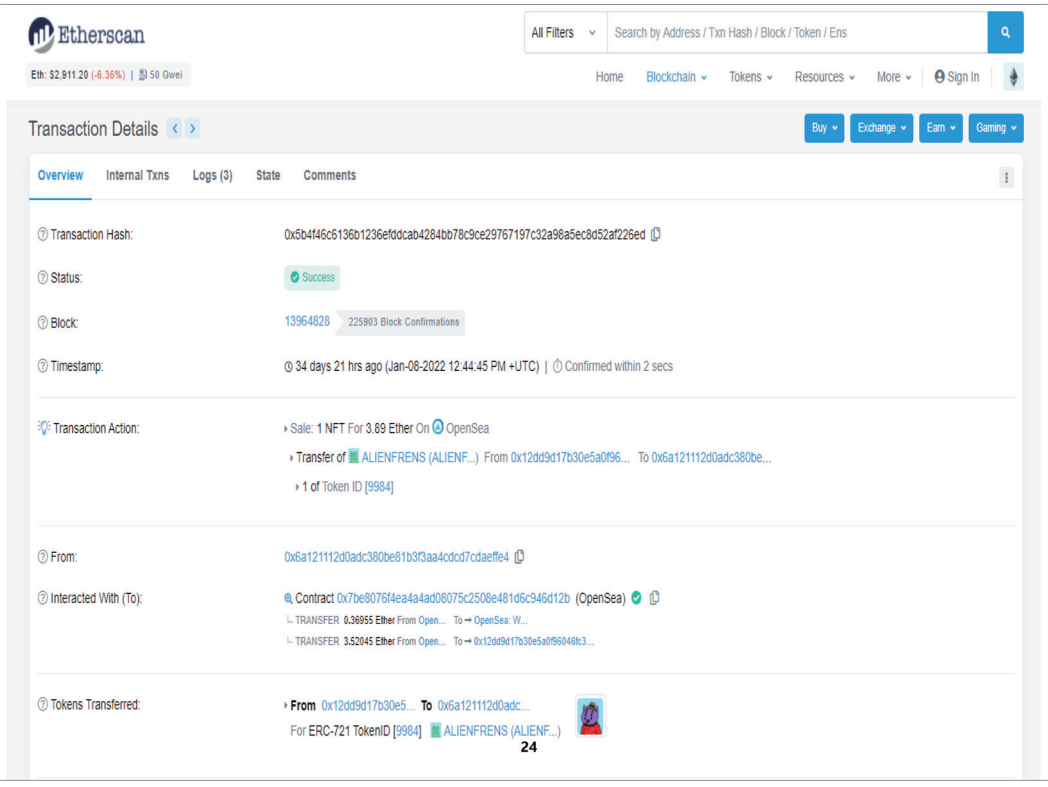

⑩ Media Data URI

22

금융시장 NFT(Non-Fungible Token)활용과 보안 이슈

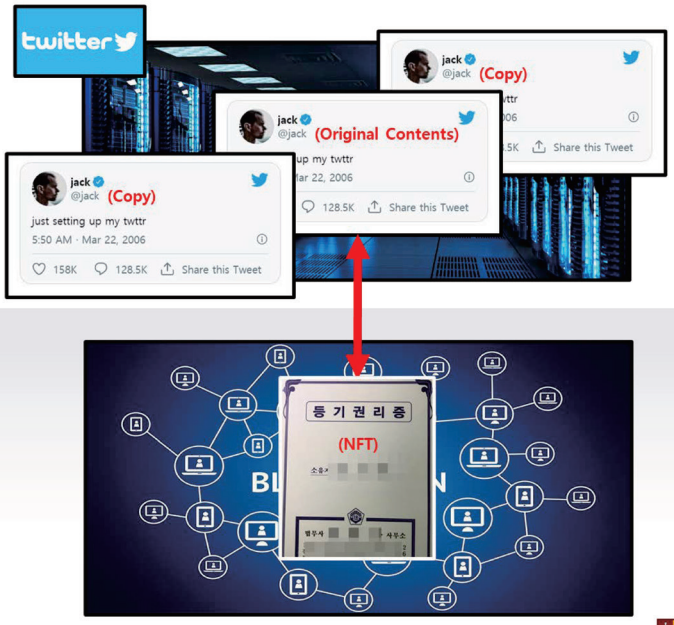
김승주 고려대 정보보호대학원 교수





김승주 고려대 정보보호대학원 교수

NFT의 단점 – 희소성 문제



25

고려대학교 정보보호대학원
Korea University
School of Cybersecurity

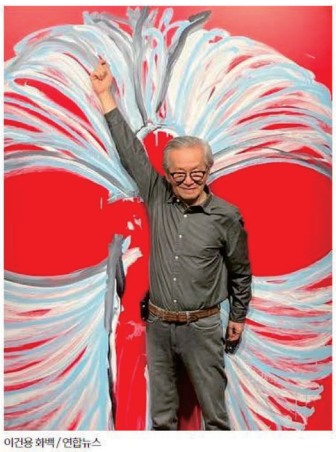
TV CHOSUN '실험미술 거장' 이건용 작품 NFT 논란..."작가 동의도 안 구해" 가 가

생활문화 전체

'실험미술 거장' 이건용 작품 NFT 논란…"작가 동의도 안 구해"

등록 2021.12.06 15:20

최윤정 기자 가 가



이건용 화백/연합뉴스

'한국 실험미술 거장' 이건용(79) 작품을 둘러싸고 NFT 저작권 논란이 불거졌다.

이시각 주요 뉴스

이성윤 수사팀 "공수처, 취재 보복이자 최악의

이재명, TK서 "尹 친일파" 맹비난…박정희엔

강원 찾은 尹, 이재명에 "대장동 당사자가 해괴한 얘기"

"적금 최대 4% 이자" 다시 은행으로 몰리는 뭉칫돈

26

금융시장 NFT(Non-Fungible Token)활용과 보안 이슈

김승주 고려대 정보보호대학원 교수

NFT = 소유욕 + 자랑하고 싶은 욕심

27

고려대학교 정보보호대학원 Korea University School of Cybersecurity

NFT의 다양한 응용들

28

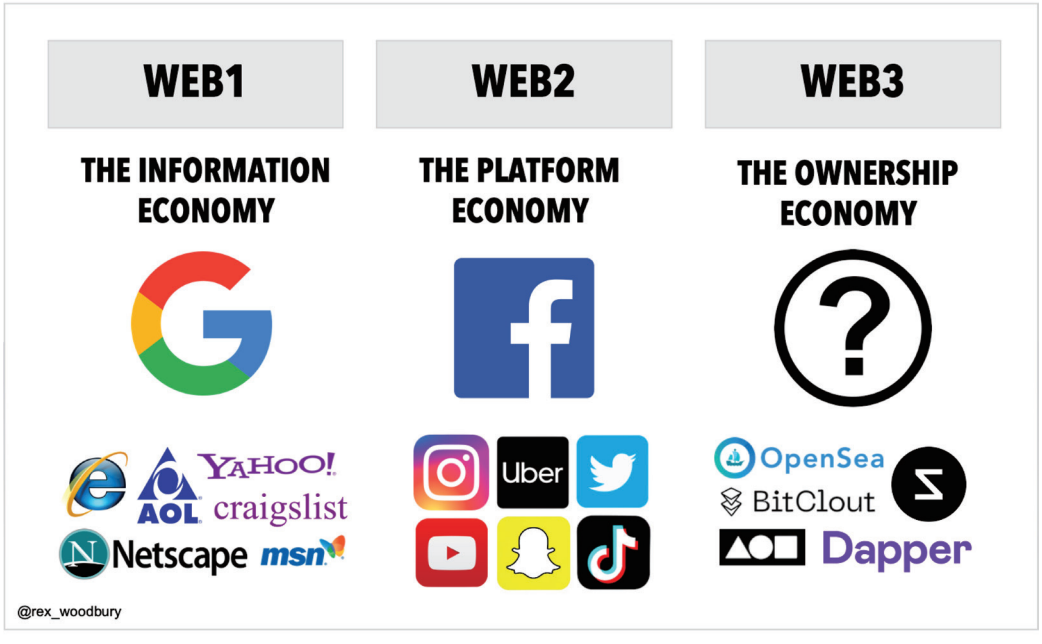
고려대학교 정보보호대학원 Korea University School of Cybersecurity

김승주 고려대 정보보호대학원 교수

NFT의 다양한 응용들

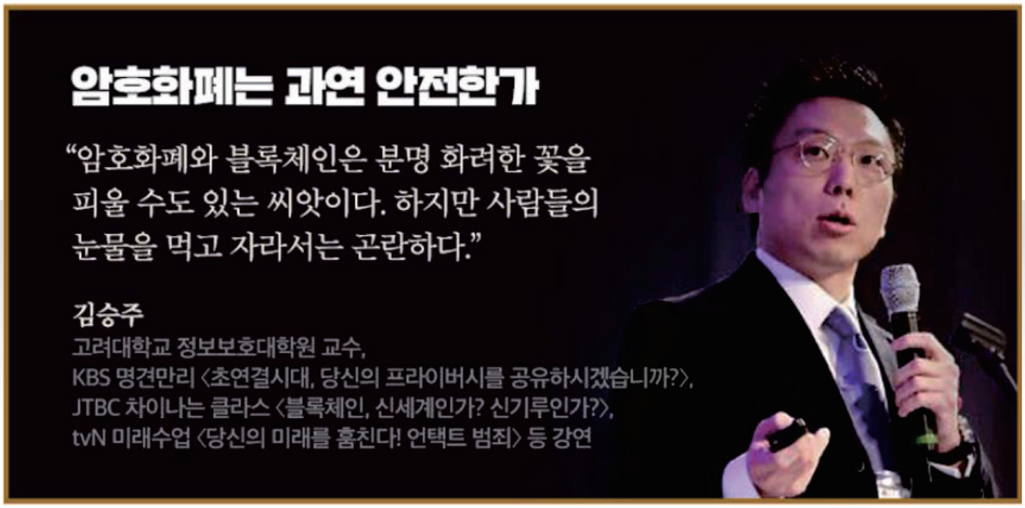
29

고려대학교 정보보호대학원 Korea University School of Cybersecurity



30

고려대학교 정보보호대학원 Korea University School of Cybersecurity



31

고려대학교 정보보호대학원 Korea University School of Cybersecurity

32

고려대학교 정보보호대학원 Korea University School of Cybersecurity

금융시장 NFT(Non-Fungible Token)활용과 보안 이슈

김승주 고려대 정보보호대학원 교수

Dong-A 2022 INFOSEC

주제발표 3

디지털화폐(CBDC) 도입이 가져올 금융보안의 변화와 새로운 보안 과제

강민석

KAIST 전산학부/정보보호대학원 교수

2022 동아 인포섹-정보보호 콘퍼런스

Dong-A InfoSec 2022-Information Security & Privacy Conference

주제발표 3

디지털화폐(CBDC) 도입이 가져올 금융보안의 변화와 새로운 보안 과제

강민석
KAIST 전산학부/정보보호대학원 교수

키워드	#디지털화폐 #CBDC #금융보안 #정보보호
핵심문장	디지털화폐(CBDC)의 도입이 가져올 새로운 보안 문제들과 이를 해결하기 위한 보안 연구 과제에 대해 논함

주요경력

- KAIST 전산학부/정보보호대학원 조교수
- 싱가포르국립대학교 전산학부 조교수

강민석 KAIST 전산학부/정보보호대학원 교수

2022 동아 인포섹 - 정보보호 콘퍼런스

디지털화폐(CBDC) 도입이 가져올 금융보안의 변화와 새로운 보안 과제

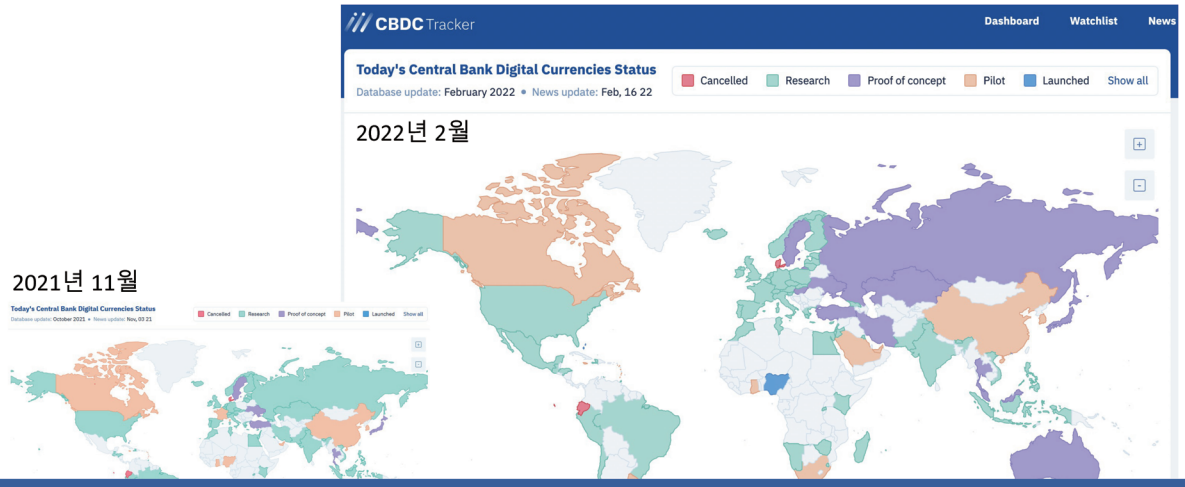
February 23, 2022

강민석
Assistant Professor
School of Computing

NetS&P Research Lab @ KAIST
KAIST

강민석 KAIST 전산학부/정보보호대학원 교수

세계의 CBDC 추진 현황



현재 개발중인 CBDC의 약 80%는 블록체인 기술 활용

Central Bank Digital Currency (CBDC) 개요

- (정의) CBDC는 지급준비금, 결제성 예금과는 별도로 중앙은행이 발행하는 디지털 형태의 화폐(현금)
  - (IMF, 'A survey of research on central bank digital currency')

  ✓ 기대: 새로운 금융 서비스의 도래
  ✓ 우려: 안정성, 해킹에 대한 걱정
  ✓ 오해: 이미 Cashless 사회 아닌가?
  ✓ 전망: e-CNY, digital Yen, e-dollar,...

- 본 발표의 목표: 곧 도래할 CBDC 시스템에서 발생할 것으로 예상되는 사이버 공격에 대해 살펴보고, 어떤 시급한 연구 과제가 있는지 토의한다.

4

강민석 KAIST 전산학부/정보보호대학원 교수

CBDC 비전

- "Cash-like" 디지털 화폐
- 효율적인 거래 처리
- 넓은 세금 망 (tax net)
- 유연한 통화 정책

5

CBDC: To Distribute, or Not to Distribute?

Centralized blockchain
(예: 중앙형 CBDC)

Fully-decentralized blockchain
(예: 비트코인, 이더리움)

Finding sweet spots!

✓ 네트워크 장애에 치명적
✓ 네트워크 partitioning 공격에 상대적으로 강인함

✓ 네트워크 장애에 유연하게 대응 가능
✓ 네트워크 partitioning 공격에 상대적으로 취약

6

강민석 KAIST 전산학부/정보보호대학원 교수

CBDC의 시스템 구조

	Centralized	Semi-Decentralized	Decentralized
Performance	Excellent, full control of infrastructure	Good, SMR with many participants	Challenging, active area of research
Censorship	Easy: single operator	Possible: particularly if operators are in the same jurisdiction	Hard: operators might not even be identified
Rewind	Easy: can be done quickly by single operator	Hard: takes longer for operators to agree, implying longer history to revert and worse violation	Extremely hard: requires cooperation by majority of possibly unidentified operators

7

CBDC Security

"보안성(키관리 등)이 디지털지갑 선택에서 가장 중요"
(UBC대학 CHI21)

"KT 통신 장애 … 전국 마비"
(연합뉴스 2021년 10월)

"개인정보 침해가 CBDC사용에 가장 큰 걱정거리"
(European Central Bank (ECB) CBDC 이용자 설문조사, 2021)

8

강민석 KAIST 전산학부/정보보호대학원 교수

세 가지 CBDC 보안 (걱정거리)

1. 건강한 거버넌스 구축을 위한 보안 기술 문제

2. 개인정보보호와 투명성 문제

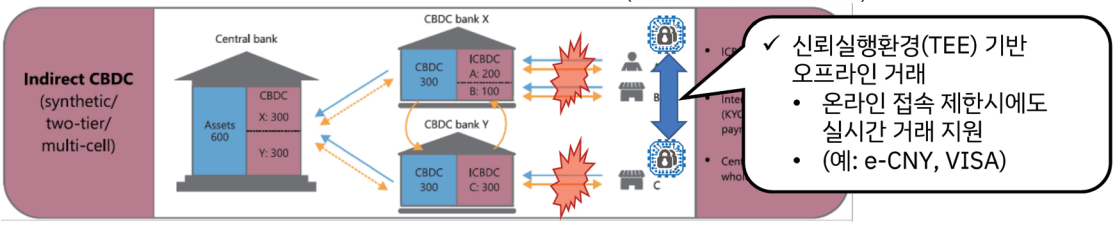
3. 재난/해킹에 강인한 시스템 디자인

9

1. 건강한 거버넌스 구축을 위한 보안 기술 문제

- CBDC 이중계층구조

(source: Auer and Boehme 2021)



✓ 장점: 중앙은행의 금융시장 개입 제한, 개인정보보호

- 보안 문제: 비밀키 관리 (폐기 및 재발급) 난이도 급증
  - ✓망분리에 의지하는 보안 시스템의 위험 (예: Stuxnet)
  - ✓"Prepare for the worst!": 중앙은행, 상업은행, TEE 등의 모든 계층에서 비밀키 침해 고려해야
  - ✓비밀키 침해사고 발생시 "실시간" 탐지 및 자동적 폐기 및 재발행이 핵심: 이 모두를 완벽하게 구현하는 시스템은 알려진 바 없음

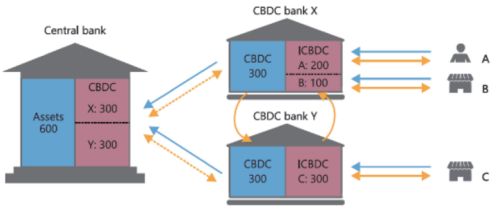
10

강민석 KAIST 전산학부/정보보호대학원 교수

2. 개인정보보호와 투명성 문제

- "개인정보 침해가 CBDC사용에 가장 큰 걱정거리" (European Central Bank (ECB) CBDC 이용자 설문조사, 2021)

- 익명성 문제
  - ✓이중계층구조 (중앙은행은 사용자 정보 접근 불가)
    => 블록체인 분석 통해 사용자 특정
    => 네트워크 패킷 분석으로 사용자 특정



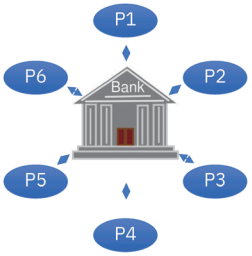
- 거래 기밀성 문제
  - ✓거래 금액 정보 (프로그램 코드) 기밀성 vs. 컴플라이언스 (돈세탁방지, 뱅크런방지)
    => 익명 거래와 컴플라이언스를 동시에 만족 가능한 영지식증명(ZKP),
    다자간보안컴퓨팅(SMPC) 기술 활발히 개발 중

11

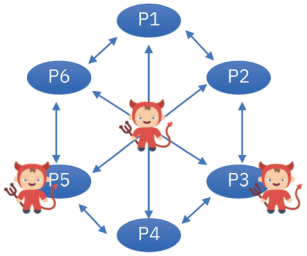
3. 재난/해킹에 강인한 CBDC 시스템 디자인

- 블록체인 합의 알고리즘: CBDC 보안의 핵심

✓ Centralized operator



✓ Decentralized operator



"정상 CBDC 서버는 올바르게 합의된 분산원장을 받게 된다."

안전성 (safety) ?
과 **지속성 (liveness)** ?

"정상 CBDC 서버는 반드시 합의를 이뤄낸다."

예) 클레이튼 프로그램 취약점 (2021)
비트코인 프로그램 취약점 (2017)
대규모 KT 네트워크 장애 (2021)
클레이스왑 네트워크 해킹 (2022)

12

강민석 KAIST 전산학부/정보보호대학원 교수

재난/해킹에 강인한 시스템 => 높은 다양성

• CBDC 디자인의 예	• 가능한 문제점	• 해결책?
✓중앙은행 내부 보안망에 모든 CBDC 서버 구축	✓중앙은행 내부망 대상 사이버/물리 공격 가능	✓물리적/조직적으로 분산된 서버 구축
✓국내 기간망을 사용한 분산 CBDC 서버 구축	✓망사업자의 지연 공격, 장애 혹은 디도스 공격	✓다중 연결성, 오버레이 등으로 다양성 증대
✓단일 소프트웨어 구현을 통한 CBDC 서버 구축	✓단일 취약점에 CBDC 전체 동작 장애	✓다중 소프트웨어 구현 강제로 다양성 증대

13

CBDC 시스템 다양성, 보안성, 그리고 문제점

- 문제점 1: 보안 목표의 부재
  - ✓"어떤 공격자의 어떤 특정한 공격 기술로부터 강인한 CBDC를 만들 것인가?"
  - ✓예: 70년대 ARPANET의 설계 목표—"핵 전쟁에도 살아남는 분산 시스템"
  - ✓한국의 CBDC는 [?] 공격에도 [?] 하는 시스템을 목표로 한다.

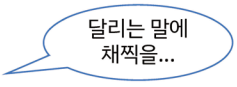
- 문제점 2: 높은 지속성(liveness) 보장의 어려움
  - ✓강력한 네트워크 공격의 실재: 경로 탈취 공격, 메시지 제거, 지연 등의 실제 공격
    - 경로 다양성 만으로는 해결하기 어려워 새로운 단대단 연결 기술 연구 필요
  - ✓다중 SW 프로그램간의 합의 동치 구현의 어려움: 다양한 합의 알고리즘의 SW 버전의 논리적 동치를 보장하기 어려움
    - 다른 언어로 구현된 어려 합의알고리즘 SW간의 동치를 보장하는 연구 필요

14

맺음말

- CBDC 보안: 지금까지 우리가 다뤄온 어떤 분산 컴퓨팅 시스템보다 더 까다롭고 어려울 것

- 세 가지 CBDC 보안 걱정거리



1. 건강한 거버넌스 구축을 위한 보안 기술 문제
2. 개인정보보호와 투명성 문제
3. 재난/해킹에 강인한 시스템 디자인

15

감사합니다

강민석/KAIST 전산학부
minsukk@kaist.ac.kr
https://netsp.kaist.ac.kr/

KAIST

Dong-A 2022 INFOSEC

주제발표 4

한국은행 CBDC 발행에 대응한 멀티에셋 디지털지갑의 핵심기술과 정보보호

박형주
KB국민은행 디지털신사업본부장

2022 동아 인포섹-정보보호 콘퍼런스
Dong-A InfoSec 2022-Information Security & Privacy Conference

주제발표 4

한국은행 CBDC 발행에 대응한 멀티에셋 디지털지갑 핵심기술과 정보보호

박형주
KB국민은행 디지털신사업본부장

키워드	#멀티에셋 #월렛 #CBDC #키 #관리
핵심문장	금융회사가 개발한 디지털 지갑을 통해 다양한 디지털 자산을 안전하게 관리

주요경력

- KB국민은행 DT전략부장(2021.1.)
- KB금융지주/국민은행 디지털전략부장 겸직(2017. 1.)

한국은행 CBDC 발행에 대응한 멀티에셋 디지털지갑 핵심기술과 정보보호

박형주 KB국민은행 디지털신사업본부

KB국민은행

『한국은행 CBDC 발행에 대응한』

멀티에셋 디지털지갑 핵심기술과 정보보호

(2022. 02. 23)

KB국민은행 디지털신사업본부

본부장 박형주

※Strictly Confidential

Contents

Ⅰ. 추진배경 03

Ⅱ. 검증방향 05

Ⅲ. 구축내용 08

Ⅳ. 향후계획 12

한국은행 CBDC 발행에 대응한 멀티에셋 디지털지갑 핵심기술과 정보보호

박형주 KB국민은행 디지털신사업본부장

Ⅰ. 추진배경_ 한국은행의 CBDC 파일럿 테스트 추진

왜 디지털화폐(CBDC) 파일럿 테스트를 추진했는가?

국외 주요국들의 CBDC에 대한 기조

기존에 CBDC에 관해 신중했던 미국, 영국, 일본, EU, 스웨덴 등이 관련 연구를 강화하겠다는 입장으로 선회

특히, 주요국중 중국은 CBDC 시범운영을 확대 실시하면서, 2022년중 CBDC 도입 가능성을 내비치고 있음

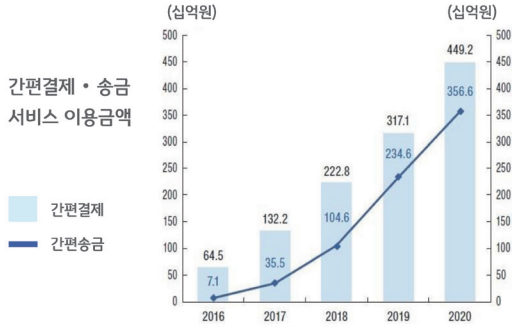
국가별 CBDC 연구 및 도입준비 추진 현황

도입	바하마, 동카리브, 나이지리아
시범운영	중국, 우크라이나, 우루과이
모의실험	유럽연합, 일본, 스웨덴, 러시아, 터키, 한국
기초연구(PoC 등)	미국, 영국, 캐나다, 호주, 노르웨이, 태국

출처 : 한국은행

국내외 지급결제 시장 환경 변화

지급결제 분야의 기술 혁신이 빠르게 이루어지고 있으며 시장 확장성 예견이 어려운 상황, 변화에 대비한 선제적 대응 필요

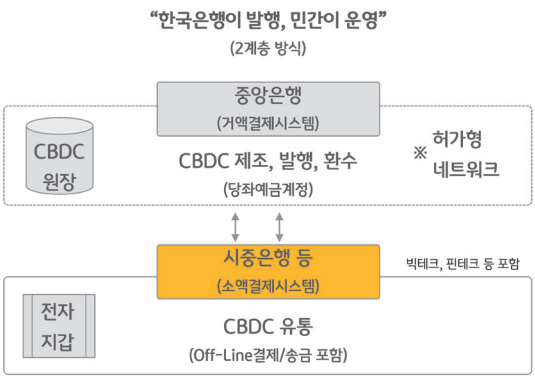


출처 : 한국은행 (※ 전자금융업자, 금융기관 및 휴대폰 제조사 기준, 일평균)

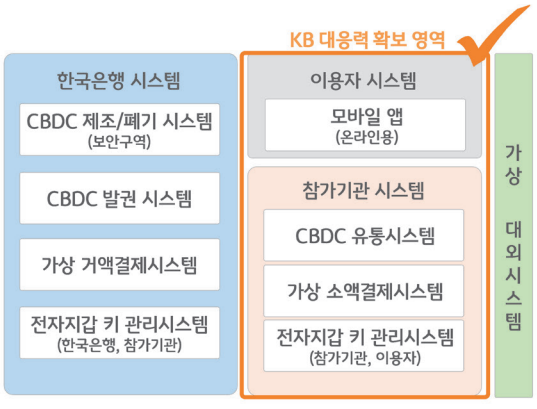
Ⅰ. 추진배경_ 한국은행의 CBDC 파일럿 테스트 추진_ • 시중은행의 역할

한국은행이 파일럿 테스트를 진행하면서 채택한 혼합형 CBDC모델에서 시중은행 역할인
① 이용자 시스템(모바일 앱) ② 참가기관 시스템(유통, 결제, 키 관리 등) 기능에 대한 KB 대응력 확보

한국은행 CBDC 모의실험 모델



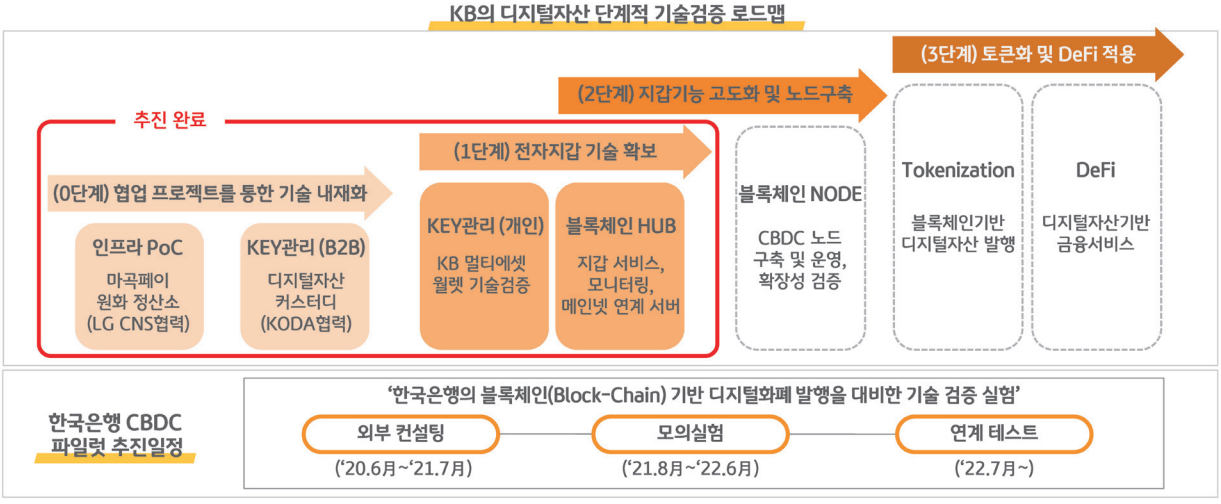
CBDC 시스템 구조 개관



박형주 KB국민은행 디지털신사업본부장

Ⅱ. 검증방향_ 한국은행 CBDC 대응 KB 기술검증 로드맵

KB의 디지털자산 지갑 서비스 역량 및 기술 확보를 목표로, 한국은행의 파일럿 추진일정에 대응하여 로드맵 구성



Ⅱ. 검증방향_ 한국은행 CBDC 대응 KB 기술검증 로드맵_ • 마곡페이 인프라 PoC

마곡페이 (LG CNS 협력) 사업에 참여하여 블록체인기반 화폐 발행 및 유통·관리에 대한 기술 인프라 PoC 진행

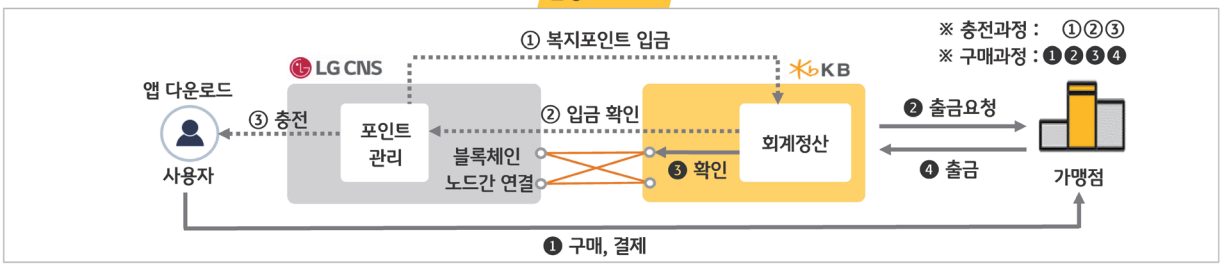
마곡페이 개요

- LG CNS의 '모나체인'기반 지역화폐로, 임직원 복지수당 등을 암호화폐로 제공하여 송금·결제 기능 제공
- 서비스대상 : LG사이언스파크 내 LG CNS 임직원 2천명

KB 개발 참여 부분

- 마곡 커뮤니티 서비스 연계 정산 프로세스 개발
- 마곡페이 잔액 대사 및 거래 모니터링 시스템 구축
- 앱 내 계좌 연계 (KB 비대면 계좌개설 연동)

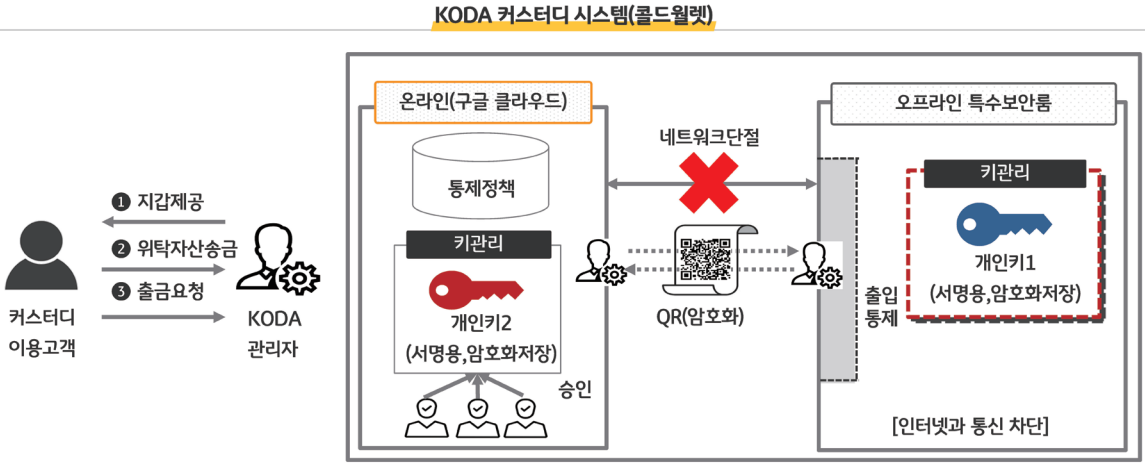
운영 프로세스



박형주 KB국민은행 디지털신사업본부장

II. 검증방향_ 한국은행 CBDC 대응 KB 기술검증 로드맵_ • KEY 관리(디지털자산 커스터디 B2B)

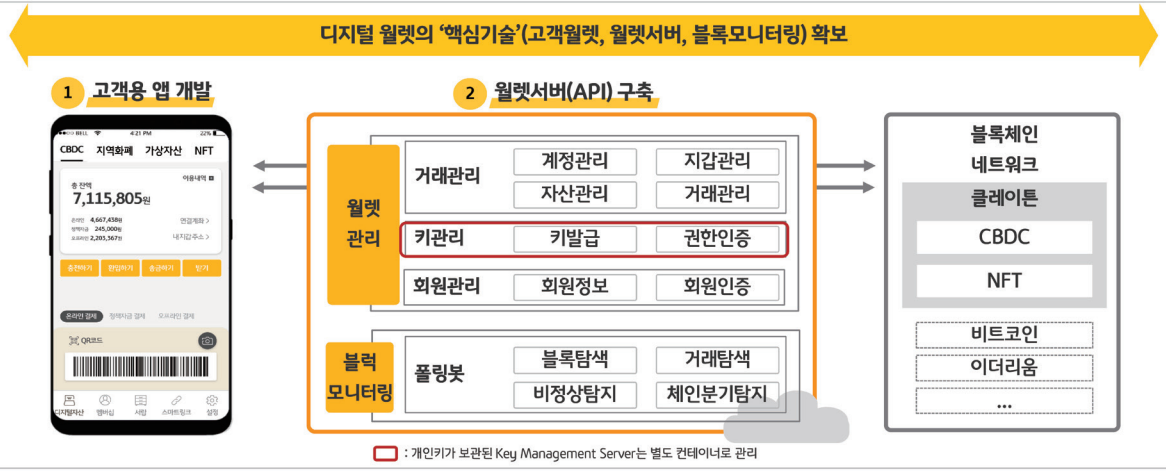
고객의 디지털자산(KEY)을 이관받아 안전하게 보관, 고객요청시 반환하는 커스터디 사업진행 (KODA)



7

III. 구축내용_ 어떻게 만들었는가?

'한국은행 CBDC 모의실험'에 사용된 블록체인 플랫폼 '클레이튼(Klaytn test-net)'을 활용하여 시중은행의 핵심기술인 '고객용 월렛 및 월렛 시스템' 기술검증 추진



8

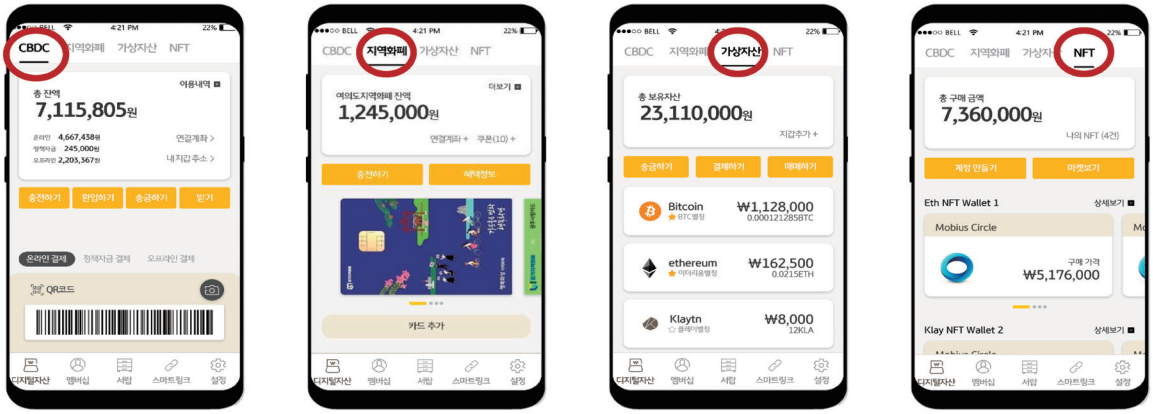
한국은행 CBDC 발행에 대응한 멀티에셋 디지털지갑 핵심기술과 정보보호

박형주 KB국민은행 디지털신사업본부장

III. 구축내용_ 어떻게 만들었는가?_ ① 고객용 월렛(앱)

다양한 디지털자산을 관리 및 거래할 수 있는 '멀티에셋지갑'을 목표로 블록체인 기반 미래 지갑의 모습을 생각하며 구현

KB 멀티에셋 디지털지갑 주요화면



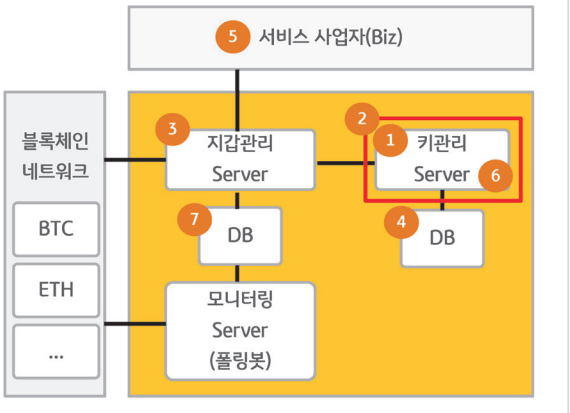
* 실제 은행 계정계 연동 및 디지털자산 발행기능 미개발

9

III. 구축내용_ 어떻게 만들었는가?_ ② 월렛서버(API) 구축

보안적으로 중요한 '키관리'서버와 API기반으로 서비스 사업자에게 관련 기능을 제공하는 '지갑관리'서버 분리 개발, 블록과 거래 모니터링, 체인 분기 및 장기간 미처리 거래에 대한 예외상황 대처를 위한 서버 구축

시스템구성도



월렛서버(API) 구축 상세

① 독립된 키 관리 서버 및 인증

② KMS(Key Manage Server) 연동 2중 암호화

③ 고객별 개인키 부여 및 자산별 지갑 생성
√ 하나의 고객 키가 해킹되어도 다른 고객의 자산을 안전하게 보관할 수 있는 구조

④ 고객의 키를 위탁받아 사용자 편의성과 보안성 높은 아키텍처

⑤ 타 플랫폼 및 자산 확장이 용이한 설계

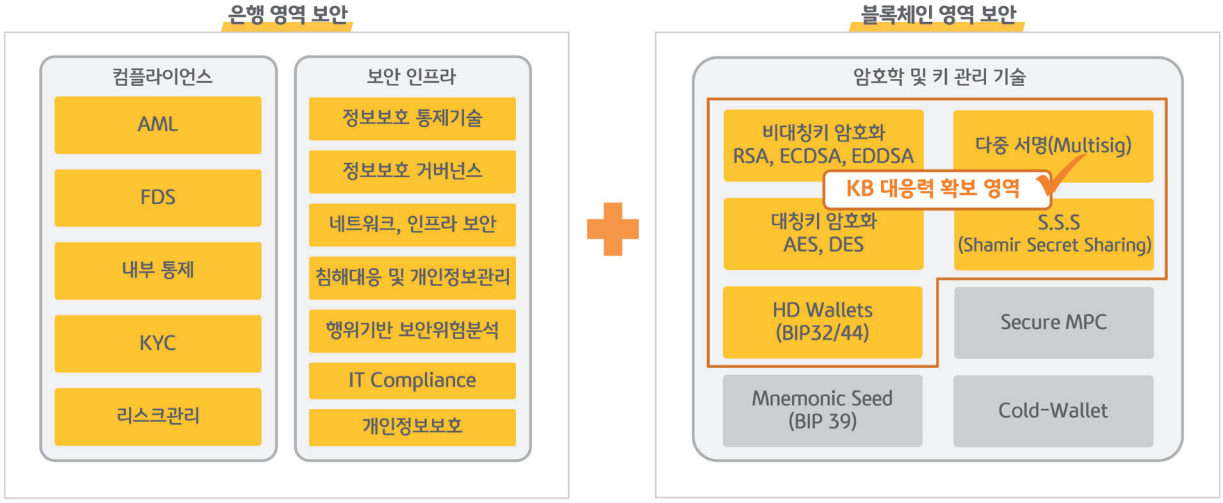
⑥ 강제집행, 청산 요건 충족, 보안성 향상을 위한 키 공동 관리 구조

⑦ 사용자 편의성을 고려한 복구

10

III. 구축내용_ KB 멀티에셋 디지털지갑 보안

은행이 기존에 보유하고 있던 보안 인프라 및 컴플라이언스에 블록체인 영역의 기술을 더해 지갑 보안성 향상

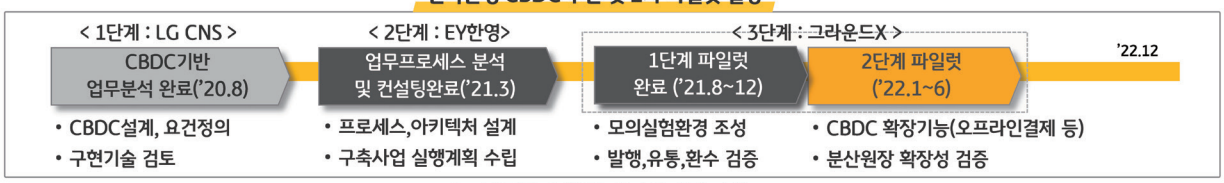


11

IV. 향후계획_ KB 멀티에셋 디지털지갑 고도화 계획

'한국은행 CBDC 2단계 파일럿' 추진 방향성에 맞추어 기술검증 수행 및 신사업 추진 예정

한국은행 CBDC 추진 및 2차 파일럿 일정



KB 기술검증 수행 및 신사업 예정 사항

구분	내용
지갑 기능 고도화	▪ 디지털자산 발행 (NFT, Token 등)
	▪ 디지털자산 거래 (CBDC ↔ NFT 등)
	▪ 키 관리 보안기술 고도화
블록체인 노드 구축 및 운영	▪ 거액결제시스템 노드 참여를 대비한 노드 구축 및 운영기술 확보 ▪ 블록 및 거래 모니터링 시스템 고도화
	▪ 분산원장 확장성 검증 (Layer 2 솔루션 검증, 네트워크 모니터링 및 장애 대응 방안 확보)
신사업 추진	▪ 디지털자산 연계 비즈모델 도출 및 외부 생태계 협업 강화 (Biz 및 보안 영역)

12

한국은행 CBDC 발행에 대응한 멀티에셋 디지털지갑 핵심기술과 정보보호

박형주 KB국민은행 디지털신사업본부장

IV. 향후계획_ KB가 생각하는 미래의 디지털지갑 모습은?

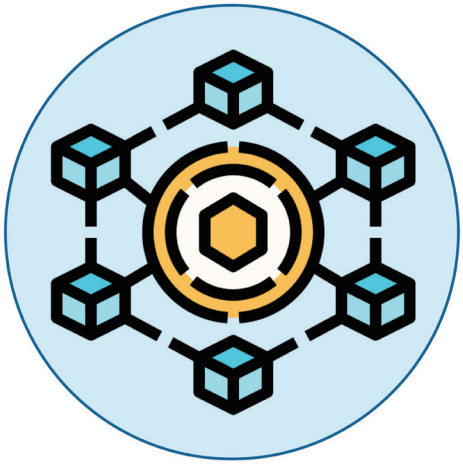
블록체인 비밀키(개인키)에 기반한 자산 및 서비스가 보편화 되어, 금융과 비금융을 아우르는 디지털지갑 구상

KB 멀티에셋 디지털지갑 미래 구상도

13

IV. 향후계획_ 미래의 KB 멀티에셋 디지털지갑 보안

천만고객이 선택한 KB모바일인증서의 보안인프라와
블록체인 보안기술의 융합을 통한 시너지 창출



14

한국은행 CBDC 발행에 대응한 멀티에셋 디지털지갑 핵심기술과 정보보호

박형주 KB국민은행 디지털신사업본부장

End of Document

감사합니다

KB 금융그룹

KB 국민은행

Dong-A 2022 INFOSEC

주제발표 5

디지털자산거래소의 보안 차별화 전략

차종현

두나무 최고정보보호책임자(CISO)

2022 동아 인포섹-정보보호 콘퍼런스

Dong-A InfoSec 2022-Information Security & Privacy Conference

주제발표 5

디지털자산거래소의 보안 차별화 전략

차종현
두나무 최고정보보호책임자(CISO)

키워드	#devsecops
핵심문장	지속적인 보안 활동으로 변화하는 외부 환경 및 위협 대응

주요경력

- 삼성증권 IT감사, 정보보호담당자
- 삼성SDS 삼성증권 주식/선물옵션 매매시스템 개발운영담당자

차종현 두나무 최고정보보호책임자(CISO)

디지털자산거래소의 보안 차별화 전략

두나무

목 차

1. 변화하는 외부 환경과 위협
2. 거래소 환경의 보안 아키텍처
3. 지속적인 보안 활동

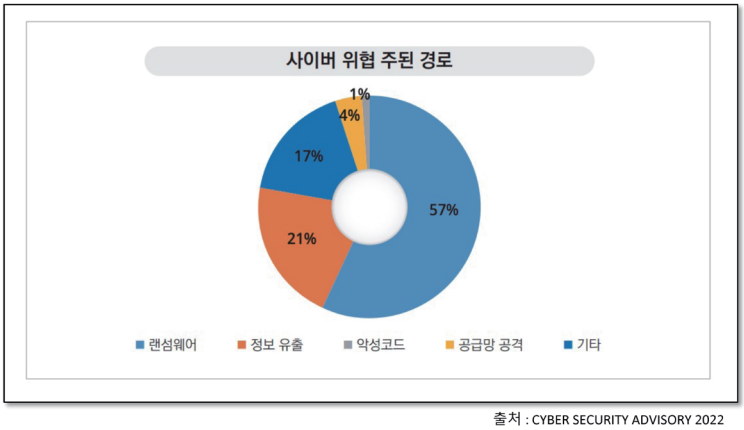
차종현 두나무 최고정보보호책임자(CISO)

변화하는 외부 환경과 위협에 대한 고찰

외부 환경

변화하는
외부 환경
과 위협

- 외부 위협 주요 경로



출처 : CYBER SECURITY ADVISORY 2022

- 랜섬웨어, 정보유출 등 다양한 경로에서 위협이 발생하고 있으며 특히, 지능화된 타겟 공격이 지속적으로 증가하고 있음

차종현 두나무 최고정보보호책임자(CISO)

내부 환경

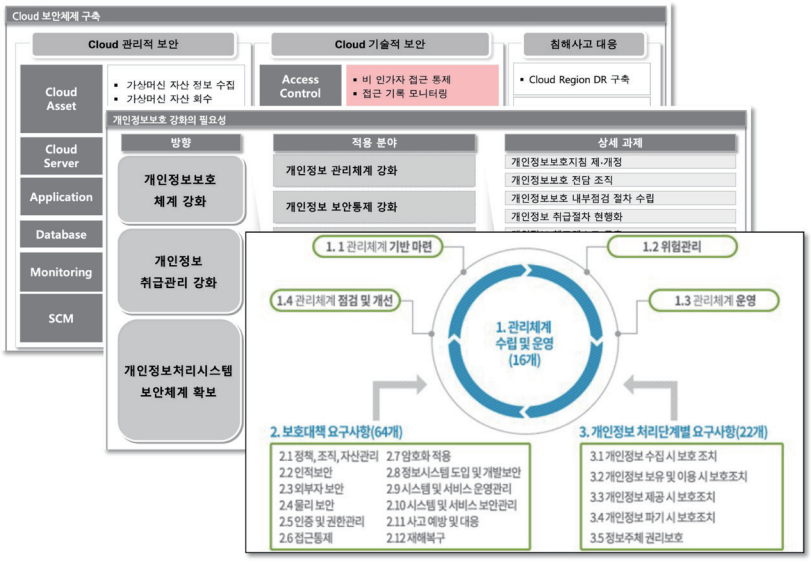
변화하는 외부 환경과 위협

- 빠르게 변화하는 비지니스 환경 대응
  - 사업 추가/변경, 각종 이벤트, 대외 요구사항
- 클라우드 환경 특성을 고려한 보안 구현
- 빈번한 업데이트(개선, 보안패치)
- 원격 재택 업무 환경
  - 사무실 환경과 동일 한 보안 환경 제공

ⓒDunamu

규제 대응

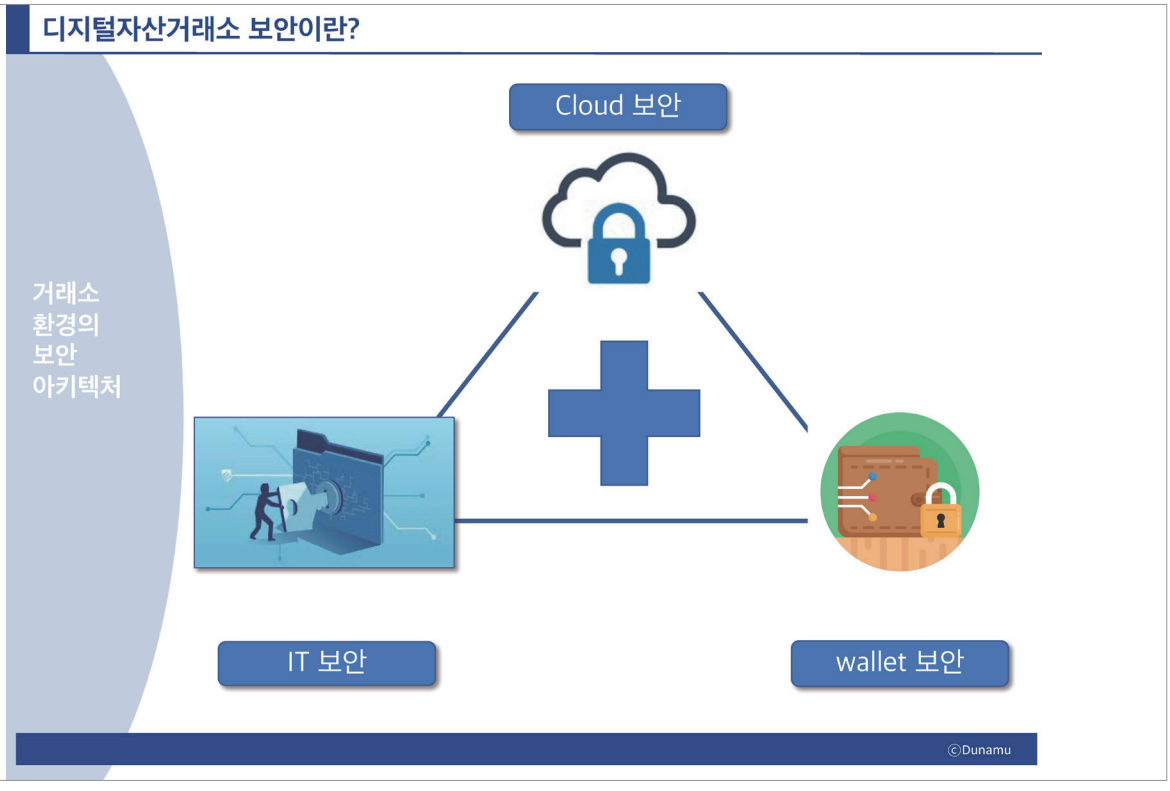
변화하는 외부 환경과 위협



ⓒDunamu

차종현 두나무 최고정보보호책임자(CISO)

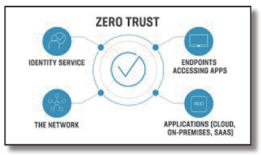
거래소 환경의 보안 아키텍처 선정 및 적용

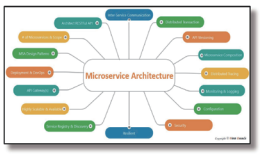


차종현 두나무 최고정보보호책임자(CISO)

차별화 전략

거래소 환경의 보안 아키텍처





제로 트러스트 보안 모델

엄격한 ID 확인 프로세스를 기반으로 하는 네트워크 보안 **모델**
인증되고 권한이 부여된 사용자와 디바이스만 애플리케이션 및 데이터에 접속하도록 허용

MSA 환경 대응

마이크로서비스 보안을 위한 심층 방어메커니즘 적용
컨테이너 기반의 개발환경을 이해하고 소스코드 취약점, 이미지 스캔 등 MSA 환경에 맞는 보안 환경 구성

안전한 원격 근무 환경

언제 어디서든 안전하게 내/외부 시스템에 접근할 수 있는 보안 시스템 구현

MSA(MicroService Architecture) : 마이크로서비스란 작고, 독립적으로 배포 가능한 각각의 기능을 수행하는 서비스로 구성된 프레임워크

클라우드 보안

Cloud 관리적 보안	
Cloud Asset	▪ 가상머신 자산 정보 수집 ▪ 가상머신 자산 회수 ▪ 가상머신 모니터링
Cloud Server	▪ 공개용 서버 보안 ▪ 악성코드 방지 프로그램
Application	▪ 인터페이스 보안 ▪ Software 설치 시 보안
Database	▪ 데이터 이관 시 보안
Monitoring	▪ 이상징후 탐지 ▪ 24시 보안관제
SCM	▪ Secure Coding ▪ 개발과 운영 분리 ▪ 변경관리

Cloud 기술적 보안	
Access Control	▪ 비 인가자 접근 통제 ▪ 접근 기록 모니터링
IAM	▪ 사용자 관리 ▪ 사용자 그룹 역할 정의 ▪ 사용자 패스워드 관리
Authentication	▪ Cloud 접속 시 강화된 인증 ▪ 외부에서 접속 시 추가 인증
Database	▪ 데이터 위.변조 방지 ▪ 데이터 저장소의 무결성 ▪ 데이터 추적성
Network	▪ DDoS 공격으로부터 방어 ▪ 네트워크 보호장비 구축 ▪ 서비스별 네트워크 분리
Encryption	▪ 암호키 Life Cycle 관리

침해사고 대응
▪ Cloud Region DR 구축
▪ 주요정보 타 Region 백업
▪ Cloud 환경의 재해 복구 계획 수립
▪ Cloud 서비스 공급자 보안 인증
▪ Cloud CDN 서비스 운영
▪ Cloud Console 모니터링
▪ Cloud 인증서 관리
▪ Cloud API 통제

"주요 암호화폐거래소의 시스템은 Cloud 기반에서 운영 중이고, Cloud에 맞는 보안 체계 구축이 필요하다."

디지털자산거래소의 보안 차별화 전략

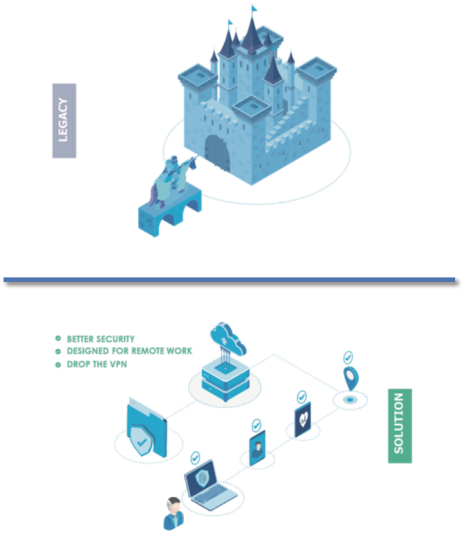
차종현 두나무 최고정보보호책임자(CISO)

인증 / 권한 / 접근제어

거래소 환경의 보안 아키텍처

- 보안 경계에 대한 변화

인증/권한/ 접근제어
(Zero Trust Security)



- 과거의 경계 방어가 아닌 워크플로어에 의한 방어로 전환

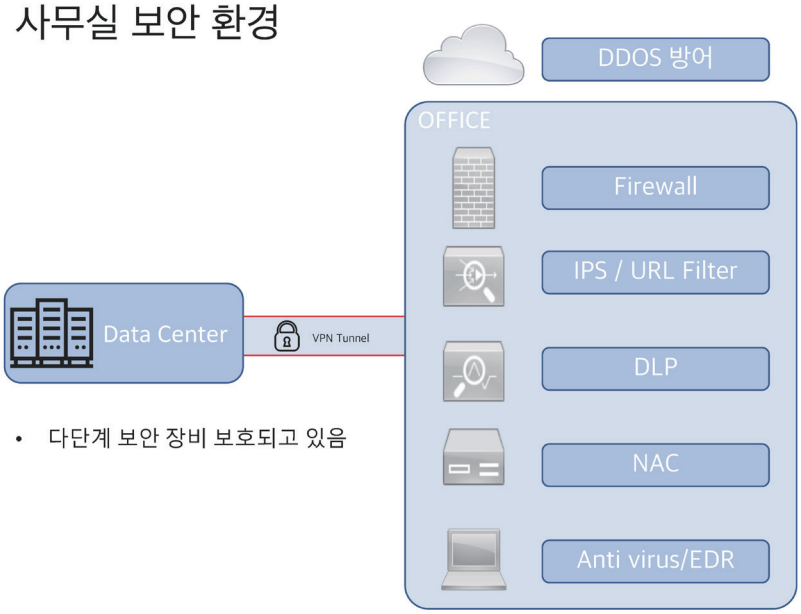
(Zero Trust Security) : 엄격한 ID 확인 프로세스를 기반으로 하는 네트워크 보안 모델

ⓒDunamu

안전한 원격 근무 환경

거래소 환경의 보안 아키텍처

- 사무실 보안 환경



- 다단계 보안 장비 보호되고 있음

ⓒDunamu

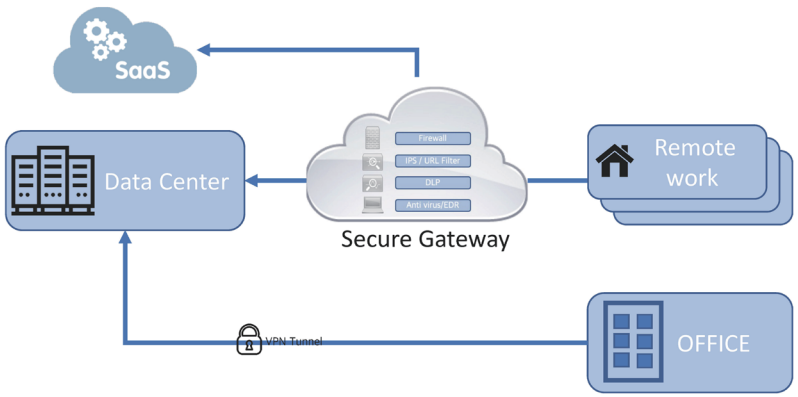
디지털자산거래소의 보안 차별화 전략

차종현 두나무 최고정보보호책임자(CISO)

안전한 원격 근무 환경

거래소 환경의 보안 아키텍처

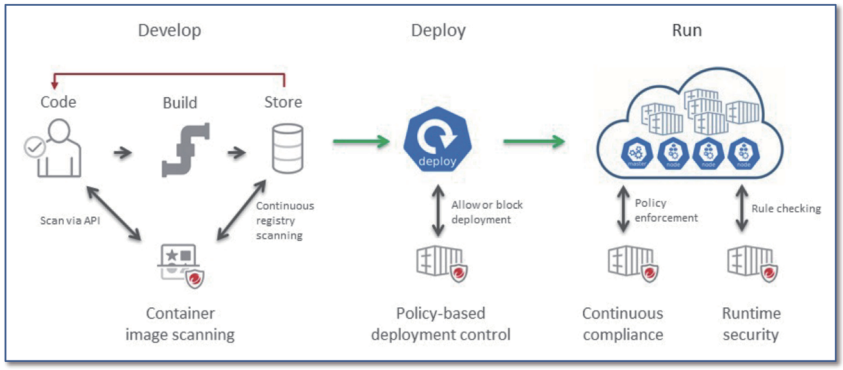
- 원격환경에서도 사무실과 동일한 보안 환경을 제공
  - ✓ 유저가 언제, 어디서 접근해도 암호화된 통신은 Secure Gateway을 통하여 DataCenter와 SaaS서비스에 접근하도록 구현
  - ✓ 외부 유해 네트워크 차단



ⓒDunamu

컨테이너 보안

거래소 환경의 보안 아키텍처



출처 : Trend Micro

- Develop : 소스코드 취약점, 이미지 스캔
- Deploy : 레파지토리 보안, 무결성 보장
- Run : 지속적인 정책 위반사항 점검

- 개발 주기 전체에서, 코드는 보안 문제와 관련하여 검토, 감사, 스캔 및 테스트 진행으로 보안 위협에 대한 지속적인 대응

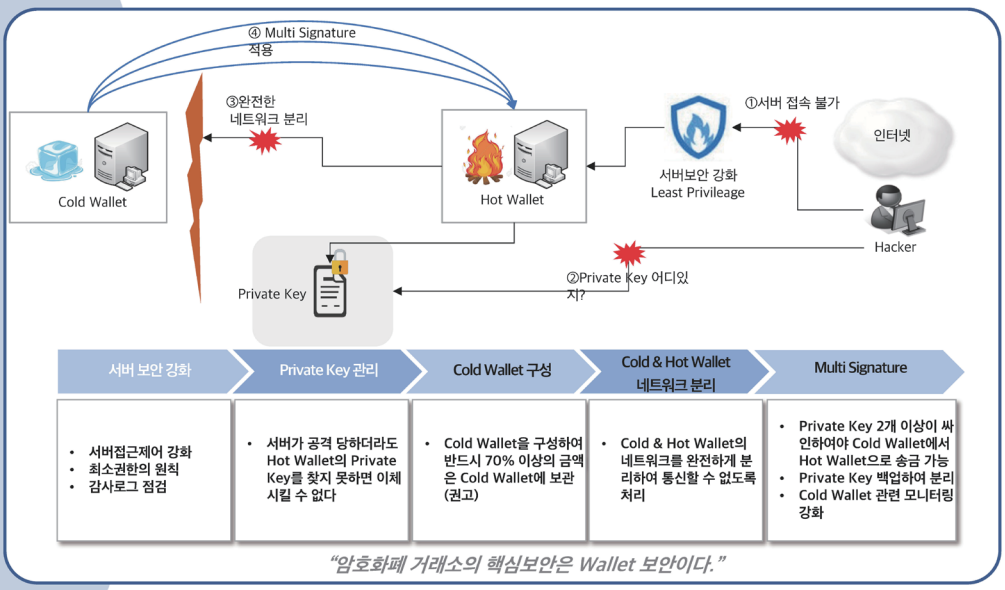
ⓒDunamu

디지털자산거래소의 보안 차별화 전략

차종현 두나무 최고정보보호책임자(CISO)

지갑 보안

• Wallet 보안 5단계



서버 보안 강화	Private Key 관리	Cold Wallet 구성	Cold & Hot Wallet 네트워크 분리	Multi Signature
• 서버접근제어 강화 • 최소권한의 원칙 • 감사로그 점검	• 서버가 공격 당하더라도 Hot Wallet의 Private Key를 찾지 못하면 이체 시킬 수 없다	• Cold Wallet을 구성하여 반드시 70% 이상의 금액은 Cold Wallet에 보관 (권고)	• Cold & Hot Wallet의 네트워크를 완전하게 분리하여 통신할 수 없도록 처리	• Private Key 2개 이상이 싸인하여야 Cold Wallet에서 Hot Wallet으로 송금 가능 • Private Key 백업하여 분리 • Cold Wallet 관련 모니터링 강화

"암호화폐 거래소의 핵심보안은 Wallet 보안이다."

ⓒDunamu

통합 및 자동화를 통한 지속적인 보안 활동

디지털자산거래소의 보안 차별화 전략

차종현 두나무 최고정보보호책임자(CISO)

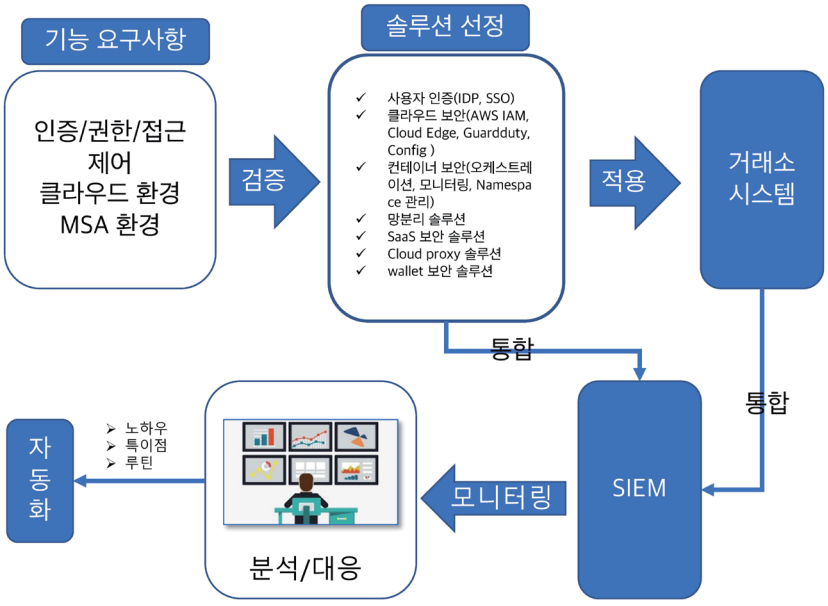
How ?

HOW ?

ⓒDunamu

선정 및 적용

지속적인
보안 활동



ⓒDunamu

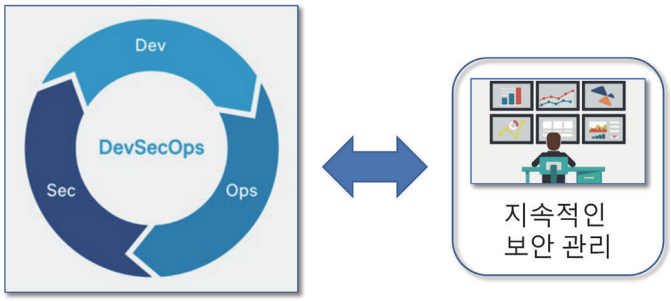
디지털자산거래소의 보안 차별화 전략

차종현 두나무 최고정보보호책임자(CISO)

지속적인 보안 활동

- DevSecOps

지속적인
보안 활동



ⓒDunamu

감사합니다

Dong-A 2022 INFOSEC

주제발표 6

NFT가 불러올 금융 플랫폼의 미래 변화

유태현
신한카드 디지털First본부장(상무)

2022 동아 인포섹-정보보호 콘퍼런스
Dong-A InfoSec 2022-Information Security & Privacy Conference

주제발표 6

NFT가 불러올 금융 플랫폼의 미래 변화

유태현
신한카드 디지털First본부장(상무)

키워드	#NFT #MZ세대 #신한카드 플랫폼 #신한pLay #디지털월렛
핵심문장	MZ세대 Needs 반영과 고객만족을 위한 금융플랫폼(신한pLay 등)의 변화와 혁신

주요경력

- 신한카드 빅데이터팀 부장(2017.01~2017.12)
- 신한카드 경영혁신팀 부장(2013.12~2016.12)

NFT가 불러올 금융 플랫폼의 미래 변화

유태현 신한카드 디지털First본부장(상무)

NFT가 불러올 금융 플랫폼의 미래 변화

- 신한카드 「My NFT」 도입 사례 중심 -

금융권 최초의 NFT 서비스 신한pLay 「My NFT」

2022.1.5日 서비스 공식 런칭 >>>

1호 NFT
(번개장터 전략적 제휴)

신한카드, 금융 플랫폼 최초 NFT 생성·조회서비스 열었다

거래·유통 기능은 차후 구축
카카오 플랫폼 '클레이튼' 기반
글로벌 생태계 확장 가능성 염두

신한카드는 국내 금융 플랫폼 최초로 대체 불가능한 토큰(NFT)을 적용한 'My NFT' 서비스를 시작했다고 4일 밝혔다. 신한카드 고객이라면 누구나 자신이 소장한 물건이나 간직하고 싶은 순간을 NFT로 등록하고 신한플레이(pLay)를 통해 등록한 NFT를 언제든지 조회할 수 있다.

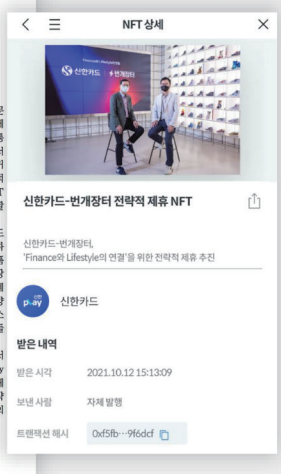
이번 서비스는 국내 금융 플랫폼 중 NFT를 활용한 첫 사례라는 점에서 의미가 있다. 또한 최근 미술, 게임 등 다양한 분야에서 블록체인 기술을 기반으로 거래되는 NFT와는 달리 고객이 신한플레이를 통해 간편하게 NFT를 생성하고, 본인만의 월렛을 통해 보관, 조회할 수 있다. 신한카드의 'My NFT' 서비스는 카카오의 블록체인 플랫폼 '클레이튼'을 기반으로 고객 누구나 카카오톡을 통해 쉽고 편리하게 만들 수 있고, 글로벌 NFT 플랫폼과의 연결과 확장이 가능하다.

신한플레이 'My NFT'

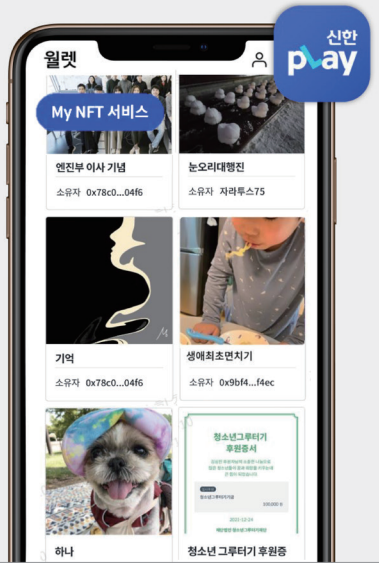
블록체인 전문 기업 '블록오디세이'와 협업을 통해 진행한 이번 서비스는 NFT의 거래·유통 기능은 적용하지 않고 NFT 생성, 조회만 할 수 있다.

향후 신한카드는 NFT를 활용하는 기업과 플랫폼들과의 연결을 통해 생태계를 지속 확장해 나갈 예정이다. 현재 전략적 제휴관계인 번개장터와 스니커즈를 비롯한 다양한 상품의 정품 인증을 위한 NFT 서비스를 구축해나가고 있으며 제조·유통사들과도 플랫폼 연결을 추진할 예정이다.

한편 신한금융그룹은 금융 플랫폼에서 NFT의 활용 가능성을 높게 평가해 'My NFT' 서비스 협력사 '블록오디세이'에 그룹 오리진을 통해 50억원 규모의 전략적 투자를 진행하는 등 그룹 차원에서의 전폭적인 지원도 이어지고 있다.



1개월 만에 2.6만개 발행
가족/반려동물, 기념, 디지털 아트, 증서 등



NFT가 불러올 금융 플랫폼의 미래 변화

유태현 신한카드 디지털First본부장(상무)

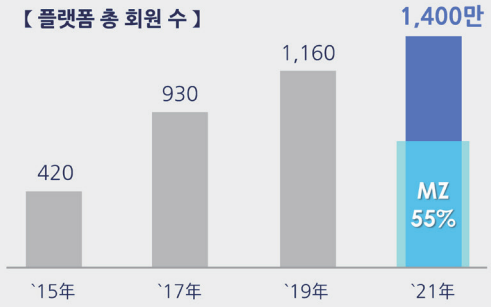
신한카드 금융 플랫폼 신한pLay

신한카드는 서비스 모델 혁신과 디지털 전환에 신한pLay 플랫폼을 적극 활용 中

Pay 플랫폼

- 세계최초 모바일 앱 방식 간편결제 출시
- 금융권 최초 플랫폼 가입자 1,000만 돌파
- 금융권 최초 디지털 월렛 출시

【 플랫폼 총 회원 수 】



신한 pLay *생활 & 금융 종합 플랫폼*
「신한pLay」('21.10月 런칭)

- **혁신금융서비스 금융사 最多 선정**(총 12개)
  - 소비 연계 해외주식 소액투자, 안면인식 결제 等
- **플랫폼을 활용한 디지털 전환**(DT) **확대**

* `21年 디지털 결제 취급액 40조원

NFT 서비스를 담은 디지털 Wallet

MZ 고객 니즈를 반영한 다양한 월렛 서비스에 디지털 자산을 추가

신한pLay 디지털 Wallet 서비스 ('20.11月~)

결제 / 뱅킹 + ID / 멤버십 + 자투리 투자 + NFT 서비스

* 누적 투자액 150억 / 가입자 3만명

NFT가 불러올 금융 플랫폼의 미래 변화

유태현 신한카드 디지털First본부장(상무)

「My NFT」 생활결제 관점으로 NFT를 재해석

고객의 생활결제 관련 유무형 가치를 블록체인 기술로 변환/저장하는 서비스

>>> 디지털 컨텐츠는 물론 실물/경험자산까지 어떠한 가치도 NFT로 표현이 가능

Why NFT? 고객의 NFT 서비스 Needs

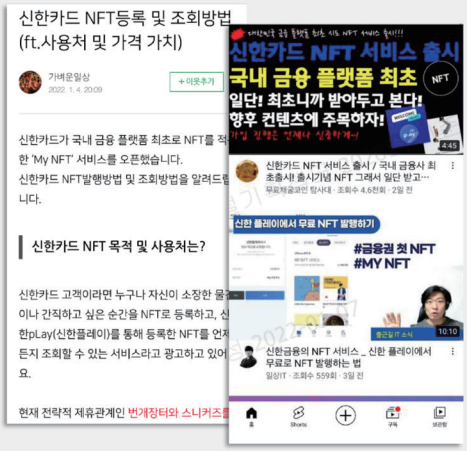
NFT에 대한 호기심 + 금융사 플랫폼 신뢰/접근성 → 뜨거운 시장 반응

▶ 「My NFT」 서비스 실제 이용 고객들의 Needs는..

1. **소유 실물 상품/자산에 대한 가치 증명** (Digital Guarantee)
2. **의미 있는 순간/경험의 안전한 기록** (Digital Archive)
3. **고유 디지털 창작물에 대한 권리 보호** (Digital Stamp)
4. **미래 가치 상승에 대한 잠재 수익 기대** (Digital Gold)

이렇게 다양한 쓰임새의 NFT를..
"믿을 수 있는 금융사 플랫폼에서 손쉽게 발행해볼 수 있어 좋다"

언론 外에도 네이버 / 유투브 等 개인 인플루언서 반응 ↑



〈네이버 블로그〉 〈YouTube〉

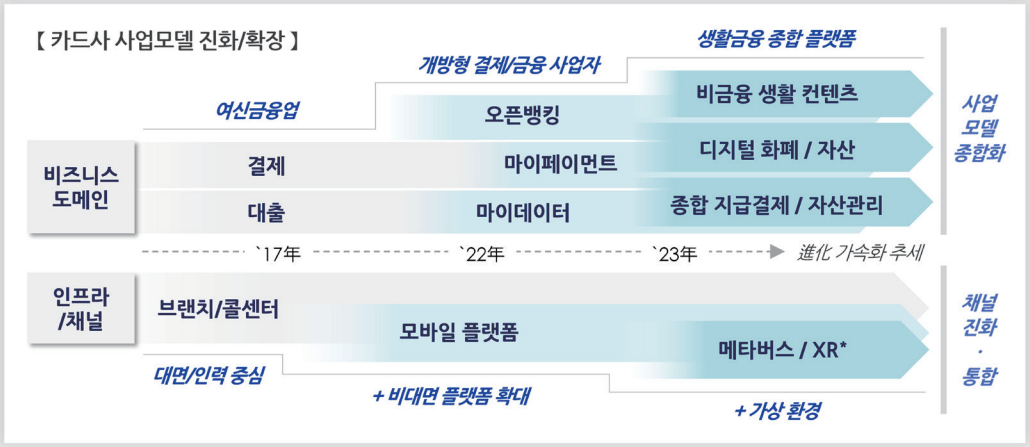
NFT가 불러올 금융 플랫폼의 미래 변화

유태현 신한카드 디지털First본부장(상무)

금융 플랫폼 미래변화 ① 사업 도메인/접점 채널 변화

신한카드의 NFT 서비스 도입은 '금융혁신의 큰 흐름' 안에서 해석

언택 (Platformization) x 언팩 (Big Blur) x 디지털 기술 (DT) x 혁신금융 정책 (Sand Box) x 고객 (Hyper Personalization)



* eXtended Reality (超실감 환경)

금융 플랫폼 미래변화 ② 거래 기반 변화

主거래 통장 → 主이용 플랫폼(디지털 Wallet) 어카운트 경쟁으로 변화

NFT가 불러올 금융 플랫폼의 미래 변화

유태현 신한카드 디지털First본부장(상무)

금융 플랫폼 미래변화 ③ 금융 파트너십 확장

금융 생태계도 디지털 핵심 기술 파트너십 중심으로 빠르게 확장 추세

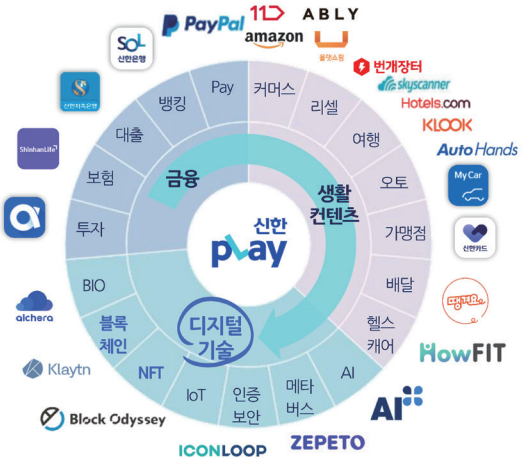
▶ 금융사 중점 파트너십 영역 및 추진 전략

기존
1. 업권外 他 금융 서비스 결합/통합
   → One-stop 금융 모델 추구
2. 고객 소비/생활 연관 異種 업종 제휴
   → 금융↔비금융 서비스 연결/확장

Open API, 블록체인 등 플랫폼 협업기반 확대

변화
3. 4차 산업혁명 미래 디지털 기술 활용
   → 금융 모델/고객경험 파괴적 혁신
   → 디지털 Eco-system 선점/주도

【 참고. 신한카드 플랫폼 제휴 영역 】



Best Practice _ 글로벌 금융사 디지털 자산 활용 사례

Major 금융사/플랫폼 중심 디지털 자산 연결 서비스 모델 활성화 中

VISA

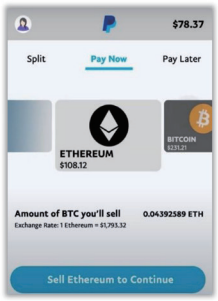
▶ 디지털 자산 기반 결제 / 혜택 제공 카드상품
※ 25개 디지털 화폐 Wallet 제휴 / 서비스 연결 中

주요 제휴사	crypto.com	BlockFi
상품	 크립토 닷컴 선불카드 (`21.3月~)	 블록파이 리워드 신용카드 (`21.7月~)
핵심 서비스	예치금 (CRO코인) 기반 온/오프라인 결제 (결제액 3% 재적립)	VISA 신용 결제 이용 → Bitcoin 리워드 (최대 1.5%)

PayPal

▶ 월렛 內 디지털 자산 연동 및 결제 / 송금

「Checkout with Crypto」 서비스 ('21.3월~, 美)



- 비트코인
- 비트코인캐시
- 라이트코인
- 이더리움

→ 달러화 자동 전환 결제

NFT가 불러올 금융 플랫폼의 미래 변화

유태현 신한카드 디지털First본부장(상무)

미래 금융 서비스 혁신을 위한 제언

블록체인은 높은 수준의 보안 기술, 이를 다루는 기관의 보안 의무/책임이 중요

(신뢰 기술) x (신뢰 기관) = 디지털 금융 모델 혁신

NFT

▶ 現 전문 블록체인 제휴 파트너를 통한 NFT 서비스(발행/조회) 제공 中
→ **금융사 직접 발행 및 거래/유통까지 One-stop 서비스 확장**

디지털 화폐

▶ VISA, PayPal 等 글로벌 금융 플랫폼 도입 사례 벤치마킹
→ **디지털 자산 보관/조회 기능 월렛 추가 및 연동 Pay 모델 국내 도입**
* 국내 디지털 자산 규모 '26년 1,000조 성장 예상 (BCG)

▶ 한국은행 CBDC 도입 검토/파일럿 中
→ **실환경 결제 및 고객 정보보호 Know-how 보유 카드사 사업 참여**
※ 신한카드, KYC/ FDS/AML/HSM/ISMS-P 등 정보보호 체계/노하우 및 결제 관련 특허* 보유
* 블록체인 기반 신용결제, 네트워크 단절시 디바이스간 결제, 고음파 활용 터치결제 等

① **혁신금융 서비스 지정을 통한 Pilot 기회 부여**
② (중장기) **금융사 진입을 위한 관련 제도 마련**

2022 동아 인포섹-정보보호 콘퍼런스

Dong-A InfoSec 2022-Information Security & Privacy Conference

디지털 자산과 금융보안

동아일보 CHANNEL A