



Understand and Implicate Bitcoin



Index

01 Currency History

- Flow Currency

02 What is the bitcoin?

- Bitcoin about Difference of opinion

03 Understand Bitcoin

- Method of gain bitcoin
- As currency
- Transaction
- Growth

04 Implicate Bitcoin

- View of Government
- Bubble & Crime

05 Closing & QnA

Currency History



본 위 화 폐 : 일 국 의 화 폐 제 도 의 근 간 이 되 는 기 초 적 인 화 폐
하 지 만 본 위 화 폐 가 생 산 되 는 생 산 국 과 이 를 수 입 해 야 하 는 수 입 국 간 의 불 균 형 이 존 재
이 에 따 라 고 안 된 것 개 인 스 의 The Economic Consequences
of the Peace, A Tract on Monetary Reform 에 서 관
화 폐 환 전 도 화 폐 제 도 에 존 략 제 안 제 에 인 가 통 을 의 하 는 것 이 힘 들 다 그 래 서 생 성 된 국 제 기 구
대 언 과 패 의 관 심
즉 앞 으 로 다 가 을 미 래 의 화 폐 는 기 존 의 화 폐 와 다 른 차 별 성 을 가 지 야 한 다



REVOLUTIONARY WEALTH

미래의 부는 우리 삶을 어떻게 바꿀 것인가

인류 역사상 단 한번도 경험해 본 적 없는 거대한 부의 혁명이 다가오고 있다! 미래의 부는 어떻게 만들어지고, 누가 그 부를 지배할 것인가? 그것은 우리 모두에게 어떤 영향을 미칠 것인가?

세계적인 미래학자 앨빈 토플러는 《부의 미래》를 통해 우리의 삶을 송두리째 바꾸어 놓을 혁명적 부에 관하여 설명한다. 그는 지금 일어나고 있는 변화가 개인, 기업, 조직, 가족, 정부 등 모든 시스템과 삶의 방식을 뒤바꾸며 새로운 가치를 창조해 낼 것이라고 강조한다. 표면적으로 관계가 없어 보이는 것들이 상호 작용하면서 만들어 내는 미래의 부는 우리 생활 전반에 혁 목동 같은 영향을 미칠 것이다.

이 책은 사물을 꿰뚫어 보는 앨빈 토플러의 뛰어난 통찰력으로 물리학, 의학 등 과학의 영역에서 경제학, 사회학, 사회심리학 등 사회과학 영역에 이르기까지 광범위한 분야를 섭렵하고 있다. 새로운 아이디어로 변모하는 이 책은 인류 역사상 가장 규모가 크고 가장 독창적이며 가장 빠르게 확장하는 미래 사회의 변화를 예견한다.

이 책은 무수한 기회와 삶의 방식이 새롭게 만들어지고 있다고 주장한다.

커다란 변혁으로 인해 부가 창출된다고 암시하고 있다.

새로운 지식이 미래를 이끌고 부를 창출한다.

탁월하고 날카롭고 독창적인 이 책은 앞으로 수 년 동안 큰 화제가 될 것이다.

뉴욕 타임스

퍼블리셔스 위클리

USA 루대이

라이브러리 저널

Alvin Toffler said
부(富, wealth)는 손으로 만
질 수 있는 화폐가 아니다. 인간
의 욕망을 채워주고 갖고 싶은
것을 해소



Real Time

통제에서 벗어난 움직임

유동성이 있어서 정부와의 통제를 벗어난 디지털 화폐 도입 시도

하지만 이를 관리하는 통제기관의 필요성

실 때

이 때, Bit Coin 주목

So, What is the Bitcoin?

Bitcoin

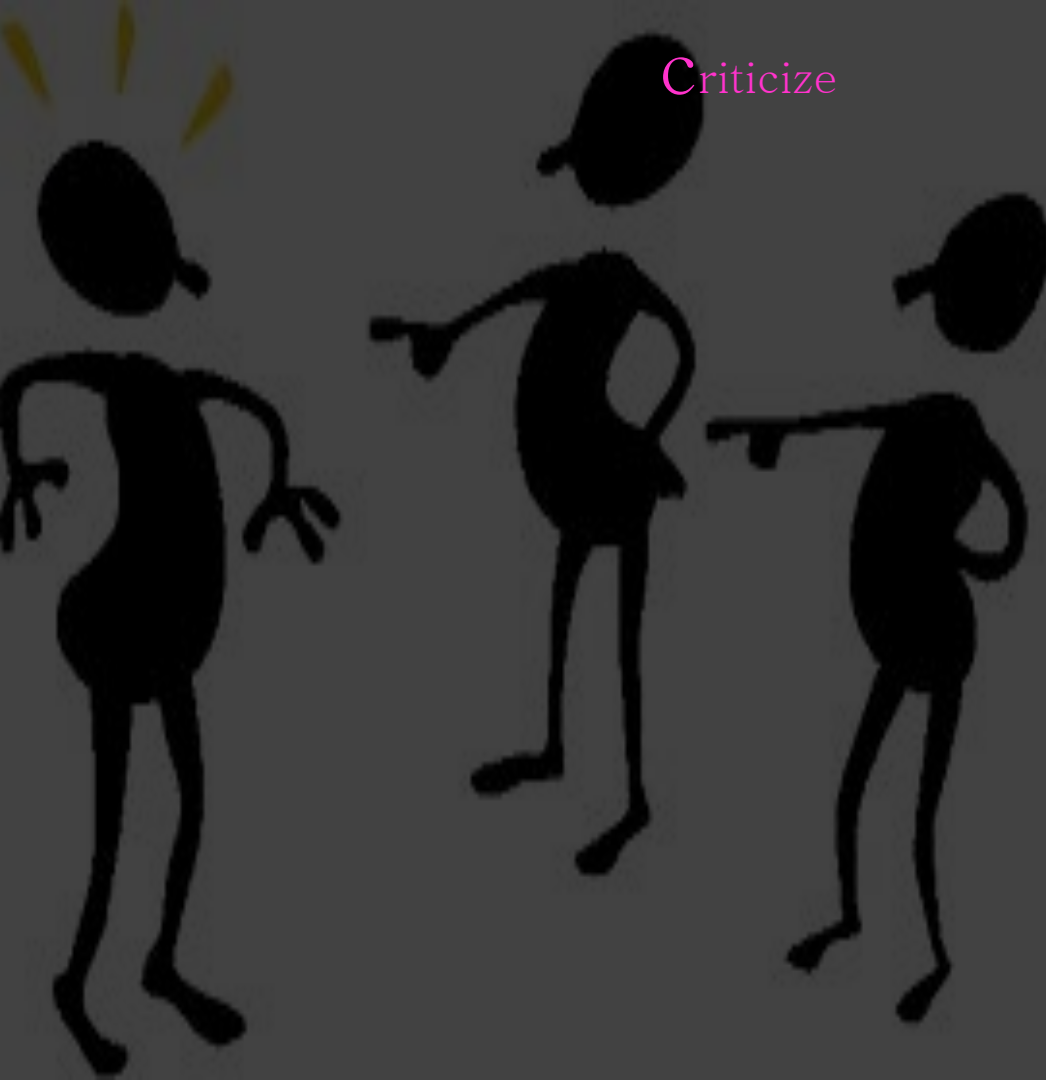


Bit Coin



Typical Fiat
Money - 金融貨幣
Low Transaction Cost - 低交易成本
Anonymity - 匿名性

Also, Anyone is not provided for the Trust to be in
use currency
No Control System



Criticize

He said

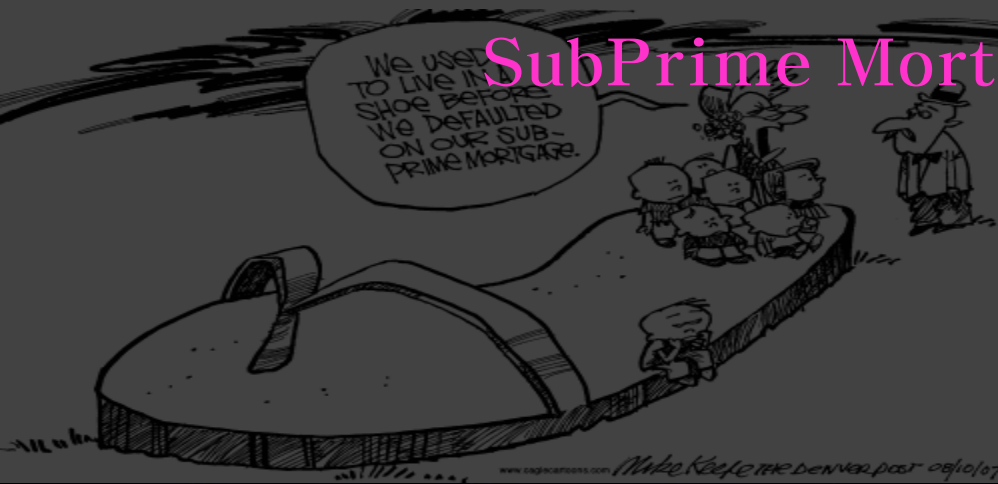
**Not Sustainable Currency
= Temporary Currency**

**No Control System
= Unstable Currency**

Therefore, It is Short Term

Nevertheless

SubPrime Mortgage



Europe Economic Crisis

현재 금융제제에 대한 불신 확산

Bit coin 확산에 영향, 하지만 이 는 동시에

B u b b l e 형성



Bit coin

Nakamoto Satoshi(가명) 프로그래머에 의해 발명

* 비트코인 작동 방식에 MIT 라이선스를 적용해 오픈소스로 공개, 많은 유저들이 이를 활용하는 계기가 됨.

P2P 방식(Point to Point)을 이용

=이는 곧 Bit coin을 통제하는 특정 기구 없음

=App만 있으면 누구나 이용 가능함

비트코인을 보관하기 위해선 '지갑'이라는 계좌 필요

*개인당 지갑의 개수 제한은 없으나 특정 사이트를 이용해야 개설 가능

Mining



TVREPORT



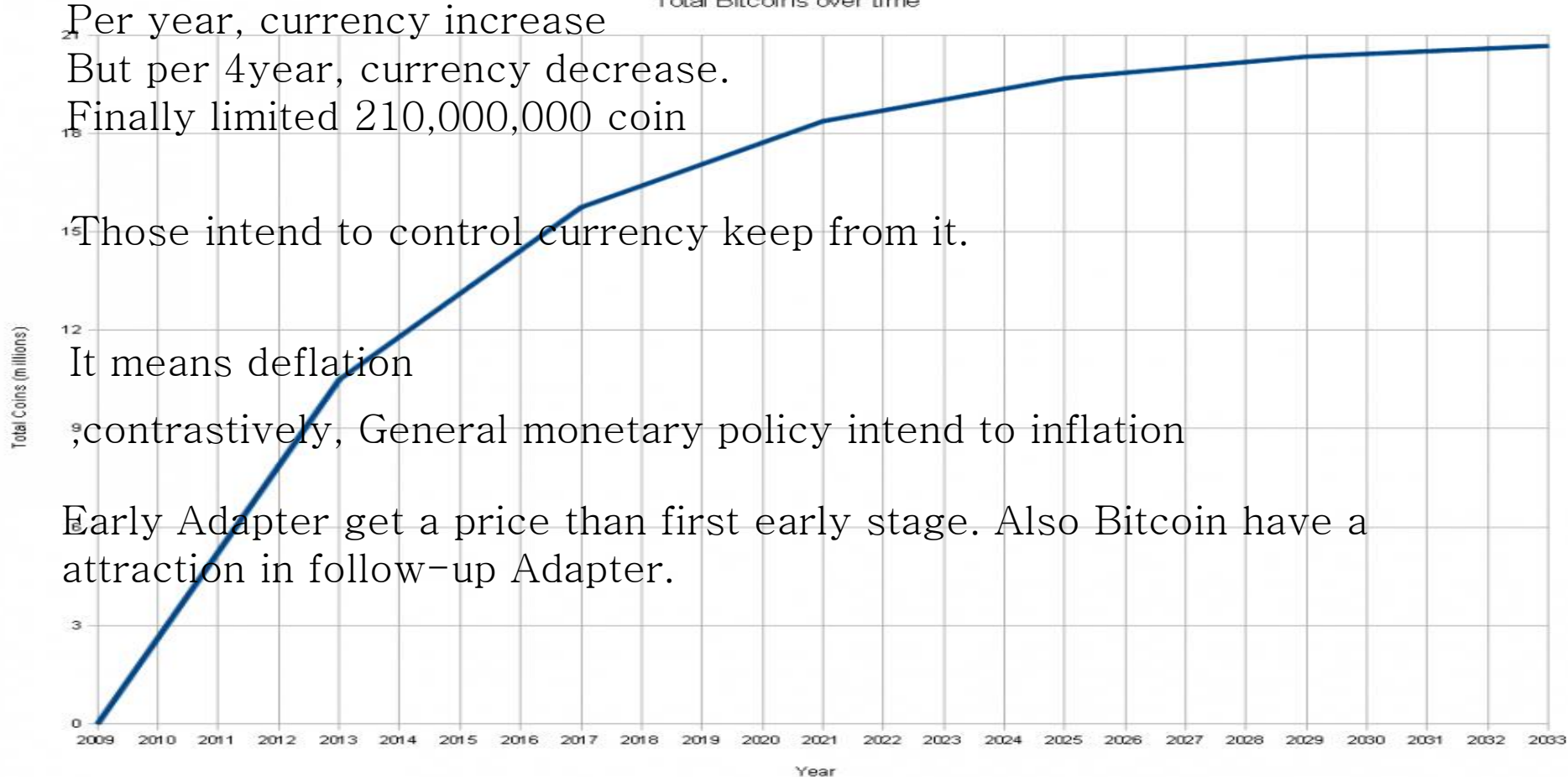
일반 컴퓨터로는 Mining
하는데 약 5년이 걸린다고 함

Bitcoin은 성능 좋은 컴퓨터로
수백 문제를 풀면 대가로 얻을 수 있다.
이러한 과정을 Mining (채굴)
이라고 한다.

= 해쉬 (Hash) 라는 조건을 가장
먼저 제공한 컴퓨터 (노드) 에게
Bitcoin 제공

Bit coin as Currency

Total Bitcoins over time



Criticize



2008년 노벨 경제학상
수상자 - 폴 크루먼

통화로서 지속 가능성
이 없다.



미 인디애나 대학 논문

게임 내에서 가상통화
마저 인플레이션을 선
호한다.

The Rise And Fall Of Bitcoin: A Brief History

by Joe Mullin JUN. 21, 2011 - 9:12 PM PDT

4 Comments

A A

SUMMARY: Bitcoin, the virtual peer-to-peer currency that was launched last year, had a meteoric rise in the last few weeks-but after a hacking attack...

초기 e-cash 개발 참여자

초기 사용자에게 유리한
구조이다.

How a Bitcoin transaction works

Transaction bitcoin

Bob, an online merchant, decides to begin accepting bitcoins as payment. Alice, a buyer, has bitcoins and wants to purchase merchandise from Bob.

WALLETS AND ADDRESSES



Bob and Alice both have Bitcoin "wallets" on their computers.



Wallets are files that provide access to multiple Bitcoin addresses.



An address is a string of letters and numbers, such as 1HULMwZEPkEPeCh43BeKJLlybLCWrDpN.



Each address has its own balance of bitcoins.

CREATING A NEW ADDRESS

Bob creates a new Bitcoin address for Alice to send her payment to.

SUBMITTING A PAYMENT



Alice tells her Bitcoin client that she'd like to transfer the purchase amount to Bob's address.



Public Key Cryptography 101

When Bob creates a new address, what he's really doing is generating a "cryptographic key pair," composed of a private key and a public key. If you sign a message with a private key (which only you know), it can be verified by using the matching public key (which is known to anyone). Bob's new Bitcoin address represents a unique public key, and the corresponding private key is stored in his wallet. The public key allows anyone to verify that a message signed with the private key is valid.

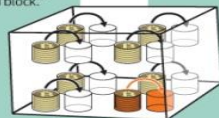
It's tempting to think of addresses as bank accounts, but they work a bit differently. Bitcoin users can create as many addresses as they wish and in fact are encouraged to create a new one for every new transaction to increase privacy. So long as no one knows which addresses are Alice's, her anonymity is protected.

Gary, Garth, and Glenn are Bitcoin miners.



VERIFYING THE TRANSACTION

Their computers bundle the transactions of the past 10 minutes into a new "transaction block."



The miners' computers are set up to calculate cryptographic hash functions.



* Each new hash value contains information about all previous Bitcoin transactions.

Hash value + Nonce



New hash value + Nonce



New hash value + Nonce



New hash value

Cryptographic Hashes

Cryptographic hash functions transform a collection of data into an alphanumeric string with a fixed length, called a hash value. Even tiny changes in the original data drastically change the resulting hash value. And it's essentially impossible to predict which initial data set will create a specific hash value.

The root of all evil → 6d0a 1899 086a... (56 more characters)

The root of all evil → 486c 6be4 6dde...

The root of all evil → b8db 7ee9 8392...

Nonces

To create different hash values from the same data, Bitcoin uses "nonces." A nonce is just a random number that's added to data prior to hashing. Changing the nonce results in a wildly different hash value.

The root of all evil ??? → 0000 0000 0000 ...

Creating hashes is computationally trivial, but the Bitcoin system requires that the new hash value have a particular form—specifically, it must start with a certain number of zeros.

The miners have no way to predict which nonce will produce a hash



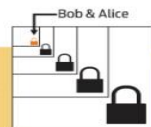
value with the required number of leading zeros. So they're forced to generate many hashes with different nonces until they happen upon one that works.



Each block includes a "coinbase" transaction that pays out 50 bitcoins to the winning miner—in this case, Gary. A new address is created in Gary's wallet with a balance of newly minted bitcoins.

TRANSACTION VERIFIED

As time goes on, Alice's transfer to Bob gets buried beneath other, more recent transactions. For anyone to modify the details, he would have to redo the work that Gary did—because any changes require a completely different winning nonce—and then redo the work of all the subsequent miners. Such a feat is nearly impossible.

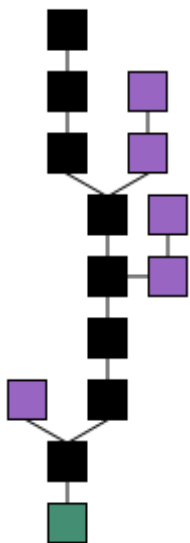


Transaction bitcoin

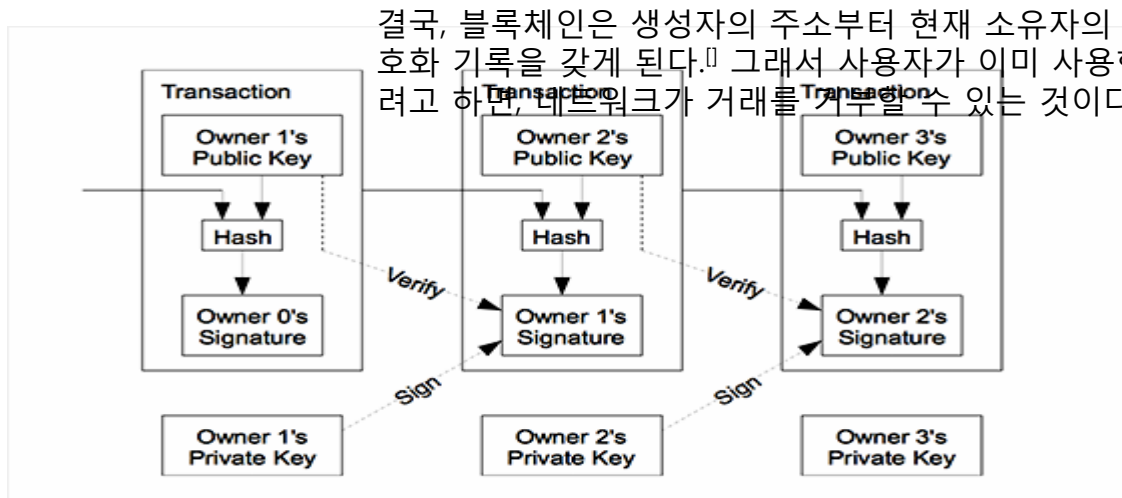
Bitcoin을 얻는 방법은 Mining 하거나 비트코인 거래소를 통해 직접 구매할 수 있음

단, 검증된 비트코인을 이용하여야 함

Bitcoin의 거래는 블록체인이라는 공개된 장부(Public ledger)에 기록됨
이를 공개 키(Public Key)로 암호화하여 보안 및 익명성을 높임



Public note = Block chain



결국, 블록체인은 생성자의 주소부터 현재 소유자의 주소까지 모든 암호화 기록을 갖게 된다.¹⁾ 그래서 사용자가 이미 사용한 돈을 재사용하려고 하면, 네트워크가 거래를 거부할 수 있는 것이다

Satoshi Nakamoto's note

Economy

Total BTC	12,757,500 BTC
Market Cap based on latest prices	5,561,632,125 USD or 4,086,354,825 EUR or 16,546,477,500 PLN or 3,520,942,425 GBP
Transactions last 24h	55,400
Transactions avg. per hour	2308.33
Bitcoins sent last 24h	462,403.10 BTC
Bitcoins sent avg. per hour	19,266.80 BTC

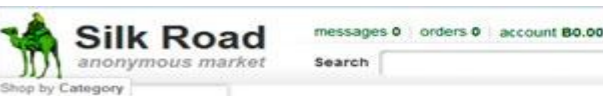
Blocks

Count	200 200
-------	---------

Exchanges

Market	Last	Volume (24h)	Bid	Ask	High	Low
bitfinexUSD	436.5100	11,178.12	436.51	438.45	458.40	430.0
bitstampUSD	439.7300	9,265.94	437.65	439.73	458.20	429.6
btceUSD	432.9000	3,764.65	432.90	433.40	447.40	426.6
lakeUSD	435.9500	1,958.88	435.95	437.60	455.38	428.9
btcnCNY	2716.2300	1,906.05	2716.00	2719.90	2819.88	2685
hitbtcEUR	322.0300	1,180.63	319.59	322.08	336.26	315.4
anxhkHKD	3460.0640	944.46	3393.32	3462.50	3516.11	3388
hitbtcUSD	442.9600	836.39	439.34	442.85	461.34	433.6
krakenEUR	319.1745	644.87	319.17	320.63	330.76	314.3
itbitUSD	433.0000	638.49	437.85	439.51	449.63	430.5
btcdeEUR	324.8900	248.88	320.00	320.00	450.00	310.0
localbtcUSD	469.2900	236.34	1320.00	396.00	985.00	387.1
localbtcGBP	275.9900	186.20	401.60	235.44	420.44	233.5

Silk Road



How Anonymous - Bitcoin is implicated in a

비트코인으로 마약 밀수, 일본 첫 적발

보도에 따르면 이 용의자는 마약밀매 사이트에 접속해 마약 거래 대금으로 인터넷 가상화폐 '비트코인'을 사용했다.

비트코인은 구입시 이름을 입력할 필요가 없어 익명성이 높기 때문에 약물, 총기의 불법거래와 자금세탁에 악용될 우려가 있다는 지적을 받아왔다.

일본 경시청에 따르면 마약을 비트코인으로 거래해 적발된 경우는 이번이 처음이라고 밝혔다.



Growth Bitcoin

2008년 "나는 제3의 신뢰기관이 필요없는 P2P로 운영되는 새로운 전자화폐를 만들고 있다“, 오픈소스 공개

2009년 10월5일 최초로 교환가치 성립 = 1,309.03BTC(1\$ 기준) by New Liberty Standard

2010년 

2011년 짐바부웨에서 4BTC가 100조 짐바부웨 달러와 교환
2월 최초로 1\$: 1BTC 성립
시장 가치 1억 3천 만\$

2012년 유럽발 금융 위기로 거품 형성 및 시장 가치 대폭 향상

2014년 현재 약 5,560,000,000\$의 시장 가치

Government intervene and monitor



Bitcoin과 같은 가상 통화 이용 자체에는 특별한 제약이 없으나, 이를 교환, 매매하는 행위는 규제 대상에 해당함

Bitcoin이 미칠 금융 당국에 미칠 영향은 미미하지만 앞으로 주시해야 함

글로벌
아시아

中 런민은행 "은행들 비트코인 관련 사업 중단하라" 재촉

비트코인 관련 계좌를 폐쇄하라고 명령하였다.
비트코인에 대해 강화된 규제를 준수하지 못하는 은행은 공개 비판의 대상이 될 것이라고 경고하기도 했다.

中·美 당국, 비트코인 위험성 재차 경고

Government intervene and monitor



미 상원의원 찰스 슈머는 2011년 '실크 로드'에 대한 비난 논평을 통해 비트코인을 온라인에서의 돈세탁 수단이라고 비난



Regulation of Bitcoin in Selected Jurisdictions

Alderney • Argentina • Australia • Belgium • Brazil • Canada
Chile • China • Croatia • Cyprus • Denmark • Estonia

European Union • Finland • France • Germany

Greece • Hong Kong • Iceland • India

Indonesia • Ireland • Israel • Italy • Japan

Kazakhstan • Netherlands

New Zealand • Nicaragua • Poland

Romania • Russia • San Marino • Serbia

Slovenia • Spain • South Korea

Switzerland • Taiwan • Thailand • Turkey

United Kingdom

United States

Venezuela

January 2014



Bubble

앞서 말한 유럽 경제 위기는 비트코인의 투기 배당이
이로 인해 투기 및 기풍

통화량이 제한된 상품화폐
- 이는 기존 화폐와 다른 점
- 하지만 이 특성으로 인해 역설적으로 지극히
의 화폐 기능 퇴색
- 약 70%의 비트코인이 전혀 유통되고 있지 않은
을 반증

비트코인의 심한 변동성
“플크루먼 - 비트코인의 환율이 나타내는 심한 변동성
이 투기를 조장하는 특성을 갖고 있다”

Crime

Pony Bofnet – damage 220,000\$

Mt. gox – damage 500,000\$

Silk road2 – damage 2,700,000\$

Sheep marketplace– damage 56,400,000\$

Silk road1– damage 127,400,000\$

Mt. gox– damage 4,360,000\$



Closed

비트코인에 관해 많은 의견이 오가고 있다. 이중 일부는 비트코인을 '신기루'라고 말하면서 성공 가능성을 평가 절하하기도 하며, 곧 망할 것이라 하기도 한다. 하지만 비트코인은 현재 많은 국가, 기관, 매체에서 집중하고 있는 것이 사실이며, 시장 역시 상당한 수준에 올라서 있다. 어떤 것도 완벽하진 않다. 문제점 때문에 우려할 수 밖에 없다. 그럼에도 불구하고 비트코인이 유행하는 것, 비트코인에 대한 여러 논문이 올라오는 것, 비트코인에 대한 연구가 계속 진행되는 것, 시장성이 확대되는 것은 비트코인의 가능성을 말하는 것은 아닐까? 혹시 누가 아나? 나중에 Bitcoin Minor라는 전문 직업이 생길지 물론 망할 수도 있겠지만 말이다.

CLOSED



Thank you

**If you have any question, raise a hand. I
have to answer your question.**