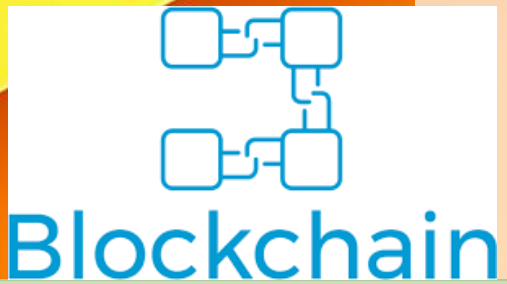
دانشگاه الزهرا

آشنایی با تکنیک بلاک‌چین و رمزارزها

لیلی بنی‌هاشمی

دانشجو دکتری علم اطلاعات و دانش‌شناسی

زمستان ۱۴۰۰



بلاک‌چین یک فناوری دیجیتالی برای ذخیره و مدیریت اطلاعات و یک فناوری دفتر کل توزیع شده است که مجموعه‌ای از همتایان را قادر می‌سازد تا با هم کار کنند تا یک شبکه واحد و غیرمتمرکز ایجاد کنند.

بلاک‌چین داده‌ها را در بلوکی ذخیره کرده، سپس آن‌ها را به هم متصل می‌کند. با ورود اطلاعات جدید، آن‌ها وارد یک بلوک جدید شده و هنگامی که یک بلوک با داده پر شد، آن را به بلوک قبلی متصل می‌کند و بدین ترتیب داده‌ها به ترتیب زمانی با هم زنجیر شوند.

انواع مختلفی از اطلاعات را می‌توان در زنجیره‌های بلوکی ذخیره کرد و در نهایت این که برچسب‌های زمانی (Timestamps) ایجاد می‌شوند تا اطمینان حاصل شود که هر معامله یا تراکنش توسط کسی قابل ردیابی، پشتیبانی و تایید است. کل سیستم ارزش افزوده و ویژگی‌های جدیدی مانند شفافیت، تغییرناپذیری و امنیت (!) را به ارمغان می‌آورد.

تاریخچه بلاک‌چین

سال	آنچه گذشت
۱۹۹۱	استوارت هابر و دبلیو اسکات استورنتا (Stuart Haber and W. Scott Stornetta) کاری بر یک زنجیره رمزنگاری از بلوک‌ها را انجام دادند که هیچکس نتواند به مهر زمانی (digital time-stamping) سند آسیب برساند. مهر زمانی بر هر اثر دیجیتال تولیدشده تاریخ و زمان قرار می‌دهد، لذا مفهوم تقدم و تاخر ثبت اثر به صورت دیجیتالی و صحت آن اجرا شد. ایده فناوری بلاک چین در واقع در سال ۱۹۹۱ مطرح شد.
۱۹۹۸	نیک زابو (Nick Szabo)، رمزنگار، در این سال بر روی یک ارز دیجیتال غیرمتمرکز کار کرد. او متوجه شد که دفتر کل (ledger) غیرمتمرکز می‌تواند برای کدهای خود اجرا (self-executing codes)، که قراردادهای هوشمند نیز نامیده می‌شوند، استفاده شود.
۲۰۰۸	ساتوشی ناکاموتو (Satoshi Nakamoto) یک بیانیه ۹ صفحه‌ای منتشر کرد که الگوی بلاک‌چین بود. او اولین بلاک بلاک‌چین را به عنوان دفتر کل معاملات با استفاده از بیت کوین به عنوان یک شی دیجیتالی (digital asset) را پیاده‌سازی کرد.
۲۰۰۹	ساتوشی ناکاموتو تراکنش استخراج ۵۰ بیت کوین (ارز دیجیتال) را انجام داد.
۲۰۱۴	بلاک‌چین ۲.۰ منتشر شد و از ارز رمزنگاری‌شده جدا شد. پتانسیل آن برای سایر حوزه‌ها و معاملات بین بانکی مورد بررسی قرار گرفت.
۲۰۱۶	دومین بلاک‌چین عمومی با نام اتریوم (Ethereum) راه‌اندازی شد. اتریوم از قراردادهای هوشمندی استفاده می‌کند که به محض برآورده شدن معیارهای تعیین‌شده بدون نیاز به تأیید شخص ثالث، به طور خودکار اجرا می‌شوند.

White Paper

تاریخچه بلاک‌چین

1991

Digital Time-stamping

Stuart Haber and W. Scott Stornetta

1998

Self-executing Codes

Nick Szabo

2008

Digital Asset

Satoshi Nakamoto

2011

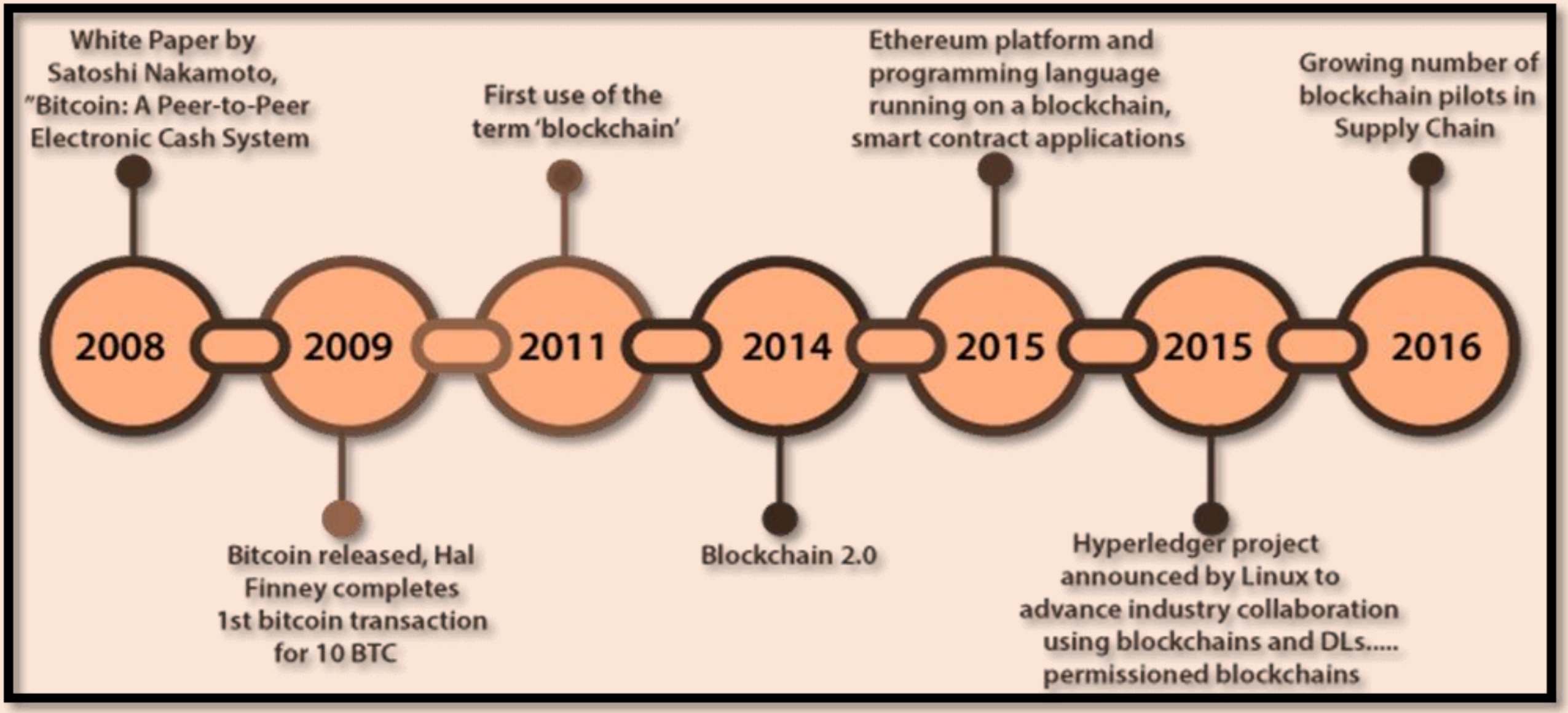
First Use of Term BlockChain

2014

BlockChain 2.0

Using BlockChain in another Industries

تاریخچه رمزارز



تاریخچه بلاک‌چین

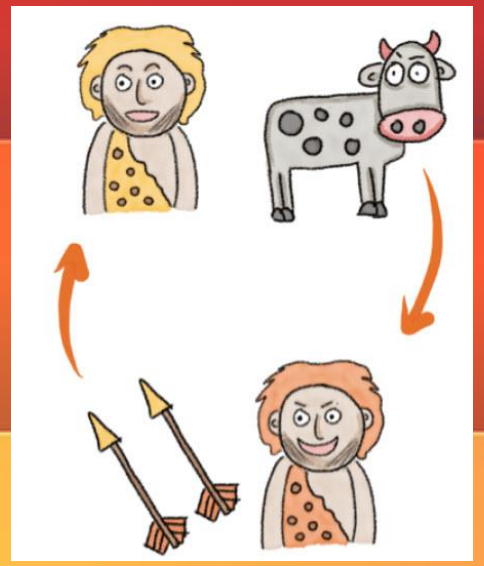
Q1 2022?

BlockChain 3.0

BLOK, BLCN, and LEGR are the three blockchain exchange traded fund (ETF)s

مبادله کالا به کالا (مبادله کالا)

9000 B.C



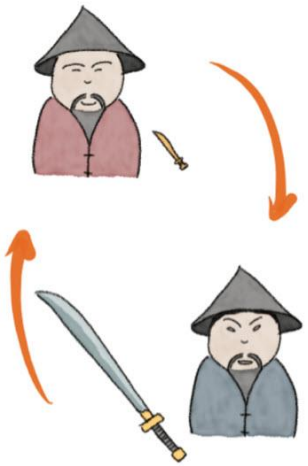
عصر برنز (commodity money)

3000 B.C

مشابه مینیاتوری برنزی

(Chinese Miniature Replicas)

1100 B.C



اولین ارز رسمی – شیر لیدیایی

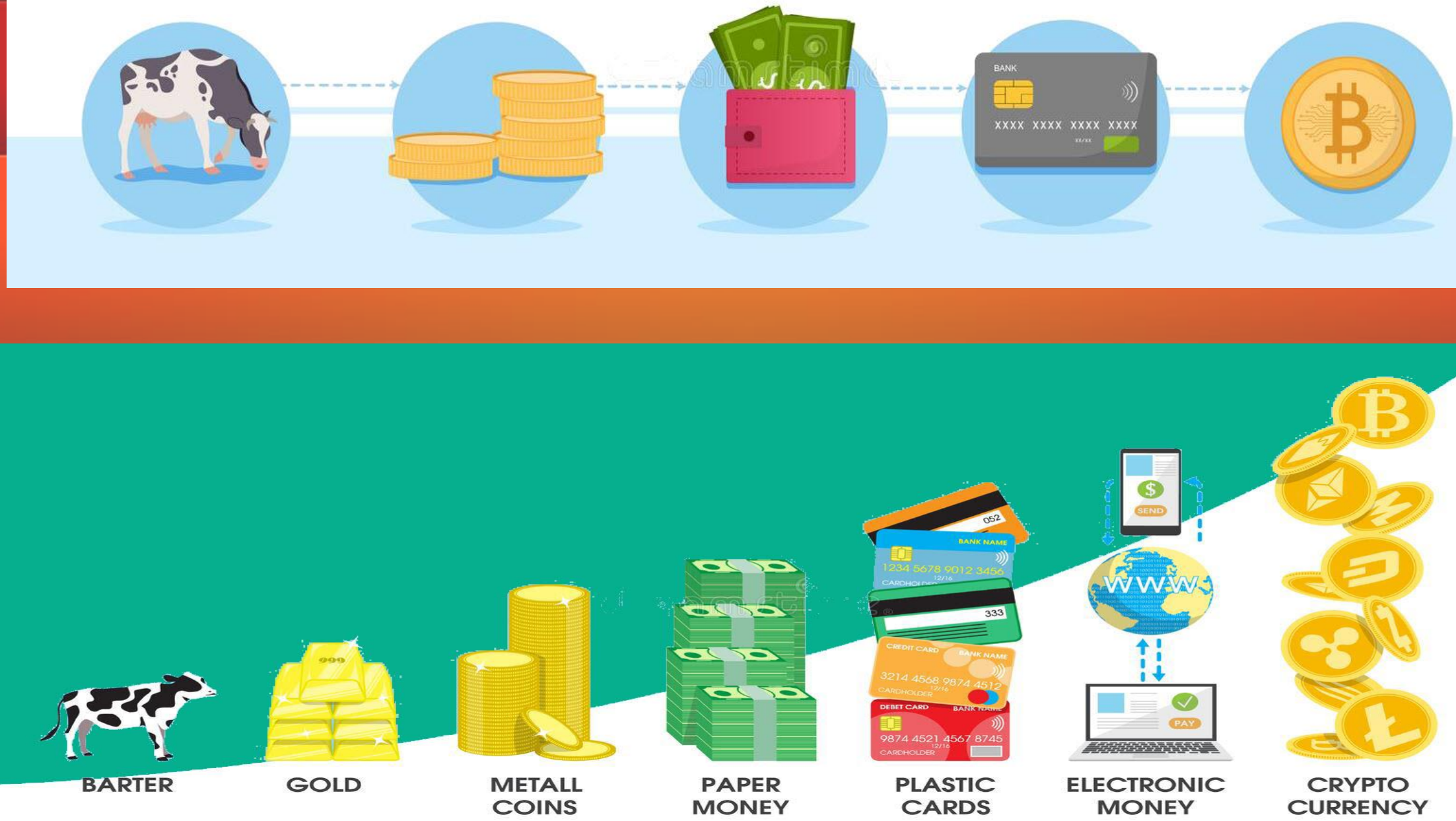
(Lydian Lion)

600 B.C

اولین اسکناس‌های کاغذی (China-The Tang Dynasty)

700 A.C

اختراع دلار آمریکا: April 2, 1792


BANK
XXXX XXXX XXXX XXXX
BARTER
GOLD
METALL COINS
PAPER MONEY
PLASTIC CARDS
ELECTRONIC MONEY
CRYPTO CURRENCY
SEND
WWW
PAY
CREDIT CARD
DEBET CARD
BANK NAME
1234 5678 9012 3456
3214 4568 9874 4512
9874 4521 4567 8745

عدم اعتماد منجر به به ظهور شخص ثالث شد.

نظام پولی بر پایه طلا (۱۸۸۰ تا شروع جنگ جهانی دوم)

اتمام دوران استاندارد طلا

بستن موقتی بانک‌ها

تبدیل طلای مردم با اسکناس‌های دلار

تبدیل آمریکا به بزرگترین منبع طلا جهان

ساخت منابع ذخایر طلای در فورت ناکس (Fort Knox)

March 3, 1933, by **Franklin D. Roosevelt**

شوک نیکسون

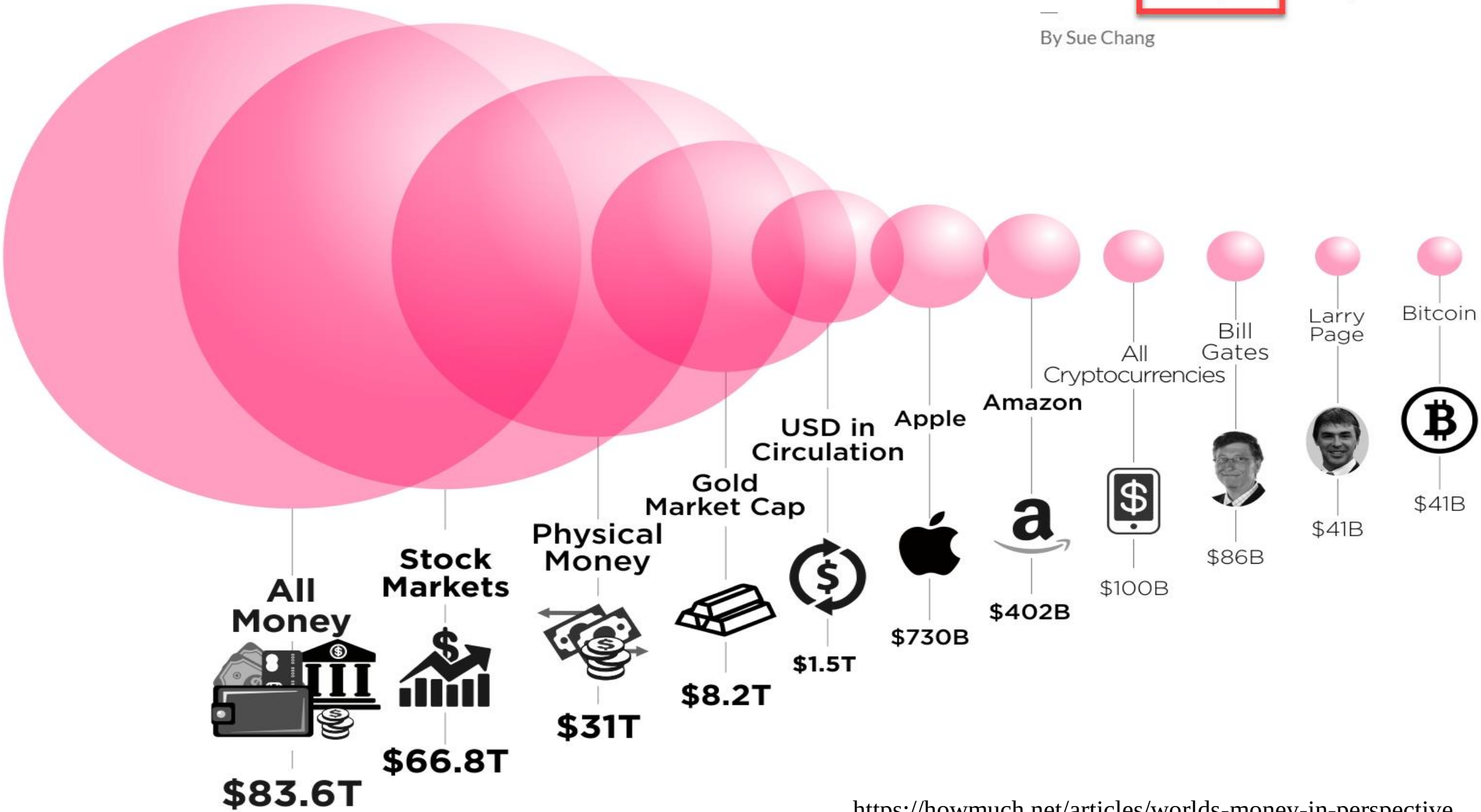
August 15, 1971, by **Richard Nixon**

اتمام دوران استاندارد طلا

تبدیل دلار به ارز بی‌پشتوانه

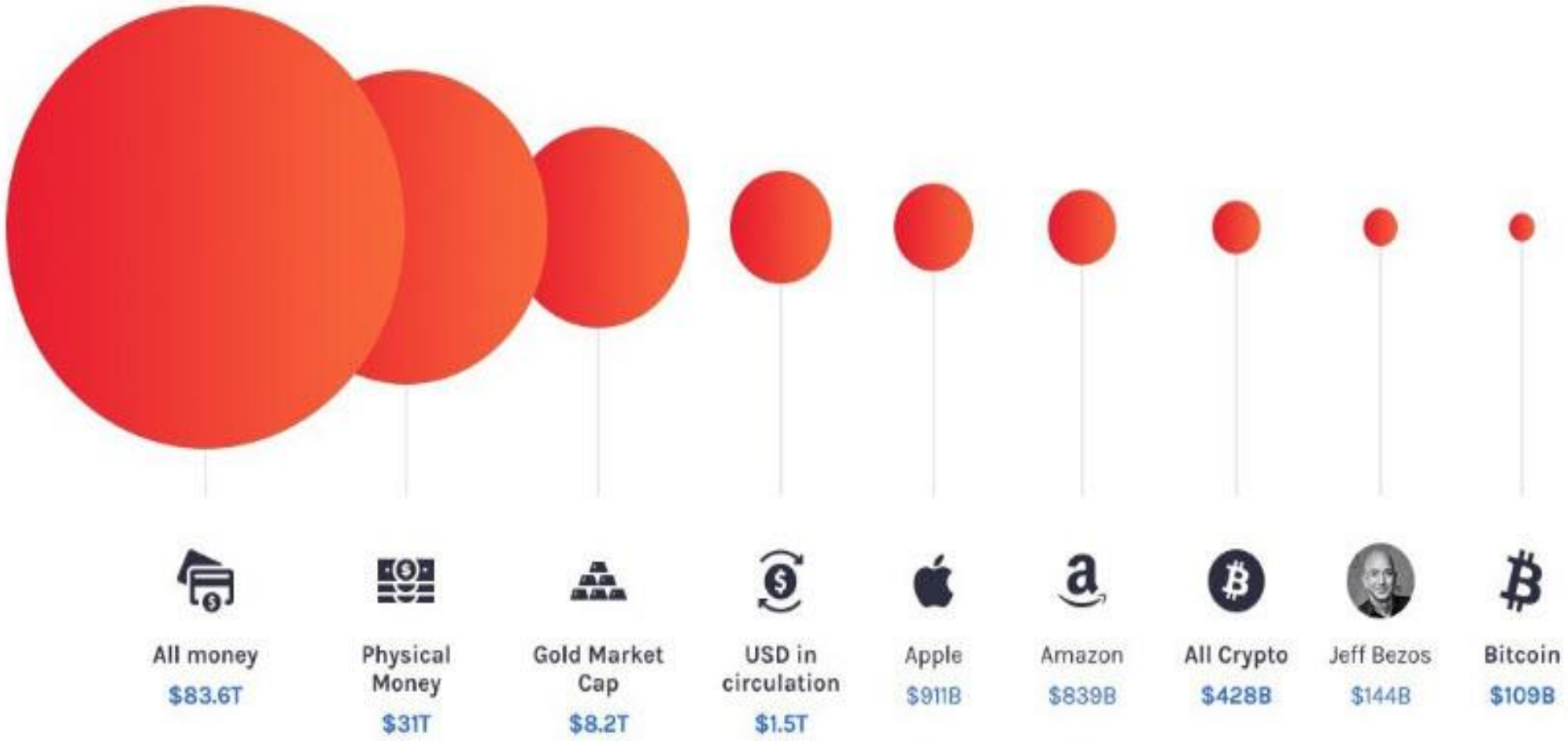
Published: June 30, 2017 at 2:18 p.m. ET

By Sue Chang



https://howmuch.net/articles/worlds-money-in-perspective

https://www.linkedin.com/pulse/world-changing-you-aurels-purics



Aurels Puričs

Bitcoin, crypto, history, biotech, science enthusiast. Trading and research.
Follow my path laurels.substack.com

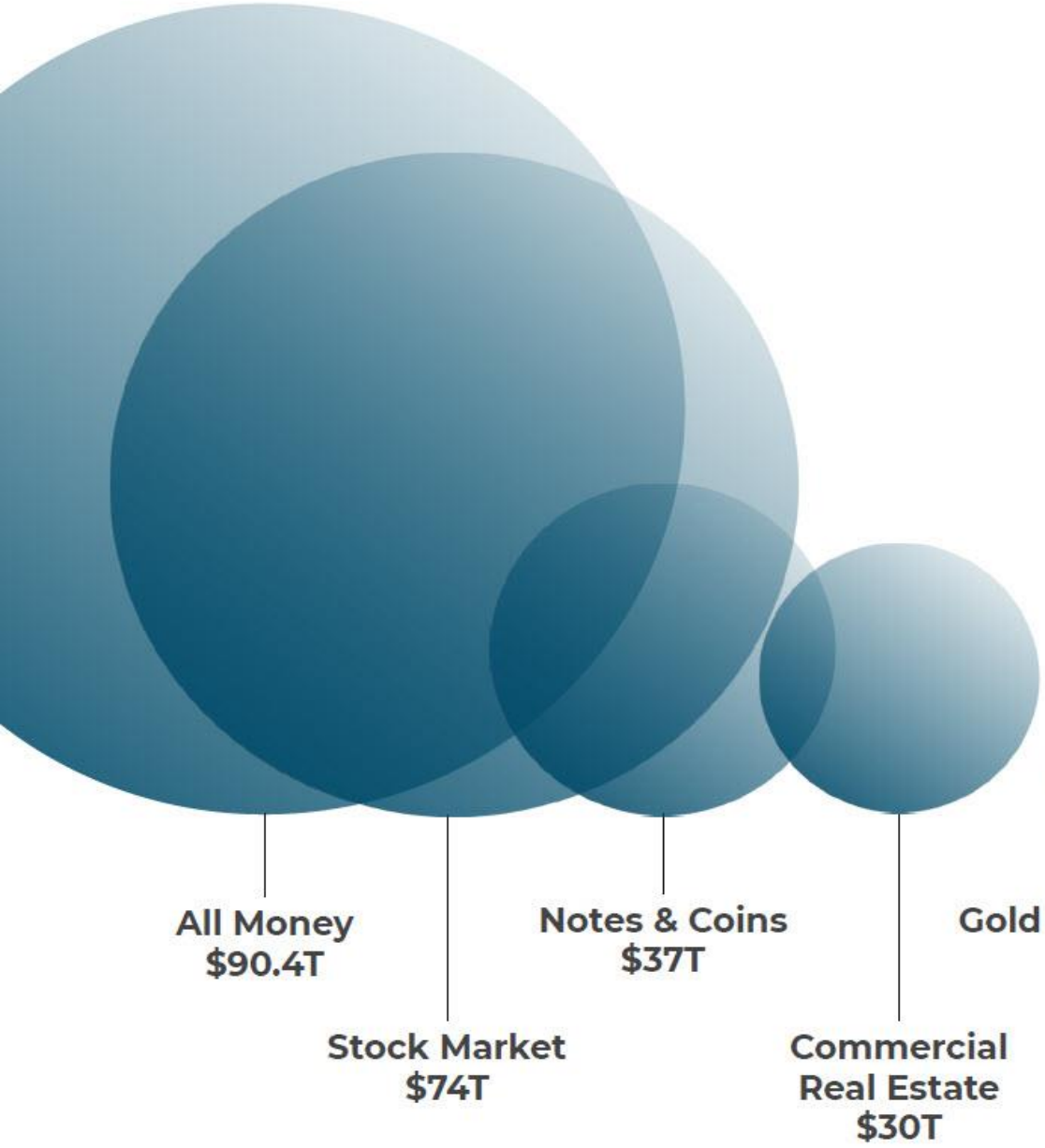
Published Oct 29, 2020

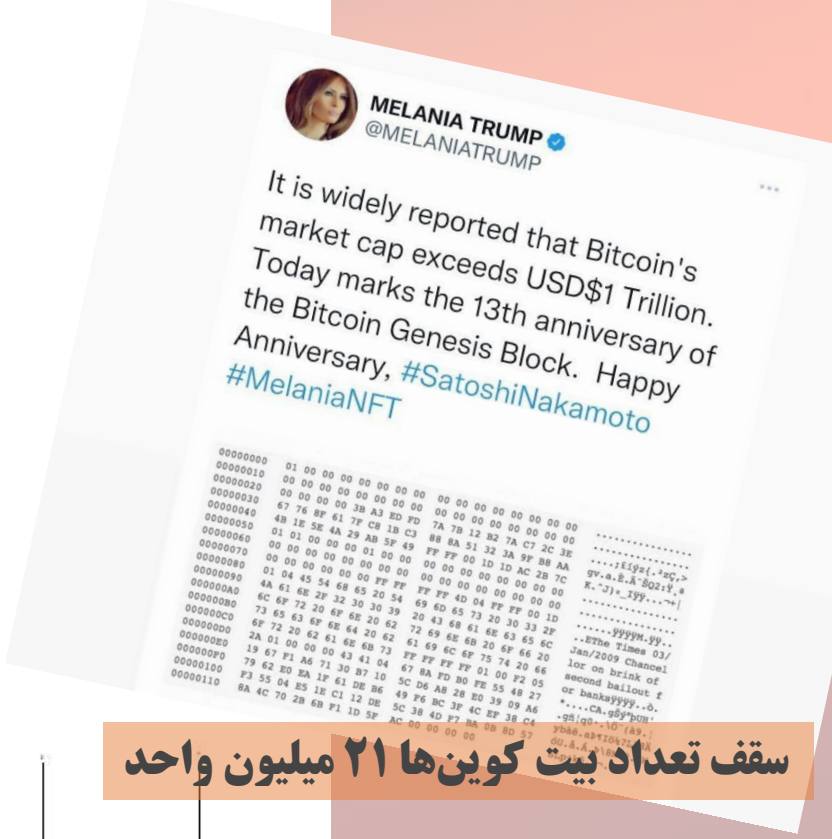
https://blog.idex.io/resources/crypto-in-perspective-a-comparison-of-global-markets-and-money

2020 Global View

طلا دارای ارزش بازاری بیش از ۶۰ برابر اندازه بیت‌کوین است.

ارزهای دیجیتال معادل ۰٫۲۵ درصد از کل پول جهان را در بر می‌گیرند.





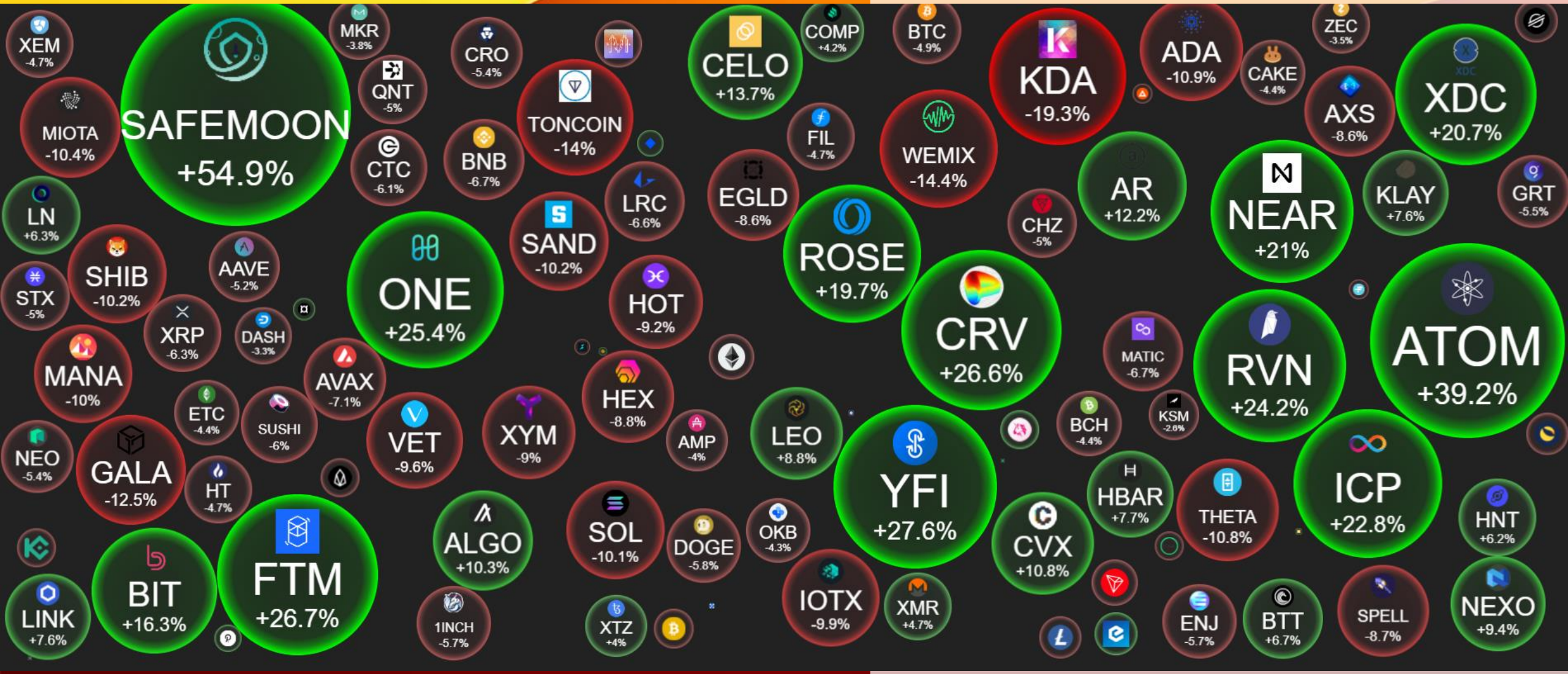
سقف تعداد بیت کوین‌ها ۲۱ میلیون واحد

تا آگوست ۲۰۲۱، ۱۸/۷ میلیون بیت‌کوین استخراج شد.
تقریباً ۲/۳ میلیون بیت‌کوین باقی مانده است.

چند رمزارز (ارز رمزنگاری شده) وجود دارد؟

بیش از ۶۵۰۰ ارز رمزنگاری شده در سپتامبر 2021 وجود دارد. اما به طور واقعی حدود ۸۰۰ نوع در بازار مالی حضور دارند.

https://templatefor.net/free-cryptocurrency-icons/


XEM -4.7%
SAFEMOON +54.9%
MKR -3.8%
CRO -5.4%
CELO +13.7%
COMP +4.2%
BTC -4.9%
KDA -19.3%
ADA -10.9%
CAKE -4.4%
ZEC -3.5%
MIOTA -10.4%
QNT -5%
TONCOIN -14%
FIL -4.7%
WEMIX -14.4%
AXS -8.6%
XDC +20.7%
CTC -6.1%
BNB -6.7%
EGLD -8.6%
AR +12.2%
LN +6.3%
LRC -6.6%
SAND -10.2%
ROSE +19.7%
CHZ -5%
NEAR +21%
KLAY +7.6%
GRT -5.5%
SHIB -10.2%
AAVE -5.2%
ONE +25.4%
HOT -9.2%
CRV +26.6%
STX -5%
XRP -6.3%
DASH -3.3%
MATIC -6.7%
RVN +24.2%
ATOM +39.2%
MANA -10%
AVAX -7.1%
HEX -8.8%
BCH -4.4%
KSM -2.6%
ETC -4.4%
SUSHI -6%
VET -9.6%
XYM -9%
AMP -4%
LEO +8.8%
YFI +27.6%
HBAR +7.7%
THETA -10.8%
ICP +22.8%
NEO -5.4%
GALA -12.5%
HT -4.7%
CVX +10.8%
HNT +6.2%
ALGO +10.3%
SOL -10.1%
DOGE -5.8%
OKB -4.3%
FTM +26.7%
BIT +16.3%
IOTX -9.9%
XMR +4.7%
ENJ -5.7%
BTT +6.7%
SPELL -8.7%
NEXO +9.4%
LINK +7.6%
1INCH -5.7%
XTZ +4%

1/4/2022

قیمت بیت کوین در ۲۷ آذر سال های مختلف

سال	قیمت (دلار)	قیمت (تومان)
۲۰۱۲	۱۳	۳۹,۴۲۹
۲۰۱۳	۱۵۸	۴۶۵,۹۴۲
۲۰۱۴	۳۴۵	۱,۲۰۷,۵۰۰
۲۰۱۵	۴۶۲	۱,۵۶۱,۵۶۰
۲۰۱۶	۷۷۵	۳,۰۴۴,۲۰۰
۲۰۱۷	۱۷,۵۰۰	۷۳,۱۶۷,۵۰۰
۲۰۱۸	۳,۲۳۲	۳۲,۱۲۶,۰۸۰
۲۰۱۹	۷,۱۳۲	۹۲,۰۱۷,۰۶۴
۲۰۲۰	۲۲,۰۰۰	۵۶۷,۶۰۰,۰۰۰

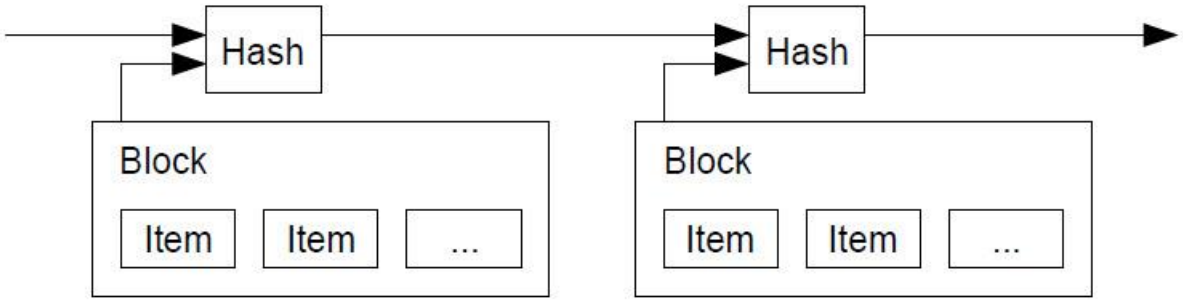
Bitcoin: A Peer-to-Peer Electronic Cash System

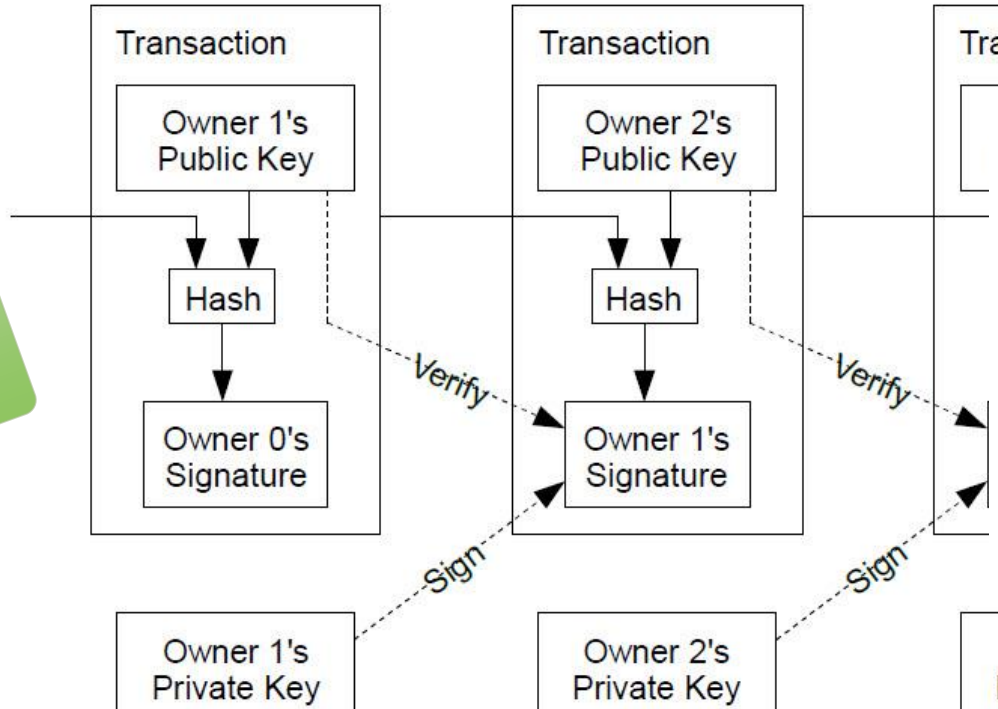
Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majo
attack the net
network itself
ba noc
ork

White Paper

Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. *Decentralized Business Review*, 21260.





Network

The steps to run the network are as follows:

1) New transactions are broadcast to all nodes.
2) Each node collects new transactions into a block.
3) Each node works on finding a difficult proof-of-work for its block.
4) When a node finds a proof-of-work, it broadcasts the block to all nodes.
5) Nodes accept the block only if all transactions in it are valid and not already spent.
6) Nodes express their acceptance of the block by working on creating the next block in the chain, using the hash of the accepted block as the previous hash.

ویژگی‌های بلاکچین

تغییرناپذیری
Immutability

شفافیت در منبع و منشاء
Provenance

اجماع Consensus

تغییرناپذیری
IMMUTABILITY

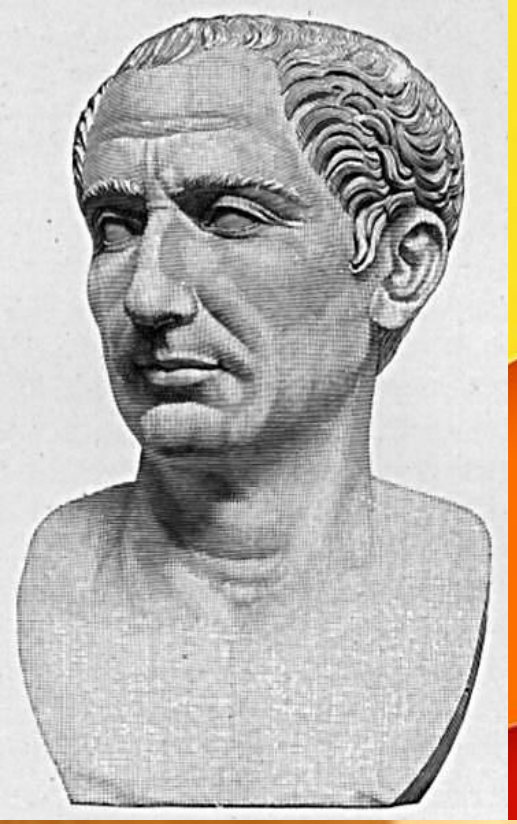
هدف: حذف شخص ثالث و واسطه و برقراری اعتماد

رمزنگاری و درهم‌سازی Hashing و الگوریتم تولید چکیده پیام	اجماع	زنجیره

رمزنگاری (CRYPTOGRAPHY)

هنر مخفی‌کردن اطلاعات یا هنر مخفی نگاه داشتن پیام

تجزیه کلمه cryptography نشان می‌دهد که "crypto" به معنی "پنهان ، مخفی"، و "graphy" نشان‌دهنده فرایند یا فرمی از ترسیم، نوشتن، نمایش، ذخیره، توصیف و غیره، یا هنر یا علمی که به چنین روندی مربوط است. بنابراین مشاهده می‌شود که cryptography در واقع علمی است که به ارتباطات مخفی مربوط می‌شود.



Plain	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Cipher	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W

(Shift 3)

CAESAR CIPHER

(SHIFT 13)

Plaintext

If he had anything confidential to say, he wrote it in cipher, that is, by so changing the order of the letters of the alphabet, that not a word could be made out.

Ciphertext

Vs ur unq nalguvat pbasvqragvny gb fnl, ur jebgr vg va pvcure, gung vf, ol fb punatvat gur beqre bs gur yrggref bs gur nycunorg, gung abg n jbeq pbhyq or znqr bhg.

Online Cipher: https://cryptii.com/pipes/caesar-cipher

اجزای رمزنگاری (Cryptography)

متن ساده (Plaintext): پیام متنی، تصویر یا محتوای باینری است که باید در طول ارتباط ایمن سازی شود. این داده‌های رمزگذاری نشده یا بدون واسطه و تغییری از فرستنده به گیرنده ارسال می‌شود.

رمزگذاری (Encryption): فرایندی است که در آن متن ساده به فرمت غیرقابل خواندن تبدیل می‌شود که توسط دریافت‌کننده می‌تواند به متن ساده تبدیل شود. کاربران الگوریتم رمزگذاری پیام را به صورت رمز (cipher) تبدیل کرده و از یک کلید مخفی (secret key) استفاده می‌کنند. طرف دریافت‌کننده نمی‌تواند پیام را بدون کلید مخفی رمزگشایی کند.

رمز (Cipher): مجموعه‌ای از رمزگذاری و رمزگشایی یک پیام را گویند که در گذشته تنها با جابجایی کاراکترها صورت می‌گرفت.

کلید مخفی: مجموعه ای از اعداد که رمز بر روی آنها کار می کند تا متن ساده را به متن رمز و برعکس تبدیل کند.

متن رمزنگاری شده (Ciphertext): متن ساده‌ای که به فرمت غیر قابل خواندن تبدیل می‌شود ، به عنوان متن رمزنگاری شده شناخته می‌شود که می‌توان آن را بر اساس کلید مخفی و الگوریتم رمزگشایی، رمزگشایی کرد.

رمزگشایی (Decryption): فرایندی است که در آن متن رمزنگاری شده با استفاده از کلید مخفی به متن ساده تبدیل می‌شود. ممکن است کلید متفاوت باشد و بر اساس نوع رمزگذاری مانند رمزنگاری کلید متقارن، از کلید یکسان برای رمزگشایی استفاده شده و یا برای رمزنگاری کلید نامتقارن، کلیدهای متفاوتی وجود دارد.

رمزنگاری (CRYPTOGRAPHY)

PlainText or Clear Text: متن ساده (آشکار)

PlainText or Clear Text: متن ساده (آشکار)

CipherText: متن رمزنگاری شده

https://www.tutorialspoint.com/cryptography/public_key_encryption.htm

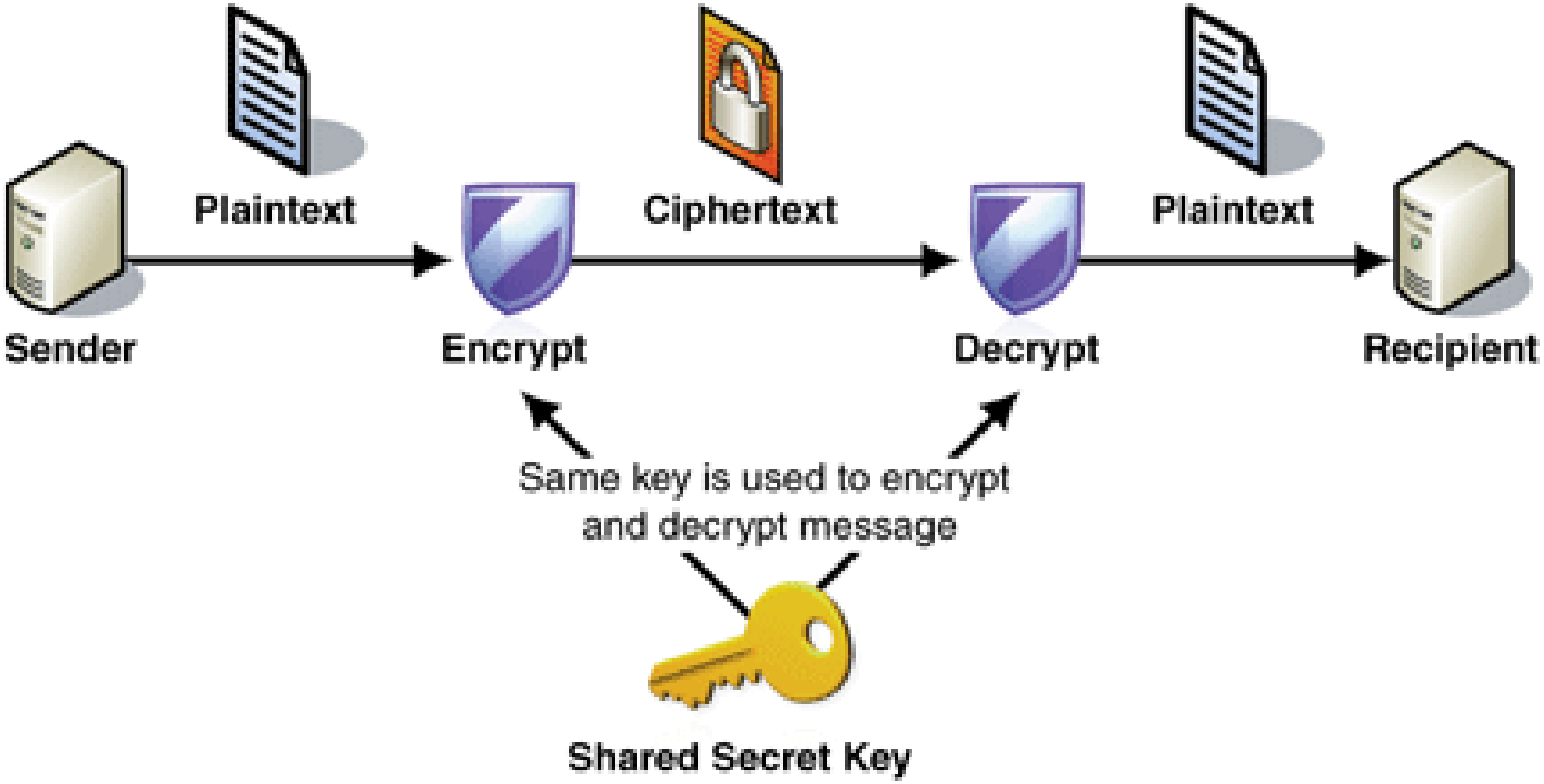
نیازمندی‌های ارتباط امن

- **محرمانگی (Secrecy)**
  به وسیله رمزنگاری با الگوریتم‌های متقارن و نامتقارن
- **یکپارچگی پیام (Message Integrity)**
  به وسیله هش
- **احراز هویت و تصدیق (Authentication)**
  به وسیله امضاء دیجیتالی و الگوریتم‌های نامتقارن

انواع رمزنگاری

- **استفاده از یک کلید (رمزنگاری متقارن)**
- **استفاده از دو کلید (رمزنگاری نامتقارن)- (عمومی و خصوصی)**

الگوریتم کلید متقارن



محرمانگی: جلوگیری از دسترسی از سایر افراد غیرمجاز
تکنیک: رمزنگاری داده

فواید:
- ✓ سادگی
- ✓ محرمانگی
- ✓ سرعت

معایب:
- × مدیریت کلید
- × فراهم‌نکردن عدم‌انکار
(Lack of non-reputation capability)

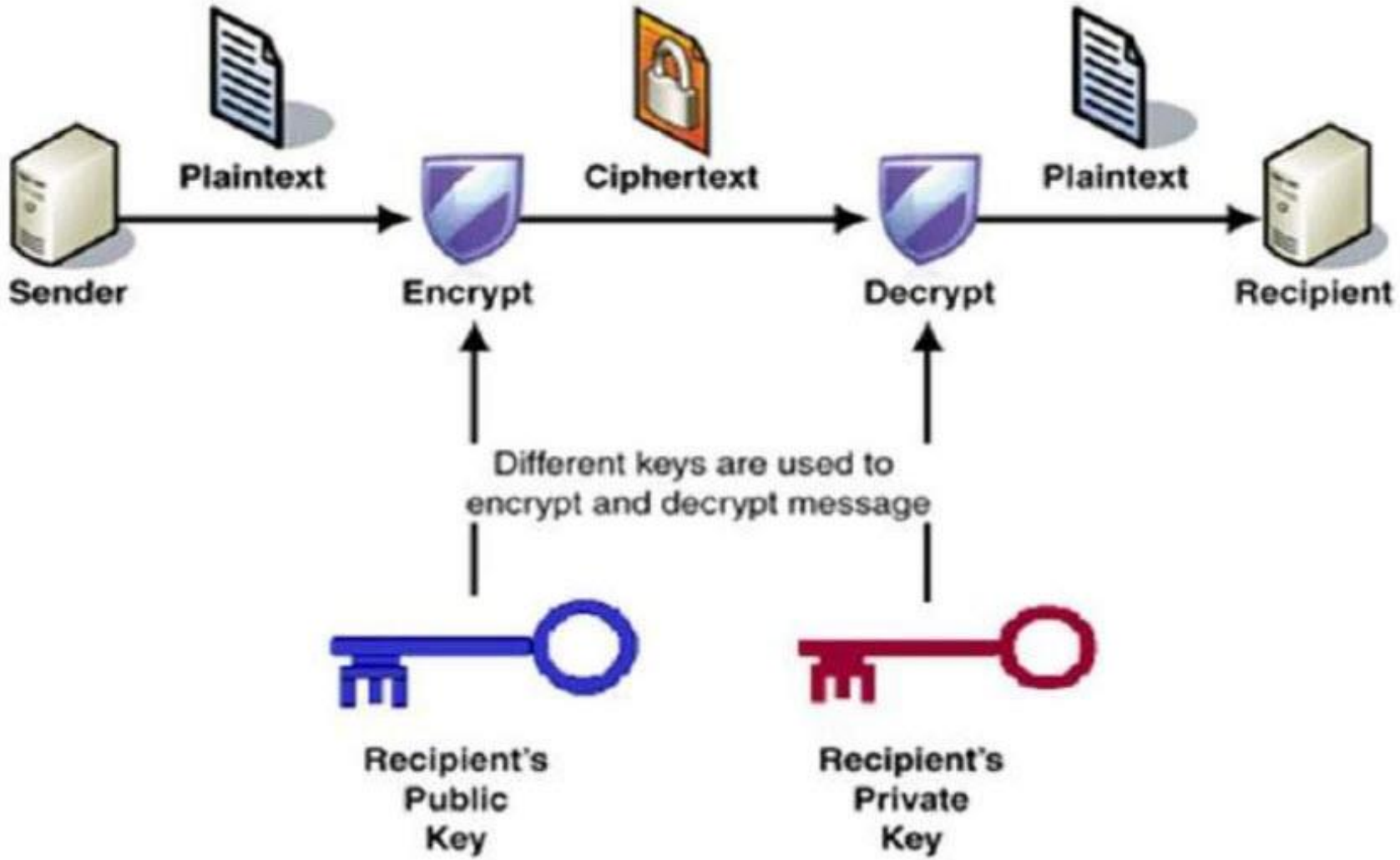
Agarwal, S. (2017). Image encryption techniques using fractal function: A review. *International Journal of Computer Science and Information Technology, 9*(2), 53-68.

برخی از الگوریتم‌های کلید متقارن

Some examples of symmetric encryption algorithms include:

- AES (Advanced Encryption Standard)
- DES (Data Encryption Standard) → Triple DES (3DES)
- IDEA (International Data Encryption Algorithm)
- Blowfish (Drop-in replacement for DES or IDEA)
- RC4 (Rivest Cipher 4)
- RC5 (Rivest Cipher 5)
- RC6 (Rivest Cipher 6)

الگوریتم کلید نامتقارن



محرمانگی: جلوگیری از دسترسی از سایر افراد غیرمجاز

تکنیک: رمزنگاری داده

فواید:

- ✓ اطمینان از عدم‌انکار
  Ensure non-reputation
- ✓ محرمانگی
- ✓ مدیریت کلید

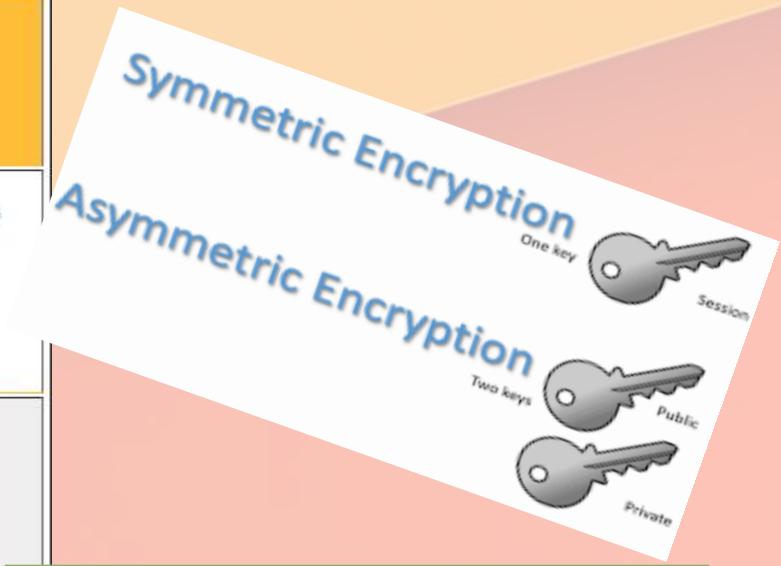
معایب:

- × کندتر از الگوریتم متقارن

Agarwal, S. (2017). Image encryption techniques using fractal function: A review. *International Journal of Computer Science and Information Technology*, *9*(2), 53-68.

Side-by-side comparison of symmetric encryption and asymmetric encryption

Comparison Factor	Symmetric Encryption	Asymmetric Encryption
Number of Cryptographic Keys	Symmetric encryption incorporates only one key for encryption as well as decryption.	Asymmetric Encryption consists of two cryptographic keys. These keys are regarded as **Public Key** and **Private Key**.
Complexity	Symmetric encryption is a simple technique compared to asymmetric encryption as only one key is employed to carry out both the operations.	Contribution from separate keys for encryption and decryption makes it a rather complex process.
Swiftness of Execution	Due to its simplistic nature, both the operations can be carried out pretty quickly.	Because of encryption and decryption by two separate keys and the process of comparing them make it a tad slow procedure.
Algorithms Employed	• RC4 • AES • DES • 3DES • QUAD	• RSA • Diffie-Hellman • ECC • El Gamal • DSA



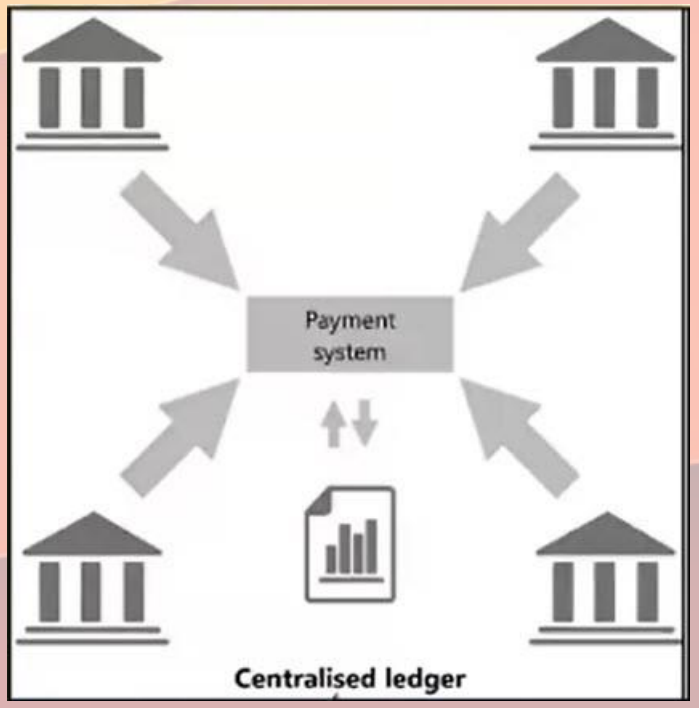
BitCoin: Using ECC + DSA
ECDSA :امضاء دیجیتال + تولید کلید

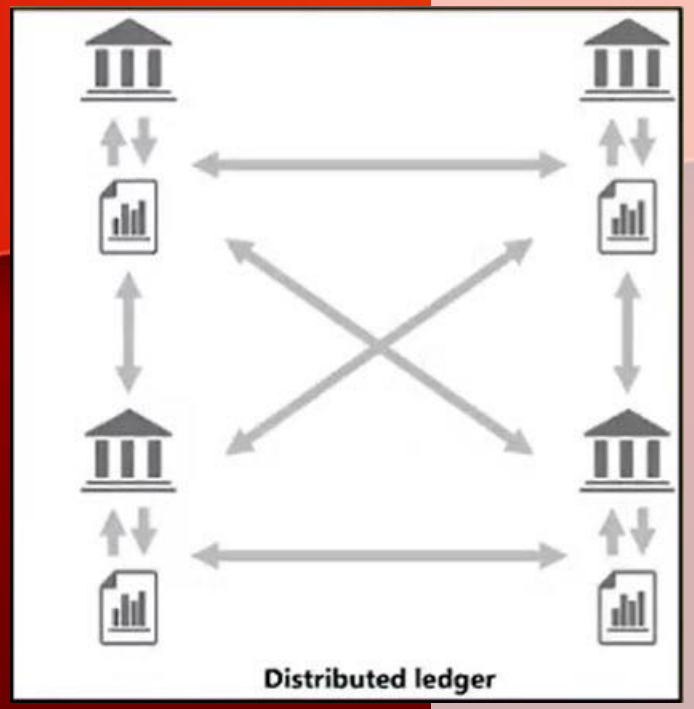
- معروف‌ترین. استفاده از اعداد اول برای تعریف کلید
- برای تبادل کلید
- الگوریتم پیچیده و استفاده از منحنی بیضوی
- کم‌تر شایع
- استفاده صرفا برای امضاء دیجیتال

https://www.rapidsslonline.com/blog/fundamental-differences-between-symmetric-and-asymmetric-encryption/

انواع دفتر کل

- ✓ Centralized Ledger
- ✓ Distributed Ledger
- ✓ Decentralized Ledger



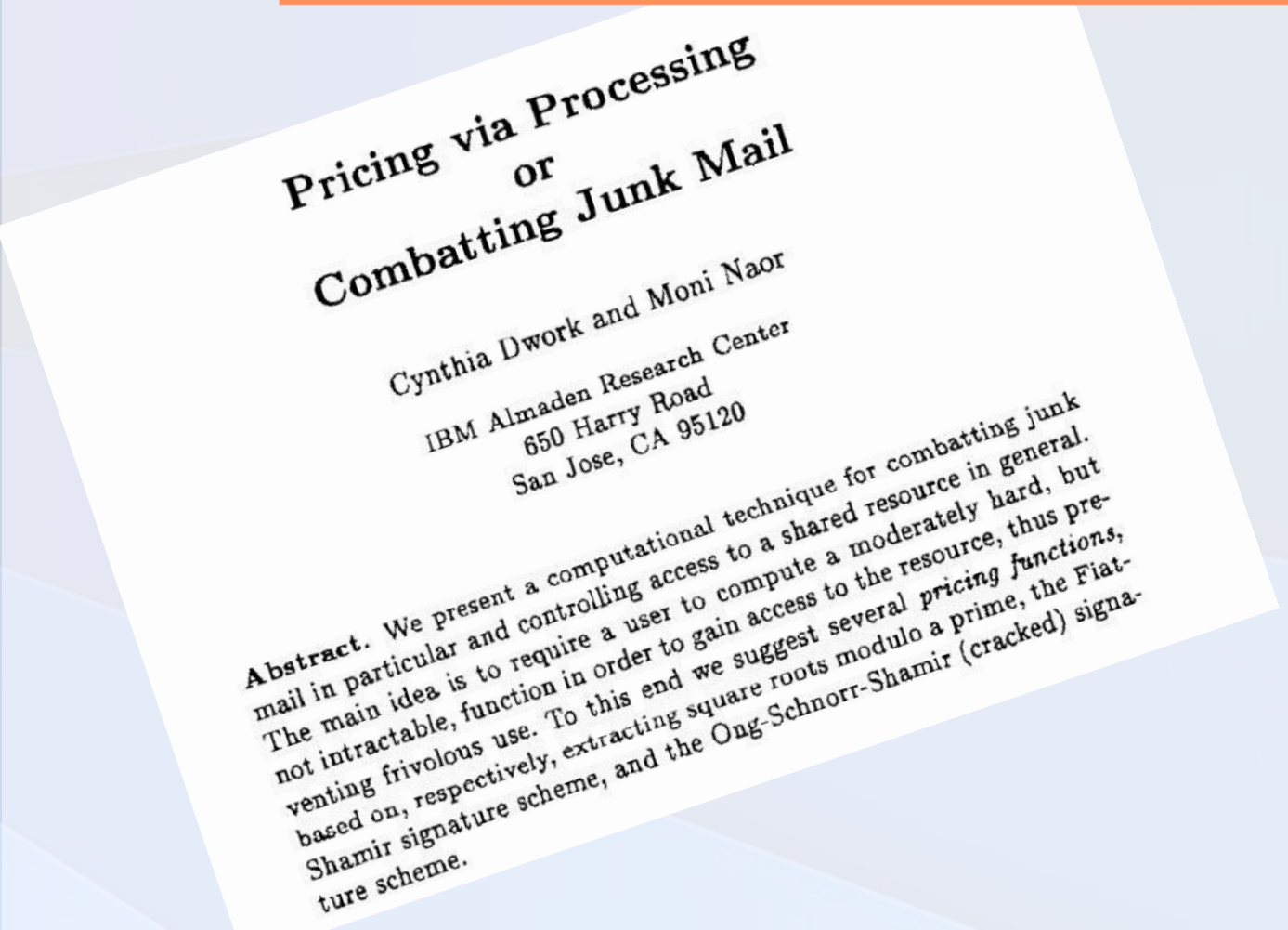


مهم‌ترین پروتکل‌های وفاق جمعی یا اجماع عمومی
(Consensus Protocol)

- **اثبات کار** (POW or Proof of Work)
- **اثبات سهام** (POS or Proof of Stake)
- **اثبات سهام با حق اعطای وکالت** (DPOS or Delegated POS)
- **اثبات زمان سپری‌شده** (POA or Proof of Elapsed Time)
- **اثبات حقانیت** (POA or Proof of Authority)
- **اثبات به روش تحمل‌ناپذیری بیزانسی**
(PBFT or Practical Byzantine Fault Tolerance)

(POW or Proof Of Work) **اثبات کار**

Dwork, Cynthia. Naor, Moni (**1993**, October). **Pricing via Processing or Combatting Junk Mail**. In *Advances in Cryptology—CRYPTO'92: 12th Annual International Cryptology Conference, Santa Barbara, California, USA, August 16–20, 1992. Proceedings* (Vol. 740, p. 139-147). Springer.



Pricing via Processing or Combatting Junk Mail

Cynthia Dwork and Moni Naor

IBM Almaden Research Center
650 Harry Road
San Jose, CA 95120

Abstract. We present a computational technique for combatting junk mail in particular and controlling access to a shared resource in general. The main idea is to require a user to compute a moderately hard, but not intractable, function in order to gain access to the resource, thus preventing frivolous use. To this end we suggest several *pricing functions*, based on, respectively, extracting square roots modulo a prime, the Fiat-Shamir signature scheme, and the Ong-Schnorr-Shamir (cracked) signature scheme.

اولین بار و برای مقابله با هرزنامه‌ها از مکانیسم اثبات کار در این مقاله کنفرانسی رونمایی شد و در سال ۲۰۰۹ (۱۶ سال بعد) این ایده توسط ساتوشی ناکاموتو به کار گرفته شد.

اثبات کار (POW or Proof Of Work)

کلیات ایده اثبات کار

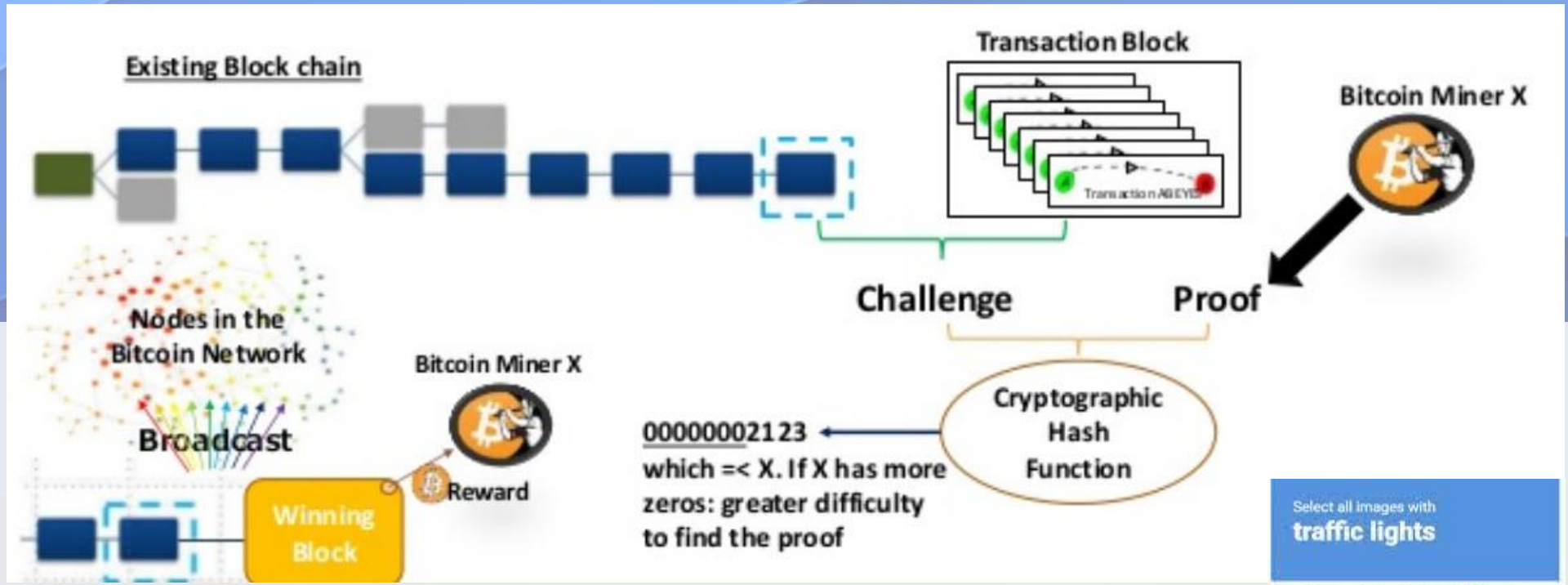
- **الزام به حل مسئله‌ای زمان‌بر**

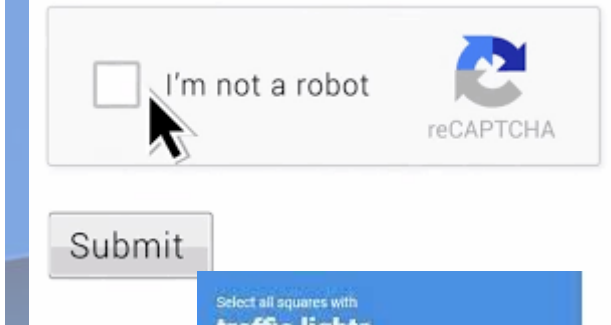
(برای مثال در بیت‌کوین چنین قوانینی تعریف شده: زمان هر بلاک ۱۰ دقیقه باشد و هر بلاک ۱ مگابایت ظرفیت داشته باشد)

- **نیاز به سرمایه‌گذاری پردازشی**

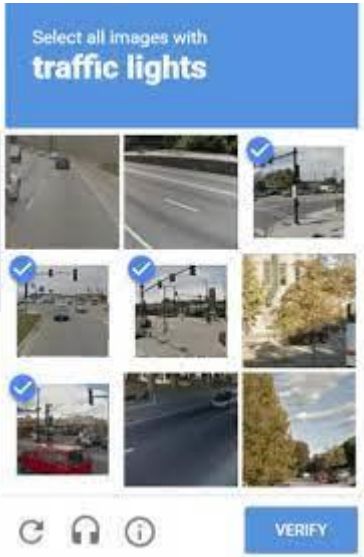
(تعریف سختی کار)

- **اثبات انجام کار توسط اولین کسی که استخراج را با موفقیت به پایان رساند**
- **قابلیت تنظیم و متغیر با زمان**


Existing Block chain
Transaction Block
Bitcoin Miner X
Challenge
Proof
Nodes in the Bitcoin Network
Broadcast
Bitcoin Miner X
Reward
Winning Block
Cryptographic Hash Function
00000002123
which =< X. If X has more zeros: greater difficulty to find the proof


I'm not a robot
reCAPTCHA
Submit


Select all squares with
traffic lights
If there are none, click skip


Select all images with
traffic lights
VERIFY


Select all squares with
traffic lights
If there are none, click skip
SKIP


Select all images with
roads
Click verify once there are none left.
VERIFY

درهم‌سازی (HASHING)

Hashing روشی است که برای بررسی یکپارچگی داده. هش تابعی است یکطرفه که اگر دو کامپیوتر متفاوت یک داده را دریافت کرده و یک تابع هش یکسان را روی آن اجرا کنند باید مقدار هش یکسانی از آن به دست آورند.

یک مثال از استفاده هش برای بررسی یکپارچگی داده این است که فرستنده یک الگوریتم هش را برای هر بسته از داده اجرا کرده و نتیجه را به بسته متصل می‌کند. دریافت‌کننده بسته همان هش را روی بسته دریافتی اجرا می‌کند و نتیجه بدست آمده را با خروجی هشی که فرستنده ارسال کرده است مقایسه می‌کند. اگر نتیجه این مقایسه یکسان بود به این معناست که بسته در حین ارسال تغییری نداشته و سالم به مقصد رسیده است. چرا که اگر یک بیت از بسته ارسالی تغییر کند هش مقصد با هش ارسالی توسط مبدا متفاوت خواهد بود و مقصد متوجه خواهد شد که بسته مشکل دارد.

Hash

اصطلاح "هش" به معنی لغوی "خرد کردن" یا "به هم ریختن" استفاده می‌شود ("chop" or "make a mess")، و در عمل داده‌های ورودی را برای به دست آوردن خروجی به هم می‌زند. به نظر می‌رسد هانس پیتر لون (Hans Peter Luhn) از IBM اولین کسی بود که از مفهوم تابع هش در یادداشتی در ژانویه ۱۹۵۳ استفاده کرد.

درهم‌سازی (HASHING)

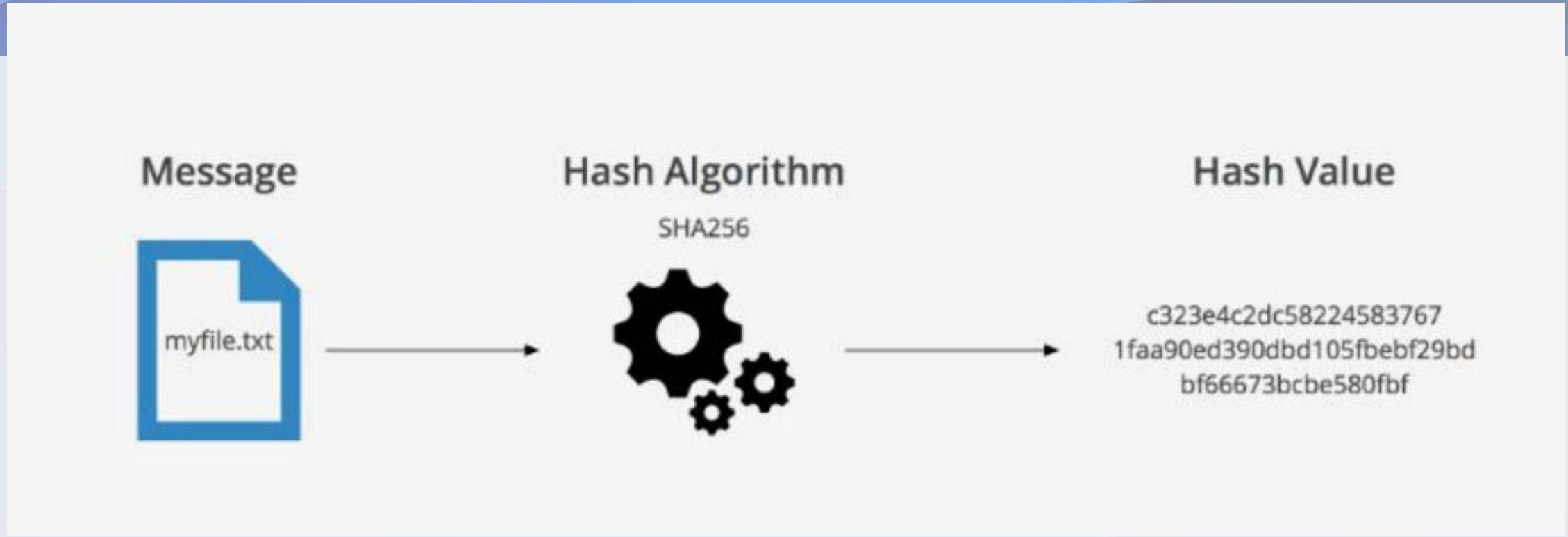
توابع معمولی هش از ورودی‌هایی با طول متغیر استفاده می‌کنند اما خروجی‌هایی با یک طول ثابت برمی‌گردانند. یک تابع هش رمزنگاری، قابلیت انتقال پیام توابع هش را با ویژگی‌های امنیتی نیز ترکیب می‌کند.

از توابع هش معمولاً از ساختارهای داده در سیستم‌های محاسباتی برای انجام وظایفی مانند بررسی یکپارچگی پیام و احراز هویت اطلاعات استفاده می‌شود.

درهم‌سازی (HASHING)

مشهورترین روش‌های Hash به شرح زیر هستند

- Message digest 5 (MD5) در این الگوریتم digest ایجاد شده ۱۲۸ بیتی است.
- Secure Hash Algorithm 1 (SHA-1) در این الگوریتم digest ایجاد شده ۱۶۰ بیتی است.
- Secure Hash Algorithm 2 (SHA-2) در این الگوریتم digest ایجاد شده می‌تواند بین ۲۲۴ تا ۵۱۲ بیت باشد.
- SHA-256 یک هش تقریباً منحصر به فرد و با اندازه ثابت ۲۵۶ بیتی (۳۲ بایتی) تولید می‌کند.
- SHA-3 نسل بعدی در راه است


Message
Hash Algorithm
SHA256
Hash Value
myfile.txt
c323e4c2dc58224583767
1faa90ed390dbd105fbebf29bd
bf66673bcbe580fbf

یک رشته ۲۵۶بیتی چقدر امنیت دارد؟

00000000000000000000000000000000 2^{32} possibilities

00000000000000000000000000000000 2^{32} possibilities

00000000000000000000000000000000 2^{32} possibilities

00000000000000000000000000000000 2^{32} possibilities

00000000000000000000000000000000 2^{32} possibilities

00000000000000000000000000000000 2^{32} possibilities

00000000000000000000000000000000 2^{32} possibilities

00000000000000000000001010110110 2^{32} possibilities

00000000000000000000000000000000 4 Billion possibilities

00000000000000000000000000000000 4 Billion possibilities

00000000000000000000000000000000 4 Billion possibilities

00000000000000000000000000000000 4 Billion possibilities

00000000000000000000000000000000 4 Billion possibilities

00000000000000000000000000000000 4 Billion possibilities

00000000000000000000000000000000 4 Billion possibilities

00000000000000000000001101000110 4 Billion possibilities

SHA256 HASH Calculator

SHA256 hash for Library string

dc20b3d5d2cddf82fad332821ca5e9a4efdcede4a273aa193d2b495bdcc92825

Avalanche Effect

SHA256 hash for library string

b718f1354f7247312eca086d9a024afe5fa717ddea5adeddd6f12bcf945b2e8c

SHA256 hash for Library1 string

f0376a8e85fb11ac26a45dcaa3bc83f4f07ba167fc308398524365d0cfa30151

https://sha256calc.com/hash/sha256

معمایی که برای اثبات کار در بلاک‌چین حل می‌شود؟

روش SHA-256 یک روش محاسبه چکیده درهم‌شده پیام ورودی برای یک بلوک داده با هر اندازه دلخواه، یک رشته ۲۵۶ بیتی تصادفی غیرقابل پیش‌بینی تولید می‌کند.

فرض که توزیع احتمال خروجی‌های تولید شده به ازاء ورودی‌های متفاوت، یک توزیع یکنواخت با احتمال (2 ^ 256) باشد.

برای شروع، یک عدد ۲۵۶ بیتی با مقدار زیر به نام Maximum Target تعریف می‌شود:

0x00000000FFFF0000000000000000000000000000000000000000000000000000

نقش الگوریتم SHA-256 در صنعت بیت کوین

روش SHA-256 یک هش رمزنگاری است که از یک اندازه تصادفی در ورودی استفاده می‌کند و خروجی در اندازه ثابت تولید می‌کند. این عملکرد قدرتمند استچرا که "یک طرفه" هستند. این ویژگی قدرتمند، آن را برای استفاده در شبکه بیت کوین ایده آل می‌کند و به دو روش اصلی مورد استفاده قرار می‌گیرد:

- ماین کردن Mining
- ایجاد آدرس بیت کوین

ماین‌کردن MINING

version	02000000
previous block hash (reversed)	17975b97c18ed1f7e255adf297599b55 330edab87803c8170100000000000000
Merkle root (reversed)	8a97295a2747b4f1a0b3948df3990344 c0e19fa6b2b92b3a19c8e6badc141787
timestamp	358b0553
bits	535f0119
nonce	48750833
transaction count	63
coinbase transaction	
transaction	
...	

Block hash

0000000000000000 e067a478024addfe cdc93628978aa52d 91fabd4292982a50

روشی است که با استفاده از آن سکه‌های جدید وارد جریان گردش مالی پروتکل بیت کوین می‌شود و همچنین برای تأمین امنیت شبکه بیت کوین استفاده می‌شود.

برای اینکه فردی واجد شرایط اضافه کردن بلوک، به بلاک‌چین بیت‌کوین باشد، ابتدا یک Node در عمل Mining شناخته شود. پس از راه‌اندازی موفقیت‌آمیز، فرد می‌تواند شروع به ساختن بلوک کند تا بعد از ایجاد به شبکه بیت‌کوین منتقل شده و توسط سایر Nodeها اعتبارسنجی شود.

۶ پارامتر برای ساخت بلوک

نسخه: شماره نسخه نرم افزار بیت کوین

هش بلوک قبلی: ارجاع به هش بلوک قبلی

Merkle Root: هش نماینده ای از تمام معاملات موجود در بلوک

Timestamp: زمانی که بلوک ایجاد شده است

Target: الگوریتم اثبات کار برای بلوک

Nonce: متغیر مورد استفاده در فرآیند اثبات کار

قراردادهای هوشمند SMART CONTRACTS

قرارداد هوشمند نوآوری بلاک‌چین است که بدون نظارت اشخاص و سازمانی خاص اجرا و پیاده‌سازی می‌شود و در واقع برنامه‌ای است کوچک که با توجه به زمان و شرایط به وجود آمده یک سری دستور را اجرا می‌کند.

در آغاز قرن ۲۱ ابداعات و تکنولوژی‌هایی مانند کلان داده‌ها، اینترنت اشیا، بلاک‌چین و ارزهای رمزنگاری شده ظهور یافتند. فناوری بلاک‌چین به عنوان بستر اصلی و فنی ارز دیجیتال بیت‌کوین، در ابتدای امر توجهات زیادی را به خود جلب کرد تا جایی که بسیاری از دولت‌ها و شرکت‌ها بخشی از فعالیت‌ها و کارکردهای خود را معطوف به توانایی‌های اجرایی بلاکچین کردند. یکی از این توانایی‌ها استفاده از فناوری بلاک‌چین در ایجاد **قراردادهای هوشمند** (خود اجرا) است که توافقاتی هستند که بدون مداخله انسان منعقد می‌شوند. اولین سوالی که ذهن افراد را در هنگام مواجهه با قراردادهای هوشمندی که در بستر بلاک‌چین منعقد می‌شوند، به خود جلب می‌کند این است که بلاک‌چین چیست؟ قبل از سال ۲۰۱۶ فناوری بلاکچین به عنوان بنیان و شالوده ارزهای مجازی شناخته می‌شد؛ اما امروزه این فناوری به منزله پیشرفتی فرصت‌ساز قلمداد شده که هم کارمزد سیستم‌های تراکنش فعلی را کاهش می‌دهد و هم امکان اجرای مدل‌های جدید امور تجاری و اجتماعی را که سابقاً غیرقابل انجام بوده، مهیا می‌نماید.

نیکومنش، فاطمه. (۱۳۹۷).

از جمله ویژگی‌ها و خصایص بلاک‌چین می‌توان به موارد ذیل اشاره کرد:

۱- تمام بلوک‌های (تراکنش‌ها) یک زنجیره باید اعتبار یک تراکنش را تایید کند. (اجماع)

۲- همه کاربران در شبکه می‌توانند همانند مالک بلوک ببینند که بلوک از کجا نشأت گرفته است.

۳- هیچکس نمی‌تواند یک بلوک (تراکنش) را بعد از آن که به دفتر کل اضافه شد، اصلاح نماید یا تغییر دهد.

۴- یک دفتر کل توزیع شده بیانگر یک مرجع به خصوص و تایید شده از مالکیت و تاریخچه تراکنش است.

۵- از انجا که دفتر کل بلاک‌چین بین بسیاری از اعضای بلاک‌چین توزیع شده است؛ لذا از بین رفتن برخی از اعضاء، سبب از بین رفتن شبکه نمی‌شود.

شفافیت، حفظ زمان، تغییرناپذیری، برگشت‌ناپذیری و قابلیت برنامه‌نویسی سبب شده که بلاک‌چین به نحو گسترده‌ای در زمینه‌های بی شماری موثر واقع شود.

نیکومنش، فاطمه. (۱۳۹۷).

قرارداد هوشمند بر بستر بلاک‌چین چگونه اجرا می‌شود؟

قرارداد هوشمند اساساً یک کد برنامه‌نویسی کامپیوتری است که قادر به تسهیل، انجام و لازم الاجرا کردن قراردادهای استفاده کنندگان از تکنولوژی بلاک‌چین است. در واقع قابلیت برنامه‌نویسی فناوری بلاکچین امکان ایجاد چنین قراردادهای خود اجرایی را می‌دهد. در حقیقت مفاد قرارداد به صورت کدهای کامپیوتری برنامه‌ریزی شده‌اند و قادر به اجرای خود به خودی خویش هستند. این قراردادها برای قراردادهایی که می‌توانند در قالب گزاره «**اگر آنگاه**» تعریف شوند، مناسب‌ترین گزینه‌اند؛ چراکه مفاد آن‌ها به راحتی قابل تبدیل به کدهای کامپیوتری هستند.

نیکومنش، فاطمه. (۱۳۹۷).

فواید قرارداد هوشمند بر بستر بلاک‌چین

۱- خوداجرایی قرارداد بر مبنای کدهای کامپیوتری

۲- ثبات: نسخه نهائی قرارداد با جزئیات کامل به صورت دیجیتال در میان تمام بلوک‌ها توزیع شده که به صورت دقیق اجرا می شود.

۳- قطعیت: عدم امکان اظهارانکار و تردید طرفین نسبت به مفاد قرارداد؛ زیرا متن قرارداد تبدیل به کد کامپیوتری شده است.

۴- محقق‌کردن شروط رایج قراردادی، به حداقل رساندن استثناءهای تصادفی یا از روی سوءنیت و نیاز به واسطه‌های مورد وثوق، کاهش زیان‌های ناشی از غَبن، هزینه‌های داوری و اجرای قرارداد و ... .

۵- اجرای قرارداد محیطی غیرمتمرکز

نیکومنش، فاطمه. (۱۳۹۷).

کاربرد بلاک‌چین در نظام حقوقی مالکیت فکری

در نظام حقوقی مالکیت فکری، خلاءهایی وجود دارد که با استفاده از فناوری بلاک‌چین می‌توان آن‌ها را حل کرد و باعث پیشرفت و بهبود نظام مالکیت فکری شد. از جمله: عدم شفافیت در مورد وضعیت حقوقی آثار تحت حمایت، مانند زمان ثبت اثر و همچنین اطلاعات در مورد هویت پدید آورنده، مشکلات مربوط به حوزه قراردادهای هوشمند در مالکیت فکری و همچنین سیستم ثبت آثار توسط بلاک‌چین که اگرچه حق ادبی و هنری به محض خلق اثر اعطا می‌شود، اما سایر حقوق مالکیت فکری مانند اختراع، علائم تجاری یا طرح‌های صنعتی فقط پس از طی فرایند خاص ثبت، به دارنده حق اعطا می‌شوند و روند ثبت این حقوق غالبا پیچیده و پرهزینه است. باتوجه به ماهیت تجارت جهانی و سرعت سریع زندگی تجاری در سیستم اقتصاد نوین، این محدودیت برای دارندگان حق بسیار قابل لمس خواهد بود و در آخر مسئله پرداخت در سیستم مالکیت فکری سنتی که بسیاری از دارندگان حق، از سیستم‌های کند، غیرمستقیم و پرهزینه در پرداخت‌های بین‌المللی گله‌مند هستند، بدین وسیله قابل حل است.

رستگار، فهیمه. (۱۴۰۰).

NFT

NON-FUNGIBLE TOKEN (NFT) **توکن غیرقابل معاوضه**

محبوبیت کنونی بازارهای توکن غیرقابل معاوضه یکی از قابل‌توجه‌ترین موفقیت‌های عمومی فناوری بلاک‌چین است. NFT از جمله حقوق قابل معامله‌ای است که با کمک بلاکچین برای هر دارایی دیجیتالی معامله می‌شود، از جمله تصاویر، فیلم‌ها، موسیقی، حتی بخش‌هایی از دنیای مجازی. مالکیت دارایی‌های دیجیتال در قراردادهای هوشمند روی یک بلاک‌چین ثبت می‌شوند. بازار NFT خارج از ارزهای رمزنگاری شده است و پژوهش‌ها نشان داده‌اند قیمت NFT با قیمت ارزهای رمزنگاری شده همبستگی پائینی با یکدیگر دارند، هرچند پژوهش‌های بیشتری را در این رابطه پیشنهاد داده شده است.

Dowling, M. (2021). Fertile LAND ...
Dowling, M. (2021). Is non-fungible …

NON-FUNGIBLE TOKEN (NFT) **توکن غیرقابل معاوضه**

NFT یک توکن دیجیتالی دقیقاً مانند بیت‌کوین یا اتریوم است. اما برخلاف سکه‌های استاندارد در بلاک‌چین بیت‌کوین، منحصر به فرد بوده و نمی‌توان آن را به ارز دیجیتال دیگری تبدیل کرد و وقتی یک NFT خریداری می‌شود به صورت منحصر به فرد آن NFT فقط برای خریدار ثبت شده و هیچ فرد دیگری نمی‌تواند از آن کپی‌برداری کند و یا شبیه آن را داشته باشد.

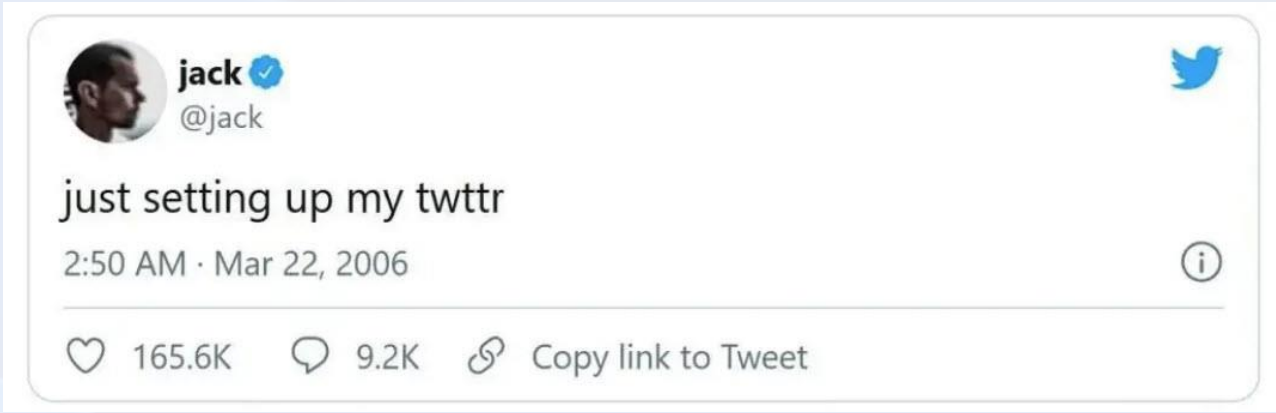
NFT به طور کلی از نظر اجرا بسیار محدود بوده و کدهای شناسایی منحصر به فردی دارند. آری یو، رئیس انجمن صنعت فناوری واشنگتن Cascadia Blockchain Council در این باره اظهار می‌دارد:

"NFT به دنبال ایجاد کمیابی و ارزش به هنر دیجیتال است."

NON-FUNGIBLE TOKEN (NFT) موارد مورد استفاده در

- Art
- GIFs
- Videos and sports highlights
- Collectibles
- Virtual avatars and video game skins
- Designer sneakers
- Music

حتی توییت هم حساب می‌شود. جک دورسی، بنیانگذار توییتر، اولین توییت خود را به عنوان NFT به قیمت بیش از ۲/۹ میلیون دلار فروخت.



موارد مورد استفاده در NON-FUNGIBLE TOKEN (NFT)

NFT این امکان را به ما می‌دهد که اصالت یک اثر هنری دیجیتال را با کمک بلاک‌چین به اثبات برسانیم و آنرا از کپی‌هایش متمایز کنیم. در دنیای واقعی هم چنین اتفاقی می‌افتد. یک اثر هنری مثلاً یک تابلوی نقاشی از یک نقاش معروف ارزش زیادی دارد. این ارزش ناشی از اصالت آن تابلو است. ممکن است کپی‌های زیادی از آن تابلو ساخته شده باشد که با تابلوی اصلی کاملاً شباهت داشته باشند، اما نسخه‌های کپی از نظر یک کارشناس یا مجموعه‌دار، ارزشی نداشته و فقط آن تابلوی اصلی است که ارزش هنری و مادی دارد. در دنیای واقعی، اعتبار و اصالت یک اثر هنری را کارشناس آن حوزه تشخص می‌دهد و آن‌را از نمونه‌های جعلی متمایز می‌سازد. در دنیای NFT این اعتبارسنجی و بررسی اصالت یک فایل دیجیتال برعهده بلاک‌چین است.

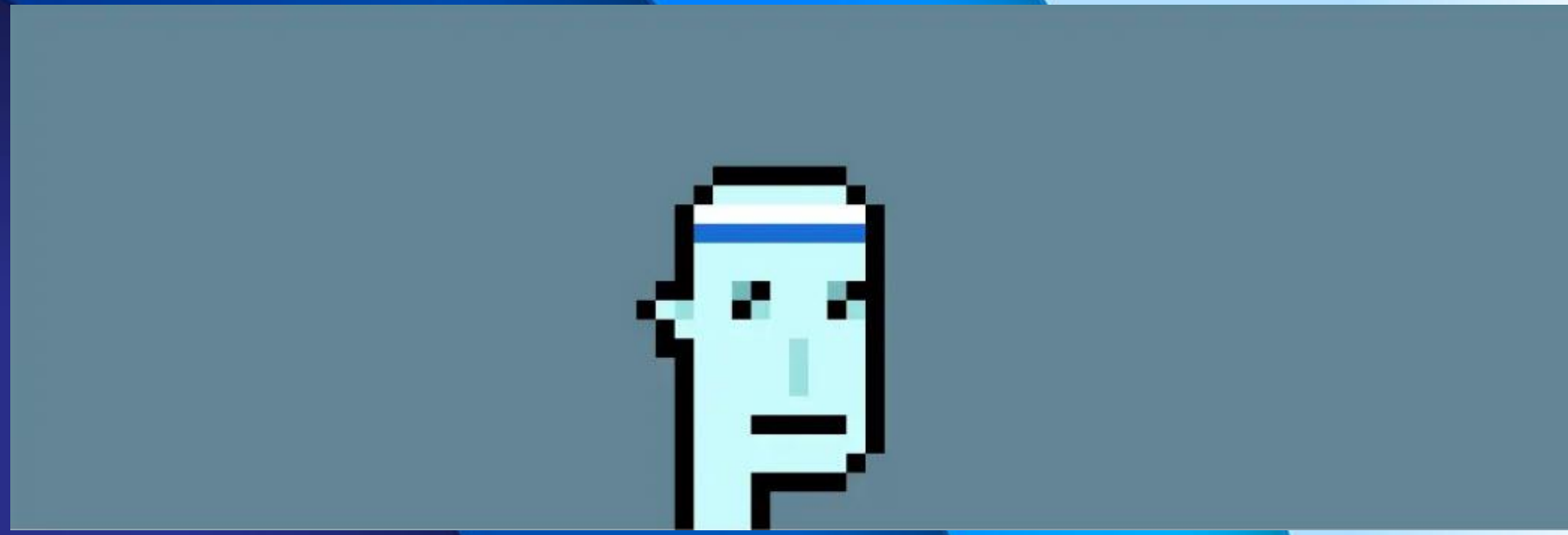
مایک وینکلمن (Mike Winkelmann)،
اثر خود به نام
«Everydays – The First 5000 Days»
را در حراجی کریستیز در ماه مارس
۲۰۲۱ با قیمتی برابر با $69.3
میلیون دلار به فروش رساند که
گران‌ترین اثر فروخته شده برای یک
NFT تا این زمان (دی ماه ۱۴۰۰) به
شمار می‌آید.

consisting of 5,000 images measuring 21,069 x 21,069 pixels

این اثر توسط برنامه‌نویس مستقر در سنگاپور،Vignesh Sundaresan، سرمایه‌گذار رمزارزها و بنیان‌گذار پروژه متاپورس NFT خریداری شد. او هزینه این اثر هنری را با استفاده از 42,329 اتر پرداخت کرد.

consisting of 5,000 images measuring 21,069 x 21,069 pixels

2. CryptoPunk #3100 – $7.58 Million

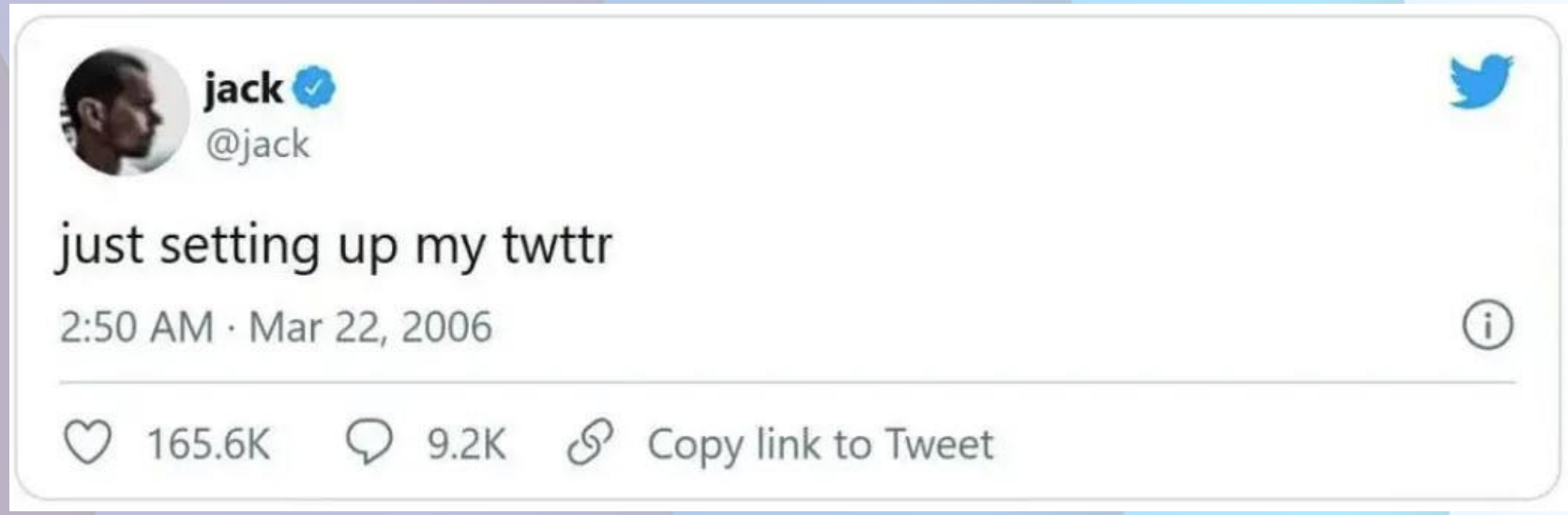


3. CryptoPunk #7804 – $7.57 Million

4. Crossroads – $6.6 Million

5. The first Tweet – $2.9 Million

Jack Dorsey tweeted the very first tweet after setting up Twitter back in 2006



سپاس از حضور شما