



Blockchain

© Sen LEI

Background

Libra & DCEP

The Byzantine  
Generals Problem

Blockchain

Cryptocurrencies

Attacks

Discussion

Cautious optimism

# Blockchain

Game Theory × Economy × Technology

Sen LEI <sup>†</sup> <sup>‡</sup>

<sup>†</sup>UCSB

University of California, Santa Barbara  
CA, U.S.

<sup>‡</sup>MiningLamp Technology  
Beijing, China

Nov, 2019



## Blockchain

© Sen LEI

### Background

Libra & DCEP

The Byzantine  
Generals Problem

### Blockchain

Cryptocurrencies

Attacks

### Discussion

Cautious optimism

- 1 Background
  - Libra & DCEP
  - The Byzantine Generals Problem
- 2 Blockchain
  - Cryptocurrencies
  - Attacks
- 3 Discussion
  - Cautious optimism





# The trust machine

Blockchain

© Sen LEI

Background

Libra & DCEP

The Byzantine  
Generals Problem

Blockchain

Cryptocurrencies

Attacks

Discussion

Cautious optimism



“

The blockchain lets people who have no particular confidence in each other collaborate without having to go through a neutral central authority. Simply put, it is a machine for creating trust.

”



# Timeline

Blockchain

© Sen LEI

Background

Libra & DCEP

The Byzantine  
Generals Problem

Blockchain

Cryptocurrencies

Attacks

Discussion

Cautious optimism



## An Introduction to Libra

White Paper • From the Libra Association Members

**Libra's mission is to enable a simple global currency and financial infrastructure that empowers billions of people.**

This document outlines our plans for a new decentralized blockchain, a low-volatility cryptocurrency, and a smart contract platform that together aim to create a new opportunity for responsible financial services innovation.



2019 年 6 月 18 日, Facebook 发布 Libra 白皮书。  
2019 年 10 月 11 日, 人民银行公开声明表示 DCEP 推出在即。



# What is Libra & DCEP?

Blockchain

© Sen LEI

Background

Libra & DCEP

The Byzantine  
Generals Problem

Blockchain

Cryptocurrencies

Attacks

Discussion

Cautious optimism

## Libra

超主权货币

M0 : € £ \$ ¥ ~~₩~~ ...

作为一种简单、无国界的货币和金融基础设施，为数十亿人提供无国界、低成本、普惠的金融服务。

## Digital Currency Electronic Payment (DCEP)

主权货币

M0 : ¥(CHY)

双离线支付

双层运营体系，避免金融脱媒。



# What is Libra & DCEP ?

Blockchain

© Sen LEI

Background

Libra & DCEP

The Byzantine  
Generals Problem

Blockchain

Cryptocurrencies

Attacks

Discussion

Cautious optimism

## Money Supply Type

- **M0** : The stock of physical currency (The narrowest definition of money)
- **M1** :  $M0 + \text{Demand deposits (checking account balances)}$
- **M2** :  $M1 + \text{Time deposits}$

Note that not all of the classifications are widely used, and each country may use different classifications.



# The Byzantine Generals Problem

Blockchain

© Sen LEI

Background

Libra & DCEP

The Byzantine  
Generals Problem

Blockchain

Cryptocurrencies

Attacks

Discussion

Cautious optimism

## The Byzantine Generals Problem

LESLIE LAMPORT, ROBERT SHOSTAK, and MARSHALL PEASE  
SRI International

Reliable computer systems must handle malfunctioning components that give conflicting information to different parts of the system. This situation can be expressed abstractly in terms of a group of generals of the Byzantine army camped with their troops around an enemy city. Communicating only by messenger, the generals must agree upon a common battle plan. However, one or more of them may be traitors who will try to confuse the others. The problem is to find an algorithm to ensure that the loyal generals will reach agreement. It is shown that, using only oral messages, this problem is solvable if and only if more than two-thirds of the generals are loyal; so a single traitor can confound two loyal generals. With unforgeable written messages, the problem is solvable for any number of generals and possible traitors. Applications of the solutions to reliable computer systems are then discussed.

Categories and Subject Descriptors: C.2.4. [Computer-Communication Networks]: Distributed Systems—*network operating systems*; D.4.4 [Operating Systems]: Communications Management—*network communication*; D.4.5 [Operating Systems]: Reliability—*fault tolerance*

General Terms: Algorithms, Reliability

Additional Key Words and Phrases: Interactive consistency

ACM Transactions on Programming Languages and Systems Vol.4, No. 3, July 1982, Pages 382-401



# The Byzantine Generals Problem

Blockchain

© Sen LEI

Background

Libra & DCEP

The Byzantine  
Generals Problem

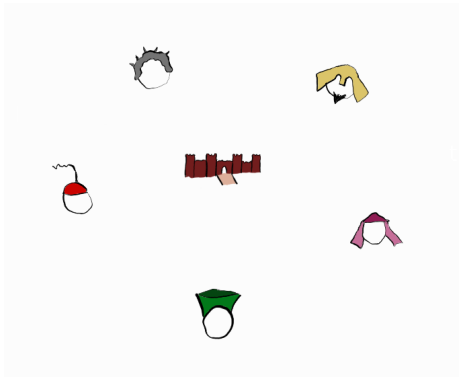
Blockchain

Cryptocurrencies

Attacks

Discussion

Cautious optimism



(image source)





# The Byzantine Generals Problem

Blockchain

© Sen LEI

Background

Libra & DCEP

The Byzantine  
Generals Problem

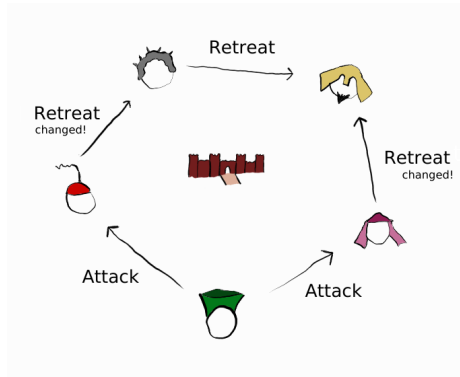
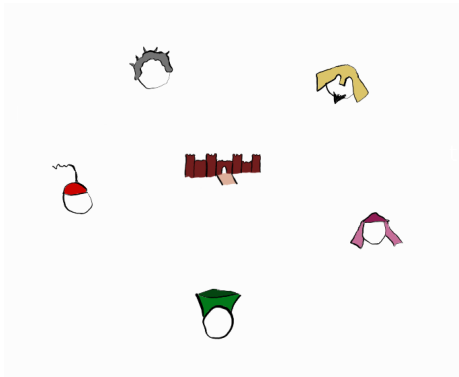
Blockchain

Cryptocurrencies

Attacks

Discussion

Cautious optimism



(image source)



# The Byzantine Generals Problem

Blockchain

© Sen LEI

Background

Libra & DCEP

The Byzantine  
Generals Problem

Blockchain

Cryptocurrencies

Attacks

Discussion

Cautious optimism

## 解决方案

- 用口头信息
- 用书面协议
- 区块链技术
  - 共识机制: Proof-of-Work (PoW)
  - 加密算法: 非对称加密



# The Byzantine Generals Problem

Blockchain

© Sen LEI

Background

Libra & DCEP

The Byzantine  
Generals Problem

Blockchain

Cryptocurrencies

Attacks

Discussion

Cautious optimism

## 解决方案

- 用口头信息
- 用书面协议
- 区块链技术
  - 共识机制: Proof-of-Work (PoW)
  - 加密算法: 非对称加密



# Sybil Attack

Blockchain

© Sen LEI

Background

Libra & DCEP

The Byzantine  
Generals Problem

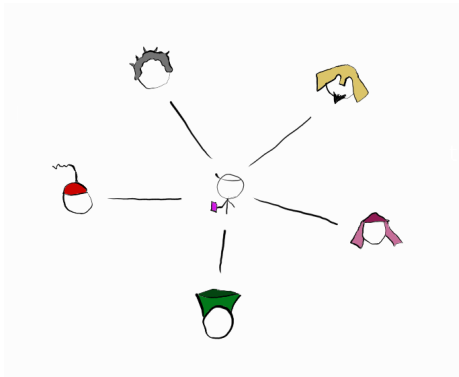
Blockchain

Cryptocurrencies

Attacks

Discussion

Cautious optimism



(image source)



# Sybil Attack

Blockchain

© Sen LEI

Background

Libra & DCEP

The Byzantine  
Generals Problem

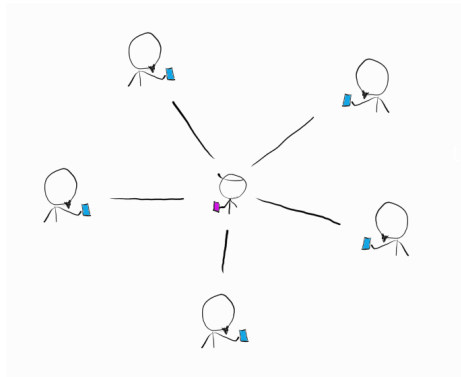
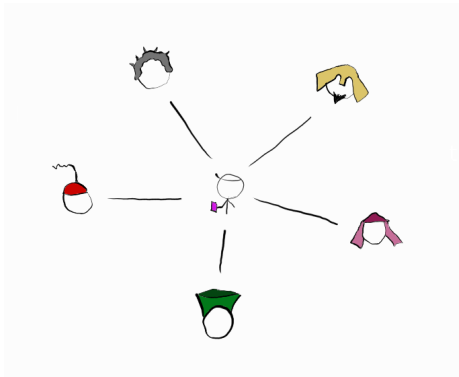
Blockchain

Cryptocurrencies

Attacks

Discussion

Cautious optimism



(image source)



© Sen LEI

## Cryptocurrencies

### Attacks





# Satoshi Nakamoto & Bitcoin

Blockchain

© Sen LEI

Background

Libra & DCEP

The Byzantine  
Generals Problem

Blockchain

Cryptocurrencies

Attacks

Discussion

Cautious optimism

## 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 majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, 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.

## Robert's Rules of Order



The Original Manual for  
Assembly Rules,  
Business Etiquette, and Conduct

Henry Robert

Foreword by Chris MacDonald and Nancy Walton



# Satoshi Nakamoto & Bitcoin

Blockchain

© Sen LEI

Background

Libra & DCEP

The Byzantine  
Generals Problem

Blockchain

Cryptocurrencies

Attacks

Discussion

Cautious optimism

## Bitcoin Solution

- Consensus Mechanism
  - Proof-of-Work (PoW)
  - Proof-of-Stake (PoS)
  - Delegated Proof-of-Stake (DPoS)
- Encryption Algorithm
  - Asymmetric-key Encryption





# Satoshi Nakamoto & Bitcoin

Blockchain

© Sen LEI

Background

Libra & DCEP

The Byzantine  
Generals Problem

Blockchain

Cryptocurrencies

Attacks

Discussion

Cautious optimism

## Bitcoin Solution

- Consensus Mechanism
  - Proof-of-Work (PoW)
  - Proof-of-Stake (PoS)
  - Delegated Proof-of-Stake (DPoS)
- Encryption Algorithm
  - Asymmetric-key Encryption



# Satoshi Nakamoto & Bitcoin

Blockchain

© Sen LEI

Background

Libra & DCEP

The Byzantine  
Generals Problem

Blockchain

Cryptocurrencies

Attacks

Discussion

Cautious optimism

## Bitcoin Solution

- Consensus Mechanism
  - Proof-of-Work (PoW)
    - Hard enough
    - Easy to verify
    - Memoryless
  - Proof-of-Stake (PoS)
  - Delegated Proof-of-Stake (DPoS)
- Encryption Algorithm
  - Asymmetric-key Encryption



区块链上的共识机制主要解决由谁来构造区块，以及如何维护区块链统一的问题。

拜占庭容错问题需要解决的也同样是誰来发起信息，如何实现信息的统一同步的问题。



# The trust machine

Blockchain

© Sen LEI

Background

Libra & DCEP

The Byzantine  
Generals Problem

Blockchain

Cryptocurrencies

Attacks

Discussion

Cautious optimism



“

The blockchain lets people who have no particular confidence in each other collaborate without having to go through a neutral central authority. Simply put, it is a machine for creating trust.

”



# The trust machine

## Blockchain

© Sen LEI

## Background

Libra & DCEP

The Byzantine  
Generals Problem

## Blockchain

### Cryptocurrencies

Attacks

## Discussion

Cautious optimism



# Other Cryptocurrencies

Blockchain

© Sen LEI

Background

Libra & DCEP

The Byzantine  
Generals Problem




Blockchain

Cryptocurrencies

Attacks

Discussion

Cautious optimism

	 Bitcoin 比特币	 Ethereum 以太坊	 EOS
所属阶段	区块链 1.0	区块链 2.0	区块链 3.0
功用	数字货币	智能合约 (通证)	应用
共识机制	工作量证明 (POW)	现在: POW 未来: POW+POS	委托权益证明 (DPOS)
区块生产	挖矿节点	挖矿节点	超级节点 (BP 区块生产者)
性能 TPS 系统的交易吞吐量	<10	~ 15	数百至数千 宣称达百万
编程	比特币脚本 UTXO	图灵完备的脚本语言 Solidity	C++/Rust/Python/ Solidity
虚拟机	—	EVM	WASM Web Assembly
开发支持	—	主要支持 智能合约	支持账户、 存储等
进一步改进	闪电网络 (Lightning Network) 等	分片 (Sharding)	—
类比	黄金挖矿	高速公路建设	房地产开发



# Attacks

Blockchain

© Sen LEI

Background

Libra & DCEP

The Byzantine  
Generals Problem

Blockchain

Cryptocurrencies

Attacks

Discussion

Cautious optimism

## Selfish-Mining Attack

*Majority is not Enough : Bitcoin Mining is Vulnerable*

## Eclipse Attacks

*Eclipse Attacks on Bitcoin's Peer-to-Peer Network*



Blockchain

© Sen LEI

Background

Libra & DCEP

The Byzantine  
Generals Problem

Blockchain

Cryptocurrencies

Attacks

Discussion

Cautious optimism

# Hype? Panacea?

对于目前国内的区块链技术水平，应该一分为二地来看。

- 应用层面居于全球前列，特别是国内有着全世界最丰富的区块链落地应用场景和行业资源。
- 原创技术创新以及理论层面尚需努力，特别是有关区块链底层的数学等基础学科研究目前是严重拖后腿的。





## Blockchain

© Sen LEI

## Background

Libra & DCEP

The Byzantine  
Generals Problem

## Blockchain

Cryptocurrencies

Attacks

## Discussion

Cautious optimism

