특집 06

비트코인의 가능성과 보안의 문제들

이종협 (한국교통대학교)

목 차 »

1. 서 론

비트코인(Bitcoin)은 안전한가? 대체로 그러하다. 그렇다면 우리는 손자나 손녀에게 재산을 비트코인으로 남겨줄 수 있는가? 대답하기 쉽지 않은 문제이다. 비트코인[1]은 기본적으로는 디지털 자산(digital asset)이다. 그렇기 때문에 무엇보다 안전하게 지켜져야 하며, 도중에 사라지는 일 없이 다른 사람에게 전달될 수 있어야 하고, 누군가에 의해 불공정하게 생겨나서 다른 이들의 자산 가치가 떨어지는 일이 없어야 한다. 비트코인은 디지털 자산이나 화폐가 존재하고 통용되기 위해 고질적으로 제기 되어오던 이러한 문제들에 대하여 비교적 근사한 방법으로 해결책을 내놓으며 현재 가장 유명한 디지털 화폐가 되었다. 또한 비트코인은 암호학을 통하여 이러한 문제들을 해결하고 있기 때문에 암호화폐(Cryptocurrency)의 일종으로 분류된다.

주기적으로 있어왔던 거래소에서의 가격 폭등으로 유명해졌지만, 비트코인은 아직도 기존의 화폐 제도와는 반대되는 구조를 가지고 있어 기대와 걱정을 동시에 받고 있다. 비트코인은 인터넷을 통한 분산된 자동화 시스템에 가깝기 때문에 편리한 지불수단이자 자동 시스템에 통합된 새로운 금융 서비스 모델로써 시장에서의 영향력을 넓혀가고 있으나, 금융에 대한 기존의 규제나 관리 방법이 비트코인에는 쉽게 적용되기 어렵다는 점에서 나라마다 다른 입장[1]을 취하고 있다.

비트코인의 보안은 항상 고려할 것이 많다. 비트코인에 대한 전체적인 이해도가 비트코인의 유명세를 쫓아가지 못하는 이유는 암호학 및 분산 구조를 이용하는 비트코인 핵심 프로토콜이 가지는 복잡성도 있겠지만, 다양한 측면으로 구성된 비트코인의 생태계 때문이기도 하다. 참여자가

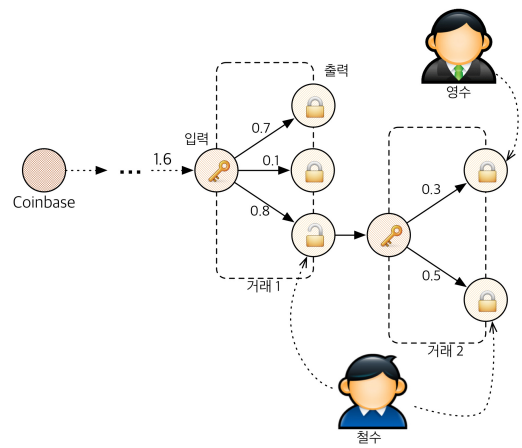
1) 국가별 비트코인의 규제 상황은 www.bitlegal.io 에서 확인할 수 있다.

많고 복잡한 시스템은 안전하게 지키기가 쉽지 않다. 복잡한 비트코인의 생태계를 안전하기 지키기 위해서는 보안의 문제점 또한 다양한 측면에서 살펴보아야 한다. 우선 비트코인의 논리적인 동작을 정의하는 핵심 프로토콜과 인터넷을 통하여 비트코인을 유지하는 P2P 구조인 비트코인 네트워크가 있다. 비트코인 프로토콜에서는 비트코인이 주장하는 화폐로서의 안전성(이중지불 방지, 분산시스템을 통한 거래 확인 등)과 관련된 보안 이슈와 복잡한 형태의 거래 구조에 대한 안전성 또한 고려되어야 한다. 또한 비트코인이 가지고 있는 대표적 특징 중에 하나인 익명성에 대하여 대립적인 연구들이 진행되고 있다. 비트코인이 저장되고 연산이 수행되는 시스템과 소프트웨어적 측면도 비트코인 보안에서 고려되어야 한다. 비트코인 프로토콜의 보안 문제점은 다수에게 영향을 주는 재앙처럼 다가올 수 있지만, 실제 비트코인 불법 탈취와 같은 해킹 사고들은 시스템과 소프트웨어의 보안 문제와 관련되어 있다.

따라서 본 논문에서는 비트코인과 관련하여 생각해 볼 수 있는 보안의 문제점들을 다양한 측면에서 살펴보고자 한다. 또한 비트코인 자체만이 아닌 비트코인을 기반으로 한 새로운 보안 서비스들과 비트코인의 현재 발전 과정에서 발생할 수 있는 보안 문제점들을 알아보고자 한다.

2. 비트코인의 동작 과정

무형의 자산이 안전성을 보장 받기란 쉽지 않다. 비트코인이 암호학을 기반으로 안전성을 유지하여 디지털 자산을 만들어 낸다고는 하지만, 바로 이 안전성을 보장하기 위하여 우리가 기존의 자산에 대하여 가지고 있던 생각들과는 때때로 반대되는 관점에서 접근하기도 한다. 이제는



(그림 1) 비트코인 거래

비트코인을 설명하기 위한 다양한 설명들은 손쉽게 찾을 수 있으므로[2], 본 논문에서는 비트코인의 안전성과 새로운 기술과 관련된 핵심적인 동작 과정에 대해서만 소개하고자 한다.

2.1 비트코인의 거래

비트코인의 가장 기본적인 구성 요소는 비트코인이 소속되는 비트코인 '주소(address)'와 비트코인 주소와 주소 사이의 비트코인의 흐름을 나타내는 '거래(transaction)' 그리고 이러한 거래들이 비트코인 노드들에 의해서 확인되는 '블록(block)'으로 이루어져 있다.

비트코인은 개념적으로 은행 계좌에 해당하는 비트코인 주소들에 비트코인들이 담기고 자신의 주소에서 다른 사람의 주소로 비트코인을 옮기며 사용할 수 있지만, 내부적으로는 색다른 방식으로 동작한다. 비트코인은 인터넷에 잠겨진 채 모두에게 공개되어 있고 비트코인을 이용하고자 하는 사용자는 자신의 (자신만이 풀 수 있는) 비트코인의 잠금을 풀어서 사용하는 방식이다.

비트코인의 동작 과정의 핵심은 비트코인 거래이다. 하나의 비트코인 거래는 비트코인이 담겨

있는 입력에서 출력에 해당하는 비트코인 주소로의 이동을 나타낸다. 비트코의 거래는 은행의 계좌 이체와 비슷하지만, 은행은 계좌 하나에 있는 돈의 일부가 다른 계좌 하나로 이동하는 과정인데 반하여 비트코인 거래는 입력의 비트코인이 모두 출력으로 옮겨져야 하며 입력과 출력 모두 단수일 필요는 없다. 비트코인 거래의 입력은 단순히 계좌나 주소가 아니라 이전에 발생했던 거래들 중에서 아직 사용되지 않은 출력과만 연결될 수 있다. 즉 이전 거래에서 받은 비트코인을 다음 거래에서 사용하는 셈이다. 비트코인이 담겨있다고 할 수 있는 (사용되지 않은) 거래의 출력은 정당한 소유자만 사용할 수 있어야 하기 때문에 일종의 '잠금 스크립트'라 불리는 방식으로 잠겨 있다. 정당한 소유자라면 다음 거래의 입력에서 자신이 소유한 출력의 잠금 스크립트를 열 수 있는 '열림 스크립트'를 제시하여 이전 거래에서 받은 비트코인을 사용할 수 있게 된다. (그림 1)은 비트코인 거래의 예를 보여준다. 철수는 <거래 1>에서 자신의 비트코인 주소로 0.8 비트코인을 받아서 이 중에서 0.3 비트코인을 영수에게 넘겨주기 위하여 <거래 2>를 작성한다. <거래 2>의 입력은 자신의 주소로 들어온 <거래 1>이며 입력에 잠겨있는 <거래 1>의 출력을 풀 수 있는 열림 스크립트를 포함한다. <거래 2>의 입력은 0.8 비트코인이었기 때문에 남은 0.5 비트코인은 다시 철수 자신의 주소로 보낸다. 실제 비트코인 거래에서는 매 거래마다 보통 0.0001 비트코인의 거래 수수료(거래 데이터의 크기에 비례한다)가 추가로 붙는다.

2.2 비트코인의 블록 마이닝

비트코인 거래간의 연결 안전성은 잠금-열림 스크립트로 보장할 수 있지만, 거래의 정당성에 대한 확인은 Bitcoin network에 연결된 노드들에 의해서 자발적으로 수행된다. 비트코인 거래가 발생하면 Bitcoin network에 연결되어 있는 모든 노드들에 전달되고, 노드들 중 하나가 확인 받지 않은 거래들을 모아서 이를 확인해주는 블록을 완성한다. 블록을 완성하면 항상 보상이 주어지는데, 정해진 액수(현재는 25 비트코인)만큼 비트코인을 생성하여 누군가에게 줄 수 있는 coinbase 거래를 자신이 생성한 블록에 포함시킬 수 있다. 이러한 보상을 얻기 위한 노드들은 블록을 만들기 위해 아직 어떠한 블록에도 들어가지 않아 확인받지 않은 거래들을 모아서 자신의 블록에 넣으려 노력하는 충실한 관찰자의 역할을 자의적으로 수행하게 된다. 하지만 블록을 만들고자 노력하는 노드들의 담합이나 속임수를 방지하기 위하여 작업증명(Proof of Work)이란 방식을 통하여 실제 어느 이상의 연산을 수행하지 않으면 답할 수 없는 퍼즐을 블록을 만들 때 마다 풀도록 한다. 블록에 대한 작업증명에 대한 조건으로써 노드는 블록에 담길 거래 정보들과 이전 블록의 hash 값과 함께 자신이 짐작한 특정 값을 넣고 다시 hash를 하여 그 결과가 기준값보다 작아야 한다. 이 조건을 만족시키기 위하여 노드는 짐작하는 값을 계속 바꾸어가며 작업을 반복한다. 이런 고된 연산의 작업 때문에 블록을 만드는 과정은 마이닝(mining)이라고 불린다. 또한 각 블록이 이전 블록의 hash값을 포함하며 확인하는 효과를 가지기 때문에 블록끼리 연속적으로 연결되어 있는 블록체인(blockchain)이 구성된다. 노드들은 가장 긴 블록체인의 마지막 블록을 최신 블록으로 삼는다.

3. 비트코인의 프로토콜 관련 보안

본 절에서는 비트코인의 프로토콜이 제공하고 있는 분산 환경에서의 비트코인 거래의 안전성과 비트코인 거래의 익명성과 관련된 보안 문제를 알아본다.

3.1 블록체인 합의 과정의 보안

Bitcoin network에 의해서 인터넷에 유지되고 있는 블록체인은 지금까지 확인된 모든 비트코인 거래들이 들어있는 단일의 긴 hash 체인이다. 발생한 블록들 간의 순차적 연결이기 때문에 당연히 하나의 블록체인만 존재해야 하지만, 마이닝 과정에서 서로 다른 노드가 동시에 블록을 생성하기 위한 답을 찾는데 성공하는 경우 일시적으로 두 개의 최신 블록이 생겨나서 블록체인이 둘로 갈라질 수도 있다. 이러한 경우 Bitcoin network의 노드들의 대다수가 어떠한 블록을 최신 블록으로 삼아서 마이닝 과정을 이어가느냐에 따라 두 블록 중 선택받지 못한 블록은 의미를 잃게 된다. 즉 Bitcoin network의 50% 이상의 마이닝 능력(연산능력)을 가지는 대다수의 뜻을 따르게 되는 셈이다. 따라서 혹시 51%의 마이닝 능력을 장악한 공격자가 나타난다면, 공격자가 블록체인에 대한 제어권을 가지며 올바르지 않은 거래들도 포함시킬 수 있는 '51%의 공격'이라 불리는 문제가 발생할 수 있다. 더욱이 Eyal과 Sirer의 논문[3]서 악의적인 마이닝 과정을 통해서 51%가 아닌 25%정도의 연산능력만으로도 불합리하게 이득을 볼 수 있음을 제시하였다. 하지만 일반적으로 현재의 Bitcoin network 전체의 연산능력이 이미 어마어마하여 (2014년 10월 현재 Bitcoin network의 초당 hash 회수 : 2.5×10^{17}) 의미있는 정도의 연산능력을 장악하기는 쉽지 않다고 여겨지고 있다.

하지만 요즘 비트코인 마이닝의 확률을 높이고자 마이닝 노드들의 연합체인 마이닝 풀(mining pool)들 위주의 마이닝이 주를 이루게 되면서 위험성이 대두되었다. 최근 대표적인 GHash란 마이닝 풀에서 일시적으로 50%이상의 연산능력을 가지는 탓에 위험성에 대비하여 대내외적인 조정 과정이 진행되었다. (2014년 10월 현재 선두 마이닝 풀의 지분은 26~27% 선이다.) 특히 블록체인 자체에 대한 장악의 가능성은 비트코인 근본적인 안전성에 관련되어 있고, 시장 가격과 항상 밀접한 관계를 가지고 있는 비트코인의 특성상, 이러한 보안 위협의 대두가 일시적으로 경제적 영향으로 나타나곤 한다.

3.2 비트코인의 익명성

비트코인에 대해 사람들이 주목하는 특징 중에 하나는 익명성이다. 비트코인의 익명성이란 거래 자체는 완벽하게 공개되지만 거래를 수행하는 실제 사람을 거래와 연관지을 수 없다는 데서 기인한다. 비트코인에서 거래의 대상이 되는 것은 실제 사람이 아닌 비트코인 주소이다. 비트코인은 주소와 주소의 실제 소유자와의 연결을 알 수 없기 때문에 익명성이 보장된다고 할 수 있다. 또한, 비트코인 주소는 제한없이 임의로 만들어 낼 수 있어 한 사람이 자신의 비트코인을 몇 개의 주소에 나누어 담아 사용하는지 또한 알 수 없다. 하지만, 이러한 익명성이 언제나 성립하는 것은 아니다. 비트코인 주소를 이용하는 거래가 발생될 때 마다 소유자에 대한 힌트가 항상 드러나게 된다.

따라서 비트코인의 익명성과 관련된 연구는 역설적이게도 두 가지 방향을 가진다. 첫번째는 비트코인의 익명성이 가지는 한계를 기반으로 거래

그래프(transaction graph) 등을 분석하여 같은 사용자에게 속하는 비트코인의 주소들을 그룹지어 특정 사용자에 해당하는 모든 주소 및 거래 내역을 알 수 있다는 탈익명화(de-anonymization) 연구들이 있다. 이와는 정반대로 비트코인의 취약한 익명성을 강화시켜주기 위한 다양한 연구 및 새로운 서비스들이 개발되고 있다.

탈익명화와 관련하여 대표적으로 비트코인의 거래 관계를 나타내는 거래 그래프를 구성하고 분석하여 같은 사람이 소유할 것으로 추정되는 주소들을 그룹짓는 연구들[4-6]이 수행되었다. 또한 거래 그래프를 통하여 비트코인의 이동이 추적 가능함을 이용하여 문제가 있는 비트코인 주소 (예를들어, 범죄에 연류된 비트코인 주소) 등과 연관된 거래들을 파악하여 위험도를 점수화하는 블랙리스트 방식과 같은 접근 방법들도 제안되고 있다[7].

이와는 반대로 비트코인의 익명성을 강화하기 위한 기법들은 거래들간의 상관관계를 숨기거나 모호하게 하는데 초점을 맞추고 있다. 그래서 거래의 연결성이 드러나는 비트코인의 블록체인이 아닌 별도의 블록체인을 통하여 익명성을 제공하고자 한다. 대표적인 익명성 강화 연구인 Zerocoin[8]과 Zerocash[9]는 블록체인의 비트코인을 익명성이 강화된 자신만의 형태로 변화시켰다가 비트코인으로 블록체인으로 복원하는 방식으로 거래가 추적되지 않도록 하여 익명성을 강화하고 있다. Darkcoin[10] 또한 자신만의 블록체인을 구성하면서 거래 관계를 난독화 하는 Darksend라 불리는 방식을 통하여 거래를 뒤섞어 추적을 어렵게 한다. 특히 거래 난독화 과정에 참여하는 노드에게 보상을 지급하여 익명성 강화에 초점을 맞추고 있다.

3.3 비트코인의 안전한 거래 구성

비트코인 거래는 일반적으로 2.1절에서 소개하는 방식으로 이루어지지만 다양한 용도에 모두 적용될 수 있는 유연성을 가지고 있다. 기본적으로 입력과 출력에 사용되는 스크립트가 자유도를 가진 프로그래밍 언어이기 때문에 이를 활용하여 다양한 거래의 형태를 만들 수 있다. Bitcoin Contracts[11]의 이름으로 소개되는 방식들에서 기존 인증 또는 금융 서비스를 바트코인을 적용하는 방법들이 주목을 받고 있다. 특히 multisig라 불리는 다중서명 기법을 포함하는 스크립트 등을 활용하며 거래를 구성하는 방법을 많이 사용하고 있다. 다양한 스크립트를 사용하면서 비트코인이 다양한 문제 해결에 사용되고 있지만[12], 스크립트의 복잡도가 올라갈수록 잘못 구성된 거래를 만들 가능성 또한 높아지고 있다. 잘못 작성된 잠금 스크립트의 비트코인은 이를 풀 수 있는 열림 스크립트를 만들 수 없어 더 이상 아무도 사용할 수 없게 버려지게 된다. 이에 맞추어 Bitcoin Contracts 식의 거래에 대한 모델을 제시하여 거래에 사용하는 스크립트의 정확도를 검증하고자 하는 연구[13]도 수행되고 있다.

4. 비트코인 시스템의 보안

비트코인이 실제 사용되는 시스템들에는 비트코인 프로토콜 자체가 아닌 사용이나 구현상에 발생할 수 있는 보안의 문제점들을 가지고 있다. 본 절에서는 비트코인 주소의 정보들이 저장되는 비트코인 지갑(wallet)과 비트코인 구현 소프트웨어의 안전성에 대하여 살펴본다.

4.1 비트코인 지갑의 안전성

비트코인 주소는 일반적으로 한 쌍의 공개키와 개인키를 생성하여 인코딩된 공개키의 hash 형태를 주소로써 사용한다. 따라서 어떠한 주소를 출력으로 하는 비트코인 거래의 잠금 스크립트는 그 주소에 해당하는 공개키 자체와 개인키로 서명한 값을 가진 열림 스크립트를 제시함으로써 풀 수 있다. 비트코인 지갑에는 이러한 주소의 개인키와 같이 열림 스크립트를 작성할 수 있는 정보를 저장한다. 따라서 지갑에 있는 정보는 자신의 비트코인을 사용하기 위해 필수적인 정보이기 때문에 지갑 정보의 노출은 바로 비트코인의 손실로 연결된다. 따라서 비트코인 지갑은 해킹을 통한 비트코인 공격의 주된 대상이다.

비트코인 지갑의 안전성 확보를 위하여 3.3절에서 언급되었던 다중서명을 위한 multisig를 지갑에 도입하는 서비스들이 활발히 이루어지고 있다. 다중서명은 설정에 따라 하나 이상의 서명이 있는 경우에만 거래가 일어날 수 있기 때문에 지갑의 다중 안전장치의 용도로 사용될 수 있다. 예를 들어 온라인 비트코인 지갑에 다중서명을 설정하고 지갑에서 거래를 수행할 때마다 온라인 지갑 사이트의 서명 외에 자신의 서명을 항상 필요로 하도록 설정하면 온라인 지갑 사이트가 해킹 공격에 의해 장악되더라도 자신의 개인키가 저장되어 있지 않기 때문에 악의적인 비트코인 인출을 막을 수 있다. 또한 다중서명은 two-factor 인증 등을 통하여 생체정보나 별도의 장비를 통해서만 비트코인의 지갑에서 인출이 가능하도록 하는 서비스로 발전하고 있다.

비트코인 지갑에 대한 해킹 공격을 근본적인 해결책으로 물리적인 비트코인 동전이나 종이 비트코인 지갑과 같은 인터넷에 연결되지 않은 오프라인의 cold storage 부류의 지갑들이 사용되어 왔다. 이와 비슷한 접근으로 온라인에 의한 위험성을 줄이고자 하드웨어 형태의 비트코인 지갑들이 사용되고 있다. Trezor와 같은 하드웨어 지갑은 조작 방지 (tamper proof) 처리된 저장 장치 내에 키를 저장하고 사용할 때에만 USB등을 통해 컴퓨터에 연결되어 사용자 인증이 되는 경우에만 내부에 저장된 키를 이용하여 서명된 거래를 컴퓨터에 전달한다. 즉 비트코인 거래를 생성할 필요가 있는 경우에만 연결되고 나머지는 cold storage와 같은 상태를 유지하는 셈이다. Cold stroage에 비하여 인증절차를 한번더 걸치기 때문에 더 안전하기는 하지만, cold storage의 분실의 문제나 이용 편이성의 문제들도 하드웨어 지갑에 역시 해당된다.

4.2 비트코인 소프트웨어의 안전성

비트코인을 다루는 소프트웨어의 버그는 치명적이다. 현재 공식적인 Bitcoin Developer Documentation[14] 사이트에서 비트코인의 모든 동작에 대하여 명확하게 설명하고 있지만, 초기의 비트코인 시스템 자체가 Satoshi Nakamoto의 직접 구현한 소프트웨어를 통해 세부적인 동작과정이 결정되어 왔기 때문에, Bitcoin Core 소프트웨어는 아직도 reference로써 영향을 주고 있다. 하지만 가장 신뢰의 대상이 되어야 하는 Bitcoin Core의 소프트웨어마저도 버그와 같은 소프트웨어 오동작의 문제에서 자유롭지 않다.

대표적인 소프트웨어 버그로 2010년 8월에 발생한 CVE-2010-5139의 취약점이 있다[15]. Integer overflow에 의한 버그로 인하여 0.5 비트코인이 184조 비트코인으로 전달되는 합당하지 않는 거래가 정상적으로 블록에 포함되어 버려 8시간 후에서야 해결이 되는 문제가 발생하였다. 이뿐만 아니라 Bitcoin Core의 bitcoind 버전이 0.7에서

0.8로 업그레이드 되며 사용하는 데이터베이스가 BerkeleyDB에서 LevelDB로 변하는 와중에 0.8 버전에서는 처리되는 블록이 0.7에서 처리되지 않는 버그가 발생하여 6시간 동안 0.7버전의 노드들과 0.8버전의 노드들이 서로 다른 블록체인을 가지는 등의 예도 있다. 이 두 문제 모두 어느 정도 시간이 지나 깊이를 가지게 된 블록의 비트코인 거래들은 안전하다라는 비트코인의 일반적인 신뢰가 소프트웨어 버그에 의해 위협받을 수 있다는 것을 보여주는 예라고 할 수 있다.

5. 비트코인 파생 서비스의 보안

비트코인의 가능성은 비트코인 자체만이 아니라 비트코인을 기반으로 한 다양한 파생 서비스들이 가능하다는 측면에서도 엿볼 수 있다. 이러한 파생 서비스들은 비트코인이 확장되면 추가적인 보안의 고려사항을 만들기도 하지만, 오히려 기존의 보안 서비스에서 제공하는 기능을 비트코인을 통해서 효과적으로 구현하는 보안 강화의 역할을 하기도 한다.

5.1 비트코인 블록체인을 이용한 보안 서비스

비트코인의 블록체인은 Bitcoin network에 연결된 세계의 노드들에 의하여 감시되고 유지되고 있어 인터넷에서 공유되고 신뢰할 수 있는 타임라인의 역할로써 활용된다. 대표적으로 비트코인 블록체인을 이용한 공증 서비스가 있다. 공증하고 싶은 문서나 메시지의 hash값을 비트코인 주소형태로 바꾸거나 이러한 목적을 위해 스크립트에서 주로 사용되는 OP_Return과 같은 명령어와 함께 포함시켜 실제 비트코인 거래를 발생되게 하고 이 거래가 블록체인에 포함되기를 기다린다. 한번 거래가 블록체인에 포함되면 거래를 만든 시점에 거래에 포함된 hash값에 해당하는 문서나 메시지가 있었음을 인터넷의 Bitcoin network 노드들에 의해 확인을 받은 셈이 된다. 또한 인터넷을 통하여 이러한 공증 사실을 언제든지 검증할 수 있다.

5.2 Sidechains

비트코인 블록체인만으로는 해결할 수 없는 문제들은 비트코인과는 다른 특성을 가지는 블록체인을 기반으로 한 암호화폐들을 이용하여 해결한다. 이렇듯 비트코인 블록체인과 비슷하지만 자신들만의 특성을 가진 독립된 블록체인들을 altchain이라고 부른다. Altchain들은 새로운 기능을 제공할 수 있지만, 비트코인과는 다른 특성을 부여하는 과정에서 비트코인이 가지고 있던 보안적 장점을 놓칠 수도 있고, 비트코인 블록체인과 분리되어 동작하기 때문에 비트코인보다도 가격 변동성이 크다는 문제점들을 가지고 있다. 이러한 문제들을 해결하고자 최근 Pegged Sidechains이라는 비트코인 블록체인과 altchain들을 상호 연동하게 할 수 있는 기법[16]이 제안되어 주목을 받고 있다. Pegged Sidechain에서는 서로 다른 블록체인 또는 altchain 사이에서 코인을 안전하게 주고 받을 수 있게 한다. 즉 비트코인 블록체인의 비트코인을 다른 althchain으로 옮겨서 사용하다가 사용이 끝나면 다시 비트코인으로 바꾸어 사용할 수 있게 되는 셈이다. 특히 altchain마다 제공하는 기능이 다르므로 비트코인 블록체인에서 특정 기능이 필요 경우 해당 기능을 사용할 수 있는 altchain에서 해당 혜택을 이용하다가 이용이 끝나면 다시 블록체인으로 돌아올 수 있게 되는 셈이다. 따라서 Darkcoin과 같이 비트코인에서 미비한 보안 서비스를 별도의 altchain으로 구성

할 뿐만이 아니라 이들 사이의 상호연동이 가능하게 됨으로써 비트코인을 이용한 서비스의 제한을 풀어버리는 또 하나의 가능성을 열게 되었다.

6. 결 론

구텐베르크의 인쇄술이 단순히 지식이 보존의 발달에서 그치는 것이 아니라 지식의 생성 과정에 대한 혁신을 가져왔듯이, 비트코인의 단순히 자동화된 디지털 화폐가 아니라 자산 형태의 전달 미디어의 역할로 발전할 수 있을 것으로 예상된다. 하지만 이러한 비트코인의 가능성을 북돋기 위해서는 비트코인의 다양한 측면에 대한 전방위적인 보안성 고려가 선행되어야 할 것이다. IT와 금융을 모두 아우르고 있는 비트코인 생태계의 특성을 바탕으로 폭넓으면서도 심도있는 보안 분석과 연구가 필요한 시점이다.

참 고 문 헌

[1] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2009, https://www.bitcoin.org/bitcoin.pdf.

[2] A. M. Antonopoulos, Mastering Bitcoin, O'Reilly Media, 2014

[3] I. Eyal and E. G. Sirer, "Majority is not Enough: Bitcoin Mining is Vulnerable," arXiv, 2013

[4] D. Ron and A. Shamir, "Quantitative Analysis of the Full Bitcoin Transaction Graph," in Proc of Financial Cryptography and Data Security, 2013

[5] D. Ron and A. Shamir, "How Did Dread Pirate Roberts Acquire and Protect His Bitcoin Wealth?" in Proc of the 1st Workshop on Bitcoin Research, 2014

[6] E. Androulaki, G. Karame, M. Roeschlin, T. Scherer and S. Capkun, "Evaluating User Privacy in Bitcoin," in Proc of Financial Cryptography and Data Security, 2013

[7] M. Möser, Ra. Böhme and D. Breuker, "Towards Risk Scoring of Bitcoin Transactions," in Proc of the 1st Workshop on Bitcoin Research, 2014.

[8] I. Miers, C. Garman, M. Green, and A. D. Rubin, "Zerocoin: Anonymous Distributed E-Cash from Bitcoin," in Proc of the IEEE Symposium on Security and Privacy, pp. 397–411, 2013

[9] E. Ben-Sasson, A. Chiesa, C. Garman, M. Green, I. Miers, E. Tromer, and M. Virza. "Zerocash: Decentralized anonymous payments from Bitcoin." In Proc of the IEEE Symposium on Security and Privacy. 2014.

[10] E. Duffield, and . Hagen. "Darkcoin: Peer-to-Peer Currency with Anonymous Blockchain Transactions and an Improved Proof-of-Work System," https://www.darkcoin.io/downloads/DarkcoinWhitepaper.pdf, 2014.

[11] Bitcoin Contracts, https://en.bitcoin.it/wiki/Contracts

[12] M. Andrychowicz, S. Dziembowski, D. Malinowski, and Ł. Mazurek, "Secure Multiparty Computations on BitCoin." In Proc of the IEEE Symposium on Security and Privacy. 2014.

[13] M. Andrychowicz, S. Dziembowski, D. Malinowski, and Ł. Mazurek, "Modeling Bitcoin Contracts by Timed Automata," arXiv.org. 2014.

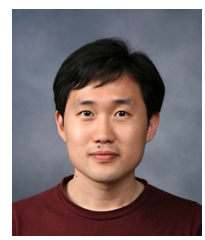
[14] Bitcoin Developer Documentation, https://bitcoin.org/en/developer-documentation

[15] CVE-2010-5139, https://en.bitcoin.it/wiki/CVE-2010-5139

[16] A. Back, M. Corallo, L. Dashjr, M. Friedenbach, G. Maxwell, A. Miller, A. Poelstra, J. Timón, and P. Wuille, "Enabling Blockchain Innovations with Pegged

Sidechains," http://www.blockstream.com/sidechains.pdf, 2014

저 자 약 력



이 종 협

이메일 : jhlee@ut.ac.kr

- 2009년 8월 연세대학교 컴퓨터과학과 졸업 (공학박사)
- 2009년 9월~2012년 2월 Carnegie Mellon, CyLab 연구소 (박사후연구원)
- 2012년 3월~현재 한국교통대학교 소프트웨어학과 조교수
- 관심분야 : 금융 보안, 소프트웨어 보안