1 小时区块链

William Zhu

1 基础技术

区块链

密码学

分布式

密码的历史

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

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

明　文	veni	vidi	vici
密　文	YHQL	YLGL	YLFL

🔑 密码的历史

字母	百分比
a	8.2
b	1.5
c	2.8
d	4.3
e	12.7
f	2.2
g	2.0
h	6.1
i	7.0
j	0.2
k	0.8
l	4.0
m	2.4

字母	百分比
n	6.7
o	7.5
p	1.9
q	0.1
r	6.0
s	6.3
t	9.1
u	2.8
v	1.0
w	2.4
x	0.2
y	2.0
z	0.1

密码的历史

德国恩格玛加密机

- 恩格玛机使用三个转子、两个插线板、一个反射器，还有复杂的转换关系
- 一台恩格玛机器一共可以提供约 10,000,000,000,000,000，即一亿亿种可能的密钥
- 如果要暴力破解，一秒钟验算一种秘钥，则耗时三万年。

AES 加密

明文
轮密钥加
字节代换
行移位
列混合
轮密钥加
字节代换
行移位
列混合
轮密钥加
字节代换
行移位
轮密钥加
密文
第1轮
第9轮
第10轮
W[0,3]
W[4,7]
W[36,39]
W[40,43]
明文
轮密钥加
逆字节代换
逆行移位
逆列混合
轮密钥加
逆字节代换
逆行移位
逆列混合
轮密钥加
逆字节代换
逆行移位
轮密钥加
密文
第10轮
第9轮
第1轮

密码新时代的开端

1976 年，那是一个春天

DH 算法

密码新时代的开端

1977 年，那又是一个春天

RSA 算法

p 61

p 53

n=pq → n 3233

Ø(n)=(p-1)(q-1) → Ø(n) 3120

e 1<e<Ø(n)且与Ø(n)互质

17

d ed=1(mod Ø(n))

ex+Ø(n)y=1

2753

17x + 3120y=1

(x,y)=(2753,-15)

公钥 (n,e)

(3233,17)

私钥 (n,d)

(3233,2753)

密码新时代的开端

密码学

对称加密

1949年香农发表了《保密系统的信息理论》

ENIGMA的兴亡

http://www.crystalradio.cn/thread-154443-1-1.html?_t_t_t=0.592332883970812

非对称加密

1976年Whitfield Diffie & Martin Hellman首次提出了基于数学难题的公钥密码机制，1978年RSA公钥密码机制的出现

RSA

第一步：随机选择两个不相等的质数p和q。

第二步：计算p和q的乘积n。

第三步：计算n的欧拉函数φ(n)

第四步：随机选择一个整数e，条件是1<e<φ(n)，且e与φ(n)互质。

第五步：计算e对于φ(n)的模反元素d。

第六步：将n和e封装成公钥，n和d封装成私钥。

技术讲解篇

对称加密
密钥 A
+
明文：hello world
加密运算
密文：#$%^&*
传输
密钥 B
+
密文：#$%^&*
解密运算
明文：hello world
加密解密使用
相同密钥
非对称加密
密钥 A
+
明文：hello world
加密运算
密文：#$%^&*
传输
密钥 B
+
密文：#$%^&*
解密运算
明文：hello world
加密解密使用
不同密钥

Dekker互斥算法

临界资源

线程 1　　线程 2　　线程 3

哲学家就餐算法

Edsger Wybe Dijkstra

Leslie Lamport

面包店排队算法

逻辑时钟

拜占庭将军问题

BFT

PBFT

PAXOS

RAFT

9个将军，除了三个叛徒，能够达成一致。

共计 9x8x7x6=3024 次运算。共计 4000 次通信。所以说，用在实际工程中，是不现实的。

2 区块链前史

1976 Diffie-Hellman 算法

Whitfield Diffie Martin Hell

1978 RSA 算法

Ron Rivest, Adi Shamir, Len Adleman

1982 不可追踪的密码学网络支付系统
1990 ecach

David Chaum

1982 拜占庭将军问题
1990 Paxos

Leslie Lamport

1985 椭圆曲线密码学
ECC

Neal Koblitz, Victor Miller

1991 电子文档时间戳

Stuart Haber, Scott Stornetta

1991 PGP

Philip Zimmermann

1992 密码朋克邮件小组

Tim May Eric Hughes

1997年哈希现金(Hashcash)

Adam Back

1998 年 Wei Dai B-Mondy

Wei Dai 戴习为

1995 年智能合约1998 年 BitGold

Nick Szabo

1999 P2P Napster

Shawn Fanning Shaun Parker

2005 可复用的工作量证明”(RPOW)

Hal Finney

2008 比特币:一种点对点的电子现金系统

Satoshi Nakamoto

RSA

Ron Rivest
Adi Shamir
Len Adleman

Neal Koblitz Victor Miller

ECC

Secp256r1 NIST

p = 2^256 - 2^32 - 2^9 - 2^8 - 2^7 - 2^6 - 2^4 - 1
= 2^256 - 2^32 -977

a = 0

b = 7

这就是中本聪挑选的曲线，并非一条流行通用的曲线。
去掉模运算，用 x y 方程简单表示为 y^2 = x^3+7。

Secp256k1

p = 2^224(2^32 - 1) + 2^192 + 2^96 - 1

a = 115792089210356248762697446949407573530086143415290314195533631308867097853948

a = 41058363725152142129326129780047268409114441015993725554835256314039467401291

The Crypto Anarchist Manifesto

Timothy C. May <tcmay@netcom.com>

A specter is haunting the modern world, the specter of crypto anarchy.

Computer technology is on the verge of providing the ability for individuals and groups to communicate and interact with each other in a totally anonymous manner. Two persons may exchange messages, conduct business, and negotiate electronic contracts without ever knowing the True Name, or legal identity, of the other. Interactions over networks will be untraceable, via extensive re- routing of encrypted packets and tamper-proof boxes which implement cryptographic protocols with nearly perfect assurance against any tampering. Reputations will be of central importance, far more important in dealings than even the credit ratings of today. These developments will alter completely the nature of government regulation, the ability to tax and control economic interactions, the ability to keep information secret, and will even alter the nature of trust and reputation.

The technology for this revolution--and it surely will be both a social and economic revolution--has existed in theory for the past decade. The methods are based upon public-key encryption, zero-knowledge interactive proof systems, and various software protocols for interaction, authentication, and verification. The focus has until now been on academic conferences in Europe and the U.S., conferences monitored closely by the National Security Agency. But only recently have computer networks and personal computers attained sufficient speed to make the ideas practically realizable. And the next ten years will bring enough additional speed t make the ideas economically feasible and essentially unstoppable. High-speed networks, ISDN, tamper-proof boxes, smart cards, satellites, Ku-band transmitters, multi-MIPS personal computers, and encryption chips now under development will be some of the enabling technologies.

The State will of course try to slow or halt the spread of this technology, citing national security concerns, use of the technology by drug dealers and tax evaders, and fears of societal disintegration. Many of these concerns will be valid; crypto anarchy will allow national secrets to be trade freely and will allow illicit and stolen materials to be traded. An anonymous computerized market will even make possible abhorrent markets for assassinations and extortion. Various criminal and foreign elements will be active users of CryptoNet. But this will not halt the spread of crypto anarchy.

Just as the technology of printing altered and reduced the power of medieval guilds and the social power structure, so too will cryptologic methods fundamentally alter the nature of corporations and of government interference in economic transactions. Combined with emerging information markets, crypto anarchy will create a liquid market for any and all material which can be put into words and pictures. And just as a seemingly minor invention like barbed wire made possible the fencing-off of vast ranches and farms, thus altering forever the concepts of land and property rights in the frontier West, so too will the seemingly minor discovery out of an arcane branch of mathematics come to be the wire clippers which dismantle the barbed wire around intellectual property.

Arise, you have nothing to lose but your barbed wire fences!

--

Tim May

Philip Zimmermann

Bitcoin P2P e-cash paper
2008-11-01 | Thread | Satoshi Nakamoto

> , and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone. Full paper at: http://www.bitcoin.org/bitcoin.pdf Satoshi Nakamoto - The Cryptography

Re: Bitcoin P2P e-cash paper
2008-11-02 | Thread | Satoshi Nakamoto

> Satoshi Nakamoto wrote: I've been working on a new electronic cash system that's fully peer-to-peer, with no trusted third party. The paper is available at: http://www.bitcoin.org/bitcoin.pdf We very, very much need such a system, but the way I understand your proposal, it does not seem

Re: Bitcoin P2P e-cash paper
2008-11-03 | Thread | Satoshi Nakamoto

> . The Bitcoin network might actually reduce spam by diverting zombie farms to generating bitcoins instead. Satoshi Nakamoto - The Cryptography Mailing List Unsubscribe by sending unsubscribe cryptography to

Re: Bitcoin P2P e-cash paper
2008-11-07 | Thread | Satoshi Nakamoto

> [Lengthy exposition of vulnerability of a systm to use-of-force monopolies ellided.] You will not find a solution to political problems in cryptography. Yes, but we can win a major battle in the arms race and gain a new territory of freedom for several years. Governments are good at cutting

Re: Bitcoin P2P e-cash paper
2008-11-08 | Thread | Satoshi Nakamoto

> , and a constant rate seems like the best formula. Satoshi Nakamoto - The Cryptography Mailing List Unsubscribe by sending unsubscribe cryptography to

Re: Bitcoin P2P e-cash paper
2008-11-09 | Thread | Satoshi Nakamoto

> think I will be able to release the code sooner than I could write a detailed spec. You're already right about most of your assumptions where you filled in the blanks. Satoshi Nakamoto - The Cryptography Mailing

eCash 电子现金

David Chaum

简单的展开一下，eCash 是用数字货币实现了纸钞的防追踪性。王美丽到银行取钱，银行从她的账户上扣除1万元，同时给她1万元纸钞。王美丽持1万元纸钞在商场购物，店家并不查验王美丽的身份，也并不记录王美丽的购物信息，店家只关心纸钞的真实性。之后，店家把1万元纸钞存进银行，银行也并不知道这1万元来自于王美丽。

电子现金支付旨在网络上重建基于现金型交易功能的作用，它可以使用密码技术和盲签名技术实现完全匿名，从而保护用户的消费信息。自从 1982 年 Chaum 最早提出一个在线的基于 RSA 盲签名完全匿名电子现金方案以来，研究者们提出了各种各样的方案。

1988年，Chaum、Fait、Naor 利用切割-选择和RSA盲签名技术提出了一个在线的匿名电子现金方案；1991年，Okamoto、ohta 采用二叉树结构表示电子现金和利用切割选择技术的可分电子现金方案；1992年，由 Brands 最早利用限制性盲签名提出了一个离线的完全匿名电子现金方案，这是迄今为效率最高的方案之一，1993年又进行了改进；1995年，Stadler、Brickel 分别提出公平电子现金方案，除具备一般电子现金的功能外，还可跟踪电子现金和所有者跟踪协议。同年 Birckel 、Gemmel 、Kravitz 引入基于可信第三方（Trusted Third Party , TTP）的跟踪。1996年，Frankel 、Tsiounis 、Yung 基于间接证明技术提出了一个公平电子现金方案；1997 年， Davida 、Frankel 和 Tsiounis 基于零知识证明技术对上述方案进行了改进，1998年，Frankel 、Tsiounis 和 Yung 利用同构加密的思想分两次对上面方案进行了改进。1998年，Anna、Zulfikar 首先提出了基于群盲签构造一个具有多个银行参与发行的完全匿名电子现金方案；1999年，杨波等提出了选用零卡通的公平电子现金方案。

白永祥：基于盲签名的 E-cash 设计与实现　　中图分类号 TP309.7　DOI:10.3969/j.issn1672-9722.2015.07.030

时间戳

How to Time-Stamp a Digital Document

Stuart Haber stuart@bellcore.com **W . Scott Stornetta** stornetta@bellcore.com

Bellcore 445 south street Morristown,N.J. 07960-1910

Stuart Haber

Abstract

The prospect of a world in which all text, audio, picture, and video documents are in digital form on easily modifiable media media raises the issue of how to certify when a document was created or last changed . The problem is to time-stamp the data , not the medium . We propose computationally practical procedures for digital time-stamping of such documents so that it is infeasible for a user either to back-date or to forward-date his document, even with the collusion of a time-stamping service. Our procedures maintain complete privacy of the documents themselves, and require no record-keeping by the time-stamping service.

B - Money & Bit Gold

b-money

Wei Dai November 1 , 1998

I am fascinated by Tim May's crypto-anarchy. Unlike the communities traditionally associated with the word "anarchy", in a crypto-anarchy the government is not temporarily destroyed but permanently forbidden and permanently unnecessary. It's a community where the threat of violence is impotent because violence is impossible, and violence is impossible because its participants cannot be linked to their true names or physical locations.

Until now it's not clear, even theoretically, how such a community could operate. A community is defined by the cooperation of its participants, and efficient cooperation requires a medium of exchange (money) and away to enforce contracts. Traditionally these services have been provided by the government or government sponsored institutions and only to legal entities. In this article i describe a protocol by which these services can be provided to and by untraceable entities.

I will actually describe two protocols. The first one is impractical, because it makes heavy use of a synchronous and unjammable anonymous broadcast channel. However it will motivate the second, more practical protocol, In both cases i will assume the existence of an untraceable network, where senders and receivers are identified only by digital pseudonyms (i.e.public keys) and every messages is signed by its sender and encrypted to its receiver.

Bit gold

Nick Szabo

A long time ago i hit upon the idea of bit gold. The problem, in a nutshell, is that our money currently depends on trust in a third party for its value. As many inflationary and hyper inflationary episodes during the 20th century demonstrated, this is not an ideal state of affairs similarly, private bank note issue, while it had various advantages well as disadvantages, similarly depended on a trusted third party.

Precious metals and collectibles have an unforgeable scarcity due to the costliness of their creation. This once provided money the value of which was largely independent of any trusted third party. Precious metals have problems, however. It's too costly to assay metals repeatedly for common transactions. Thus a third party (usually associated with a tax collector who accepted the coins as payment) was invoked to stamp a standard amount of the metal into a coin. Transporting large values of metal can be a rather insecure affair, as the British found when transporting gold across a U-boat infested Atlantic to Canada during World War i to support their gold standard. What's worse, you can't pay online with metal.

Thus, it would be very nice if there were a protocol whereby unforgettably costly bits could be created online with minimal dependence on trusted third parties, and then securely stored, transferred, and assayed with similar minimal trust. Bit gold.

My proposal for bit gold is based on computing a string of bits from a string of challenge bits, using functions called variously "client puzzle function,""proof of word function,"or"secure benchmark function." The resulting string of bits is the proof of word. Where a one-way function is prohibitively difficult to compute backwards, a secure benchmark function ideally comes with a specific cost, measured in compute cycles, to compute backwards.

P2P 协议

Shawn Fanning

Sean Park

哈希现金

防范垃圾邮件

Hashcash

Hashcash is a proof-of-work algorithm, which has been used as a denial-of-service counter measure technique in a number of systems.

A hashcash stamp constitutes a proof-of-work which takes a parameterizable amount of work to compute for the sender. The recipient (and indeed anyone as it is publicly auditable) can verify received hashcash stamps efficiently. Hashcash was invented by Adam Back in 1997

At this point it is most widely used as the bitcoin mining function.

The email anti-spam tool, like the proof-of-work algorithm, is also called hashcash and is used to create stamps to attach to mail to add a micro-cost to sending mail to deter spamming. The main use of the hashcash stamp is as a white-listing hint to help hashcash users avoid losing email due to content based and blacklist based anti-spam systems.

Hashcash source code includes a library form, and also the algorithm is extremely simple to code from scratch with the availability of a hash library. Verification can be done by a human eye (count leading 0s) even with availability of common preinstalled command line tools such as sha1sum. The algorithm works with a cryptographic hash, such as SHA1, SHA256 or coming SHA3 that exhibits 2nd-preimage resistance. Note that 2nd-preimage resistance is a stronger hash property than the collision resistance property.

- Hashcash FAQ.
- Hashcash format info
- Hashcash Paper Aug 02 - "Hashcash - A Denial of Service Counter-Measure" (5 years on), Tech Report, *Adam Back*
- The site is slowly moving over to this new domain, some of the content is still here: http://www.cyberspace.org/hashcash/

Adam Back

可重用的工作量证明

Reusable Proofs of Work

by Hal Finney
(hal dot finney at gmail dot com)

News | What Is This? | Theory | Security | Try It Out! | FAQs | Presentation | Download

(The RPOW project is now terminated. These pages are maintained for historical purposes.)

The RPOW system provides for proof of work (POW) tokens to be reused. A POW token is something that takes a relatively long time to compute but which can be checked quickly. RPOW uses hashcash, which are values whose SHA-1 hashes have many high bits of zeros.

Normally POW tokens can't be reused because that would allow them to be double-spent. But RPOW allows for a limited form of reuse: sequential reuse. This lets a POW token be used once, then exchanged for a new one, which can again be used once, then once more exchanged, etc. This approach makes POW tokens more practical for many purposes and allows the effective cost of a POW token to be raised while still allowing systems to use them effectively.

Hal Finney

谁是中本聪

Dave Kleiman

Jed mcCaled

Neal King、Vladimir Oksman
和 Charles Bry

CSW

Hal Finney

Nick Sazbo

Dai Wei

望月新一

多利安中本

比特币 - 一种点对点的电子现金系统

1. 简介
2. 交易
3. 时间戳服务器
4. 工作量证明
5. 网络
6. 激励
7. 回收硬盘空间
8. 简化的支付确认 SPV
9. 价值的组合与分割
10. 隐私
11. 计算
12. 结论

点对点

克服双花

传统隐私模型

新隐私模型

进程

进程

2008 年 11 月 1 日，中本聪在论坛上发表白皮书。

2009 年 1 月， 中本聪发布比特币 0.1 版。

2009 年 1 月 3 日，中本聪挖掘出第一个区块。

2009 年 1 月中，哈尔芬尼第一个下载比特币客户端并运行

2009 年 1 月 12 日，哈尔芬尼收到来自中本聪的 10 个比特币，这是第一笔交易

2009 年秋天，比特币网站的维护者马迪，用 5050 个比特币，交换了 5.02 美元

2010 年 5 月 22 日，拉斯洛用 10000 个比特币换了 2 个披萨

2010 年 7 月 18 日，MT.GOX 上线运行

2011 年 4 月 罗杰大举买入比特币，将价格从 1.89 美元拉升到 3.30 美元

2011 年夏， 时代周刊及福布斯分别长篇报道比特币，引发社会对比特币的关注

Andreas M. Antonopoulos

Mastering Bitcoin

3 区块链技术原理

非对称加密

P2P 协议

时间戳

POW

交易-区块-链

UTXO

复式记账交易

张三		李四	
输入	金额	输出	金额
1	0.1 BTC	1	0.4 BTC
2	0.35 BTC		

交易费：0.05 BTC

Merkel

智能合约

C4bbcb1fbec99d65bf59d85c8cb62ee2db963f0fe106f483d9afa73bd4c39a8a
密钥转换
（单路）
Key conversion
(one-way)
Privkey (send money
with this)
私钥（用这个来发送钱）
0478d430274f8c5ec1321338151e9f27f4c676a008bdf8638d07c0b6be9ab35c71a
1518063243acd4dfe96b66e3f2ec8013c8e072cd09b3834a19f81f659cc3455
SHA256
Pubkey
公钥
RIPEMD-160
c4c5d791fcb4654a1ef5e03fe0ad3d9c598f9827
4abb8f1a
SHA256 x2
Base 58
1JwSSubhmg6iPtRjtyqhUYYH7bZg3Lfy1T
Address (receive money
with this)

复式记账交易

张三		李四	
输入	金额	输出	金额
1	0.1 BTC	1	0.4 BTC
2	0.35 BTC		

交易费：0.05 BTC

交易成链

交易编号：90000					
Input		**Output**			
来源交易		付款人	收款人	金额	时间
88888		Alice	Bob	10 USD	20170909

交易编号：90011					
Input		**Output**			
来源交易		付款人	收款人	金额	时间
90000-1		Bob	Eva	10 USD	20180101

交易编号：90088					
Input		**Output**			
来源交易		付款人	收款人	金额	时间
90011-1		Eva	Tom	5 USD	20180101
90055-1		Eva	Jason	3 USD	20180101
		Eva	Alice	4 USD	20180101
		Eva	Eva	1 USD	20180101

复式记账交易

张三		李四	
输入	金额	输出	金额
1	0.1 BTC	1	0.4 BTC
2	0.35 BTC		

交易费：0.05 BTC

POW 之钟

POW - 骰子、电表、钟、账本、投票、印钞机

区块链
新区块摞上去
大家都同意了
创世块
矿机 1
矿机 2
矿机 3
矿机 4
矿机 5
矿机 6

矿机收入
挖矿所得
交易费

2140
每区块 0 个比特币
每四年报酬减半
2016
每区块 12.5 个比特币
每四年报酬减半
2012
每区块 25 个比特币
每四年报酬减半
2009
每区块 50 个比特币
矿机 1
矿机 2
矿机 3
矿机 4
创世块
区块链
区块20000
区块20000
区块20001
挑选长得区块链

交易

交易输入

Alice 付款至 Bob 10 元人民币

Bob Bob

Alice 付款至Bob 10 元人民币

Bob 签名字迹打印体

Bob 手写签名

Bob 手写交易内容

交易输出

Bob 付款至 Eva 10 元人民币

Eva

锁定脚本

OP_DUP OP_HASH160 <Bob Key Hash> OP EQUALVERIFY OP_CHECKSIG = Bob

解锁脚本

<Bob Signature> <Bob Public Key> = Bob Alice 付款至Bob 10 元人民币

共识机制

拜占庭-算法 有奸细，跳过奸细

POW -机制 无奸细，自由选择

共享账本 **交易排序** **排序权利**

P2P 环境下确定最长链机制

掷骰子 防篡改 投票基准

POW

Copyright William Zhu - 微信号：Nweiner

共识机制

POA 共识 - 机制 有奸细，杀掉奸细

共享账本 **节点审批加入** **轮流记账**

强制共识

Fabric 共识-机制 有奸细，杀掉奸细

共享账本 **背书签名** **排序**

强制共识

CA = 身份共识　　排序 = 数据共识　　背书签名 = 业务共识

Copyright William Zhu - 微信号：Nweiner

比特币数据结构

```
{
"hex" :
"0100000003c9f3b07ebfca68fd1a6339d0808fbb013c90c6095fc93901ea774101
03489ab7000000008a473044022055bac1856ecbc377dd5e869b1a84ed1d5228c
987b098c095030c12431a4d524902205552313 0a9d0af5fc27828aba43b464ecb1
991172ba2a509b5fbd6cac97ff3af0141048aefd78bba80e2d1686225b755dacea8
90c9ca1be10ec98173d7d5f2fefbbf881a6e918f3b051f8aaaa3fcc18bbf65097ce8d
30d5a7e5ef8d1005eaafd4b3fbeffffffffc9f3b07ebfca68fd1a6339d0808fbb013c90c
6095fc93901ea77410103489ab7010000008a47304402206b993231adec55e608
5e75f7dc5ca6c19e42e744cd60abaff957b1c352b3ef9a022022a22fec37dfa2c646c
78d9a0753d56cb4393e8d0b22dc580ef1aa6cccef208d0141042ff65bd6b3ef0425
3225405ccc3ab2dd926ff2ee48aac210819698440f35d785ec3cec92a51330eb0c7
6cf49e9e474fb9159ab41653a9c1725c031449d31026affffffffc98620a6c40fc7b3a
506ad79af339541762facd1dd80ff0881d773fb72b230da010000008b483045022
040a5d957e087ed61e80f1110bcaf4901b5317c257711a6cbc54d6b98b6a8563f0
2210081e3697031fe82774b8f44dd3660901e61ac5a99bff2d0efc83ad261da5b4f
1d014104a7d1a57e650613d3414ebd59e3192229dc09d3613e547bdd1f83435cc
4ca0a11c679d96456cae75b1f5563728ec7da1c1f42606db15bf554dbe8a829f3a8
fe2ffffffffff0200bd01050000000001976a914634228c26cf40a02a05db93f2f98b768
a8e0e61b88acc096c7a6030000001976a9147514080ab2fcac0764de3a77d10cb7
90c71c74c288ac00000000",
"txid" :
"028cfae228f8a4b0caee9c566bd41aed36bcd237cdc0eb18f0331d1e87111743",
"version" : 1,
"locktime" : 0,
"vin" : [
{
"txid" :
"b79a4803014177ea0139c95f09c6903c01bb8f80d039631afd68cabf7eb0f3c9",
"vout" : 0,
"scriptSig" : {
"asm" :
"3044022055bac1856ecbc377dd5e869b1a84ed1d5228c987b098c095030c1243
1a4d524902205552313 0a9d0af5fc27828aba43b464ecb1991172ba2a509b5fbd6
cac97ff3af01
048aefd78bba80e2d1686225b755dacea890c9ca1be10ec98173d7d5f2fefbbf881a
6e918f3b051f8aaaa3fcc18bbf65097ce8d30d5a7e5ef8d1005eaafd4b3fbe",
"hex" :
"473044022055bac1856ecbc377dd5e869b1a84ed1d5228c987b098c095030c12
431a4d524902205552313 0a9d0af5fc27828aba43b464ecb1991172ba2a509b5fb
d6cac97ff3af0141048aefd78bba80e2d1686225b755dacea890c9ca1be10ec9817
3d7d5f2fefbbf881a6e918f3b051f8aaaa3fcc18bbf65097ce8d30d5a7e5ef8d1005e
aafd4b3fbe"
},
"sequence" : 4294967295
},
{
"txid" :
"b79a4803014177ea0139c95f09c6903c01bb8f80d039631afd68cabf7eb0f3c9",
"vout" : 1,
"scriptSig" : {
"asm" :
"304402206b993231adec55e6085e75f7dc5ca6c19e42e744cd60abaff957b1c352
b3ef9a022022a22fec37dfa2c646c78d9a0753d56cb4393e8d0b22dc580ef1aa6ccc
ef208d01
042ff65bd6b3ef04253225405ccc3ab2dd926ff2ee48aac210819698440f35d785ec
3cec92a51330eb0c76cf49e9e474fb9159ab41653a9c1725c031449d31026a",
"hex" :
"47304402206b993231adec55e6085e75f7dc5ca6c19e42e744cd60abaff957b1c3
52b3ef9a022022a22fec37dfa2c646c78d9a0753d56cb4393e8d0b22dc580ef1aa6
cccef208d0141042ff65bd6b3ef04253225405ccc3ab2dd926ff2ee48aac21081969
8440f35d785ec3cec92a51330eb0c76cf49e9e474fb9159ab41653a9c1725c03144
9d31026a"
},
"sequence" : 4294967295
},
{
"txid" :
"da30b272fb73d78108ff80ddd1ac2f76419533af79ad06a5b3c70fc4a62086c9",
"vout" : 1,
"scriptSig" : {
"asm" :
"3045022040a5d957e087ed61e80f1110bcaf4901b5317c257711a6cbc54d6b98b
6a8563f02210081e3697031fe82774b8f44dd3660901e61ac5a99bff2d0efc83ad2
61da5b4f1d01
04a7d1a57e650613d3414ebd59e3192229dc09d3613e547bdd1f83435cc4ca0a1
1c679d96456cae75b1f5563728ec7da1c1f42606db15bf554dbe8a829f3a8fe2f",
"hex" :
"483045022040a5d957e087ed61e80f1110bcaf4901b5317c257711a6cbc54d6b9
8b6a8563f02210081e3697031fe82774b8f44dd3660901e61ac5a99bff2d0efc83a
d261da5b4f1d014104a7d1a57e650613d3414ebd59e3192229dc09d3613e547bd
d1f83435cc4ca0a11c679d96456cae75b1f5563728ec7da1c1f42606db15bf554db
e8a829f3a8fe2f"
},
"sequence" : 4294967295
}
],
"vout" : [
{
"value" : 0.84000000,
"n" : 0,
"scriptPubKey" : {
"asm" : "OP_DUP OP_HASH160 634228c26cf40a02a05db93f2f98b768a8e0e61b
OP_EQUALVERIFY OP_CHECKSIG",
"hex" : "76a914634228c26cf40a02a05db93f2f98b768a8e0e61b88ac",
"reqSigs" : 1,
"type" : "pubkeyhash",
"addresses" : [
"1A3q9pDtR4h8wpvyb8SVpiNPpT8ZNbHY8h"
]
}
},
{
"value" : 156.83000000,
"n" : 1,
"scriptPubKey" : {
"asm" : "OP_DUP OP_HASH160 7514080ab2fcac0764de3a77d10cb790c71c74c2
OP_EQUALVERIFY OP_CHECKSIG",
"hex" : "76a9147514080ab2fcac0764de3a77d10cb790c71c74c288ac",
"reqSigs" : 1,
"type" : "pubkeyhash",
"addresses" : [
"1Bg44FZsoTeYteRykC1XHz8facWYKhGvQ8"
]
}
}
],
"blockhash" :
"0000000000007c639f2cbb23e4606a1d022fa4206353b9d92e99f5144bd74611",
"confirmations" : 147751,
"time" : 1301705313,
"blocktime" : 1301705313
```

SPV 机制图

区块体
交易
……
交易
区块体
交易
……
交易
区块体
交易
……
交易 001
全节点钱包 B
Pre Hash
Nonce
Merkel Root
Timestamp
区块头
1 1 0 0 0 0 0 0 1 1 1 1 1 1 1 1
A 发送自己的 Bloom 过滤器给全节点钱包
• B 利用 A 的 Bloom 过滤器
• 发送符合过滤器条件的交易 001 至 A
• 发送交易 001 的 Merkle 验证路径至 A
Bloom 过滤器
SPV 钱包 A
哈希 h034
哈希 h012
哈希 h002
哈希 h001
交易 002
交易 001

Bitcoin Logic

Ethereum Logic

脚本与虚拟机

Unlocking Script
(scriptSig)
+
Locking Script
(scriptPubKey)
<sig> <PubK>
DUP HASH160 <PubKHash> EQUALVERIFY CHECKSIG
Unlock Script (scriptSig) is provided by the user to resolve the encumbrance
Lock Script (scriptPubKey) is found in a transaction output and is the encumbrance that must be fulfilled to spend the output

EVM
code
storage
ROM
RAM
non-volatile
stack
args
memory
ROM
RAM
volatile
[[<addr>]]
@@<addr>
[<addr>]
@<addr>
Calldataloaded <byte>

4 区块链的意义

2009年2月11日 比特币启动

The Times 03/Jan/2009 Chancellor on brink of second bailout for banks。

政治经济法律学者

约翰 洛克
亚当·斯密
阿克顿勋爵
弗里德里希·奥古斯特·冯·哈耶克
路德维希·海因里希·艾德勒·冯·米塞斯
罗伯特·诺齐克
穆瑞·罗斯巴德

密码朋克黑客天才程序员

大卫乔姆（盲签名发明人）
菲利普·希默曼（PGP技术的开发者）
约翰·吉尔摩（太阳微系统公司的明星员工）
斯蒂文·贝洛文（美国贝尔实验室研究员，哥伦比亚大学计算机科学教授）
布拉姆·科恩（BT下载的作者）
蒂姆希·C·梅（英特尔公司前首席科学家）
阿桑奇（维基解密创始人）
哈尔·芬尼（PGP加密的发明人之一）
尼克·萨博 （智能合约发明人，律师程序员学者）

经济模型

The Times 03/Jan/2009 Chancellor on brink of second bailout for banks

通缩的货币

货币的发行机制

哈耶克

competitive private currencies that permits the market alone to choose the dominant currency the world over

社会学的意义

人类历史上，罕见的，未受暴力保护，未被暴力消灭的自治社群组织

功用篇

去中心化交易
交易合法
防止双花
共识生态
隐私
验证交易
UTXO
交易签名
时间戳
工作量证明
区块链存储
发币机制
公私密钥对
SPV
默克尔树
P2P协议

G

功用篇

匿名 保护隐私
数据明文
对称加密
无法篡改
共享账本
永不停机
难以攻击
信任与共识
效率低下
容量有限
去中心化
权力的重新分配

权力篇

任何计算机都可参与，都有成为节点的权力（公开链条）

每个节点都有保护用户隐私的权力（公私钥）

每个节点都有访问全部数据的权力（全账本下载）

每个节点都有互相获取数据的权力（P2P部署）

每个节点都有验证交易的权力（交易验证）

每个节点都有打包记账的权力（矿机挖矿）

每个节点都有货币发行权（货币发行及矿机挖矿）

每个节点都有选择分叉的权力（比特币客户端的选择权）

在比特币生态中：

每位参与者都有阅读开源代码的权力（比特币客户端代码开源）

每位开发者都有参与写代码的权力（参与开源社区的开发）

每位黑客都有攻击系统的权力（最珍贵的权力）

代码开发权

代码访问权

记账参与权

数据访问权

人类社会的组织方式

中央集权

联邦分权

- 自治组织
- 基于共识的宪法
- 保护自由，鼓励多样化
- 分权与制衡
- 法律面前的平等
- 民主的手段，多数vs少数
- 投票选举代议制社会活动

去中心化的组织生命力大于中央控制的组织

造物的9大规律

分布式状态

自下而上的控制

培养递增收益

模块化生长

边缘最大化

礼待错误

不求目标最优；但求目标众多

谋求持久的不均衡

变自生变

N 维纳博士

将要消失的……物件

将要变化的……组织

“

No, don’t ‘bring it on.’
The project needs to grow gradually so the software can be strengthened along the way. I make this appeal to WikiLeaks not to try to use Bitcoin. Bitcoin is a small beta community in its infancy. You would not stand to get more than pocket change, and the heat you would bring would likely destroy us at this stage

比特币系统还很不成熟，阿桑奇所带来的对于比特币的关注会摧毁比特币

”

哈耶克： 自由就是不被强制

罗斯巴德： 自由就是不被暴力侵犯所有权

字段名	数据类型	主键	外键	非空	唯一	自增	默认值	字段描述
account_id	int	是	否	是	是	是		账户 ID,仅作主键用
account_name	varchar(20)	否	否	是	否	否		户主姓名
account_no	char(19)	否	否	是	是	否		银行账号
account_id_number	char(18)	否	否	是	否	否		户主身份证号
account_password	varchar(50)	否	否	是	否	否		账户密码
account_sms	int	否	否	是	否	否	1	短信提醒,1 开通,0 未开通
account_mobile	char(11)	否	否	否	否	否		户主手机号码
account_sum	double	否	否	是	否	否	0.00	账户余额
account_satus	int	否	否	是	否	否	0	账户状态,0 正常,1 冻结,2 注销

0100000003c9f3b07ebfca68fd1a6339d0808fbb013c90c6095fc93901ea77410103489ab7000000008a473044022055b
ac1856ecbc377dd5e869b1a84ed1d5228c987b098c095030c12431a4d52490220555523130a9d0af5fc27828aba43b46
4ecb1991172ba2a509b5fbd6cac97ff3af0141048aefd78bba80e2d1686225b755dacea890c9ca1be10ec98173d7d5f2fef
bbf881a6e918f3b051f8aaaa3fcc18bbf65097ce8d30d5a7e5ef8d1005eaafd4b3fbeffffffffc9f3b07ebfca68fd1a6339d0808
fbb013c90c6095fc93901ea77410103489ab7010000008a47304402206b993231adec55e6085e75f7dc5ca6c19e42e74
4cd60abaff957b1c352b3ef9a022022a22fec37dfa2c646c78d9a0753d56cb4393e8d0b22dc580ef1aa6cccef208d01410
42ff65bd6b3ef04253225405ccc3ab2dd926ff2ee48aac210819698440f35d785ec3cec92a51330eb0c76cf49e9e474fb91
59ab41653a9c1725c031449d31026affffffffc98620a6c40fc7b3a506ad79af339541762facd1dd80ff0881d773fb72b230da
010000008b483045022040a5d957e087ed61e80f1110bcaf4901b5317c257711a6cbc54d6b98b6a8563f02210081e369
7031fe82774b8f44dd3660901e61ac5a99bff2d0efc83ad261da5b4f1d014104a7d1a57e650613d3414ebd59e3192229d
c09d3613e547bdd1f83435cc4ca0a11c679d96456cae75b1f5563728ec7da1c1f42606db15bf554dbe8a829f3a8fe2ffffffff
f0200bd01050000000001976a914634228c26cf40a02a05db93f2f98b768a8e0e61b88acc096c7a6030000001976a9147
514080ab2fcac0764de3a77d10cb790c71c74c288ac00000000

“数字”

说了就算数！

区块链 VS 人工智能篇

区块链

机器时代的组织
机器时代的价值

人工智能

机器时代的智慧
机器时代的决策

物联网

机器时代的万物

5 行业发展及应用

比特金，莱特银

域名币

万事达币

OP_RETURN

区块链 2.0

- Token
- 资产描述
- 存证
- 供应链
- 保险
- 交易所
- 游戏
- 内容与社交
- 投票与选举
- 物联网
- 可编程货币

共识篇

```
pragma solidity ^0.4.21;

contract Coin {                                   创建一个叫 “Coin” 的合约
    address public minter;                        定义公共变量 Minter，用来存放以太坊地址
    mapping (address => uint) public balances;    定义公共变量 balances，mapping 类型

    // Events allow light clients to react on
    // changes efficiently.
    event Sent(address from, address to, uint amount);定义 “事件”，在日志中记录 From,to,amount

    // This is the constructor whose code is
    // run only when the contract is created.
    function Coin() public {                      初始化 Coin 这个合约
        minter = msg.sender;                      将初始化的以太坊地址，设置为 minter
    }

    function mint(address receiver, uint amount) public {      定义功能 mint，用来发行代币
        if (msg.sender != minter) return; 代币发行只能由 minter 地址执行，其他地址执行则出错
        balances[receiver] += amount;  发行代币到 receiver 地址
    }

    function send(address receiver, uint amount) public { 定义功能 send，用来转移代币
        if (balances[msg.sender] < amount) return;     如果要转移代币的地址余额不足，则报错
        balances[msg.sender] -= amount; 转移代币的地址减去相应数量的余额
        balances[receiver] += amount;  接受代币的地址加上相应数量的余额
        emit Sent(msg.sender, receiver, amount);       记录日志
    }
}
```

据 etherscan.io 网站在 2018 年 6 月12 日的数据显示，以太坊上的 ERC 20 代币智能合约共计 90738 种。可据可靠数据统计，2018 年第一季度，在以太坊上筹集的资金就高达 65 亿美元。

2018 年 6 月12日，以太坊上共约 3700 万账户地址，每日交易量达 150 万笔。以太坊全球共有17000 个节点，开发者社区共有 25 万名开发者。

据 stateofthedapps.com 网站在 2018 年 6 月12 日的数据显示，以太坊上共部署了 1600 个应用。

据 cap-radar.com 网站 2018 年 6 月份统计，以太坊上的 Dapp 应用，以游戏种类占比最大，达到 70%；赌博类次之，为 10%；交易市场为 2.7%；其它类型共约 17%。

共识篇

PBFT

一致性达成算法

Paxos

计算机中最常用的一致性算法

Raft

简单的 Paxos

dBFT

投票选择节点

PoSt

硬盘空间投票

Pool

基于 PBFT

PoW

每个 CPU 一票

PoS

一个币龄一票

DPoS

代议制，一币龄一票

Casper

用币投注

Ripple

俱乐部

PoET

严格每个 CPU 一票

比特币是现金

以太币是应用的驱动 ERC 20

Ripple 币是桥梁货币

如果链失去了币，就是鸟儿失去了.....

STEEM 有三种币

YEE COIN

流行区块链篇

比特币：反贼气质浓郁的电子货币

以太坊：我乖一点，我是去中心化的IT基础设施

超级账本：我更乖，我是企业的IT基础设施

Quorum：我最乖，我替你保密哦，银行永生

EOS：我快，每秒百万交易

闪电网络：我更快，TPS 无上限

雪球：区块？链？.....天下无链，看我 DAG 大法

RIPPLE：汇款，换汇找我，干掉SWIFT

Steem：发帖挣钱，点赞评论也挣钱

IPFS：网站.....HTTP 该换一换了

多链：一键发链

侧链：天下链条是一家，一定要沟通

Cosmos：链的互联网

电报：给我 20 亿美元，一统天下

区块链应用篇

数字货币

自治组织

黄金投资

汇款

网站

发帖挣钱

资产登记

60 万颗钻石

游戏

证券交易所

保险

版权

供应链

投票与选举

赌博

存证

尼克萨博 虽然暴徒还可以暴力攫取物质资产，但延续存在的正确的所有权记录将是留在盗用者眼中的眼中钉。

资产描述 - Everledger

存证 - Factom

经过这样的分层架构的处理，Factom 能够对海量的数据进行存储与存证。64M 的 “目录区块” 可以管理约 500 万个 “记录” 文件，而这 500 万个文件，对应在比特币上，可能只是交易里的一个 40 字节的信息。

供应链 - Provenance

生产者 - 原初产品的生产，诸如棉花种植、捕鱼等。

工长 - 对原材料进行加工的企业，例如鱼罐头加工厂。

登记中心 - 对供应商上其他角色进行认证与登记的组织。

标准组织 - 对供应链各个环节提供标准、规范、合规性要求的组织。

验证者与审计者 - 基于标准，对各个环节、角色、产品进行验证与审计的组织。

用户 - 也就是消费者。

保险 - InsurChain

证券交易所 - Linq

chain.com

游戏 - Cryptokitties

ERC 20

ERC 777

ERC 1404

ERC 1410

ERC 1400

迷恋猫的英文叫做 croptokitties，直译过来就是密码学猫咪的意思。这种猫咪确实不同于传统互联网游戏中的角色，每一只猫咪都是独特的，其基因控制着诸如眼睛的形状、毛的颜色、花纹、嘴巴形状等 7-8 种特性，而每一种特性具有 256 种变化可能性，这样一来，几乎不可能重复，每一只猫都是独特的。猫咪之间可以繁育，通过算法将父母猫咪的基因杂糅一起，而这算法是不公开的。

賭博 - Bitcasino, peer plays

PeerplaysDB.com

Block explorer and database for the Peerplays blockchain.

Recent Blockchain Activity
Displaying most recent irreversible blocks.

View more blocks

14918001 Current Height

13 Reversable blocks awaiting concensus

Height	Time	Witness	Transactions	Operations
14917987	2018-11-10 10:43:21 UTC	scissors-witness	0	0
14917986	2018-11-10 10:43:18 UTC	spacecrypt-witness	0	0
14917985	2018-11-10 10:43:15 UTC	educatedwarrior-witness	0	0
14917984	2018-11-10 10:43:12 UTC	bitcoinsig	0	0
14917983	2018-11-10 10:43:09 UTC	taconator-witness	0	0
14917982	2018-11-10 10:43:06 UTC	melea-trust	0	0
14917981	2018-11-10 10:43:03 UTC	agoric.systems	0	0
14917980	2018-11-10 10:43:00 UTC	winner.winner.chicken.dinner	0	0
14917979	2018-11-10 10:42:57 UTC	houdini-witness	0	0

内容/社交 - Cryptokitties

投票选举 - Agora

What is Agora ?

Agora is a blockchain-based voting ecosystem allowing anyone anywhere to vote online from a digital device in a fully secure, easy and certain way.

Agora 是一家瑞士的公司，专注于投票技术，公司成立于 2015 年。他们的区块链技术，基于自己的链 Skipchains 和 Bitcoin, Bitcoin 公链在方案中起到存证的作用。SkipChain 的共识算法中，有三种节点，一种是写节点，具有最高信任，可以进行区块打包；一种是认可的第三方认证节点，可以对区块数据进行验证签字；第三类是只读节点，仅仅可以同步点数据。

2018 年 8 月，Agora 开始 ICO，发布自己的 Token。

物联网 - Polkadot

- 设备固件哈希：将设备固件的哈希值存入区块链，这样，设备的状态得以验证，任何对设备的篡改与攻击，就得以防范。
- 指令认证：当设备之间需要通信，为了保证安全，保证指令信息未被劫持和篡改，设备需要将指令先提交区块链，以作存证。而执行指令的设备，要将接收的指令，与区块链上指令对比，确保一致，方才执行。
- 设备身份协议：每件设备都拥有区块链上的公私钥对，设备之间传递消息，利用非对称加密的加密和签名技术，保证信息的传递安全与来源无误。
- 设备商营：区块链上的认证代理，可对设备进行审核与验证，并赋予设备商誉身份。
- IOT数据管理：用区块链去中心化的模式，管理 IOT 数据的存储、传输与查询检索。

四个阶段

银行

货币
简单资产
简单合约
无预言机

交易所

证券
复杂资产
可编程产权
简单合约
预言机

保险

复杂合约
可编程业务
复杂预言机
自治组织

物联网

多链互联
价值网络
可编程世界

6 法律法规

- 是否可以持有数字资产，是否可以交易
- 机构投资是否可以持有数字资产
- 数字资产是否受法律保护
- 个人或机构可否发行数字资产 （开放|封闭） （功用）
- 是否可以经营数字资产交易场所
- 数字资产是否归为证券，并受证券法管辖
- 区块链的备案制度

区块链来源：

A Cypherpunk’s Manifesto

by Eric Hughes

Privacy is necessary for an open society in the electronic age. Privacy is not secrecy. A private matter is something one doesn’t want the whole world to know, but a secret matter is something one doesn’t want anybody to know. Privacy is the power to selectively reveal oneself to the world.

区块链关于：

隐私、事实、所有权、信任、共识、组织、协作、自由、权力、规则、法律

Copyright William Zhu - 微信号：Nweiner