순환 신경망을 활용한 양자 내성 암호화폐 가격 예측

김현지*, 임세진**, 강예준**, 김원웅**, 서화정*
*한성대학교 IT융합공학과
**한성대학교 컴퓨터공학과
khj1594012@gmail.com, dlatpwls834@gmail.com, etus1211@gmail.com,
dnjsdndeeee@gmail.com, hwajeong84@gmail.com

Prediction of the price of quantum-resistant cryptocurrency using recurrent neural network

Hyun-Ji Kim*, Se-Jin Lim**, Yea-Jun Kang**, Won-Woong Kim**, Hwa-Jeong Seo*
*Dept. of IT Convergence Engineering, Hansung University
**Dept. of Computer Engineering, Hansung University

요 약

양자 알고리즘인 그루버나 쇼어 알고리즘에 의해 현존하는 암호 체계들이 무너질 수 있으며, 블록체인 네트워크를 기반으로 타원곡선 암호 및 타원곡선 전자서명을 사용하는 암호화폐의 안전성 또한 위협받고 있다. 따라서 암호화폐에도 양자 컴퓨터에 대한 대응책이 필요하다. 본 논문에서는 시계열 예측에 적합한 순환형 신경망을 활용하여 양자 저항성을 가지는 암호화폐들의 가격을 예측하고 분석한다. 데이터가 부족하였으나 학습 결과 0.005 이하의 손실을 달성하였으며, 최근 15일의 데이터를 통해 예측한 결과, 모두 소폭 상승할 것으로 나타났다. 향후에는 더 많은 데이터를 통해 더 정확한 예측이 가능한 신경망을 설계하고 다양한 양자 관련 이슈들을 참고하여 분석을 수행하고자 한다.

1. 서론

양자컴퓨터의 시대가 다가옴에 따라 암호알고리즘의 안전성이 위협받고 있다. 양자 알고리즘인 그루버 알고리즘 또는 쇼어 알고리즘을 활용한 공격을 통해 기존의 암호 체계를 붕괴시킬 수 있으며, 이를 대비하여 현재 사용되고 있는 암호 알고리즘을 교체해야 한다. 이러한 공격에 안전하도록 양자 컴퓨터로도 풀기 어려운 수학적 난제들에 기반한 양자 내성 암호들이 연구되고 있으며, 양자 내성 암호를 활용한 블록체인과 이를 기반으로 하는 암호화폐들도 등장하고 있다.

2. 관련연구

2.1 양자컴퓨터

양자 컴퓨터는 고전적인 비트와 게이트 대신 양자 역학의 중첩과 얽힘 원리를 활용한 큐비트와 양자 게이트를 사용하여 연산한다. 큐비트는 기존 비트와 같은 역할을 하지만 중첩 상태를 통해 측정하기 전까지 모든 값이 확률로 존재하여 0과 1의 상태를 동시에 가지며 연산할 수 있으므로 고전 컴퓨터로는 해결하기 어려운 문제도 빠른 속도로 풀어낼 수 있다. 따라서 고전 컴퓨터로는 풀어내기 어려운 암호 알고리즘 또한 양자 컴퓨터에 의해 무너질 수 있다. 대표적인 양자 알고리즘으로는 그루버 알고리즘 및 쇼어 알고리즘이 존재한다.

그루버 알고리즘의 경우 n-bit 안전성을 갖는 대칭키 알고리즘을 $\sqrt{n}$-bit로 떨어뜨릴 수 있다. 따라서 2배의 키 길이를 갖는 대칭키 암호 알고리즘을 사용해야한다. 쇼어 알고리즘은 큰 정수의 소인수 분해 문제를 해결할 때 필요한 주기 찾기 문제를 효율적으로 풀어낼 수 있으므로 소인수 문제 및 이산대수 문제에 기반하는 공개키 알고리즘인 RSA, ECC (Elliptic Curve Cryptography) 체계가 무너질 수 있다.

2.2 양자 저항 암호화폐

블록체인 네트워크를 기반으로 하는 암호화폐도 암호 알고리즘이 사용되므로 양자컴퓨터의 위협이 존재한다. 비트코인의 경우, 타원곡선 암호를 통한 개인키 생성, 타원곡선 전자서명과 개인키를 통해 트랜잭션에 대한 전자서명을 수행한다. 그러나 타원곡선 전자서명은 쇼어 알고리즘에 의해 해결될 수 있다. 따라서 암호화폐에도

양자 컴퓨터에 대한 대응책이 필요하며, 다음과 같이 양자 저항성을 가진 암호화폐들이 출시되고 있다.

2.2.1 Byteball (Gbyte) [1]

비트코인과 같은 기존 암호화폐들의 경우 블록체인 네트워크를 기반으로 하여 작업증명 알고리즘을 통해 채굴을 진행한다. 그러나 Byteball은 블록체인 네트워크를 활용하지 않으므로 채굴과정이 없다. 그 대신에 3세대 블록체인이라고도 불리며 비가역적 일방향성의 특징을 갖는 방향성 비순환 그래프(Directed Acyclic Graph)를 사용한다. 기존 블록체인이 블록을 생성하여 블록체인 네트워크를 구성하듯이, DAG의 유닛(블록)들이 비순환적이며 무작위형태로 생성된다. 각 유닛들은 모두 협력 관계에 있으므로 거래가 발생하는 즉시 각 유닛에서 다른 유닛들에 대한 검증을 수행한다. 즉, DAG 기반의 암호화폐에서는 블록 형성 과정이 없고 채굴이 존재하지 않는다. 또한, Byteball은 생성된 유닛이 부모 유닛과 부모 유닛의 조상 유닛까지 순차적으로 확인하므로, 하나의 유닛의 내용을 변경하기 위해서는 그 조상 유닛까지 모두 변경해야한다. 따라서 DAG 기반의 코인은 안전성이 높으며 트랜잭션 처리 속도 및 채굴을 위한 자원 소모까지 감소시킬 수 있다.

2.2.2 Quantum Resistant Ledger (QRL) [2]

QRL은 양자 컴퓨터에 대한 보안성을 핵심으로 한 양자 내성 암호화폐이다. 이를 위해 양자 내성 암호 중 Lamport 및 Winternitz 일회성 해시 기반 암호 및 XMSS (Extended Merkle Signature Scheme)를 사용한다. 일회성 해시 기반 암호는 하나의 서명만 가능하지만 QRL의 경우 머클트리를 활용한다. 머클루트가 생성될 때까지 여러 개의 키 쌍 중 공개키 해싱을 반복하여 더 큰 구조로 결합시켜 일회성을 극복할 수 있다.

2.2.3 Nexus (NXS) [3]

Nexus는 571-bit 개인키와 1024-bit 해시 알고리즘(Skein과 Keccak을 결합)을 사용하여 양자 저항성을 가진다. 256-bit 키를 사용하는 비트코인보다 더 긴 키 길이를 사용하여 안전하고, 양자컴퓨터를 이용하여 지갑 주소로부터 공개키를 알아내기까지 계산 상 1000억년이 걸린다고 한다. 또한, 작업 증명 채널로 프라임 채널과 해싱 채널을 사용하고 지분 증명을 위해 홀딩 채널을 사용하므로 기존의 블록체인에 비해 보다 더 탈중앙화 된 형태이다. 그러나 키 및 해시 크기가 기존보다 훨씬 큰 1024-bit를 사용하므로 다양한 하드웨어에서 수용하기는 어렵다.

2.2.4 HyperCash (HC) [4]

양자 저항성을 가진 암호화폐의 종류 중 하나로 원래는 HCash였으며 현재는 HyperCash로 변경되었다. HCash는 작은 공개키 및 서명크기를 가진 효율적인 양자 내성 서명 체계인 BLISS와 MSS/LMS를 통합하였다. 또한, BLISS에 대한 부채널 공격 대응책을 마련하여 부채널 공격 및 51% 공격에 대해 더 안전하다. 그러나 HCash가 사라지고 HyperCash가 된 후, 블록체인과 방향성 비순환 그래프 둘 다를 기반으로 할 수 있으며 정보 공유 또한 자유롭다. 또한, 작업증명(Proof of Work)과 지분증명(Proof of Stake)를 결합하여 시스템의 전반적인 보안을 강화할 수 있다. 현재는 양자 내성이 아니지만 OpenSSL과 함께 동작하는 Ring-LWE 키 교환 프로토콜을 개발하여 양자 저항 암호화폐로 나아갈 계획임을 밝혔다.

2.2.5 Cellframe (CELL) [5]

NIST의 양자 내성 암호 공모전에 출전한 서명 알고리즘들을 몇 가지 구현한 양자 내성 암호화폐이다. 처음에는 NewHope, NTRU, Frodo, SIDH 등의 알고리즘을 사용하였으며, 현재는 Zero Knowledge Post Quantum 서명인 Picnic에 초점을 두고 있다. 기본적으로 Crystal-Dilithium 디지털 서명을 사용하며, 두 개 이상의 서명 알고리즘을 조합하여 사용할 수 있다. 서로 다른 서명 알고리즘을 사용하여 네트워크 간의 연결 고리가 될 수 있고, 하나 이상의 키를 사용하므로 더 안전한 거래가 가능하다. 2022년 3분기에 양자 키 교환 알고리즘 구현할 예정이며 2021년에는 또 다른 양자 내성 서명 알고리즘들을 적용할 계획이다.

2.3 순환 신경망 (Recurrent Neural Network) [6]

순환 신경망은 시간에 따라 변화하는 시계열 데이터 학습에 적합한 인공신경망의 종류이다. 네트워크 내부에 상태를 저장하고 과거의 데이터를 참조할 수 있으므로 과거와 현재의 종속 관계를 분석하여 예측할 수 있다. 그러나 기울기 소실로 인해 거리가 먼 데이터 간에는 종속성을 확보할 수 없는 장기종속성 문제가 있고, 이를 보완하기 위한 다양한 순환 신경망 구조가 존재한다. Simple RNN, LSTM (Long Short Term Memory), GRU (Gated Recurrent Unit) 등의 모델이 있으며, 시계열 데이터 예측, 언어 번역, 음성 인식, 이미지 캡셔닝, 비디오 분석과 같은 분야에 활용된다.

3. 시스템 제안

본 논문은 양자 저항성을 가지는 5개의 암호화폐들에 대해 학습한 후, 가격을 예측하는 것을 목표로 한다.

3.1 데이터 수집 및 구성

학습에 필요한 데이터는 암호화폐 거래소로부터 수집한다. '코인마켓캡'으로부터 과거 데이터를 수집하였다. 각 화폐마다 해당 거래소의 거래시작일로부터 현재 시점까지의 데이터를 수집하였으며, 암호화폐 별로 거래 시작일이 다르므로 수집한 데이터의 수는 다르다. 양자내성 코인들은 보통 2015년, 2018년 또는 2021년부터 거래되어서 기존 코인들에 비해 상대적으로 적은 데이터를 확보하였으며, 더 정확한 예측을 위해서는 더 많은 데이터가 필요하다. 각 데이터 셋은 한 행에 1일 단위이며, Fig 1의 예시와 같이 총 4개의 특징(시작 가격, 가장 높은 가격, 가장 낮은 가격, 종료 가격)으로 구성된다. 또한, 각 데이터들은 학습을 위해 MinMaxScaler를 사용하여 0~1 사이 값으로 정규화한다.

Open	High	Low	Close
0.72	0.74	0.57	0.67
0.67	0.76	0.47	0.71
0.66	1.46	0.66	1.36

Fig 1. Dataset of QRL

3.2 순환 신경망 구성

시계열 데이터를 학습하고 다음 날의 가격을 예측하기 위해서 many to one 형태의 순환 신경망을 구성한다. 순환 신경망 중 장기 종속성 문제를 보완한 LSTM을 사용하였으므로 시퀀스 길이를 n으로 설정하여 n개의 샘플을 가지고 과거의 데이터들을 반영할 수 있다. 또한, 각 데이터들은 4개의 특징을 가지므로 입력 데이터 형태를 (시퀀스 길이,4)로 지정해준다. 여러 암호화폐에 대해 충분한 성능을 달성하도록 구성한 신경망은 Fig 2와 같이 2개의 LSTM 레이어(각 units = 32, 64)와 출력 레이어로 Fully-Connected(units = 1)를 사용하였다. 손실함수는 'mean squared error'를 사용하였고, 최적화 함수로는 일반화성능이 좋은 Adam(학습률 0.01)을 사용하였다. 이 외에도 시퀀스 길이를 설정해야하는데 해당 부분은 4장에서 실험을 통해 언급하도록 한다.

Layer (type)	Output Shape	Param #
input_7 (InputLayer)	[(None, 7, 4)]	0
lstm_12 (LSTM)	(None, 7, 32)	4736
lstm_13 (LSTM)	(None, 64)	24832
dense_6 (Dense)	(None, 1)	65

Fig 2. Architecture of Neural Network in this work

4. 실험 및 평가

본 실험에서는 Intel Xeon CPU (25GB RAM)과 Nvidia GPU (25GB RAM)를 지원하는 클라우드 기반 서비스인 Google Colaboratory를 사용하였고, 프로그래밍 환경으로는 Python 3.7.11 및 Tensorflow 2.6.0을 사용하였다.

4.1 학습 결과

3.1절과 같은 데이터를 활용하여 학습을 진행하였다. 또한, 3.2절에 언급하였듯이 적절한 신경망 구성을 위해 시퀀스 길이를 설정해주어야 한다. 데이터 셋의 한 행은 하루에 대한 정보를 나타내므로 시퀀스 길이를 7로 설정할 경우, 최근 일주일의 데이터를 반영할 수 있다. 거래 시작 시점이 최근이어서 데이터가 적은 암호화폐의 경우, 더 많은 과거데이터들을 반영하도록 시퀀스 길이를 설정할 경우 손실 값이 감소하는 것을 알 수 있었다. 그러나 시퀀스 길이가 길면 무조건 좋은 성능을 달성할 수 있는 것은 아닐 뿐만 아니라 시퀀스 길이가 길어질수록 학습에 소요되는 시간이 늘어난다. 따라서, 적절한 시퀀스 길이를 설정해주어야 한다. Table 1은 해당 시퀀스 길이를 7일, 15일, 30일로 설정하여 비교한 결과이다. 총 5개의 암호화폐 중 4개인 Gbyte, QRL, HyperCash, CELLframe은 시퀀스 길이를 15로 하였을 때, 검증데이터 기준으로 가장 좋은 성능을 보였다. 따라서 해당 신경망의 시퀀스 길이는 15로 설정하였다. 이와 같이 설정된 네트워크로 실험한 결과 대부분의 암호화폐 데이터 셋의 학습 및 검증 데이터에 대해 0.005 이하의 손실을 달성하였다.

Table 1. Training (T) /validation (V) loss according to the sequence length (column : sequence length)

		7	15	30
Gbyte	T	0.0013	0.0012	0.0012
	V	2.6540e-04	**1.6496e-04**	1.7065e-04
QRL	T	5.9681e-04	3.7292e-04	3.3954e-04
	V	0.0012	**0.0011**	0.0013
NXS	T	2.2884e-04	2.1974e-04	2.0530e-04
	V	**1.9091e-05**	5.5147e-05	6.7026e-05
HC	T	4.8330e-04	3.1832e-04	2.6332e-04
	V	0.0016	**0.0012**	0.0013
CELL	T	0.0047	0.0029	0.0024
	V	0.0057	**0.0048**	0.0064

4.2 가격 예측 결과

Table 2는 훈련된 신경망을 통해 시퀀스 길이에 해당하는 가장 최근의 15일의 데이터(학습에 사용하지 않은 테스트 데이터)로 각 암호화폐의 가격을 예측한 결과이다. 해당 데이터들은 정규화 되었으므로 예측 결과 또한 정규화 된 상태이다. 따라서 역정규화를 통해 실제 예측 가격을 계산하였다.

Table 2. Results of tomorrow's price prediction for each cryptocurrency (Average price, units : USD)

	Current Price	Tomorrow Price (Prediction)
GByte	23.75	24.26
QRL	0.16	0.18
NXS	0.51	0.55
HC	0.69	0.72
CELL	1.03	1.08

Table 3은 대상 암호화폐들을 네트워크 구조, 작업 증명, 사용되는 암호 알고리즘에 대해 정리한 표이다. 이 중, NIST 공모전 finalist인 알고리즘은 NTRU, Crystal-Dilithium이며, Picnic은 alternate이다[7]. HyperCash (HC)의 경우 Ring-LWE 기반의 키 교환 알고리즘을 도입할 예정인데, NTRU가 Ring-LWE 기반의 알고리즘이며, 이 외에도 LWE 기반의 암호들이 다수 진출한 상태이다. 또한 앞서 언급하였듯이 기존의 블록체인 형태가 아닌 방향성 비순환 그래프를 사용하는 Gbyte는 양자 저항성을 가지며, Stein과 Keccak을 결합한 해시 기반의 Nexus(NXS) 또한 1024-bit의 해시를 사용하므로 양자 저항성을 가진다. 이처럼 양자 저항성을 가지는 암호화폐들은 평균 5%의 증가율 (최소 2%, 최대 12%)을 보이며 전반적으로 작은 폭으로 가격이 증가할 것으로 예측되었다.

Table 3. Details of quantum resistant cryptocurrencies

	Architecture	Proof of Work	Cryptographic Algorithm
Gbyte	DAG	-	-
QRL	Block Chain	PoW	Lamport and Winternitz one-time signatures, XMSS
NXS	Block Chain	Hybrid PoW &nPoS	Skein + Keccak (1024-bit)
HC	Block Chain /DAG	PoW +PoS	**Ring-LWE** key exchange (예정)
CELL	Block Chain	PoW	NewHope, **NTRU**, Frodo, SIDH, **Picnic**, **Crystal-Dilithium**

5. 결론

본 논문에서는 순환 신경망을 통해 양자 저항성을 가지는 암호화폐들의 가격을 예측하였다. 학습 대상인 5개의 양자 내성 암호화폐들은 네트워크 구조 또는 사용되는 암호 알고리즘을 통해 양자 저항성을 확보하였다. NIST의 양자 내성 암호 공모전에서 finalist, alternate에 진출한 암호 알고리즘들이 적용되었으며, 해시함수의 경우 더 긴 키 길이를 통해 안전성을 보장하도록 하였다.

일반적으로 신경망은 많은 데이터를 기반으로 훈련할 때 더 좋은 성능을 보이지만 양자 저항 암호화폐의 경우 비교적 최근 거래가 시작되어 데이터가 부족한 한계점이 있었다. 훈련된 신경망을 통해 가격을 예측한 결과 모두 소폭 상승할 것으로 나타났다.

향후에는 더 많은 데이터를 기반으로 더 정확한 예측이 가능한 신경망을 설계하고, 양자 컴퓨터 개발 현황 및 계획이나 양자 내성 암호 공모전 결과 등과 같은 이슈들과 관련하여 분석하고자 한다.

6. Acknowledgment

이 논문은 부분적으로 2021년도 정부(과학기술정보통신부)의 재원으로 정보통신기술진흥센터의 지원을 받아 수행된 연구임(No.2018-0-00264, IoT 융합형 블록체인 플랫폼 보안 원천 기술 연구, 50%) 그리고 부분적으로 2021년도 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(No. NRF-2020R1F1A1048478, 50%).

참고문헌

[1] Churyumov, Anton. "Byteball: A decentralized system for storage and transfer of value." URL https://byteball. org/Byteball. pdf (2016).

[2] Peter Waterland, “Quantum Resistant Ledger (QRL)”, 2016. 11.

[3] Nexus: A Peer-to-Peer Network [Internet] Available:http://media.abnnewswire.net/media/en/docs/93416-Nexus_WhitePaper.pdf

[4] Hcash: The New Standard of Value [Internet] Available:https://h.cash/themes/en/images/Hcash+Whitepaper+V0.8.5.pdf

[5] Cellframe [Internet] Available: https://cellframe.net/CllfrmWPbeta.pdf

[6] Connor, Jerome T., R. Douglas Martin, and Les E. Atlas. "Recurrent neural networks and robust time series prediction." IEEE transactions on neural networks 5.2 (1994): 240-254.

[7]https://csrc.nist.gov/projects/post-quantum-cryptography/round-3-submissions