블록체인 기술과 보안 고려사항

(보안기술연구팀, 2017.8.17.)

1 개요

□ EU 산하 정보보호기구인 ENISA*는 최근 발표한 보고서[1]를 통해 금융권에서 블록체인 시스템 도입 시 고려해야할 보안 이슈(Cybersecurity challenges)와 보안 강화방안을 제시

> * ENISA(European Union Agency For Network and Information Security) - EU 국가 및 기업과 함께 정보보안 관련 정보 수집/분석 및 컨설팅 등의 역할을 수행하며, 네트워크 및 정보 보안 강화를 위한 보고서 및 권고안 등을 발표

□ 본 보고서에서는 ENISA 보고서의 내용을 중심으로 금융권에서 안전한 블록체인 시스템 도입을 위해 참고 가능한 보안 위협과 이에 대한 대응방안을 제시

2 금융권 블록체인 도입 시 보안위협

□ 금융권에서 블록체인 도입 시 고려가 필요한 보안위협을 **(1) 키 관리, (2) 거래 검증 및 합의, (3) 참여자 권한관리, (4) 블록체인 S/W 보안, (5) 서비스 보안**으로 분류

<금융권 블록체인 도입 시 보안위협 요약>

분류	보안위협	설명
키 관리	① 키 도난 및 분실	공격자에게 키를 도난당하거나 분실된 키가 악용될 경우 자산 및 기밀거래 메시지 유출

1) ENISA,「Distributed Ledger Technology & Cybersecurity : Improving information security in the financial sector」, 2016.12.

	[2] 취약한 키 생성	취약한 키 생성 알고리즘으로 인해 키 재생성 공격이 가능할 경우 자산 및 기밀거래 메시지가 유출 가능
거래 검증 및 합의	[3] 합의 가로채기	참여자 중 과반수(또는 운영주체)를 장악하여 블록체인의 합의 과정을 조작
	[4] 사이드 체인 내 비정상 거래 발생	메인 체인에서 유효하지 않은 자산이 사이드 체인에서 거래 가능
참여자 권한관리	[5] 개인정보 침해	거래정보에 대한 참여자의 접근권한 관리 부족시 개인정보 침해 가능
	[6] 권한 오남용	참여자의 내·외부 권한관리 부족시 금융회사 및 내부직원에 의한 보안사고 등 발생 가능
블록체인 S/W 보안	[7] 블록체인 S/W 취약점	블록체인 S/W에 보안 취약점이 존재할 경우 키 도난, 합의 조작, DDoS 공격 등에 악용가능
	[8] 스마트 컨트랙트 취약점	스마트 컨트랙트에 취약점이 존재할 경우 자산 유출, 개인정보 침해, DDoS 공격 등에 악용가능
서비스 보안	[9] 분산 서비스 거부 공격	다수 참여자가 악성코드 등을 통해 공격자에게 장악될 경우 대량의 스팸거래를 발생 가능하며 이로 인해 블록체인 서비스가 중단 가능
	[10] 가용성 저하	블록체인의 처리속도 한계, 거래정보 급증으로 인해 추가 서비스 개발 및 확대 제한 등의 가용성이 저하
	[11] 비정상거래 탐지 불가	비정상거래에 대한 사전 탐지 및 차단 기술이 부족하여 사기거래, 자금세탁, 이중지불 등의 거래가 발생 가능
	[12] 상호운용성 미제공	블록체인 간 자산교환, 기능 확장 등 연계 필요시 책임주체 및 표준규격이 명확하지 않아 예상치 못한 보안위협 발생 가능

(1) 키 관리

1 키 도난 및 분실

○ 블록체인에서 참여자의 개인키(이하 '키')는 정당한 참여자로서 활동을 승인·증명하는 수단으로 공격자에게 **도난당할 경우 정상 참여자로 위장한 공격자의 다양한 공격에 노출**

○ **(키 도난)** 참여자 단말에 저장된 키가 공격자에게 도난당할 경우 해당 키로 보호되던 자산 및 기밀거래 유출 가능

– 키가 암호화 등 보호기술이 적용되지 않은 원문(plain text)상태로 저장되었거나 서명 등에 사용된 이후에도 메모리에 남아 있는 경우 공격자가 접근 가능

– 자산 거래를 위한 서명과 거래 메시지 암호화에 동일한 키를 사용할 경우 키 유출 시 피해가 확대

○ **(키 분실)** 참여자가 키에 대한 접근권한을 상실*하거나 키를 분실**할 경우 자산 이전이 불가능해질 수 있으며 공격자가 키를 획득하여 악용한 경우에도 확인이 불가

> * 예) 키 사용 시 입력이 요구되는 PIN 번호 등 분실
> ** 예) 키가 보관된 보안토큰(HSM 등), 키가 인쇄된 종이 등 분실

2 취약한 키 생성

○ 블록체인에서 암호 키 생성방식이 안전하지 않을 경우* 공격자는 **키 재생성 공격을 통해 참여자의 키를 획득 가능**

> * 키 생성방식이 안전하지 않다는 것은 키 생성에 사용되는 난수 생성방식의 문제로 공격자가 난수 값(또는 범위)을 추측 가능함을 의미하며 이 경우 무작위 대입 공격을 통한 키 재생성 공격이 가능

– 일반적으로 블록체인 참여자의 키는 가상화폐 지갑 등의 클라이언트 S/W를 통해 생성되는데 **일부 S/W가 안전하지 않은 키 생성방식을 사용하는 것으로 확인**[2)]

○ 또한, 공격자가 양자 컴퓨팅을 활용할 경우 현재 안전한 것으로 간주되는 키 생성방식도 취약해질 수 있으며, 직면한 위협은 아니지만 장기적 관점에서 고려 필요

(2) 거래 검증 및 합의

3 합의 가로채기

○ 일반적으로 **퍼블릭 블록체인*은** 참여자 중 과반수(majority)의 동의로 합의를 도출하므로 **공격자가 과반수를 장악할 경우 거래 유효성 검증** 프로세스를 조작 가능

* 누구나 참여 가능한 블록체인 유형으로 합의를 위해 과반수의 동의가 필요한 작업증명(PoW) 등의 방식을 사용
** 자산의 거래를 요청한 참여자가 자산에 대한 정당한 소유자인지 여부, 해당 자산이 기 사용되지 않은 자산인지 여부 등 검증

○ 비트코인의 경우 공격자가 블록체인 네트워크의 전체 해싱 파워 중 51% 이상을 장악(이하 '51% 공격')하여 다른 모든 채굴자보다 블록을 빨리 생성함으로써 합의 가로채기가 가능

– 51% 공격은 필요인프라 비용으로 인해 현실적으로 불가능하지만 클라우드 컴퓨팅 등을 통해 인프라 확보 비용이 점차 저렴해짐에 따라 공격이 현실화될 가능성 존재

2) Coindesk, Open-Source Tool Identifies Weak Bitcoin Wallet Signatures, October 16th 2014., N. Heninger, How not to generate random numbers, May 13th 2015, University of Pennsylvania.

– 공격자는 51% 공격을 통해 이미 사용한 자산을 재사용하거나 특정 거래를 거부하는 것이 가능

○ 또한, 대부분의 블록체인에 합의 가로채기를 시도한 참여자에 대한 패널티 부과 정책이 존재하지 않아 지속적인 공격 시도가능

○ **프라이빗 블록체인*은** 규제기관 또는 운영위원회 등(이하 '운영주체')의 정책 하에 운영되므로 해당 **운영주체를 장악 및 권한을 도용하는 것만으로도 블록체인 전체를 장악 가능**

* 운영주체에 의하여 검증 및 승인된 주체만 참여가능 한 블록체인 유형

– 이 경우, 블록체인에 취약한 정책 및 S/W를 적용하거나, 운영주체의 합의지분이 높은 경우 합의 가로채기 공격 등이 가능하며 공격가능 범위는 운영주체의 권한 범위에 따라 상이

4 사이드 체인 내 비정상거래 발생

○ 사이드 체인*은 비트코인 등 주요 블록체인(이하 '메인 체인')의 부족한 기능**을 확장하지만 이 과정에서 유효하지 않은 자산의 이전 등 부작용 발생

* 비트코인 등 주요 블록체인(메인 체인)과 상호연계하여 가상화폐 호환성을 제공하거나 스마트 컨트랙트, 거래 기밀성 등의 기능을 추가 제공하는 블록체인 ** 느린 처리속도, 기밀성 및 스마트 컨트랙트 기능 미제공, 참여자 식별불가 등

○ 공격자에 의해 메인 체인에서 **유효하지 않은 자산이 사이드 체인으로 이전되어 정상적으로 거래 가능**

○ 또한, 사이드 체인의 서비스가 중단되면 사이드 체인 상에서 발생했던 대량의 거래를 메인 체인에 반영해야 하는데 이 경우 메인 체인에 높은 부하가 발생 가능

– 사이드 체인이 서비스 중단되면 대체 토큰의 최종 소유자가 보유한 메인 체인 상의 계좌로 소유한 대체 토큰만큼의 자산을 이전하는 등의 사후처리 필요

(3) 참여자 권한관리

5 개인정보 침해

○ **퍼블릭 블록체인**의 참여자는 누구나 본인이 직접 참여하지 않은 거래의 정보를 포함하여 **모든 거래이력을 다운로드 및 조사할 수 있어 개인정보 침해가 발생 가능**

– **프라이빗 블록체인**은 일반적으로 거래정보의 기밀성 보장이 가능*하나 **참여자 권한관리 미흡 등으로 개인정보 침해가 발생 가능**

> * 프라이빗 블록체인 구성이 가능한 Hyperledger fabric, R3 Corda는 거래 기밀성을 보장 가능하도록 각각 Channel, Notary service 기능을 제공

○ 또한, 일반적으로 블록체인은 기 등록된 거래정보에 대한 삭제 기능이 제공되지 않아 '잊혀질 권리'의 보장이 불가

– 기 등록된 거래정보를 삭제 가능한 경우에도 모든 참여자가 동일한 거래정보를 보관하고 있어 완전히 삭제되었음을 보장하기 어려움

○ 블록체인 참여자뿐만 아니라, 스마트 컨트랙트도 개인정보를 처리(조회, 추가, 삭제 등)할 수 있어 **스마트 컨트랙트에 의한 개인정보 침해가 발생 가능**

6 권한 오남용

○ 블록체인은 분산 구조로 인해 참여자 권한관리 등 **거버넌스 통제가 모든 참여자에게 일관성 있게 적용됨을 보장하기 어려움**

– 금융회사별로 특정 기관과의 거래만 허용 및 특정 서비스만 제공할 수 있도록 제한하거나, 거래 종류별로 내부직원의 서명 및 승인 권한을 분리하는 등 통제가 필요하지만,

– 이러한 통제가 일관되지 않을 경우 금융회사 및 내부직원의 **권한 오남용으로 인한 보안사고 발생 가능**

(4) 블록체인 S/W 보안

7 블록체인 S/W 취약점

○ 주요 블록체인 S/W*는 다수 전문가에게 검토되어 비교적 보안성이 높으나 **알려지지 않은 취약점이 존재 가능****

* 블록체인의 거래요청 및 유효성 검증, 합의, 네트워크, 스마트 컨트랙트 등 관련 기능을 제공하기 위한 모든 S/W(플랫폼, 응용프로그램, 라이브러리 등)
** 블록체인 S/W는 일반적으로 오픈 S/W로서 전문가의 검토를 거쳤으나, 최근 유명 오픈 S/W에서 배포된 후 약10~25년 만에 취약점이 발견[3]된 만큼 블록체인 S/W에도 잠재적인 취약점 존재 가능

– 이러한 보안 취약점이 악용될 경우 키 유출, 거래 유효성 조작, 개인정보 침해 등 다양한 보안위협에 노출가능

○ 블록체인 S/W에 취약점이 존재한다는 것은 모든 참여자에게 동일한 취약점이 존재함을 의미하며, 분산 구조로 인해 **보안 패치가 모든 참여자에게 적용되었음을 보장하기 어려움**

3) Bash Shell, OpenSSL, GNU C Library가 배포된 후 약 10~25년 만에 Shellshock, Freak, Ghost 취약점이 발견(참고 - 금융보안원, 오픈소스 SW 사용 위협 및 대응 방안, 전자금융과 금융보안 제3호, 2016.1.)

8 스마트 컨트랙트 취약점

○ 스마트 컨트랙트는 블록체인에서 실행되는 프로그램이므로 다른 S/W와 같이 **코드에 결함이 존재할 수 있으며 계약이 복잡할수록 오류 발생 가능성이 높음***

* 현재 대부분 블록체인에서 스마트 컨트랙트 코드의 보안 수준은 개발자의 능력에 의존하며 별도의 보안성 검증 절차 및 기능은 존재하지 않음

– 스마트 컨트랙트에 존재하는 보안 취약점이 공격자에게 악용될 경우 계약 조건에 어긋난 비정상적인 코드 실행으로 자산의 손실 및 개인정보 침해가 발생 가능

○ '16.5월 발표된 보고서[4]에 따르면 인터넷에 공개되어 있는 이더리움 스마트 컨트랙트 템플릿 코드 중 상당수에 심각한 취약점이 존재

– 실제로 '16.6월 발생한 이더리움 DAO[5] 사건의 경우 스마트 컨트랙트 코드에 존재했던 취약점으로 인해 5,900만 달러가 공격자에게 이체됨

○ 또한, 공격자는 **스마트 컨트랙트 기능을 악용하여 악성코드 등 악의적인 코드를 블록체인에 저장 및 실행 가능**

– 익명성이 보장되는 블록체인의 경우 블록체인 상에서 악성 코드 판매/구매를 위한 거래도 처리 가능

(5) 서비스 보안

9 분산 서비스 거부(DDoS) 공격

○ 공격자는 블록체인의 분산된 노드를 통해 네트워크에 대량의

4) P. Vessenes, Ethereum Contracts are Going to be Candy for Hackers, May 2016.
5) 이더리움의 스마트 계약 기능을 활용한 탈중앙화된 투자 플랫폼

스팸거래를 발생시킴으로써 **거래 유효성 검사 시간을 지연시켜 블록체인 전체에 대한 서비스 거부 공격을 수행**

– 실제로 '16.3월 비트코인은 평균보다 높은 수수료를 제시*한 대량의 스팸거래로 인해 서비스가 거의 중단되었으며,

> * 채굴자는 블록생성 시 더 많은 수수료를 받기 위해 수수료가 높은 거래를 우선 포함시키며 이로 인해 평균적인 수수료를 제시한 거래는 블록에 포함되지 못하여 정상 거래에 대한 서비스 거부 현상이 발생

– 이후 비트코인의 채굴자는 비정상적으로 높은 수수료를 제시하는 거래 등 블록생성 시 의심되는 거래에 대한 우선순위를 낮춰 유사한 공격에 대응

○ DDoS 공격을 위한 스팸거래 요청은 악성코드에 감염된 참여자에 의해 발생될 수 있으며 분산 구조로 인해 **전체 참여자에 대한 악성코드 감염여부 확인 등 대응이 어려움**

○ 프라이빗 블록체인의 경우 의심 거래를 발생시키는 참여자를 네트워크에서 차단하는 등의 조치가 가능하지만 공격자가 많은 수의 노드를 장악할 경우 여전히 DDoS 공격이 가능

10 가용성 저하

○ 블록체인 이용자 등 참여자가 급증하고 시간이 지나면서 거래량이 증가 및 누적됨에 따라 **거래 처리속도의 한계와 거래정보 관리에 대한 부담이 증가하여 가용성이 저하**

– 일반적으로 금융회사는 풀(full) 노드*로서 블록체인의 전체 거래정보를 모두 보관하는데 전체 거래정보량의 급격한 증가[6]에 따라 추가 서비스 확대가 제한

6) 비트코인의 경우 최근 4년(2012년 7월 ~ 2016년 7월)간 450% 증가

* 전체 거래이력을 보관하며 거래 유효성 검증, 합의 등 블록체인 참여자로서의 모든 기능을 수행하는 노드

– 일반적으로 거래 유효성 확인은 모든 참여자가 수행하므로 참여자 수가 증가할수록 거래 처리속도가 저하*되며 이로 인해 높은 처리성능이 요구되는 서비스 개발이 제한

* 참여자 간 처리성능이 일관되지 않을 경우 처리시간은 더 증가

11 비정상거래 탐지 불가

○ 퍼블릭 블록체인은 익명성으로 인해 거래 참여자 식별이 불가능하여 **사기거래, 자금세탁 및 테러자금 조달을 위한 거래 등 비정상거래에 대한 탐지가 어려움**

– 비정상거래가 발생한 이후 이에 사용된 계좌의 소유자를 식별* 및 추적하는 것은 가능하지만 비정상거래 시도를 사전에 차단하는 것은 어려움

* 거래소 등에서 가상화폐를 기존통화로 교환 시 가상화폐 계좌의 소유자를 식별가능

○ 또한, 금융사기 및 고객 실수로 인한 비정상거래라 할지라도 **거래의 유효성만 검증되면 정상거래로 처리되며 이후 거래 취소, 강제이체 등의 대응이 어려움**

– 프라이빗 블록체인은 이러한 비정상거래에 대한 대응이 가능하지만 참여자 간 합의 등 절차 필요

○ 이외에도 다음과 같은 비정상거래 유형이 존재

– (이중지불) 자산에 대한 거래가 확정되기 전에 대가를 제공받고 거래를 취소하거나 자산을 재사용하는 공격

– (유출된 키 서명) 공격자 의해 유출된 정상 참여자의 키로 서명된 거래

– (정책 미준수 거래) 기 수립된 서비스 정책에 어긋난 거래로서 프라이빗 블록체인에서 참여자가 허가 받지 않은 서비스에 대하여 거래를 요청한 경우 등이 해당

⑫ **상호운용성 미제공**

○ 블록체인 간 자산이전, 기능 확장, 연계 서비스 개발 시 블록체인 간 호환성이 요구되나 **상호운용성이 제공되지 않아 예상치 못한 보안위협이 발생가능**

– 블록체인 간 연계 및 상호운용을 위해서는 블록체인 간 자산 교환에 대한 책임주체와 비정상 거래가 타 블록체인에 확산될 경우 대책 등에 대한 고려 필요

○ 또한, 현재는 블록체인별로 서로 다른 지갑 S/W를 사용하여 키 생성 알고리즘, 거래요청 및 통신 프로토콜 등이 호환되지 않으므로 표준 지갑규격 개발 등에 대한 고려 필요

3 보안 대응방안

□ 금융권에서 블록체인 도입 시 고려가 필요한 보안위협에 대한 대응방안을 제시

(1) 키 관리

① **(키 도난 및 분실)** 공격자에 의해 키가 유출되지 않도록 키를 안전하게 보관하고 키 도난 및 분실에 대응

○ (관련 가이드 준수) 신뢰 가능한 기관에서 발간한 안전한 키 저장 및 보관에 대한 최신 보안 가이드 준수

○ (키 분실 및 도난 대응) 키를 분실하여 자산을 거래하지 못하거나 도난당한 키가 공격자에 의해 악용되는 것을 방지하기 위해 다음과 같은 정책 및 기술을 적용

– (키 복구) 키를 분실한 경우 정상적인 자산 거래가 가능하도록 키 복구 기능*을 적용하고 복구 시 추가 인증절차** 마련

* 예로, 신뢰된 기관에서 분실된 키를 복구 ** 키 복구 시 정상 참여자임을 인증하는 절차를 제공

– (다중 서명) 거래 서명에 다중 서명기술(multi signature)*을 적용하여 공격자가 거래 서명에 필요한 모든 키를 획득하지 않는 한 불법 거래를 시도하지 못하도록 대응

* 복수의 키로 서명해야만 거래요청이 가능하며 키는 자산의 소유자와 제3의 기관 등이 관리

– (용도별 키 할당) 업무 및 용도(거래 서명, 거래 메시지 암·복호화 등)별로 키를 구분하여 사용함으로써 키 유출로 인한 피해를 해당 키가 사용되던 업무로 제한

– (암호화 및 사용 후 즉시 삭제) 서명키가 원문 상태로 저장되지 않도록 파일 저장 시 암호화하거나 키 사용 후 메모리에서 즉시 삭제하는 등의 보호기술 적용

2 **(취약한 키 생성)** 공격자가 키를 재생성하지 못하도록 키를 안전한 방식으로 생성 및 검증

○ (안전한 키 생성) 신뢰 가능한 기관에서 발간한 안전한 키 생성에 대한 최신 보안 가이드[7] 준수

○ (안전성 검증) 검증기관으로부터 키 생성 알고리즘 등을 확인받고 키의 안전성을 검증

(2) 거래 검증 및 합의

3 **(합의 가로채기)** 내·외부 공격자에게 장악된 노드로 인해 거래 유효성이 조작되지 않도록 모니터링 및 차단

○ (비정상 참여자 모니터링) 블록체인 내에서 과반수 합의를 장악하기 위해 비정상 행위를 수행하는 참여자 모니터링

– 예로, 비트코인에서 51% 공격을 수행하기 위해 과도하게 처리 성능을 높이거나 많은 수의 거래를 처리(거래검증 및 블록생성)하는 노드가 있는지 모니터링

○ (수수료 부과 및 거래 처리량 제한) 거래에 수수료를 부과하여 많은 참여자가 거래검증에 참여하도록 유도*하고 특정 노드가 대량의 거래를 처리하기 어렵도록 거래 처리량을 제한

* 다수의 정상 참여자가 거래 수수료를 획득하기 위해 거래 유효성 검증 등 합의에 참여함으로써 공격자가 과반수 합의를 장악하기 어려워짐

○ (참여자 검증) 프라이빗 블록체인의 경우 참여자의 보안수준이 일관성 있게 유지되도록 신규 참여자에 대한 보안성 검증 기준을 강화·마련하고 지속적으로 관리

4 **(사이드 체인 내 비정상거래 발생)** 메인 체인의 유효하지 않은 자산이 사이드 체인으로 이전되어 정상 거래되는 것을 차단

○ (합의 통합) 두 체인의 거래검증 및 블록생성 등 합의과정을 통합하여 메인 체인의 자산이 유효하지 않을 경우 사이드 체인에서 거래가 불가하도록 차단

7) Smart, N., et al. "Algorithms, key size and parameters report.", ENISA (2014). 등 참고

(3) 참여자 권한관리

5 **(개인정보 침해)** 블록체인에서 개인정보 침해가 발생하지 않도록 거래와 무관한 제3자의 접근을 통제

○ (채널 구성) 기밀거래는 전체 노드가 아닌 일부 검증노드와 별도 채널을 구성하여 거래 유효성을 검증함으로써 거래정보 유출을 최소화

○ (거래정보 삭제) 거래정보 보관기간에 대한 규정을 수립하고 기간 경과 후에는 거래 무결성 확인에 필요한 정보만 남기고 개인정보 침해가 우려되는 세부 거래정보는 삭제

– 세부 거래정보는 일부 풀 노드가 보관하고 거래 유효성은 풀 노드를 통해 확인

○ (참여자 식별 및 접근통제) 참여자를 식별 가능한 경우 운영주체가 인증서 등 참여자 식별정보를 관리하고 이를 기반으로 거래정보에 대한 접근을 통제

○ (거래 암호화) 거래정보를 암호화하여 거래 당사자 등 권한을 가진 참여자만 거래에 접근할 수 있도록 통제하며 필요시 복수 키로 암호화하여 통제를 강화

6 **(권한 오남용)** 금융회사 및 내부직원이 허가되지 않은 거래 및 서비스에 참여하는 것을 차단

○ (스마트 컨트랙트 기반 통제) 참여자의 거래 및 서비스 참여에 대한 통제규칙을 스마트 컨트랙트로 프로그램화하여 적용

○ (내부직원 통제) 거래에 대한 내부직원의 서명을 식별 및 통제 가능하도록 내부 거버넌스 통제 절차를 수립

(4) 블록체인 S/W 보안

7 **(블록체인 S/W 취약점)** 블록체인 S/W에 존재할 수 있는 보안 취약점을 악용한 해킹공격 차단

○ (코드 검토) 블록체인 플랫폼 및 응용프로그램, 관련 라이브러리 등의 블록체인 S/W 개발 시 취약점 제거를 위하여 자체 또는 제3의 기관을 통해 코드 검토 수행

○ (보안 테스트) 블록체인 S/W에 대해 공격자의 입장에서 모의 침투 테스트를 수행하여 개발 시 발견 못했던 취약점을 탐지 및 제거

○ (안전한 개발 방법론) 소프트웨어 개발 생명주기를 기반으로 블록체인 S/W를 체계적으로 개발하고 안전한 S/W 개발을 위해 개발 단계별로 요구되는 보안강화 활동*을 수행

> * 보안 요구사항 도출, 시큐어 코딩, 코드검토(정적 테스팅), 보안 테스팅 (동적 테스팅, 침투 테스팅 등) 등

8 **(스마트 컨트랙트 취약점)** 스마트 컨트랙트 코드에 존재할 수 있는 보안 취약점을 악용한 비정상거래 등 악성행위를 차단

○ (코드 검토 및 악성코드 탐지) 스마트 컨트랙트 배포 이전에 코드 검토를 통해 보안 취약점 존재 여부와 악성코드 감염 여부를 확인

○ (검증된 코드 사용) 데이터 읽기·쓰기와 같이 일반적으로 사용되는 함수는 표준 라이브러리로 개발하여 배포 및 사용하거나 보안성이 검증된 스마트 컨트랙트 코드를 사용

(5) 서비스 보안

9 **(분산 서비스 거부 공격)** 대량 스팸거래 요청 등의 DDoS 공격으로 인해 블록체인 서비스가 중단되지 않도록 대응

○ (스팸거래 차단) 유효성 검사 시간을 지연시킬 목적으로 요청되는 스팸거래(예 : 높은 거래 수수료를 제시한 거래) 요청을 차단

* 거래 수수료를 부과하지 않을 경우 공격자가 대량의 스팸거래를 제한 없이 요청 가능하므로 적정 수준의 수수료 부과 필요

○ (거래요청 건수 제한) 공격자가 대량의 스팸거래를 요청하지 못하도록 참여자별 거래요청 건수를 제한

○ (거래 허용 참여자 관리) IP주소, 인증서 등을 기반으로 거래 요청이 허가된 참여자 목록(white list)을 관리

10 **(가용성 저하)** 거래 처리속도 저하와 전체 거래정보의 크기 증가 등으로 인한 가용성 저하 문제를 개선

○ (유효성 검증 참여자 제한) 거래 유효성 검증을 전체 참여자가 아닌 신뢰 가능한 일부 검증노드와 수행하여 유효성 검증에 참여하는 노드의 수를 줄임으로써 처리속도를 개선

– 다만, 일부 검증노드만으로 거래 유효성을 검증함에 따라 잘못된 검증으로 인해 유효하지 않은 거래가 정상처리 가능

○ (선택적인 거래정보 저장) 일반 노드는 거래 해시정보가 포함된 블록헤더만 보관하고 세부 거래정보는 풀 노드를 통해 확인함으로써 일반 노드의 거래정보 관리 부담을 완화

– 다만, 공격자가 풀 노드로 참여하여 일반 노드에게 조작된 거래정보를 정상 거래정보로 속여 자산을 재사용하는 등의 악의적인 비정상 거래가 가능

⑪ **(비정상거래탐지 불가)** 블록체인에서는 자금세탁거래 등 비정상 거래가 발생하더라도 거래 취소 등의 대응이 어려우므로 사전에 탐지 및 차단

○ (거래 허용 참여자 관리) 신뢰 가능한 기관에서 제공하는 거래 허용 참여자 목록을 활용하여 비인가자에 의한 자금세탁거래 등으로 의심되는 거래를 차단

> * EU 집행위원회는 거래소 등 블록체인의 게이트웨이 역할을 수행할 주체에게 적용할 PKI 기반의 자금세탁방지 기술을 연구 중

⑫ **(상호운용성 미제공)** 블록체인 간의 신뢰 가능한 자산이전 기술 및 표준규격을 개발하여 안전한 서비스 연계가 가능하도록 상호운용성 제공

○ (Pegged 사이드 체인) 중계자 없이 블록체인 간 자산을 교환하기 위한 기술인 Pegged 사이드 체인 기술*을 활용하여 자산 이전 시 신뢰성을 제공

> * 예를 들어, 메인 체인에서 사이드 체인으로 자산을 이전하는 경우 메인 체인의 자산을 특정 계좌로 이체하여 동결(lock)하고 이에 해당하는 대체(proxy) 토큰을 사이드 체인에서 발급하는 방식

○ (표준규격 개발) 블록체인 간 연계에 필요한 데이터 형식, 통신 프로토콜, 자산이전 절차, 키 생성·관리 등에 대한 표준 개발

4 향후 과제

□ **(추가 보안 고려사항 검토)** 블록체인 서비스 개발 및 보안기능 추가에 따라 발생 가능한 보안위협 등 고려사항을 지속적으로 검토

○ 예로, 가용성 저하에 대한 대응방안으로, ‘유효성 검증 참여자 제한’이나 ‘선택적인 거래정보 저장’을 적용할 경우 추가적인 보안위협이 발생가능

□ **(최신 연구동향 검토)** 블록체인의 보안위협에 대한 대응방안 등 관련 보안기술에 대한 신규 개발 및 개선이 계속될 것으로 예상되므로 최신 보안기술 연구동향을 지속 검토할 필요

○ (양자 컴퓨팅) 향후 양자 컴퓨팅 기술의 실용화에 대비하여 양자 컴퓨팅에도 안전한 키 생성기술 및 관련 동향에 대해 검토 필요

○ (거래정보 삭제 기술) 블록체인에 등록된 거래정보는 수정·삭제가 불가하여 금융권 도입 시 보관기한이 만료된 개인정보의 삭제, 비정상거래의 취소 등 대응이 어려우나 최근 거래정보에 대한 수정·삭제 기술 연구[8]가 진행 중이므로 검토 필요

○ (보안 표준) 블록체인 서비스 제공 및 블록체인 간 연계 시 안전성 제공을 위해 다양한 보안 표준이 개발될 것으로 예상되므로 관련 표준화 현황을 지속 검토 및 개발에 적극 참여

□ **(평가기준 마련)** 제시한 보안 위협 및 대응방안을 기반으로 금융권 블록체인 시스템에 대한 평가항목을 도출하고 제공될 서비스의 중요성 등을 고려하여 세부 평가기준을 개발

8) Redactable Blockchain – or – Rewriting History in Bitcoin and Friends (IEEE European Symposium on Security and Privacy 2017) 등