

Blockchain 101

指導教授：林宗男

助教：陳秉珪

1

About this course

Goal

- Understanding the importance of blockchain
- Learning the basic cryptography and consensus algorithm used in blockchain
- Building a prototype of blockchain to know how it works
- Understanding the concept of smart contract
- Scripting your own smart contract

Schedule (5 weeks)

■ 1. 09/18 Blockchain 101

■ 2. 10/02 Pseudo-Bitcoin

Announcement of HW1

■ 3. 10/16 Pseudo-Bitcoin, Smart Contract

Announcement of HW2


■ 4. 10/30 Smart Contract

■ 5. 11/13 More... & Demo your HWs

Deadlines 00:00 AM

Grading Policy

- 40% HW1 + 30% HW2 + 30% Bonus
- Bonus:

		
2 points	5 points	10 points
Easy(E)	(M)	Hard(H)

About Bonus

- ceiba 作業區
- Wrong answer would get partial credits

2

Blockchain101

Ask questions

Ledger

How to ensure the ledger would not be modified?

Who should maintain the ledger?

...?

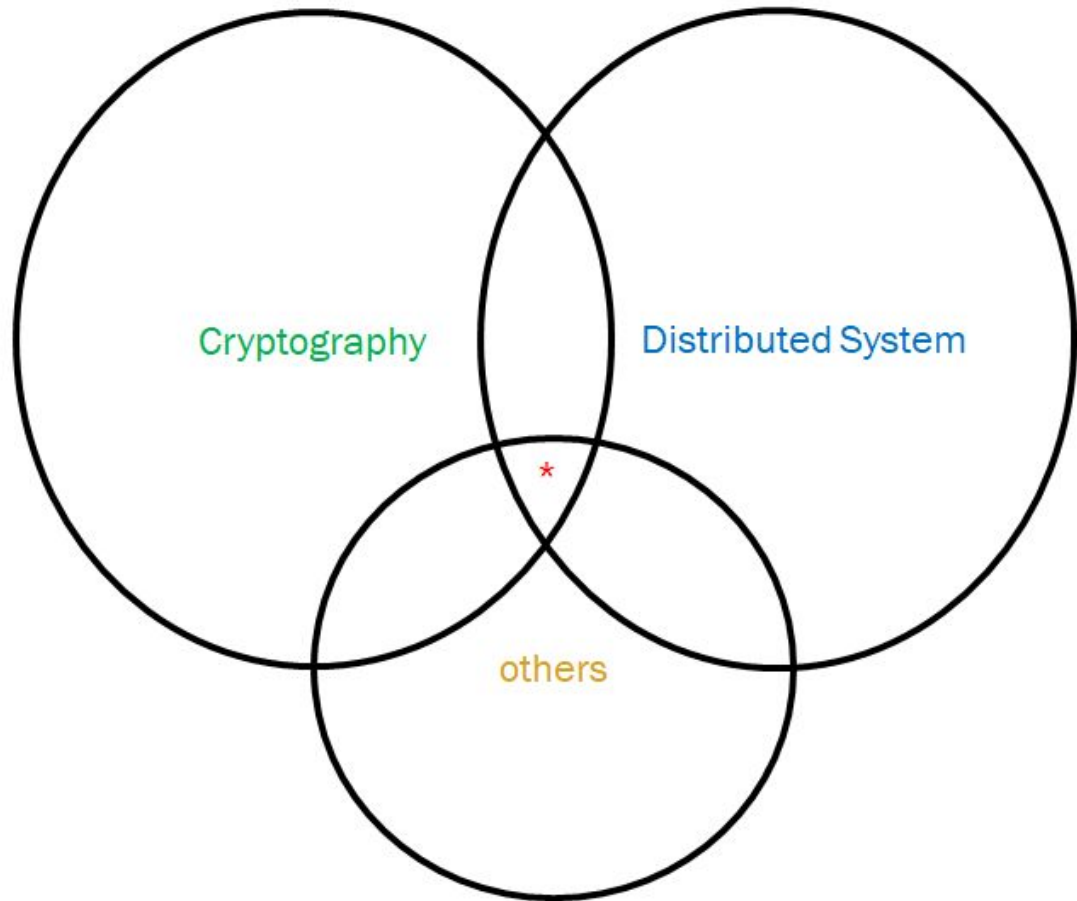
Account

How to prove that you are you?

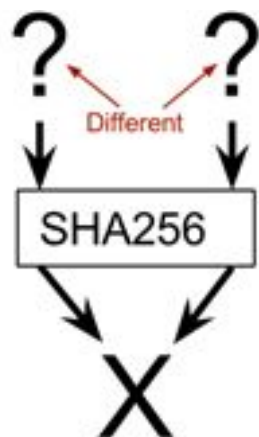
...?

Key Problems

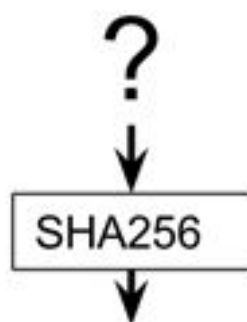
- (Confidentiality) -> Privacy
- Integrity
- Message Authentication
- Non-repudiation
- ...
- Distributed Consensus
- Scalability
- ...
- Database
- Business



Hash

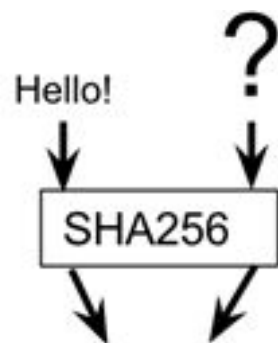


Collision resistance



334d016f755cd6dc58c53a86e1
83882f8ec14f52fb05345887c8
a5edd42c87b7

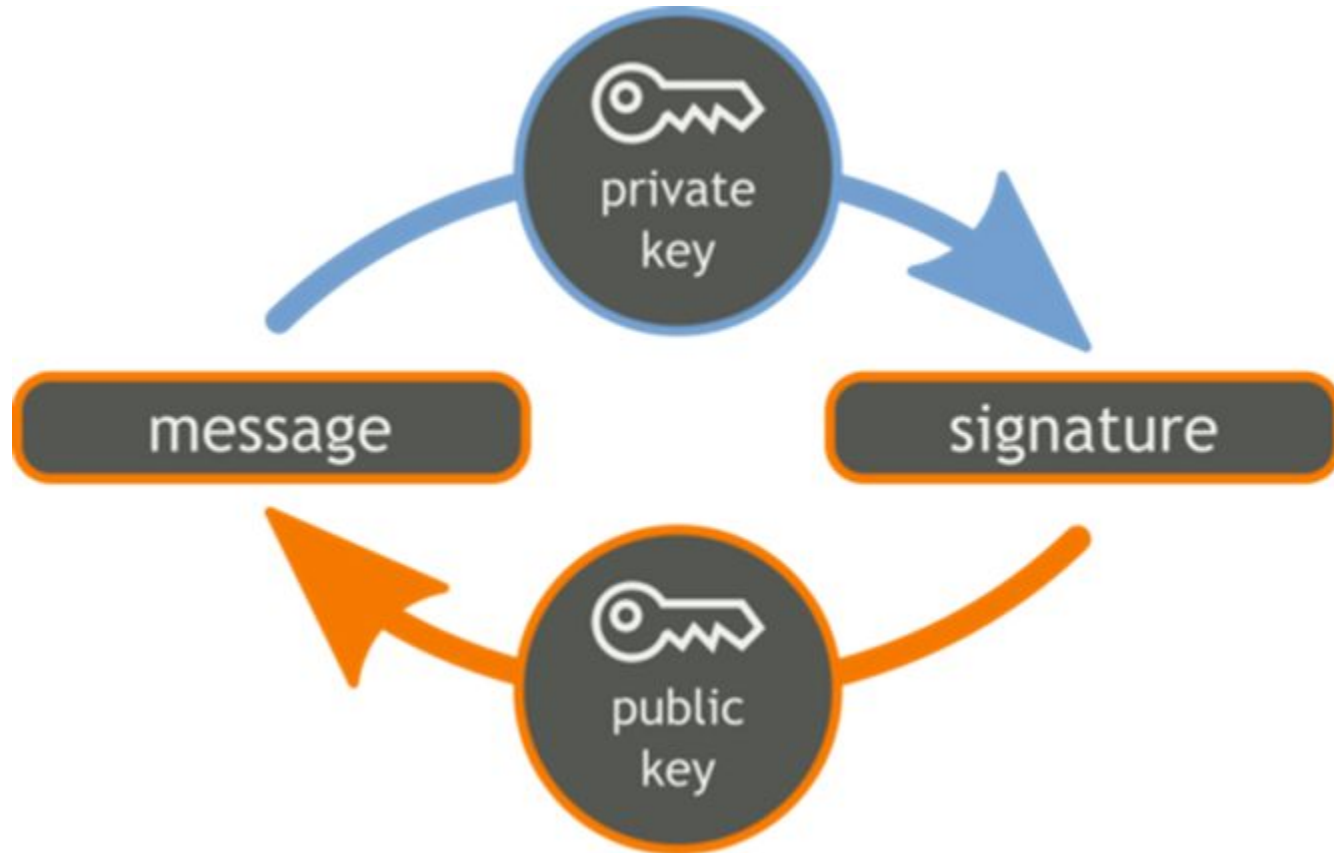
Preimage resistance



334d016f755cd6dc58c53a86e1
83882f8ec14f52fb05345887c8
a5edd42c87b7

Second-preimage
resistance

Public-key cryptography



Course Materials

Ledger:

<https://anders.com/blockchain/>

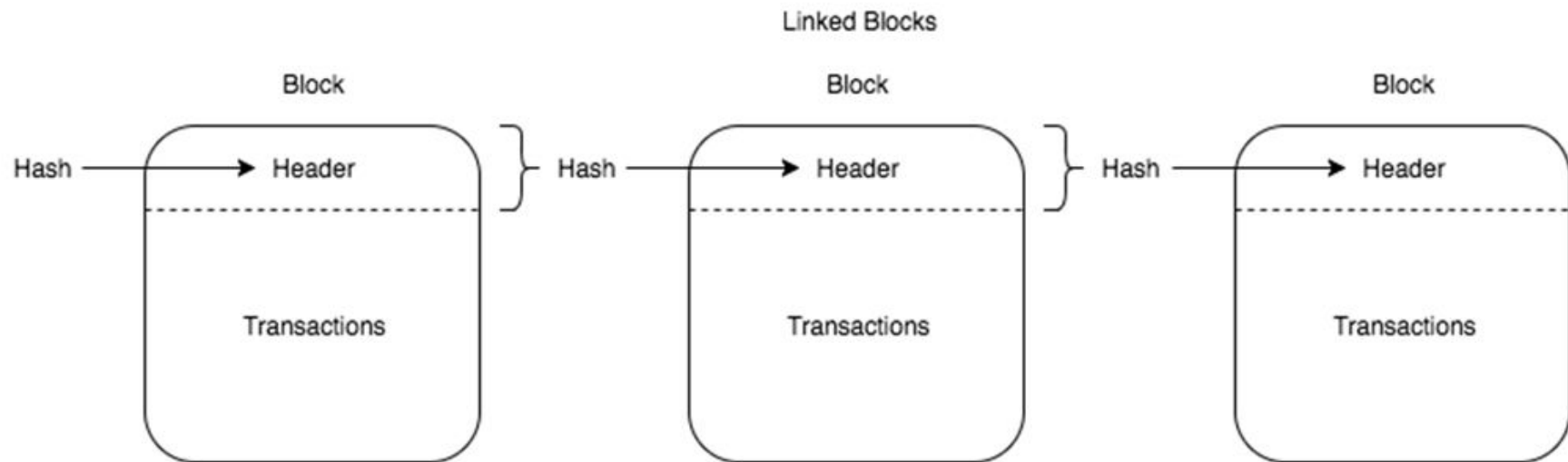
Account:

<https://anders.com/blockchain/public-private-keys/>

In Ethereum:

0xb1ed364e4333aae1da4a901d5231244ba6a35f94
21d4607f7cb90d60bf45578a

Blockchain



Proof-of-???

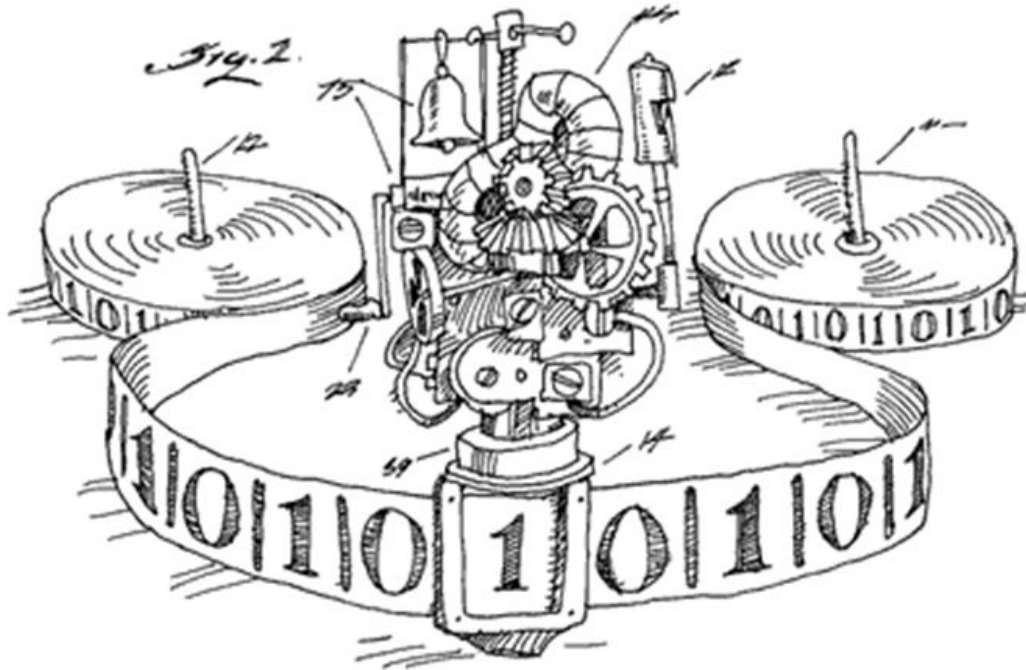
- Proof of Work (PoW): $\text{hash}(\text{nonce}) \leq M/D$, $\text{hash}(\cdot) \in [0, M]$, $D \in [1, M]$

(Bonus H-1, M-2)

- Proof of Stake (PoS): $\text{hash}(\text{hash}(B_{\text{prev}}), A, t) \leq \text{bal}(A) * M/D$, $D = (1/T_{\text{ex}}) * \sum_a \text{bal}(a)$

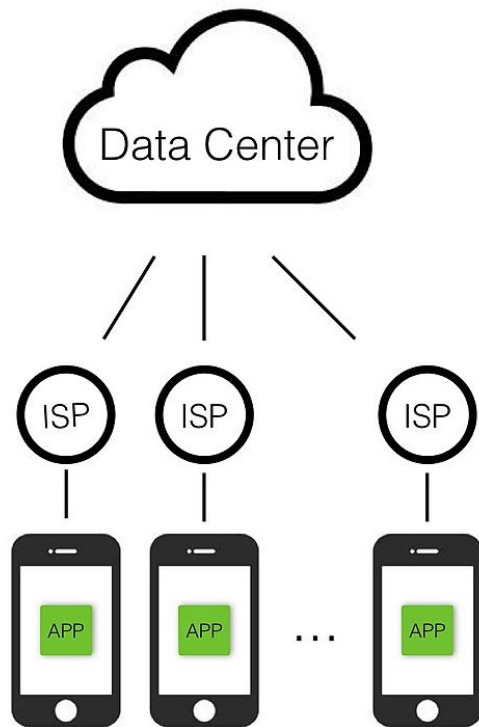
Blockchain 2.0

Smart contract!

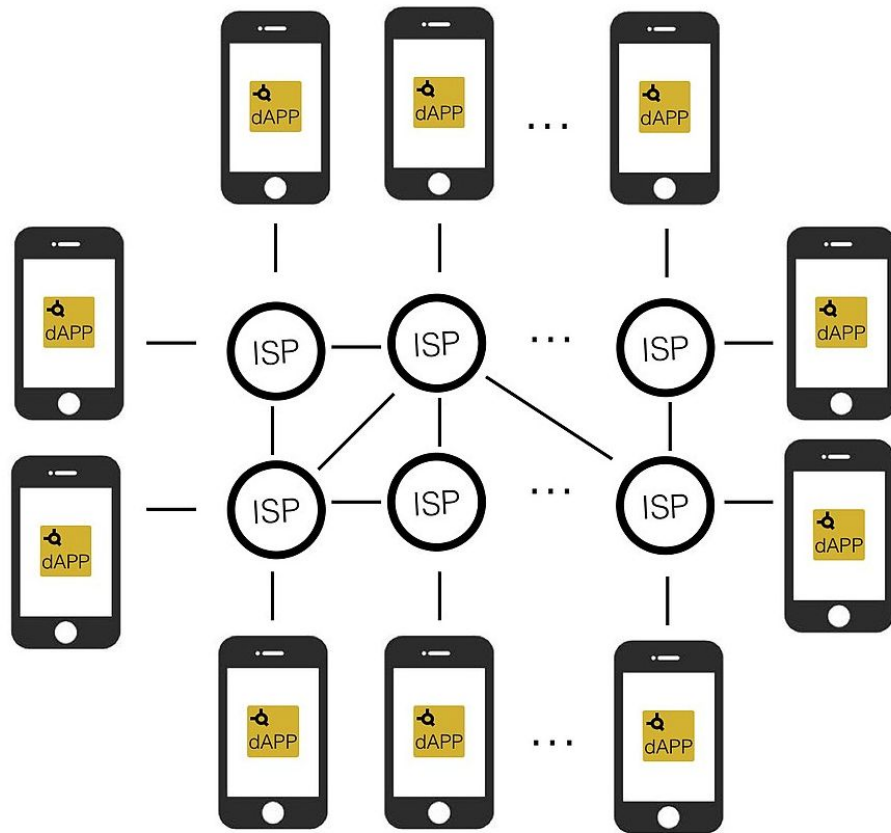


- Tape
- Head
- Table
- Register
- EVM is Turing complete

Apps



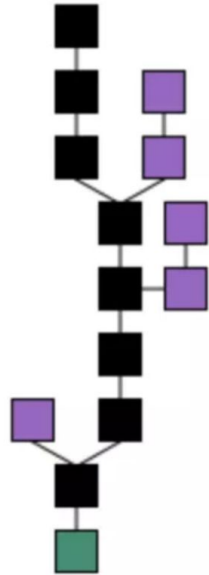
dApps



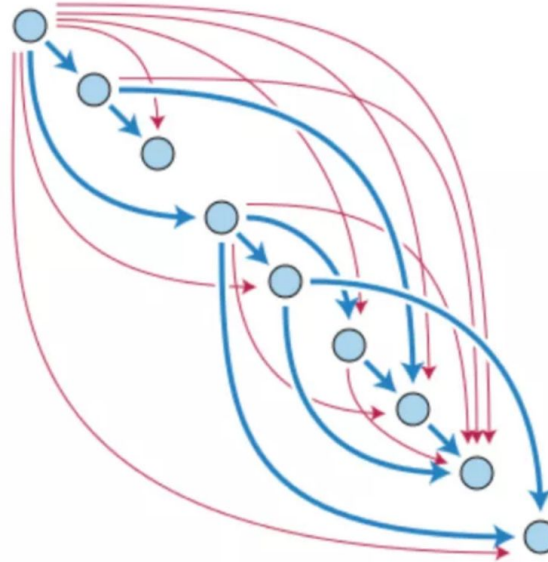
Blockchain 3.0

DLT(Distributed ledger technology)

Blockchain



DAG



3

Bonus

■ Deadline: 04/23 (Tue.) 12:00 A.M.

E-1 Bitcoin在2009/1/3的創世區塊中紀錄下了什麼訊息？(Hint1: 一則新聞)

4a5e1e4baab89f3a32518a88c31bc87f618f76673e2cc77ab2127b7afdeda33b



E-2 岳昕依法規申請北大公開教授性侵女學生事件而遭到迫害，這名教授的名字是？

0x2d6a7b0f6adeff38423d4c62cd8b6ccb708ddad85da5d3d06756ad4d8a04a6a2



M-1 在最多允許 n 個作惡節點的情況下，能確保達成一致的拜占庭系統節點至少需 m 個。試求 n 與 m 的關係式。



H-1 對Bitcoin來說，若整個系統每秒能運算 r 次雜湊函數計算新的nonce（其他運算時間可省略），時間 t 內挖到有效區塊的機率為何？（Hint: 已知當 $\theta \ll 1$ 時， $\log(1-\theta) \approx -\theta$ 。）

M-2 承H-1，若對於礦工 i 來說，每秒能運行 r_i 次運算，由他挖出新區塊的機率為何？

