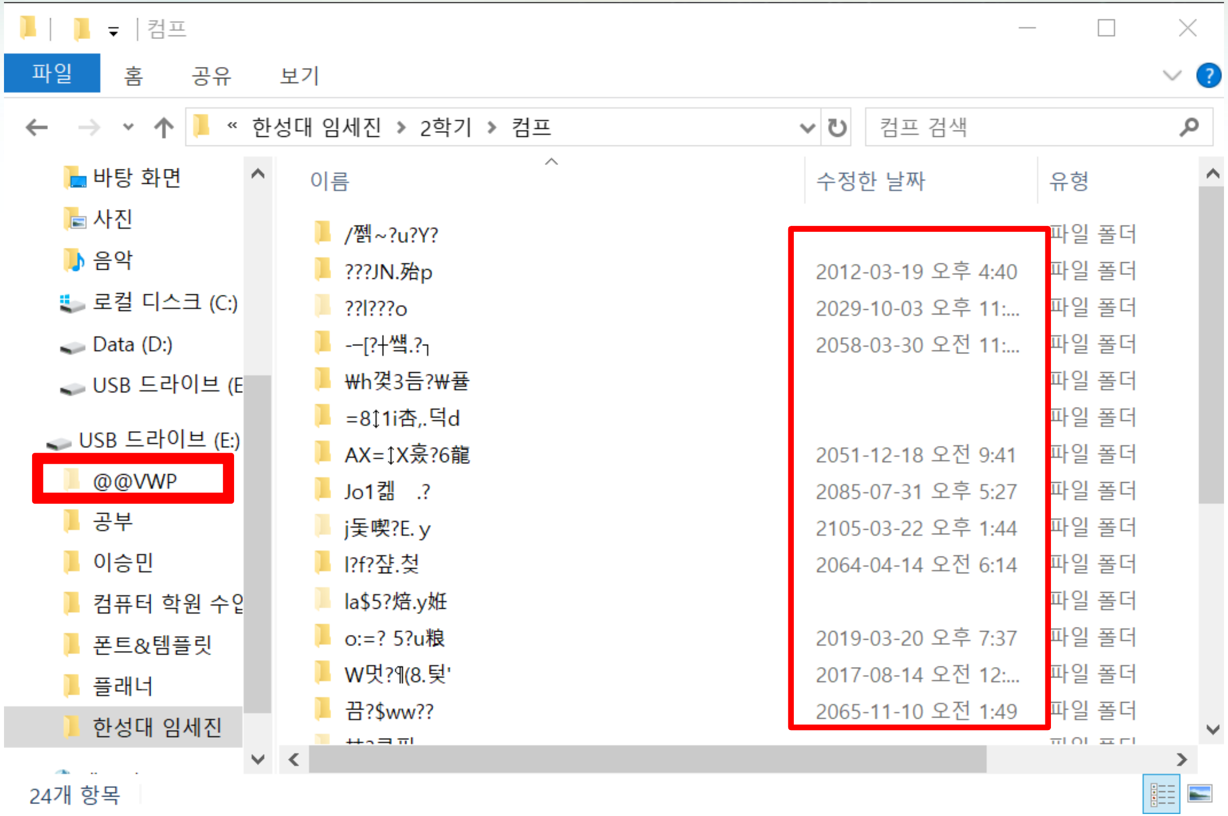
사이버 보안 관련 연구

1871227
IT공과대학
임세진

목차

랜섬웨어 - 나의 사례



컴프
파일
홈
공유
보기
« 한성대 임세진 › 2학기 › 컴프
컴프 검색
바탕 화면
사진
음악
로컬 디스크 (C:)
Data (D:)
USB 드라이브 (E:)
@@VWP
공부
이승민
폰트&템플릿
플래너
한성대 임세진
이름
수정한 날짜
유형
2012-03-19 오후 4:40
2029-10-03 오후 11:...
2058-03-30 오전 11:...
2051-12-18 오전 9:41
2085-07-31 오후 5:27
2105-03-22 오후 1:44
2064-04-14 오전 6:14
2019-03-20 오후 7:37
2017-08-14 오전 12:...
2065-11-10 오전 1:49
파일 폴더
24개 항목

랜섬웨어란?

시스템을 잠그거나 데이터를 암호화하여 사용할 수 없도록 하고
이를 인질로 금전을 요구하는 악성 프로그램

왜 감염될까?

감염 경로는 다른 악성코드들처럼 다양

- 초기의 랜섬웨어
  - 성인사이트에 접속하거나 불법 소프트웨어를 다운로드 할 때
  - 스팸메일의 첨부파일 실행 시키거나 발신처가 불확실한 URL 링크 클릭 시
- 최근의 랜섬웨어
  - 보안패치가 되지 않은 PC 사용자가 감염된 웹 사이트에 접속만하더라도 감염

랜섬웨어 - 예방법


1 모든 소프트웨어는 최신 버전으로 업데이트하여 사용합니다.
운영체제 OS
응용 프로그램 SW
최신 보안 업데이트
2 백신 소프트웨어를 설치하고, 최신 버전으로 업데이트 합니다.
신뢰할 수 있는 백신
안티 익스플로잇 도구
백신 설치, 최신 업데이트
3 출처가 불명확한 이메일과 URL 링크는 실행하지 않습니다.
스팸메일 첨부파일
URL 링크
이메일 및 URL 실행 주의
4 파일 공유 사이트 등에서 파일 다운로드 및 실행에 주의합니다.
P2P 토렌트
블로그
파일공유 사이트
신뢰할 수 없는 사이트
파일 다운로드 및 실행 주의
5 중요 자료는 정기적으로 백업합니다.
문서
사진
별도 매체 백업


Avira
알약
AppCheck
클리너

랜섬웨어 - 전문기관

일부 랜섬웨어에 대한 복구 툴 무료로 제공

국내 랜섬웨어 대응센터

- 안랩 : http://www.ahnlab.com/kr/site/securityinfo/ransomware/index.do
- 이스트시큐리티 : http://www.estsecurity.com/ransomware#decryption
- 하우리 : http://www.hauri.co.kr/Ransomware/index.html
- 랜섬웨어침해대응센터 : https://www.rancert.com

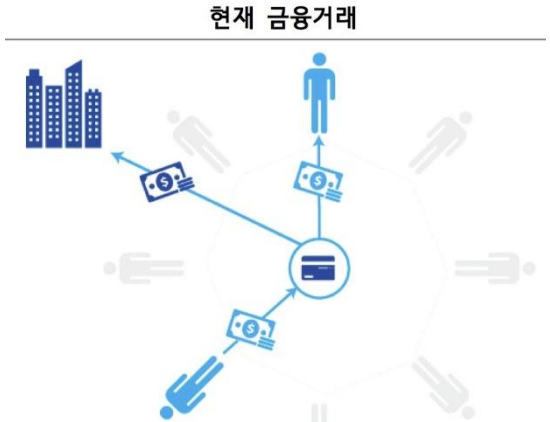
블록체인

블록체인(Block Chain)이란?

모든 거래자의 전체 거래장부 공유 및 대조를 통해 거래를 안전하게 만드는 보안

기존 거래방식

은행
=>



즉, 거래내역을 최소한만 저장
최소한의 인원만 접근 (본인, 직원, 관계자 등)

블록체인

비밀은 적은 사람이 알아야 안전하다는 기존의 사고를 깬 블록체인 기술!

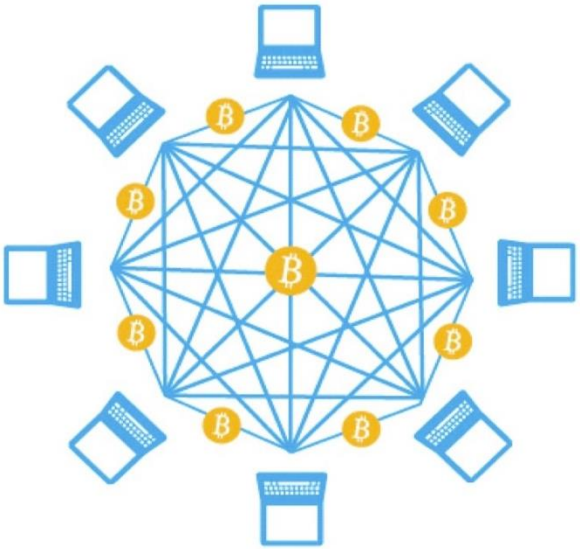
새로운 거래기록 저장(10분간격)

-> 기존의 거래기록과 비교해서

올바른 거래인지 확인(유효성 확인)

-> 모든 거래기록이 있는 블록체인에 연결

블록체인 금융거래

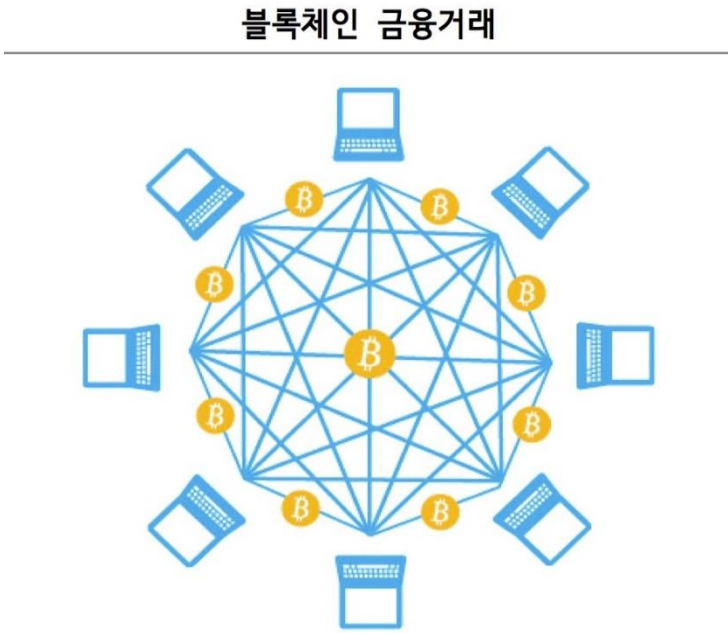


블록체인

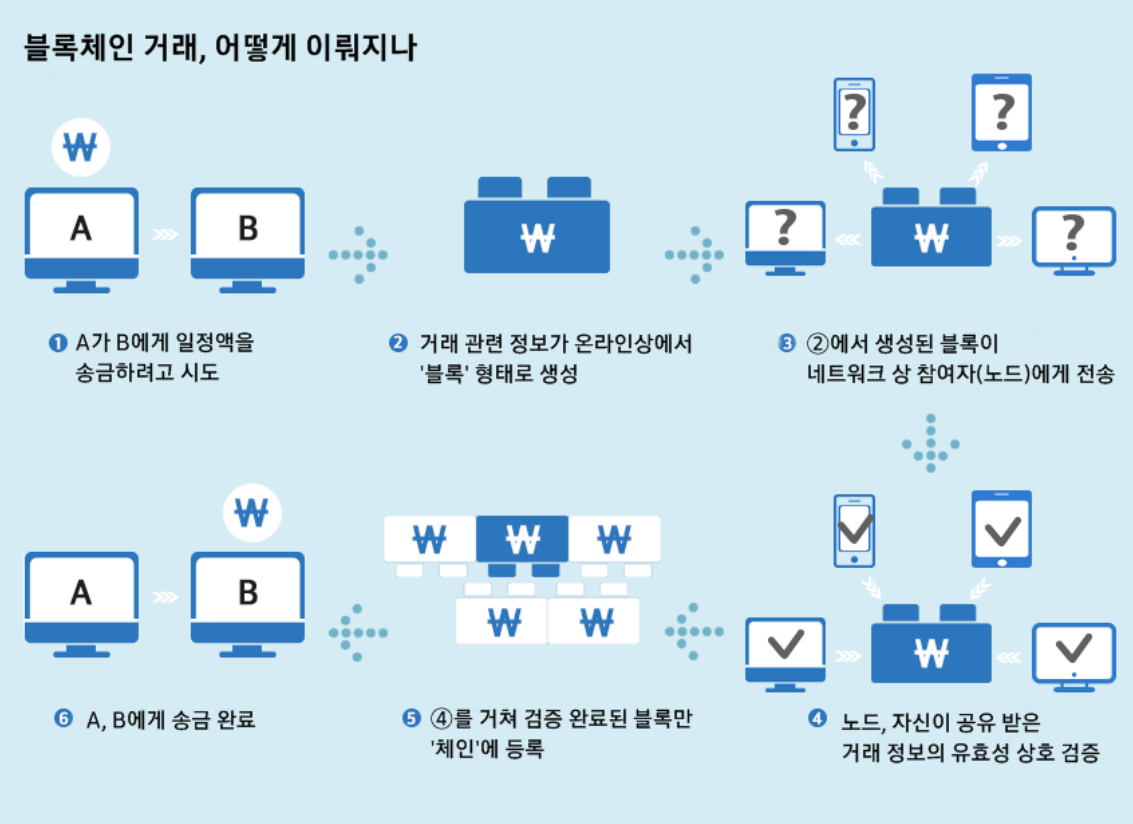
비밀은 적은 사람이 알아야 안전하다는 기존의 사고를 깬 블록체인 기술!

차이점 : 블록체인을 이용하는 모든 사람들에게

암호화된 거래기록을 서로 공유



블록체인 - 예시


블록체인 거래, 어떻게 이뤄지나
₩
A
B
❶ A가 B에게 일정액을 송금하려고 시도
₩
❷ 거래 관련 정보가 온라인상에서 '블록' 형태로 생성
?
?
?
₩
❸ ②에서 생성된 블록이 네트워크 상 참여자(노드)에게 전송
₩
₩
₩
₩
₩
❹ 노드, 자신이 공유 받은 거래 정보의 유효성 상호 검증
₩
₩
₩
₩
₩
❺ ④를 거쳐 검증 완료된 블록만 '체인'에 등록
₩
A
B
❻ A, B에게 송금 완료

공공거래장부를 어떻게 믿을 수 있을까?

- 10분 간격으로 모든 거래 내용을 비교

  연결된 과반수 pc들의 정보와 내 정보 비교

  -> 과반수 이상 동의 -> 블록화

  Ex) 과반수 동의 vs 미동의

  ⇒ 과반수 동의 블록은 블록화 되고, 미동의한 블록은 폐기
- 위조하려면 블록체인 사용자 컴퓨터의 과반수보다 높은 연산력 필요 => 불가능 (위조 해킹이 매우 어려움)

블록체인의 특징

1. 공공거래장부

거래자 모두 거래장부 공유하기 때문에

위·변조 여부는 대조해보면 됨

2. 거래내역 위조 어려움

10분 안에 과반수의 거래장부를 위조할 가능성X (연산력이 턱없이 부족)

블록체인의 핵심 기술

해시(Hash)

문장 내용이 완전히 같으면 완전히 같은 해시 값을 가짐

But, 문장이 일부라도 다르면 완전히 다른 해시 값을 가짐

따라서 해시 값 조합을 통해 원문을 유추할 수 없음

해시 적용해보기

Results	
Original text	SeJin
Original bytes	53:65:4a:69:6e (length=5)
Adler32	055601da
CRC32	d651d190
Haval	9bc03da01ee212e0c921e61a797af8fb
MD2	ec50df30abb66af79af6c283be8e048b
MD4	7782b7f8ad23723534b1e9fd7cf61138
MD5	292bc7140f795431d8a4ce4ee3388676
RipeMD128	22903618d8894ec7bdfe9e4614ba0815

Results	
Original text	SeJun
Original bytes	53:65:4a:75:6e (length=5)
Adler32	056e01e6
CRC32	30268ccd
Haval	428fddcdeaa695510a594816c8575331
MD2	1701246d833af574adb8491b53e923ea
MD4	2b994ca4ea0c8ace35030320fbd5951d
MD5	e3f615b9c3468f8ce37e811a9876ca87
RipeMD128	d58b534625db6a214773e51cba34ea96

블록체인에서 해시를 활용하는 방법

동일한 해시 값을 가지고 있으면

원본 내용을 보지 않고도 원본 내용이 같음을 비교가능!

문장 길이에 관계없이 일정한 길이의 값으로 변경하므로

적은 데이터 양으로 원본 내용 모두 완전히 같음을 비교가능

=> 빠르게 정확하게 비교 가능

블록체인의 종류

퍼블릭(Public) 블록체인

모든 참여자의 장부공유 및 대조를 통해
거래를 안전하게 만드는 보안기술

모든 참여자가 차별없이 장부의 관리에 참여
가능

프라이빗 (private) 블록체인

특정집단(허가된 집단, 개인)에게 사용권을
주는 것

프라이빗 블록체인

장점

- 참여자 제한 -> 빠른 처리속도
- 선별적 정보공유

-> 특화된 정보 관리에 유리

-> 높은 확장성

즉, 다양한 산업에 적용하기 유리한 형태임

- 블록체인의 특징도 가짐 <기존의 체계에 비해 위·변조 방지 뛰어남>

단점

- 퍼블릭 블록체인에 비해 소수가 참여하므로 위·변조 주의

블록체인 개발 시 자금 모집 방법

1. ICO(initial coin offering)

개발자들은 개발 계획서 작성 -> 외부 투자자들이 그걸 보고 판단

먼저 발급받는 대신 투자하겠다!

- 개발평가 기준이 없고, 개인이 판단(사기 여부 등)해야함
- 자금모집 장벽(X) 위험성이 높다

블록체인 개발 시 자금 모집 방법

2. IEO(initial exchange offering)

기준을 추가적으로 만들어 안전성을 높인 것

암호화폐 거래소가 기준 (최소한의 작동모델 제공) 을 만들어 판단 후,

투자자들에게 투자가치여부를 알려줌

- ICO에 비해 안전성이 높다.
- 거래소의 위험(신뢰할 수 있는가?)
- 최소 작동 모델이 필요

새로운 암호 화폐, 블러드 코인

블러드코인

18.09.09 출시된 채굴형 코인

그래픽카드로 채굴했던 비트코인과는 달리, CPU로 채굴하는 방식이기 때문에 누구든지 컴퓨터만 있으면 블러드 코인을 채굴할 수 있다.

새로운 암호 화폐, 블러드 코인

모바일버전 pc버전 둘 다 있음

최근에는 베트남 서버도 열려서 채굴량이 감소하고 있다고 하니

빨리 시작하는 것이 유리!

집과 회사 컴퓨터만 돌려도 하루에 2000~3000개 정도를 모을 수 있음

추천인 제도를 통한 가중치를 통해 돈을 벌어들일 수 있음

가중치가 늘어나면 하루에 10만원도 벌 수 있음

Thank you