

## | 목차 |

지은이 소개 .....	5
들어가며 .....	13

### 1부 — 비트코인과 블록체인의 개괄

<b>1장</b>	<b>비트코인의 탄생 .....</b>	<b>21</b>
	1.1 비트코인 논문 .....	22
	1.2 블록과 체인 .....	25
	1.3 비트코인의 단위와 거래 방식 .....	27
	1.3.1 비트코인의 단위 종류 .....	27
	1.3.2 비트코인 최대 매장량: 2,100만 BTC .....	29
	1.4 비트코인은 왜 만들었을까? .....	33
	1.4.1 데이비드 차움과 추적이 불가능한 거래 시스템 .....	34
	1.4.2 사이퍼펑크 .....	35
	1.4.3 비트코인을 만든 목적 .....	37
	1.5 지급 결제 시스템 .....	39
	1.6 암호화폐는 아무나 발행해도 되나? .....	41
	1.6.1 암호화폐라는 명칭의 적절성 .....	42
	1.7 암호화폐 개수 .....	43
	1.7.1 전체 암호자산 중 비트코인의 비중 .....	44

<b>2장</b>	<b>블록체인과 관련된 용어</b>	<b>47</b>
2.1	기본 용어 정리	47
2.1.1	노드와 피어	47
2.1.2	일의 분산 대 일의 중복	48
2.1.3	브로드캐스팅	51
2.1.4	암호화폐, 가상화폐, 거래소 등	52
2.1.5	트랜잭션	53
2.1.6	채굴	54
2.1.7	지갑 소프트웨어	54
2.1.8	수수료	60
2.2	블록체인의 정의	64
2.2.1	비트코인 블록체인의 정의	65
2.2.2	블록체인의 기능적 관점의 정의	67
<b>3장</b>	<b>블록체인을 이루는 기반 기술</b>	<b>69</b>
3.1	해시함수	69
3.1.1	암호화 해시	70
3.1.2	SHA-256과 해시 퍼즐	72
3.1.3	암호화 해시의 응용	75
3.1.4	블록체인에서의 암호화 해시함수 활용	76
3.2	암호화 기법	80
3.2.1	비대칭 암호화 기법	83
3.2.2	블록체인에서의 전자서명과 비대칭 암호화 기법	88
3.3	해시 퍼즐	89
3.3.1	작업증명	89
3.3.2	비트코인 장부	90
3.3.3	해시 퍼즐	91

<b>4장</b>	<b>블록체인의 작동 원리</b>	<b>101</b>
4.1	누가 기록할 것인가?	103
4.1.1	브로드캐스팅을 통한 전달	103
4.1.2	리더 선출 - 누가 기록할 것인가?	106
4.2	어떻게 저장할 것인가?	108
4.2.1	신뢰의 부재 - 모든 노드의 검증	108
4.3	비동기화 시스템에서의 탈중앙화 합의	112
4.3.1	서로 다른 진실의 충돌	114
4.3.2	서로 다른 진실의 통일 - 탈중앙화 합의	116
4.3.3	거래의 안전성 - 확인	117
4.4	이중사용	120
4.4.1	블록체인 실험 - 이중사용의 방지	123
4.5	소프트포크와 하드포크 - 유지보수의 악몽	124
4.5.1	과거에는 무효하던 규칙을 유효화 - 하드포크	127
4.5.2	과거에는 유효하던 규칙을 무효화 - 소프트포크	129
4.5.3	세그윗과 세그윗 2X	132
4.5	채굴의 독점	134
4.6	51% 공격	137
<b>5장</b>	<b>블록체인의 변형</b>	<b>141</b>
5.1	이더리움과 스마트 컨트랙트	141
5.1.1	스마트 컨트랙트	143
5.1.2	암호화폐와 토큰	147
5.1.3	블록체인에 관한 닉 사보의 평가	150
5.2	하이퍼레저와 프라이빗 블록체인	151
5.2.1	하이퍼레저 패브릭	152
5.3	지분증명 등 그 밖의 변형	155
5.3.1	지분증명	155
5.3.2	그 밖의 변형	157
5.4	비잔틴 장군 문제	157

## 2부 — 암호화폐와 금융 그리고 블록체인의 미래

<b>6장</b>	<b>화폐와 비트코인</b>	<b>163</b>
6.1	금과 달러	164
6.1.1	금	164
6.1.2	세계 최초의 지폐 - 은 보관증	165
6.1.3	금본위 달러 - 금 보관증	166
6.1.4	종이 달러 - 명목화폐의 시작	171
6.1.5	현대통화이론	172
6.1.6	돌 화폐의 섬	173
6.1.7	종이돈의 위험 - 초인플레이션	175
6.2	화폐의 조건	176
6.2.1	교환의 기능	177
6.2.2	가치 척도의 기능	179
6.2.3	가치 저장의 기능	179
6.2.4	사용의 편의성	180
6.2.5	화폐로서의 비트코인	181
6.3	투자와 투기	182
6.3.1	철저한 분석	182
6.3.2	원금의 안전성 보장	185
<b>7장</b>	<b>블록체인과 미신</b>	<b>190</b>
7.1	목적과 수단 - 탈중앙화의 비용	191
7.2	블록체인으로는 절대 수수료를 낮출 수 없다	193
7.2.1	중재와 중계	193
7.2.2	블록체인과 직거래	195
7.3	블록체인은 데이터베이스가 아니다	198
7.3.1	진실의 무게	198
7.4	블록체인은 보안 도구가 아니다	201
7.5	탈중앙화의 실체	203

7.5.1	The DAO 사건	204
7.5.2	그 누구도 ‘개입’되지 않는 시스템이란 존재할 수 없다	208
7.5.3	탈중앙화와 통제 불능	208
7.6	시중의 블록체인 프로젝트 사례	210
7.6.1	뱅크 사인	210
7.6.2	K생명의 소액 보험금 지급 시스템	211
7.6.3	호주의 전력 직거래	212
7.6.4	사례를 통해 본 프로젝트의 핵심	212
<b>8장</b>	<b>암호화폐와 시세조종</b>	<b>214</b>
8.1	암호화폐 중개소	215
8.1.1	중개소의 숫자 놀음 - 오프체인 거래	217
8.1.2	중개소와 시세조종	219
8.2	매매 회전을	224
8.3	중개소의 해킹	225
8.3.1	암호화폐 지갑에는 암호화폐가 없다	227
8.4	비트코인과 자금세탁	228
8.4.1	비트코인과 세금 회피	231
8.5	다크코인 - 자금세탁의 진화	232
8.5.1	자금세탁의 추적	234
8.6	FATF와 가상자산	236
8.6.1	특정금융거래 정보의 보고 및 이용 등에 관한 법률	237
8.6.2	가상자산 규제에 대한 각국 동향	240
<b>9장</b>	<b>디지털 자산</b>	<b>242</b>
9.1	디지털화 자산	242
9.1.1	자산 유동화 증권과 자산 유동화 토큰	243
9.2	디지털 자산	246
9.2.1	디지털 자산의 가치	247
9.2.2	가상자산의 실체와 사적 자치	250

9.3 ICO .....	251
9.3.1 ICO의 진화 - IEO와 STO .....	254
9.4 발행시장과 유통시장의 분리 .....	255
9.5 스테이블 코인 - 테더와 리브라 .....	256
9.5.1 테더 .....	257
9.5.2 페이스북 리브라 .....	258
9.6 CBDC .....	261
9.7 진정한 디지털 자산 .....	263
9.7.1 디지털 자산이 가져야 할 속성 .....	264
9.8 결론 .....	265
<b>부록 1 비트코인 블록의 구조 .....</b>	<b>268</b>
<b>부록 2 해시 퍼즐 개념 설명 .....</b>	<b>278</b>
<b>부록 3 비트코인 주소 .....</b>	<b>284</b>
<b>부록 4 트랜잭션 스크립트 .....</b>	<b>290</b>
참고문헌 .....	306
찾아보기 .....	308

## | 들어가며 |

이 책의 1판인 『비트코인과 블록체인, 탐욕이 삼켜버린 기술』을 쓸 당시인 2017년 말, 비트코인은 전대미문의 광풍 속에서 2천 5백여만 원 이상으로 치솟았다가 이후 가파르게 하락해 한때 3백만 원대까지 곤두박질치기도 했다. 그 광풍은 이제 다소 수그러들었지만 2판의 증쇄본을 교정하고 있는 2021년 4월 현재 그 정점인 8천만 원을 기록했다가 다시 가파르게 폭락해 5천만 원대로 떨어지고 있다.

비트코인을 둘러싼 현상을 한마디로 설명하기는 힘들다. 금속 덩어리에 불과한 금을 향한 인류의 집착이나 미술품 등에 천문화적인 가치가 형성되는 것을 생각해보면 비트코인을 둘러싼 현상을 단지 그들만의 광풍으로 치부하기에는 부족해 보인다.

2021년 4월 23일을 기점으로 살펴보면 전 세계 암호화폐 증개소는 수만 개가 되지만 그 중 370여 개 정도만 어느 정도 실거래가 일어나고 있으며, 이들 증개소에서 거래되는 암호화폐 종류는 무려 9,434개에 이른다.<sup>1</sup> 국내에는 최소 100여 개 이상의 증개소가 있는 것으로 추정되는데, 매매 대행업체까지 포함하면 그 수는 훨씬 더 많을 것이다. 통계로 보면 전 세계적으로 증개소는 하루 20개 이상 새로 생겨나고, 이들이 취급하는 암호화폐 수는 하루 5개 정도 늘어나는 셈이다.<sup>2</sup> 이렇듯 암호화폐와 이를 취급하는 증개소가 기하급수적으로 늘어나는 이유는 암호화폐를 만드는 데 필요한 기술 장벽이 낮기 때문이다. 한마디로 쉽게 돈벌이가 되는 것에 비해 별다른 기술이 필요 없기 때문이다.

역시 2021년 4월 기준 지구상에서 하루 300조 원 이상, 국내에는 약 15~20조 원대의 거래가 이뤄지는 것으로 추정된다. 2018년 초 국내 암호화폐 거래가 하루 10조 원대로 정

---

1 [www.coinmarketcap.com](http://www.coinmarketcap.com) 2021년 4월 23일 기준

2 후속 장에서 살펴보겠지만, 코인의 전 단계라 할 수 있는 소위 '토큰'은 하루 최소 수백 개씩 늘어난다.

점을 찍다가 다시 1조 원대로 전에 비해 1/10으로 줄어들었으나, 2021년 또 다시 광풍이 불면서 이제는 2018년 광풍의 두 배인 20조 원을 육박하고 있다. 그러나 이 거래 중 대다수는 시세조종을 위한 가장거래라는 분석이 있으며, 세계적으로 여러 중개소가 자국에서 시세조종 혐의로 재판 중이다. 특히 가장매매<sup>3</sup>가 업계에 만연하고 있는 것은 공공연한 비밀이기도 하다.

많은 사람들이 블록체인과 암호화폐의 실체를 크게 오해하고 있는 가장 큰 원인은 제대로 된 정보를 접하기 어렵기 때문이다. 대학 교수들까지 포함된 가짜 전문가들과 금전적 이득을 노리는 끈들이 거짓되고 부풀려진 영터리 지식을 꾸준히 전파하고 있으며 이런 왜곡된 정보는 아무런 여과 없이 받아쓰기 언론을 통해 대중에게 깊숙이 번져 나가고 있다.

한편, 과학기술정보통신부는 2018년 블록체인 활성화라는 명목으로 5천 566억 원이라는 막대한 규모의 예비 타당성 조사를 신청했다가 한국과학기술평가원<sup>KISTEP</sup>에 의해 사업목표의 구체성이 떨어지고 '핵심원천기술의 실체가 불명확하다'는 사유로 기준점 이하의 점수를 받아 보류되기도 했다. 과학기술정보통신부는 이 계획을 일부 수정해 2021년부터 2025년까지 5년 동안 총 4천억 원 규모의 국비를 투자하는 '블록체인 R&D 연구사업'에 관한 예비 타당성 조사를 준비 중에 있는 것으로 알려졌다. 그런데 그 전에 과학기술정보통신부 공식 블로그에 있는 그릇된 내용부터 수정해야 할 듯하다. 공식 블로그에는 블록체인을 다음과 같이 엉뚱하게 설명하고 있다.<sup>4</sup>

“사토시 나카모토라는 일본 개발자가 중앙집권화된 금융 시스템의 위험을 감지하고 블록체인이라는 기술을 적용해 개발한 암호화폐로서 세계 100대 화폐 안에 들어갈 정도로 눈부신 성장을 했다.”

사토시 나카모토는 가명이며 개인이 아닌 집단을 지칭하고 일본과는 아무런 관련이

3 거짓 거래를 통해 거래량을 부풀리고 가격을 조종하는 행위

4 [https://blog.naver.com/with\\_msip/221526233898](https://blog.naver.com/with_msip/221526233898)



없다. 또한 금융 시스템의 위험을 감지하고 암호화폐를 만들었다(?)는 소설 같은 정보는 어디서 가져온 것인지 알 길이 없다. 무엇보다 비트코인은 화폐가 아닌데 세계 100대(?) 화폐라는 엉뚱한 주장은 황당하기까지 하다. 2020년 기준으로 유엔 회원국 193개에서 통용되는 화폐는 180여 개이고 그중 상당수는 다른 국가 화폐에 고정된 환율을 사용하고 있어서 실질적인 독립 화폐는 고작 130개 정도에 불과하다. 또 인플레이션 때문에 실질적으로 화폐 역할을 제대로 수행하지 못하는 것들을 제외하면 100개가 되지 못하는데, 세계 100대 화폐 안에 들어가는 ‘눈부신’ 성장이란 도대체 무슨 의미인가?

블록체인 활성화를 위해 수천억 원의 예산을 집행하겠다는 과학기술정보통신부의 공식 블로그에 이런 황당한 내용이 버젓이 게재돼 있다는 것은 블록체인에 관한 잘못된 지식 이 사회 전반에 얼마나 만연해 있는지 단적으로 잘 보여주는 사례라 하겠다.

비트코인은 미래의 화폐이므로 반드시 투자해야 한다고 주장하거나 암호화폐 투기에 관한 정부 규제를 미래 기술에 관한 탄압으로 주장하는 이가 있다면, 아마도 용어를 혼동했거나 그다지 믿을 만한 사람이 못 된다. 비트코인은 이미 소수 세력에 의해 장악당한 채 산소 호흡기와 인공 심장으로 명맥만 간신히 유지하는 중환자와 같다. 설계상의 결함으로 한시바삐 수술이 급하지만 이해관계가 상충되는 탓에 수술은 엄두도 못 내고 응급약만 간신히 처방하고 있다. 또 암호화폐를 거래한다고 생각하는 대부분의 사람은 실제로 암호화폐를 단 한 번도 사용해본 적이 없다. 그들은 단지 비트코인 거래소라 이름 붙인 중개소의 숫자 놀음에 상대방 은행 사이의 가상계좌를 통한 인터넷 뱅킹만 부지런히 하고 있다.

1판을 집필할 당시, 책의 목적은 비트코인과 블록체인에 관해 올바른 이해를 돕는 것이었다. 그 후 3년이란 세월이 흘렀지만 여전히 많은 사람이 혼란을 겪고 있고 그 양상도 다소 변했다. 한편 2020년 3월 5일에는 특정금융거래정보의 보고 및 이용 등에 관한 법률(이하 특정금융정보법)의 개정안이 국회를 통과하면서 ‘가상자산’이라는 법률용어가 새로이 등장했고, 2021년 3월 25일부터 전격 시행되기에 앞서 현재 6개월의 유예기간이 주어

진 상태이다. 이제 2021년 9월이 되면, 동 법이 본격 시행될 것이고 그에 따라 극소수 대형 증개소를 제외한 요건을 맞추지 못한 대다수 증개소는 아마 문을 닫게 될 것이다. 이 증쇄본에는 최신 상황을 일부 반영했으나, 단순 증쇄본이므로 그 반영에는 한계가 있다는 점에서 독자 여러분에게 양해를 구한다.

애초에 1판을 한 번 더 증쇄만 하려던 계획을 수정해 전면 개정한 2판을 내기로 결심한 계기는 몇 가지 있다. 가장 큰 이유는 블록체인에 관해 잘못된 인식이 여전히 사회 전체에 만연해 있으며 일부 기업은 오히려 혼란을 부추겨 금전적 이익을 취하려는 그릇된 현실을 바로잡기 위함이다. 이를 위해 새로운 내용을 상당 부분 보강해야 할 필요성이 있었다. 그래서 2판은 다음과 같은 부분에서 1판과 크게 달라졌다.

1판에서는 기술적 부분에 대해서도 비교적 상세히 다뤘지만 2판에서는 이 부분을 과감하게 요약 정리하며 그 분량을 대폭 줄였다. 그동안 강의와 세미나를 통해 일반인들이 어려워하던 기술적 원리 부분을 비유를 통해 좀 더 쉽고 요약적으로 설명했던 노하우를 접목한 것이 주요했다. 이를 통해 1판보다는 내용이 많이 쉬워졌고 좀 더 친근해졌지만 블록체인의 기본 원리는 더 깊이 이해할 수 있게 했다. 블록체인에 관한 개발자 수준의 기술 원리와 배경을 알고 싶은 독자라면 대한민국학술원이 선정한 2019년 교육부 우수학술도서인 또 다른 저서 『블록체인 해설서』를 읽어 보시기를 권한다.

또, 1판에서는 거의 다루지 않았던 가상자산과 디지털 자산 부분을 대거 추가했다. 비트코인이 화폐인가에 관한 기초적인 부분을 명확히 설명하는 데 중점을 뒀던 1판과 달리, 2판에서는 디지털 자산과 디지털화 자산의 구분과 함께 가상자산의 정의와 가상자산의 기술적 실체가 무엇인지 명확히 설명하고 현재 어떠한 법령 체계가 준비 중에 있는지 살펴본다.

이 책은 두 개의 부로 나뉜 아홉 개의 장과 세부적 기술 설명으로 이뤄진 다섯 개의 부록으로 구성했다. 순서대로 책을 읽는 것이 가장 좋지만, 비트코인의 구조와 원리를 어느 정도 알고 있는 독자는 바로 2부를 읽어도 무방하다. 2부를 읽다가 세부적인 기술의 이해가 필요하면 1부에서 선택해 찾아볼 수 있다.

1부는 비트코인과 블록체인을 전반적으로 소개한 후 비트코인 블록체인의 기술적 부분을 상세히 설명한다. 그러나 1판과 달리 주로 비유와 함축을 통해 쉽게 설명하는데 집중했다. 1부는 2부를 이해하기 위한 기초다.

2부는 비트코인과 블록체인을 경제적 관점에서 기술한 내용으로, 그야말로 이 책의 핵심이다. 6장에서는 비트코인이 화폐가 아닌 이유를 설명한다. 또 비트코인의 설계상 약점을 살펴보고 이를 극복하기 위해 현재 어떤 논의가 진행 중인지 알아본다. 화폐의 측면에서 비트코인을 살펴보고 암호화폐를 둘러싼 금융가의 탐욕을 설명한다. 워런 버핏<sup>Warren Buffett</sup>의 스승 벤저민 그레이엄<sup>Benjamin Graham</sup>이 설명한 투자의 정의에 비춰 암호화폐를 둘러싼 광풍이 투자가 될 수 없는 이유를 설명한다. 7장에서는 블록체인을 둘러싼 잘못된 미신들을 파헤치고 설명한다. 8장에서는 가상자산과 함께 암호화폐를 통해 수익을 극대화하는 이들을 알아보고 검은 자본의 세탁을 포함한 암호화폐의 어두운 단면을 조명해본다. 9장에서는 디지털 자산과 디지털화 자산을 자세히 구분해 설명한다. 이와 함께 진정한 디지털 자산이 지향해야 할 방향을 제시한다.

## 이 책의 대상 독자

1판 『비트코인과 블록체인, 탐욕이 삼켜버린 기술』과 마찬가지로 2판 역시 모든 독자를 대상으로 썼다. 비트코인과 블록체인의 개념과 작동 원리는 물론, 그로부터 파생된 가상 자산 시장까지 담았다. 일반인은 물론 IT 개발자, 언론 그리고 정책 수립 책임자 모두 암호화폐와 블록체인이 무엇인지 좀 더 명확히 이해할 수 있게 구성했다. IT 지식이 많을수록 책의 효용이 더욱 커질 수는 있겠지만 전체 맥락을 이해하는 데 필수적이진 않다.

### 일러두기

이 책에서 활용한 참고 자료는 A, B, C... 등과 같이 영문 첨자로 표기했으며, ‘참고문헌’에서 자세한 정보를 확인할 수 있다.