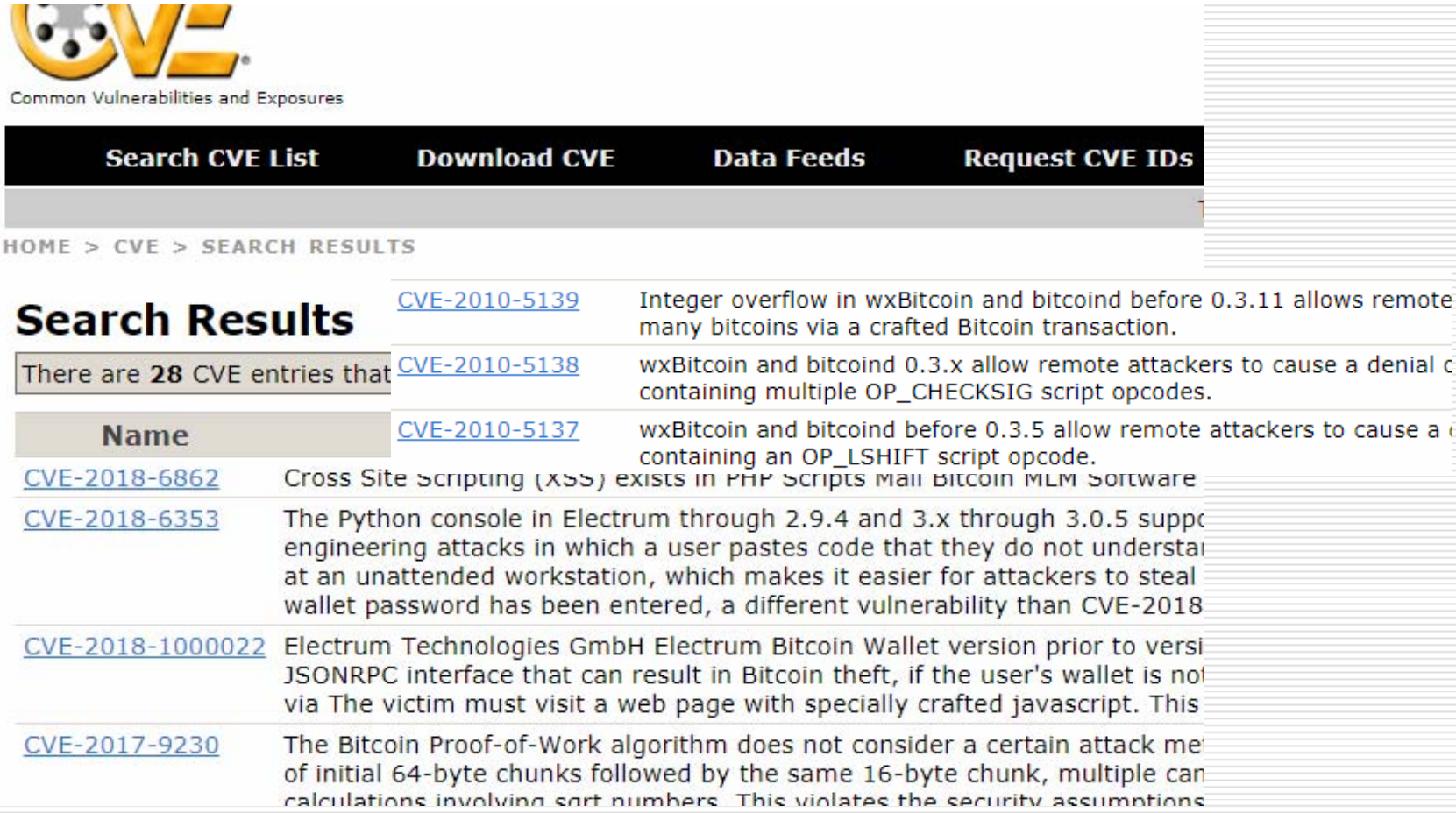

보안측면에서 본
블록체인 구현 과제
2018. 4. 26.


Ⅰ. 블록체인과 보안
Ⅱ. 보안 구현 과제
Ⅲ. 결론과 질의응답

비트코인 취약점



Common Vulnerabilities and Exposures

Search CVE List | Download CVE | Data Feeds | Request CVE IDs

HOME > CVE > SEARCH RESULTS

Search Results

There are **28** CVE entries that

Name	
CVE-2018-6862	Cross Site Scripting (XSS) exists in PHP Scripts Mall Bitcoin MLM Software
CVE-2018-6353	The Python console in Electrum through 2.9.4 and 3.x through 3.0.5 suppo engineering attacks in which a user pastes code that they do not understa at an unattended workstation, which makes it easier for attackers to steal wallet password has been entered, a different vulnerability than CVE-2018
CVE-2018-1000022	Electrum Technologies GmbH Electrum Bitcoin Wallet version prior to versi JSONRPC interface that can result in Bitcoin theft, if the user's wallet is no via The victim must visit a web page with specially crafted javascript. This
CVE-2017-9230	The Bitcoin Proof-of-Work algorithm does not consider a certain attack me of initial 64-byte chunks followed by the same 16-byte chunk, multiple can calculations involving sqrt numbers. This violates the security assumptions
CVE-2010-5139	Integer overflow in wxBitcoin and bitcoind before 0.3.11 allows remote many bitcoins via a crafted Bitcoin transaction.
CVE-2010-5138	wxBitcoin and bitcoind 0.3.x allow remote attackers to cause a denial c containing multiple OP_CHECKSIG script opcodes.
CVE-2010-5137	wxBitcoin and bitcoind before 0.3.5 allow remote attackers to cause a containing an OP_LSHIFT script opcode.

블록체인과 보안

'백도어 이슈' 중국서 **해킹 불가** '**블록체인** 스마트폰' 만든다니...
조선비즈 | 2018.03.27. | 네이버뉴스
하지만 타사의 아이디어를 도용하거나 백도어(기기 사용자 주인의 허락없이 개인 정보가 빠져나가는 것) 같은 **해킹** 이슈로 유명한 중국에서 **해킹**이 **불가**능한 **블록체인** 기술을 내놓는 게 의아하다는 지적도 나온다. 26일...

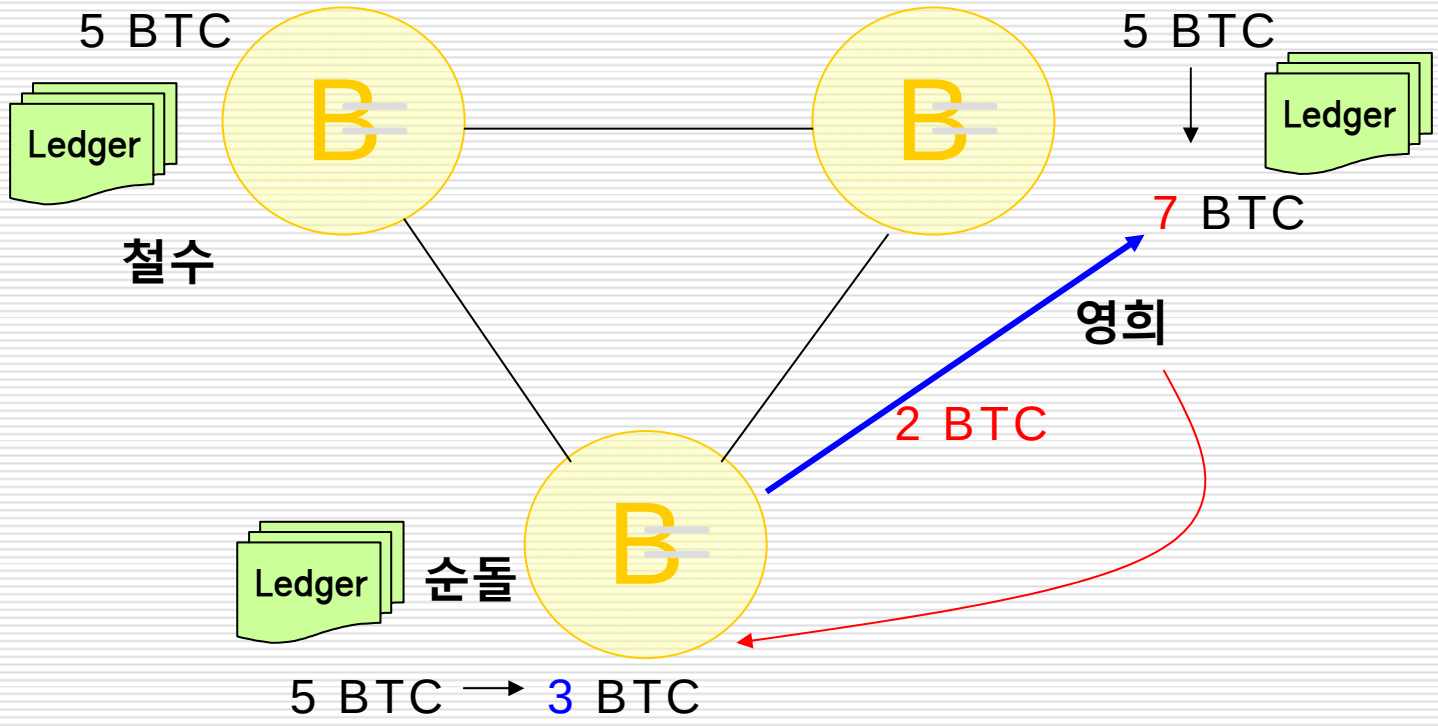
[NES 2018] "**블록체인**도 **해킹** 무풍지대 아니다…보안정[illegible]
디지털데일리 PICK | 2018.04.13. | 네이버뉴스
때문에, **블록체인**을 활용한다고 **해킹**과 위변조가 [illegible]
<최민지 기자>cmj@ddaily.co.kr [제13회] 'NES[illegible] 시회 컨퍼런스에 여러분을 초대합니다. 독자 여러분...

기획) **블록체인** 4차 산업혁명의 핵심 인프[illegible]
사실상 **해킹** 및 위변조가 **불가**한 **블록체인**[illegible] 움직임은 전 세계적으로 일어나고 있다. 세계 최[illegible] Trust & Clearing Corporation)는 2017년 1월

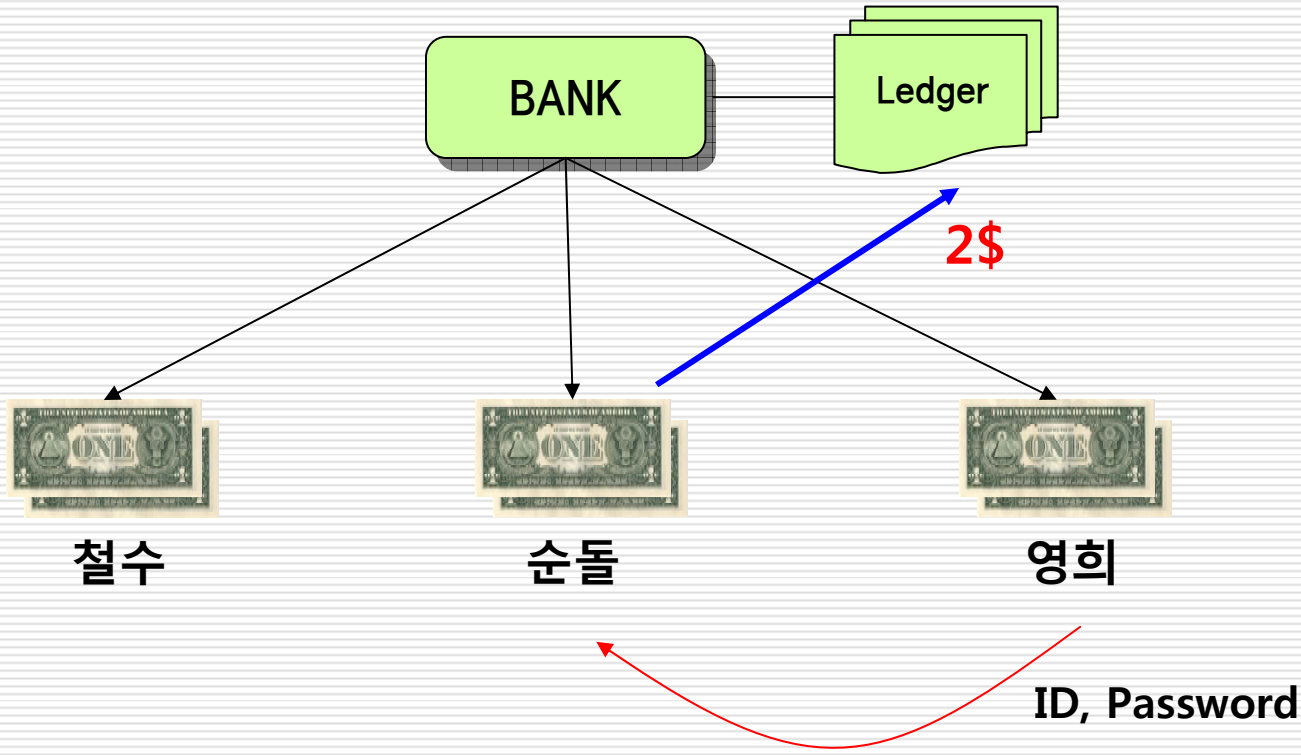
블록체인은 '**해킹불가**'인데… 기[illegible]탁, 왜?
국민일보 | 2018.01.28. | 네[illegible]
'**해킹 불가**' 기술인 **블록체[illegible]** 가상화폐, 왜 이런 역설적인 상황이 벌어진 걸까? 현재 가상[illegible] 술을 거래에 사용하[illegible]
└ **블록체인**은 '**해킹**

<'가상화폐 정부 입장' 발표>'**블록체인**' **해킹 불가** 보안체계… 금융 이어...

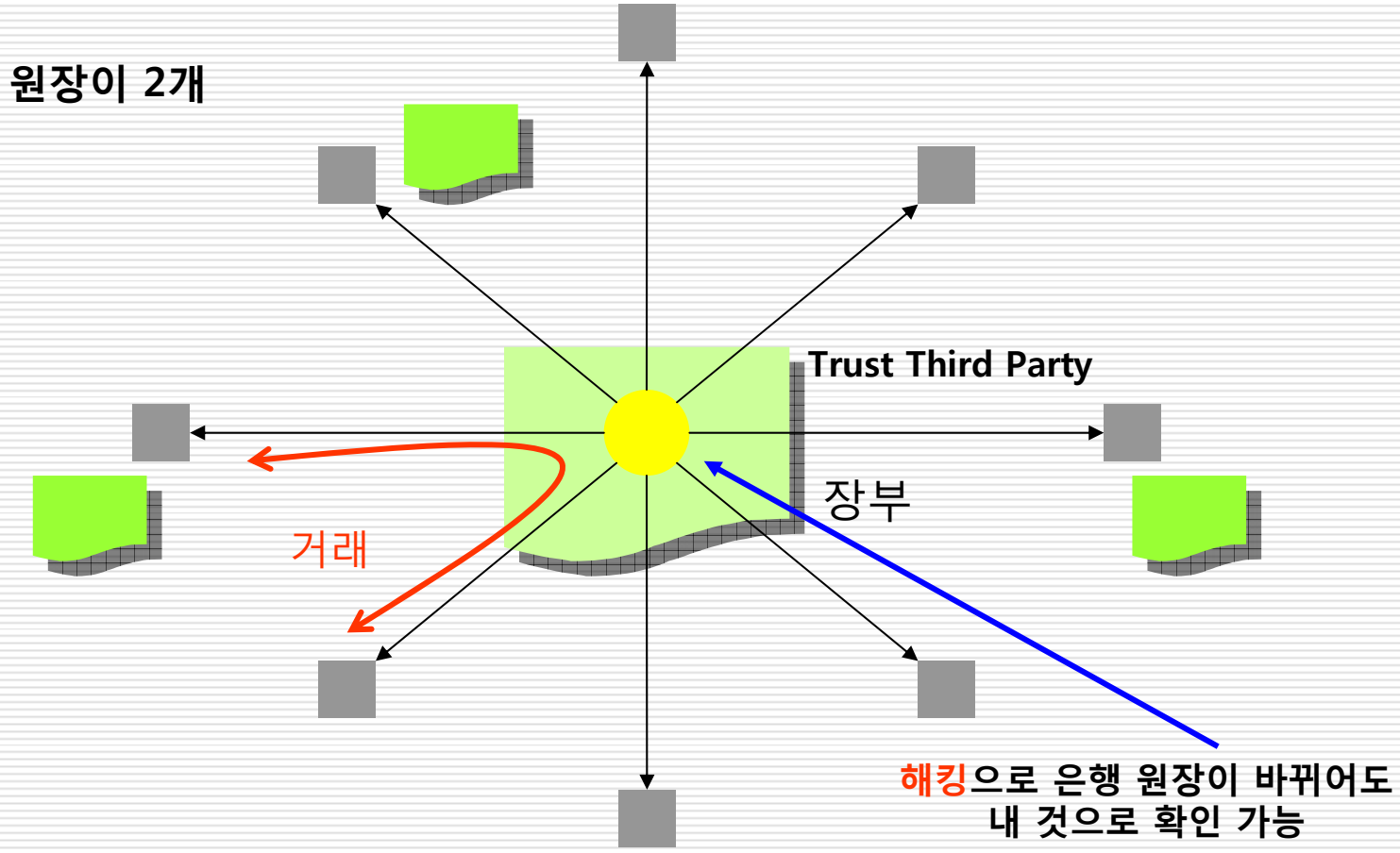
Hacking or NOT?



Hacking or NOT?



은행 시스템 (해킹)



Hacking or NOT?

BANK

은행이 해킹 당함
은행을 해킹

블록체인

거래소가 해킹 당함
지갑이 해킹 당함

블록체인은 해킹 불가

Hacking or NOT?

BANK

은행이 해킹 당함
은행을 해킹

↓

이용자 PC 해킹

은행 해킹은 불가

블록체인

거래소가 해킹 당함
지갑이 해킹 당함

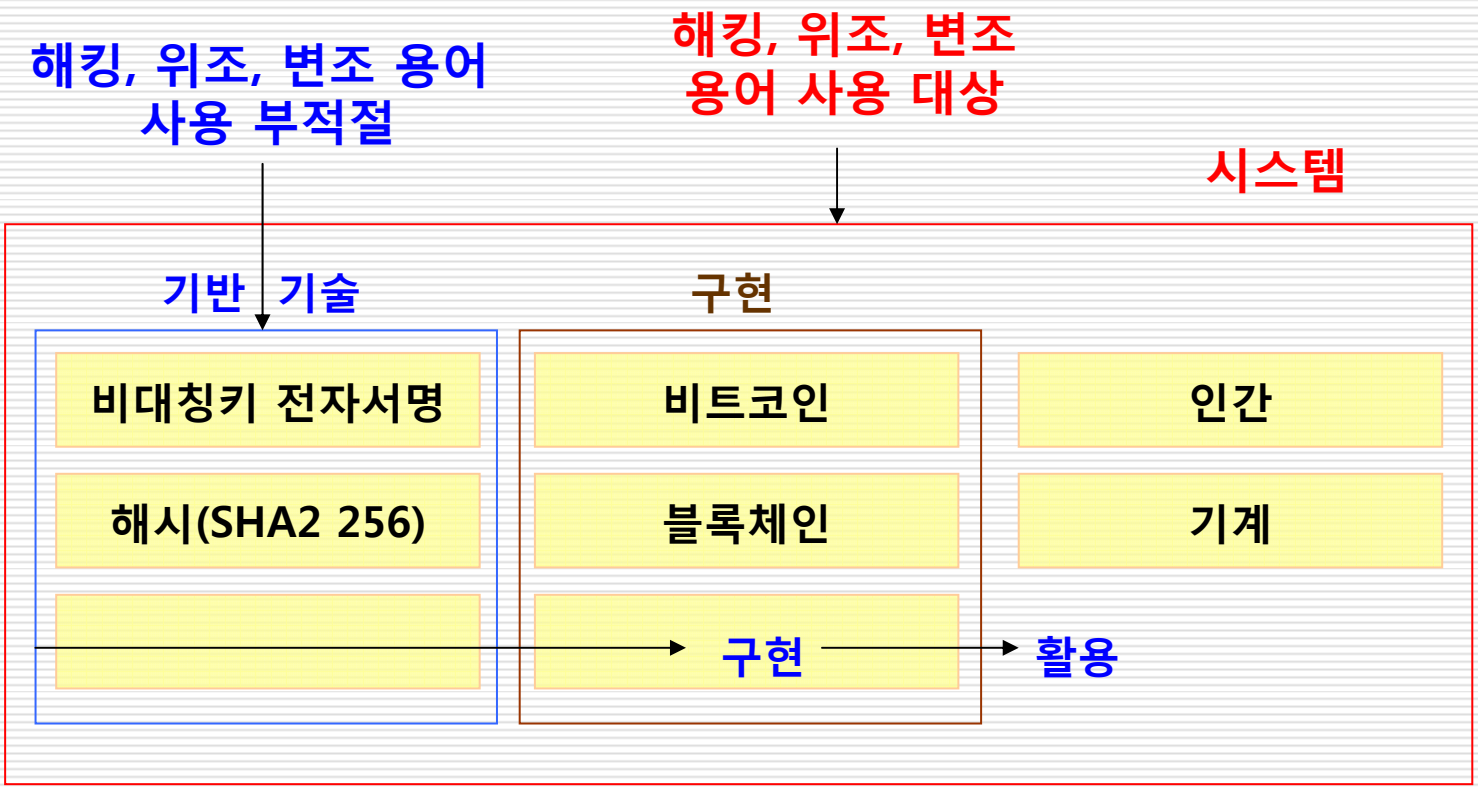
블록체인은 해킹 불가

용어 정의

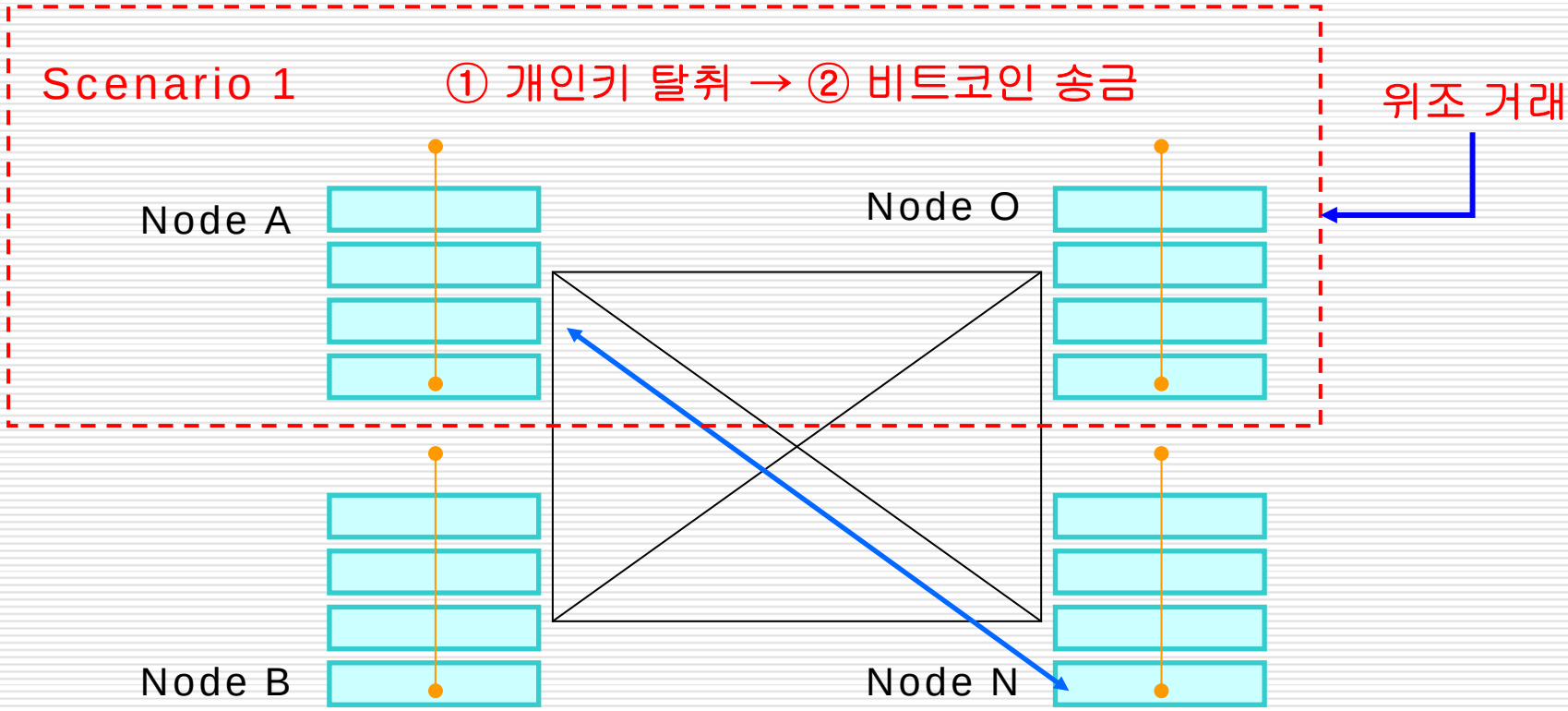
해킹(Hacking)

기본 행위	+	2차적 행위 또는 목적
정당한 접근권한 없이 또는 허용된 접근권한을 넘어 정보통신망에 침입 ① 사용자 또는 관리자 권한 획득 ② 시스템 자체 취약점 활용		① 아무런 행위 없음 ② 위조, 변조 행위 ③ 데이터 파괴 ④ 데이터 유출 ⑤ 업무 지연, 기타

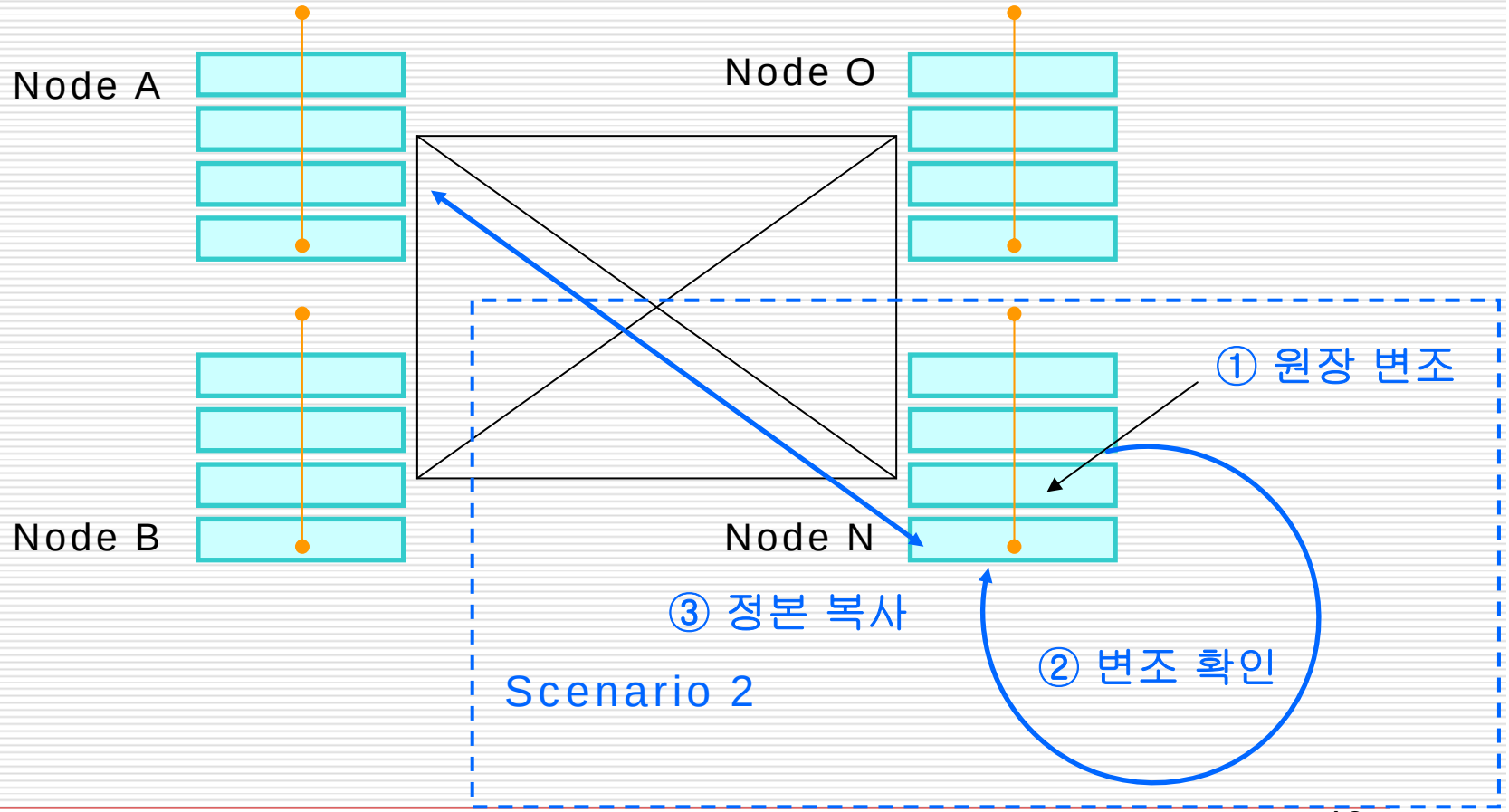
용어 사용


해킹, 위조, 변조 용어
사용 부적절
해킹, 위조, 변조
용어 사용 대상
시스템
기반 기술
구현
비대칭키 전자서명
해시(SHA2 256)
비트코인
블록체인
인간
기계
구현
활용

블록체인 위 • 변조



블록체인 위 • 변조



블록체인?

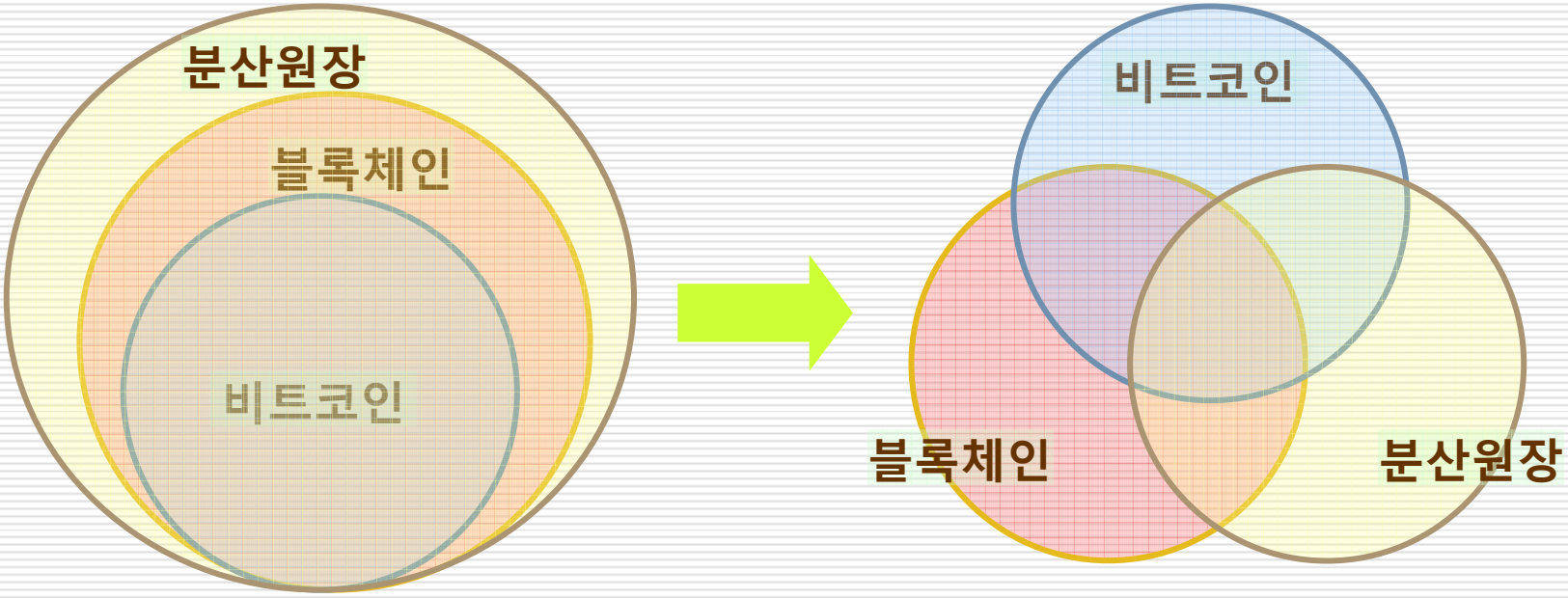
Blockchain : Chain of Blocks → Database

: System Technology → Distributed Ledger
(with distributed
ledger concept)

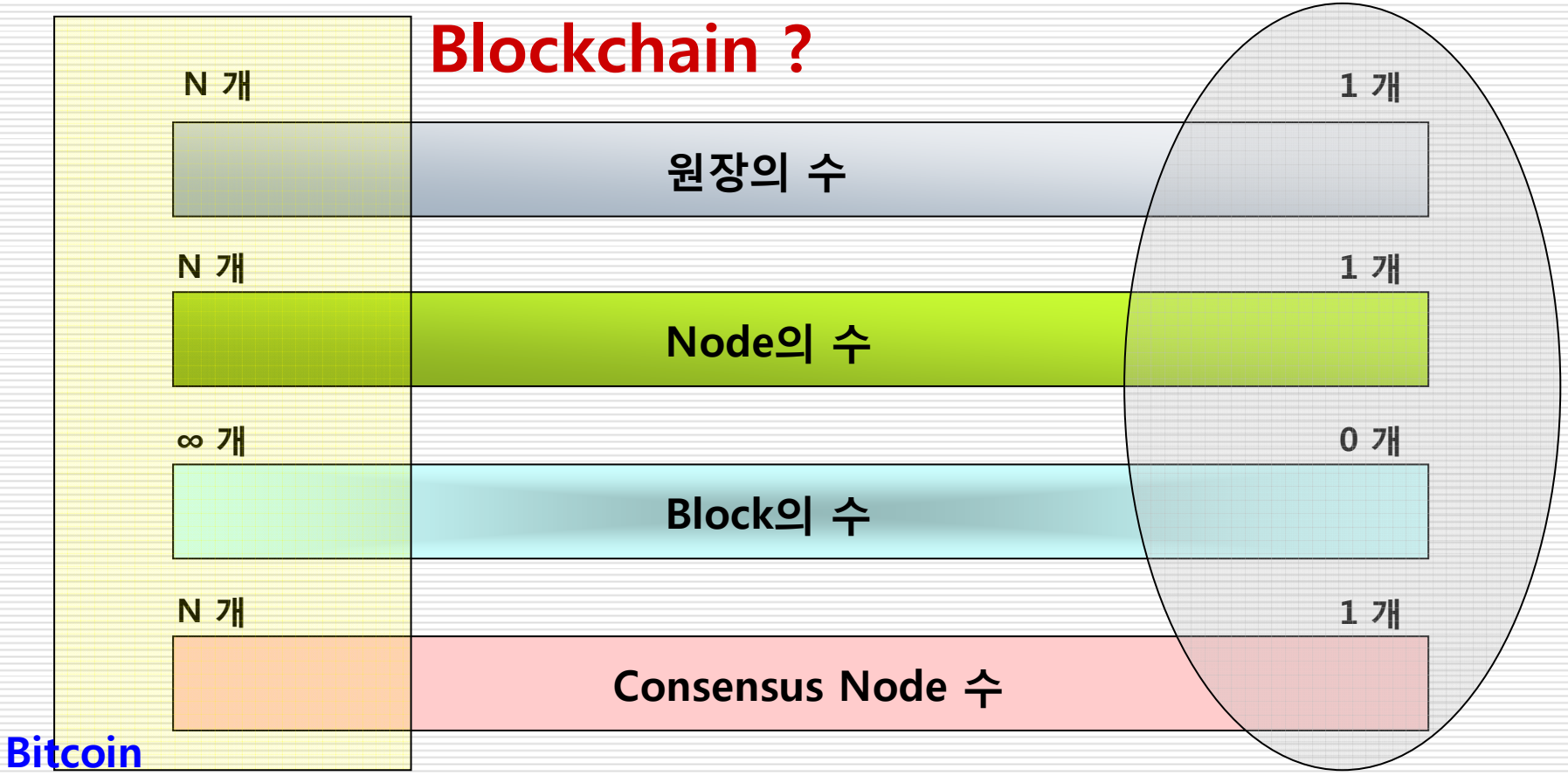
: Application → Application System
(Ex : Bitcoin Blockchain)

비트코인, 블록체인, 분산원장

R3 Corda : no block chain
Bitcoin : chain of digital signatures



블록체인(사슬덩이)


Blockchain ?
N 개
원장의 수
1 개
N 개
Node의 수
1 개
∞ 개
Block의 수
0 개
N 개
Consensus Node 수
1 개
Bitcoin

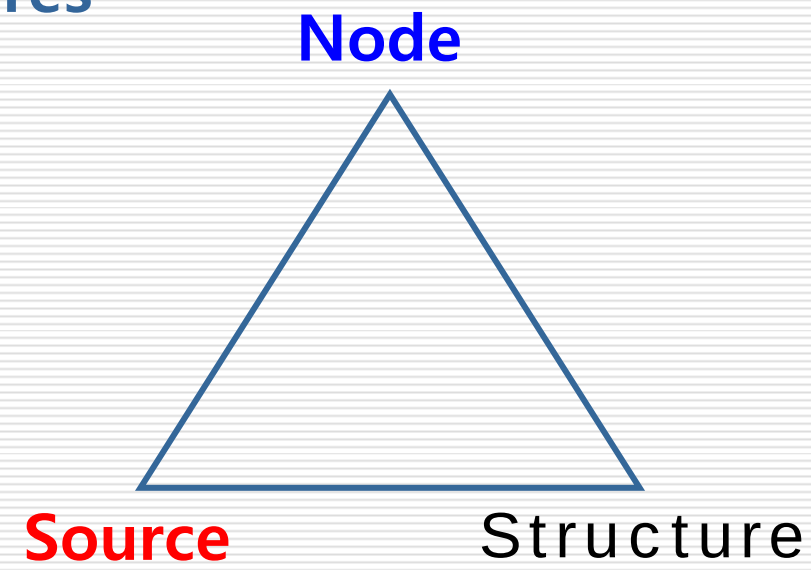
용어 사용의 혼선


Ⅰ. 블록체인과 보안
Ⅱ. 보안 구현 과제
Ⅲ. 결론과 질의응답

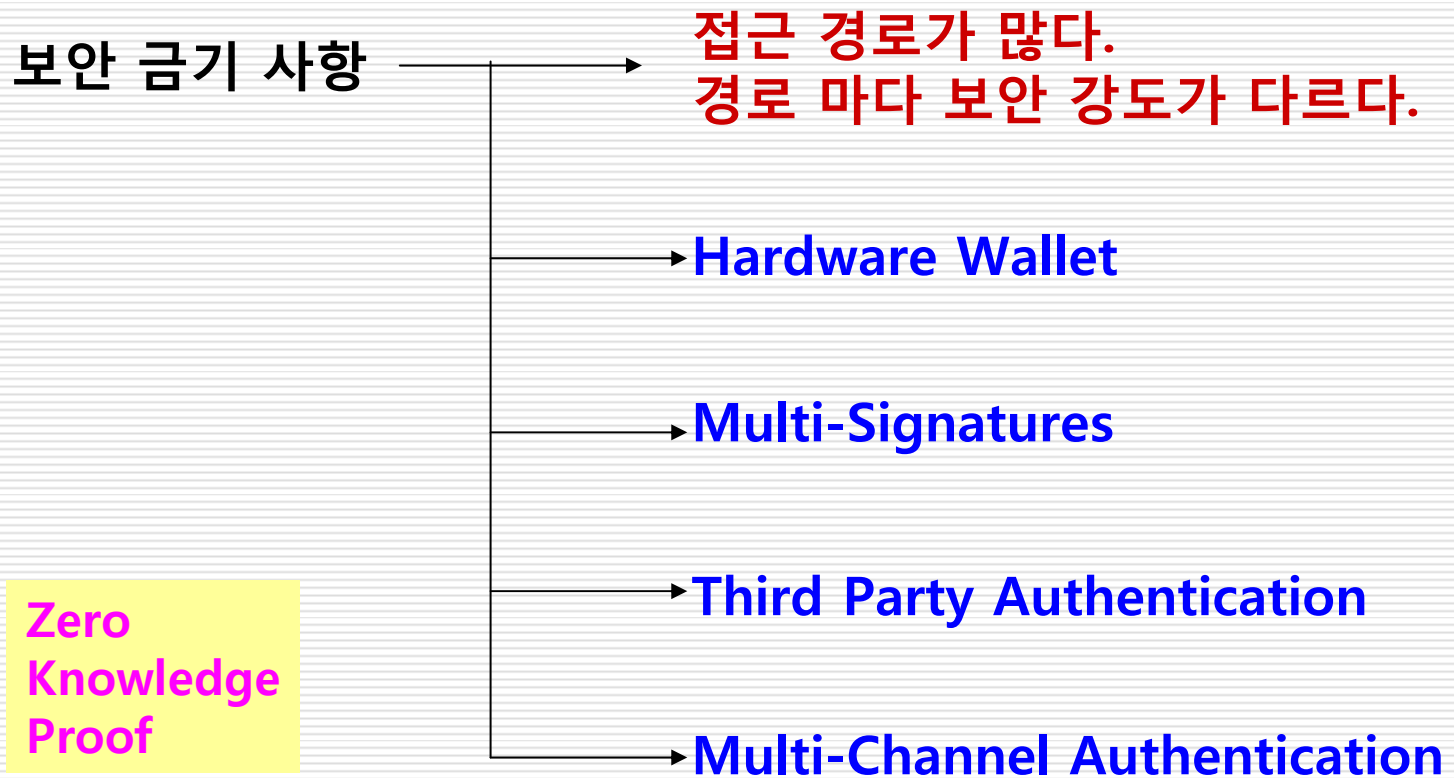
블록체인 보안 요소

Blockchain

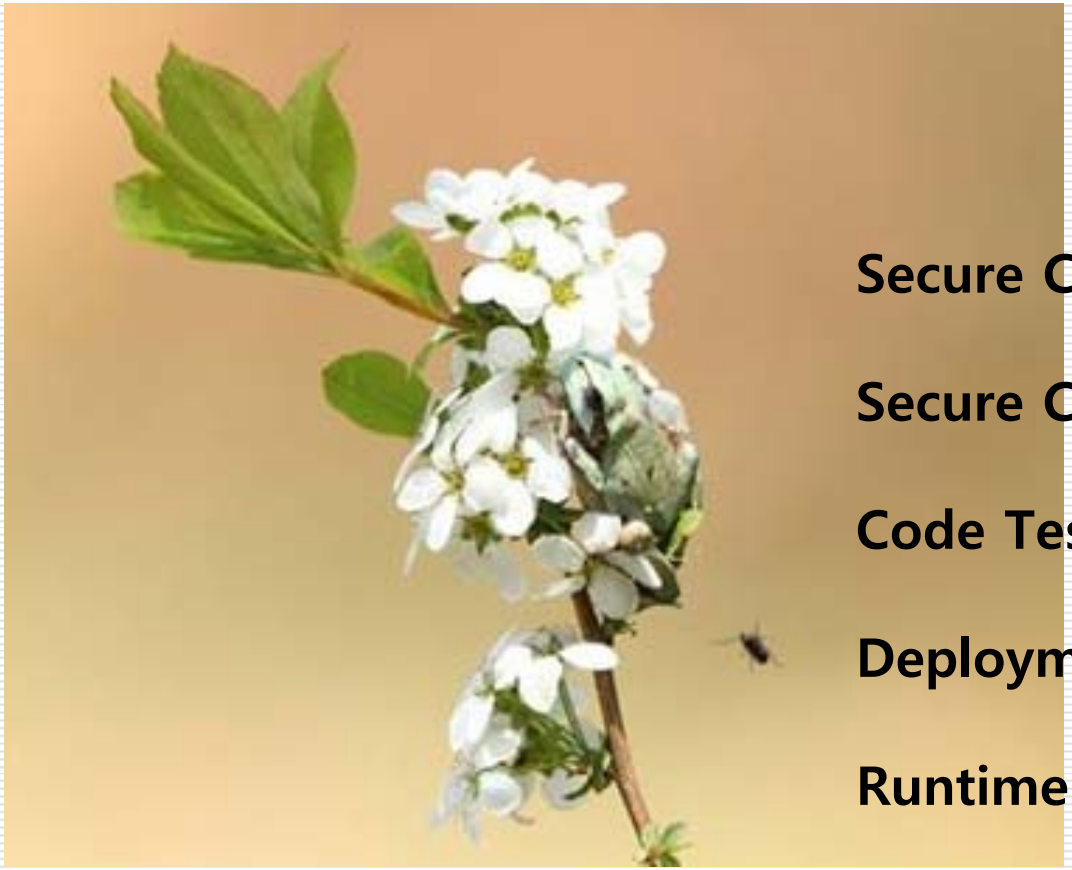
Vulnerabilities and Exposures



Blockchain 취약점(Node)



Blockchain 취약점(Source)



Secure Coding Guidelines

Secure Coding Practices

Code Testing

Deployment Procedures

Runtime Monitoring

Blockchain 취약점(Structure)

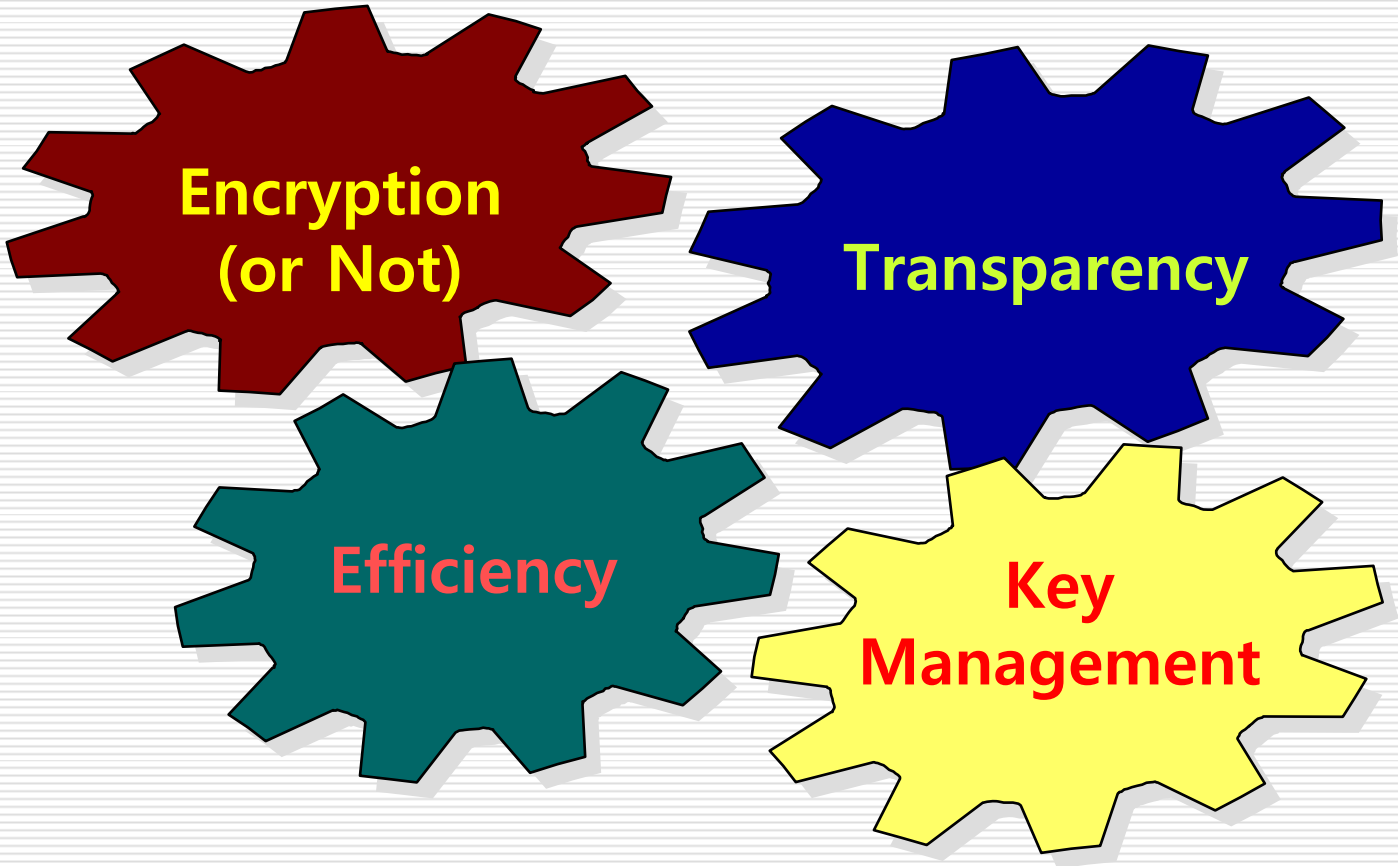
DDos Attack

IDS

Firewall

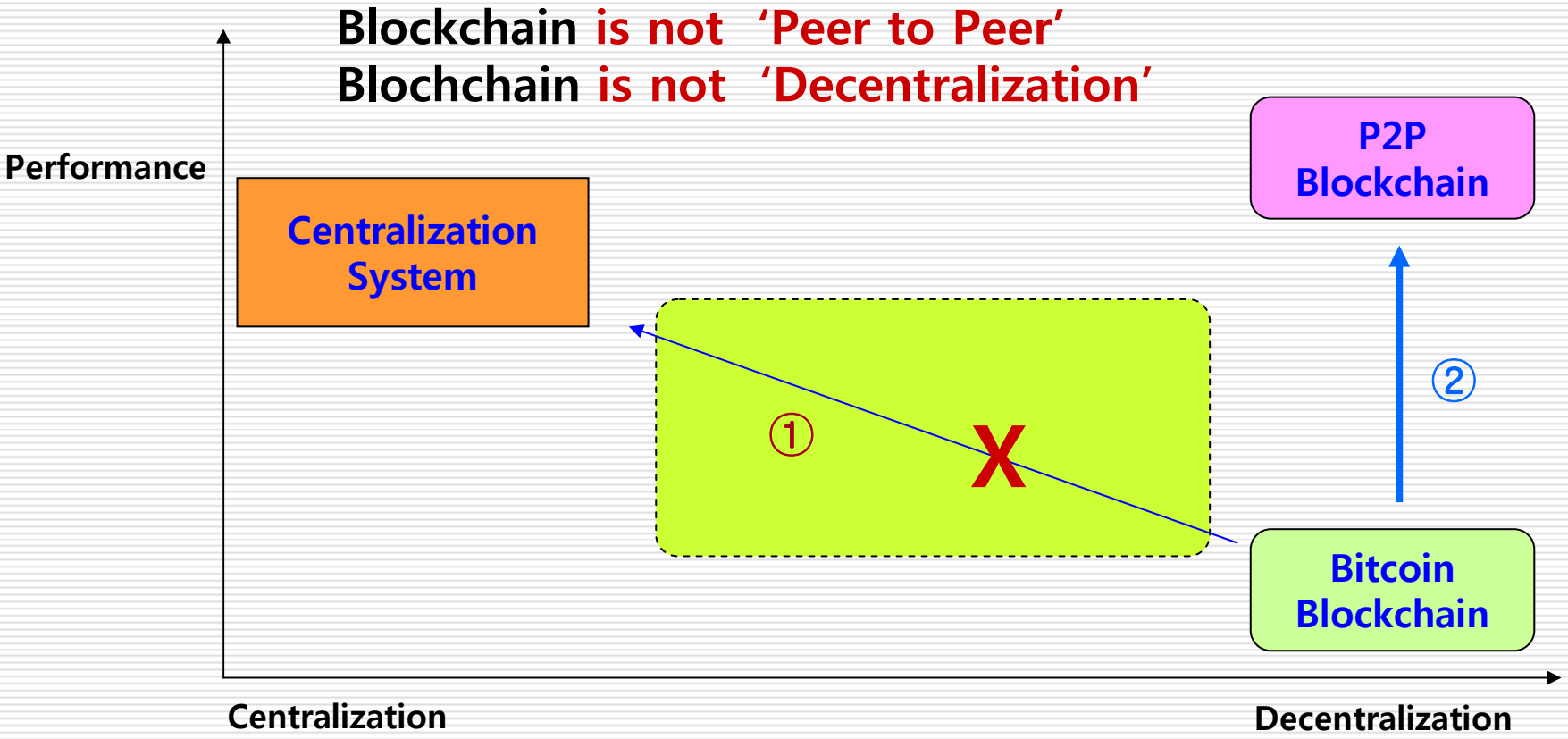
Phishing

Blockchain Privacy




Ⅰ. 블록체인과 보안
Ⅱ. 보안 구현 과제
Ⅲ. 결론과 질의응답

‘블록체인/가상통화’의 진화 방향



풀어야 할 과제


Node의 해킹 취약
스마트계약
데이터보호와 Privacy
출현 사상 유지
분산, 개방, 참여, 투명
Efficiency
Efficiency
Efficiency

Contacts

발표자 : 한호현 (경희대학교 컴퓨터공학과 교수)
Phone : 050-2272-9261
email : howhan@khu.ac.kr