2017 한국인터넷거버넌스포럼(KrIGF) 워크숍 보고서

세션명	블록체인 패러다임 : 정보 보안과 제도적 거버넌스			
일시	2017.9.15.(금) 13:30~15:00		장소	세종대학교 광개토관 소회의실 2
참석자	사회	최은창(Free Internet Project)	발제	최은창(Free Internet Project)
	패널	김경곤(고려대학교 정보보호융합학과)		김종승(SK텔레콤 Blockchain TF)
		민경식(한국인터넷진흥원)		박성준(동국대학교 국제정보대학원)
플로어	약20명 참여			

워크숍 취지

사이버 해킹, 랜섬웨어, 바이러스 등으로 인한 인터넷 침해사고는 정보사회의 발전을 저해하는 요소이므로 이에 대응할 수 있는 기술표준, 제도, 정책 등이 필요하다. 이는 인터넷 거버넌스에 정보보호 아젠다가 포함되는 이유이기도 하다. 인터넷 거버넌스를 위해서는 핵심적 인프라의 강건성을 유지하고, 침해를 방지하고 개인정보를 포함한 민감한 데이터의 흐름과 사용과정 전체의 안전성을 확보하는 것이 관건이다.

그러나 최근 인터넷 호스팅 업체가 랜섬웨어에 감염되어 관리하던 서버와 5천여개의 사이트가 마비되는 일이 벌어졌다. 사이버보안의 취약성을 파고든 랜섬웨어 감염 사태는 인터넷 거버넌스에 커다란 도전을 제기하였다. ITU의 인터넷 보안 위협 통계에 따르면 전 세계에서 430만개의 악성코드 발견되었고 웹사이트의 75%에는 보안패치가 없으며 사이버 공격의 50% 이상이 중소규모 기업들(SME)에 집중되어 있다.

이런 상황에서 랜섬웨어를 막기 위한 방법으로 블록체인 암호화 기술을 응용한 데이터의 관리가 주목을 받고 있다. 세계경제 포럼은 블록체인을 4차 산업혁명을 이끌 기술로 선정했다. 블록체인은 사물인터넷 (IoT) 보안에 활용되고 있으며 금융 및 공공 산업 등ICT 인프라에 널리 활용될 것이다. 보안성 높인 공공 거래 장부 블록체인의 보안성과 효용성에 주목한 금융기관들은 중앙집중형 서버에 모든 거래 기록을 저장하는 기존 방식에서 데이터를 블록 단위로 나눠 분산 저장하는 방식으로 전환하려고 하고 있다. 블록체인 기술은 인공지능과 사물인터넷 등 첨단 IT 기술들과 결합하여 새로운 서비스로 제공될 수 있다.

은행이 분산형 디지털 장부(distributed ledger)를 사용하게 되면 기존의 공인인증서 시스템은 사라지게 된다. 블록체인 기술이 활용되면 랜섬웨어의 공격이나 온라인 뱅킹의 해킹은 어려워질 것이다. 은행들은 고객 데이터베이스 관리와 보안 비용도 절감할 수 있을 것이다. 블록체인은 네트워크를 기반으로 한 기술이므로 다수의 이해관계자들 영향을 받게 된다. 무엇보다 블록체인은 신뢰성을 검

	증하는 인증 시스템을 바꿀 것이다. 라우팅 인증(RPKI), 공개키 암호화방식의 전자 서명 메커니즘을 도메인 이름 시스템(DNS)에 도입한 DNSSEC 등은 폐기될 가능성이 크다. 인터넷 발달의 기반이 된 TCP/IP와 마찬가지로 블록체인도 폭넓은 조율이 필요한 기반 기술이다. 인터넷 거버넌스의 관리 시스템도 달라지게 만들 것이다. 이러한 배경에서 블록체인 기술의 적용이 사이버 보안과 인터넷 거버넌스에 어떠한 함의를 가지는가를 살펴보고 의견을 들어보는 기회를 제공할 필요가 있다. 블록체인의 도입과정에서 여러 기술적 제도적 이슈등이 제기될 수 있으므로 멀티스테이크 홀더들의 다양한 목소리를 듣고 공론화 할 필요성이 있다. 블록체인은 기존의 인터넷 거버넌스에 어떤 변화를 가져올 것인가?

1. 퍼블릭한 용도의 블록체인, 블록체인 거버넌스 논의 (최은창 발제자)

- 퍼블릭한 용도의 블록체인, 진정한 인터넷으로써의 P2P 네트워크의 활용 가능성
- 산업화 자체로 비트코인 뿐 아니라 블록체인의 공공영역으로 확장해가야 함
- 인터넷이 단순한 기술이 아닌, 하나의 산업적 혁신의 모멘텀이 되었던 것처럼 블록체인 역시 제2의 인터넷 혁명이 될 것
- 블록체인 거버넌스는 어떻게 진행될 것인가?

(1) IGF for Public Policy

- 인터넷거버넌스포럼(IGF) : 정부, 기업, 시민사회, 학계, 기술 커뮤니티, 이용자 등 멀티스테이크홀더의 정책 대화를 위해 만들어진 포럼
- 2005년 국제전기통신연합(ITU)가 개최한 정보사회세계정상회의(WSIS)의 결과
- 튀니스 어젠더(Tunis Agenda)의 72항에 따라 2006년 아테네에서 IGF가 처음 개최
- 이후 UN차원에서 각 국가 및 지역별로 IGF가 해마다 개최
- 인터넷 거버넌스와 달리 블록체인 거버넌스는 어떻게 진행될 것인가?

(2) 블록체인 패러다임

- P2P 네트워크 : 진정한 인터넷, 탈중앙화의 힘과 사람들의 협력이 새로운 가치를 만들 것(위키피디아, 오픈소스 네트워크 등)
- 블록체인은 P2P의 가치를 그대로 가지고 온 것. 4차 산업 혁명의 주요 동력으로 주목받고 있음
- 금융 서비스 분야에서 거래 수수료 시간 비용 절감 및 감독, 규제 비용 절감 가능. 전세계 극빈자 수를 줄일 수 있음
- 비금융분야에서는 디지털 정보의 보관, 디지털 인증, 스마트 계약, 물류 추적 관리 가능
- Smart Contract의 실현 : 거래 비용의 급감. 그러나 시스템 실패의 경우 누가 나서는가? 또한, 책임의 소재는 어디에 있는가?
- 전자정부, 정부공공, 행정 서비스 : 블록체인 활성화위한 기술 표준화 및 법제도적 정비가 필요

(3) Key Question

- 블록체인 활용은 금융영역과 비금융영역이 존재
- 블록체인의 활용사례 : 사물인터넷, 빅데이터, 물류, 인증, 스카트 계약간의 관계
- 현재의 인터넷 보안, 인증 시스템에 블록체인이 미치는 변화와 영향력 전망?

- 블록체인은 해킹되지 않고 안전한가?(앤드 포인트 보안, DDoS , 제로데이 취약점, DAO 사건)
- 블록체인 기술 표준화의 방향?
- 블록체인 패러다임이란 무엇인가?
- 블록체인과 적합한 제도적 거버넌스, 법제도의 변화 방향은?

2. Blockchain 범용기술, GPT로 가능한가? (김종승 패널)

- 산업혁명에 기반이 되는 범용기술로 과연 블록체인이 성립하느냐?
- 디지털 트랜스포메이션과 사회경제 혁신 : 블록체인은 새로운 사회질서의 변화를 일으킬 수 있다
- AI, IoT 데이터 및 기술과 블록체인이 결합하고, 서비타이제이션 모델로 드러날 때 이러한 변화가 가능할 것

⑴ 블록체인 효과

- 신뢰 : 거래가 발생하는 전 프로세스에 걸쳐 여러 이해관계자의 검증을 통해 데이터의 신뢰성 보장, 모든 영역에서 비용 효율적인 신뢰 기반 거래 환경 제공, 과거 중앙 집중적인 기관이 신뢰를 담당했다면 달리 분산된 모든 주체 사이의 신뢰가 가능함
- 정보보안 : 참여자간 정보 공동 소유로 부정행위 가능성이 낮음. 보안이 취약한 영역에서 기존 방식 대비 탁월한 보안성 제공 가능. 과거의 실 패 케이스에 대해 대안이 될 수 있음
- 투명성 : 모든 거래 기록에 대한 공개적 접근 가능, 거래 양성화를 통한 투명성 확보가 가능하고, 각종 규제 비용 절감에 활용 가능, 정보의 격차, 불일치로 인한 사회적 비용을 절감할 수 있음

⑵ 기업에서 블록체인을 활용한 케이스

- 인증 : 기존의 중앙집중 방식의 ID 통합시도에서 발생된 대규모 투자, ID 중복, 이중 유지보수 비용 지불의 이슈를 해결 가능. 올해 10월 공동사설인증서 개발로 기존 공인인증서 문제 해결 가능
- 물류 : 관세, 항만청, 여러 공공기관의 20여개의 기관에서 사용하는 종이문서 행정을 디지털로 변환하면 신뢰성 증가. 규모의 문서를 디지털로 전환하는 데만 해도 비용이 20% 정도 절감됨, 관세 이슈를 해결하는 것이 문제임. 중기적 관점에서 상용화 될 것
- 푸드 체인 : 유통, 공급망 전반의 추적 역량, 투명성을 제고하는 것이 목적, 먹거리에 대한 사람의 관심, 신선한 식품의 유통경로, 생산지, 부패를 막기 위해 블록체인 기술을 응용해서 확인가능, 실시간 감시를 위해 IoT 기술을 활용한 콜드체인 확인(중국 Wal-Mart와의 협력)
- 에너지 : 민간에서 P2P로 전력 거래 가능(블록체인을 활용, 거래 시스템과 기존 전력 계통을 상호 연계), 전기차 충전 지불 시스템(중계자 없는 무계약 지불 시스템 개발 – 충전, 지불 프로세스를 충전소를 상호 작용하여 결재 절차를 저동으로 관리)
- SK에서 개발하고 있는 사업 : 전기화재 감정/감식을 위한 아크 데이터 수집·분석을 통해 방화원인 규명 및 방화지역 파악(법적 참고자료로 사용)
- 보험요율 산정을 위한 건강 데이터 수집 : 개인의 건강데이터를 기반으로 한 보험료 할인 적용으로 스마트 계약 체결 지원
- 블록체인을 통해 과거에는 가능하지 않았던 신뢰관계 구조가 가능하기 때문에 비용 절감 가능, 연결을 가능하게 함으로써 서로 중복되지 않는 똑같은 데이터를 공유할 수 있다는 것이 특징

⑶ 커먼스(Commons)경제

- 암호화 화폐: 각국의 규제들이 강화됨에 따라 투기성향의 목적은 점점 투명해 질 것
- 블록체인이 초래할 다양한 사회경제적 변화(자본 조달 시달에서의 변화) : 2017년 상반기 VC(벤처 캐피탈)

보다 ICO로 자금 조달한 시장이 훨씬 큼. 상당부분 허수이고 사행성이지만, 간혹 대단한 기업이 있음
- 커먼즈 경제 : 공유경제와는 다른 개념, 공적 공유가 사회적으로 확산된다면 사회 인프라나 간접 자본이 커먼즈의 성장을 통한 혁신이 가능, 수평적인 협력을 통한 자원의 새로운 생산, 소유, 분배, 운영에서 변화가 일어날 것

⑷ 거버넌스와 규제의 상호 보완성

- 블록체인은 법과 규제의 변화를 수반할 수밖에 없는 기술임. 거버넌스와 규제의 균형을 교려해야 할 것
- 여러 사회 문제점으로 인해 발생하는 문제점의 보완이 필요
- 테스트베드를 통해 문제점을 파악하고, 해결해서 점차 제도권으로 편입해야 할 것

3. 블록체인 확산의 어려움 (민경식 패널)

- 탈중앙화, 분산화된 구조 등 블록체인이 가지고 있는 철학이 실제로 실현되기 위한 과정은 매우 어려울 것

⑴ 블록체인 확산이 어려운 이유

- 이상적인 기술이지만, 현실적으로 참여자들의 노력이 필요함
- 현재로서는 실무적 도입이 힘들 것
1. 실제품을 바꿔치기 할 경우의 문제점 : 포장지 속의 내용물을 신뢰할 수 없음
2. 기업의 연합체 중 해킹이 가능한 위협 존재
- 기업들이 관리 권한을 가지고 있는 구조의 경우 : 빅브라더를 견제할 수 있는 거버넌스가 필요
- 개인의 데이터 주권 사회가 올 것 : 기술적인 문제보다는 사람간의 합의를 고민해야 함

4. 블록체인의 실제 적용과 확산의 가능성 (박성준 패널)

- 현재는 블록체인 실질적인 적용이 가능하지 않을 수 있으나, 기술 발전에 따라 미래에는 가능성이 있음

⑴ 블록체인 확산의 가능성

- 기술자가 바라보는 블록체인의 기술적인 면도 좋으나, 인문학 및 사회학적으로 바라보는 시각 또한 많아졌으면 함
- 블록체인을 활용해서 국가, 세계를 바꿀 수 있는 있는, 가치를 증대시킬 수 있는 기대와 노력을 하고 있음

5. 블록체인과 보안 (김경곤 패널)

⑴ DAO 해킹

- 최근 DAO(이더리움 기반 블록체인 투자기관)의 취약점으로 이더리움 블록체인이 해킹 당한 사례가 있음
- 환불을 계속하면 돈이 지속적으로 들어오는 취약점(Recursive call Vulnerability)을 악용하여, 하드포킹을 통해 해커 돈을 모두 빼돌려 버림
- 블록체인은 분산 기술이기 때문에 누가 나서서 해결할 것인가?

⑵ 블록체인 해킹

- 개인보다는 조직적인 범죄 집단에서 본격적인 해킹 시작함. 나름의 보안 기술도 어렵지 않게 해킹 가능
- 공격 유형 : Attacks against blockchain infrastructure(Mt, Gox 사례, Bitfinex 해킹), Attacks Against Code (Dao), Attacks against blockchain sites(inputs.io 사이트 해킹, steemit 해킹), Attack against hot wallet

(블록체인 지갑 해킹, VC Bo Shen 해킹, Ransomware), Attacks against cold wallet(Bitfinex 해킹), Attacks against node(블록체인 노드 공격, Geth node Crash, 크립톤 51% attack)
- 특히 북한에서는 한국의 가상화폐 거래소 해킹을 시도 중임
- 블록체인의 암호화도 양자 컴퓨터를 통해서 해킹 가능(ECC 알고리즘의 취약성) : 10년 이내로 비트코인 같은 가상화폐의 붕괴 가능성에 대한 대안이 필요함
- ex) NSA : 양자 컴퓨터에 대응 가능한 암호 알고리즘 개발 중

6. 블록체인의 안전성 및 블록체인 거버넌스의 필요성 (박성준 패널)

- 가상화폐의 보안 문제는 가상화폐 절도일 뿐 위조나 변조가 아니다

(1) 블록체인의 안전성

- 현재 발생한 가상화폐 대상 해킹은 블록체인의 위조나 변조가 아닌 보관시스템의 취약점을 이용한 절도
- 양자컴퓨터가 나오면 전세계적 보안문제가 될 것. 모든 전자정보의 보안 알고리즘이 붕괴됨. 따라서 양자컴퓨터를 예로 들어 블록체인이 안전하지 못하다는 것은 비약임
- 블록체인 관련 보안 방식이 개발 중
  1. 비트코인 시큐리티 모델의 안전성
  2. 프라이버시(남에게 준 내 정보를 내가 통제 가능성)가 내제된 방식

(2) 블록체인 거버넌스의 필요성

- 거버넌스에서 해킹에 대한 모델을 정립할 필요가 있음
- 블록체인은 새로운 컴퓨터고 새로운 네트워크이며, 인류의 가치 번영을 위해 어떻게 활용할지 깊이 있는 논의가 필요함
- 블록체인이라는 혁명적인 기술을 사용할 때 우리 모두가 누릴 수 있는 가치의 합의가 필요함

7. 마무리 (최은창 펠로우)

- 아크 데이터를 받아서 어떤 명목으로 받았는지 증명을 해야 함
- 블록체인 시스템이 보편화되다면 좀 더 투명해지고, 혁명이 될 것이며, 앞으로 블록체인 거버넌스가 활발히 논의되어야 할 것

질의	**(플로어)** - 블록체인이 굉장히 파격적인 기술이라는 것은 인정하는데, 이것이 인터넷 위의 하나의 계층인지 궁금하다. **(박성준 패널)** - 인터넷 HTTP 프로토콜 정도의 인프라 개념으로 바뀔 것. Web 3.0과 깊이 연계될 것이다.
	(플로어) - 기술은 기술자가, 거버넌스는 정책자가 각기 다른 의견을 주장하고 있다. 앞으로 거버넌스가 되고 하나의 일관성이 형성되려면 둘 사이의 대화가 필요하다. - 블록체인을 거버넌스 레벨로 이야기하려면 서로 간의 대화를 좀 더 업그레이드

	해야 할 것 같다. **(민경식 패널)** - 블록체인 오픈포럼이 이미 존재하며 다양한 분과가 있다. 거버넌스는 거버넌스 분과가 생기면 그 문제를 해결할 수 있을 것 같다. 블록체인 법계 연구회의를 만들 예정이다.
	(플로어) - 블록체인에 관련된 법을 만드는 이유는 무엇인가? - 법을 통한 정부의 블록체인의 통제는 블록체인의 정신에서 벗어난다. 다양한 국가에서 가상화폐를 화폐로 인정하고 있다. 이처럼 민간에서 자유롭게 거래하고 있는 블록체인을 왜 법으로 통제하려는 측면이 있는지? **(박성준 패널)** - 국내에서 블록체인의 기술을 활성화하기 위해서는 법적 도움을 받아야 한다. - 크게 3가지 법이 필요하다고 본다. 블록체인 기본법, 암호화폐법, 스마트 계약법 **(최은창 패널)** - 블록체인법은 규제라기보다는, 인프라를 조성해서 그 근거를 만들어 주는 것