MN CERT/CC

Mongolian Cyber Emergency Response Team / Coordination Center

MNSEC 2018

Information Security in Blockchain

T.Uuganbayar /www.icn.mn/

2018.10.05

The Corporate Hotel & Convention Centre

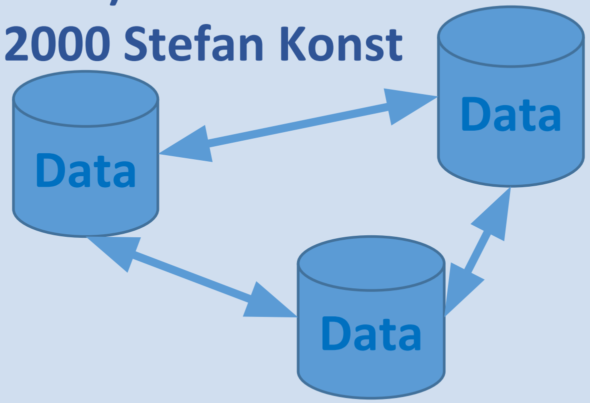
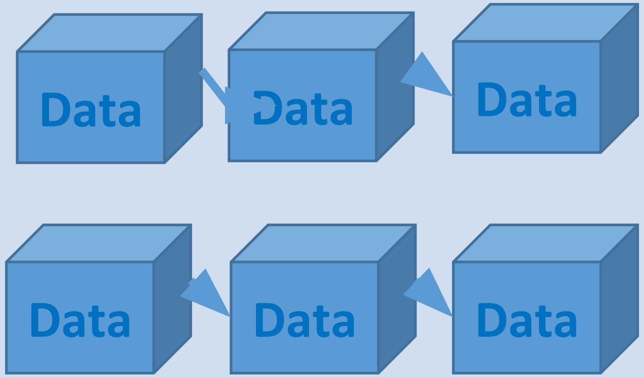
Information

Citizens	Company	Government
• Ability • Data 	• Assets • Money 	• Authority • Power

Information

Action	Trust	Risk
• Collection / Saving • Transmission / Sharing • Procession / Computing 	• Person • System • 3rd Party 	• Threat • Vulnerability • Value

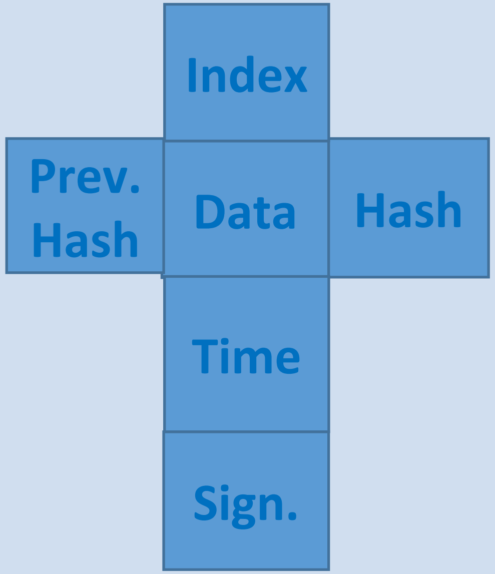
Blockchain

Database	Distributed DB	Blockchain
• Software • Hardware • Network • Physikal • Personal • Procedural 	• 1991 Stuart Haber, W. Scott Stornetta (DDB) • 1996 Ross J. Anderson • 1998 Bruce Schneider, John Kelsey, Nick Szabo (Bit Gold) • 2000 Stefan Konst  	• 2008 Satoshi Nakamoto (?) (Bitcoin) • 2013 Vitalik Buterin (Etherium) 

Blockchain

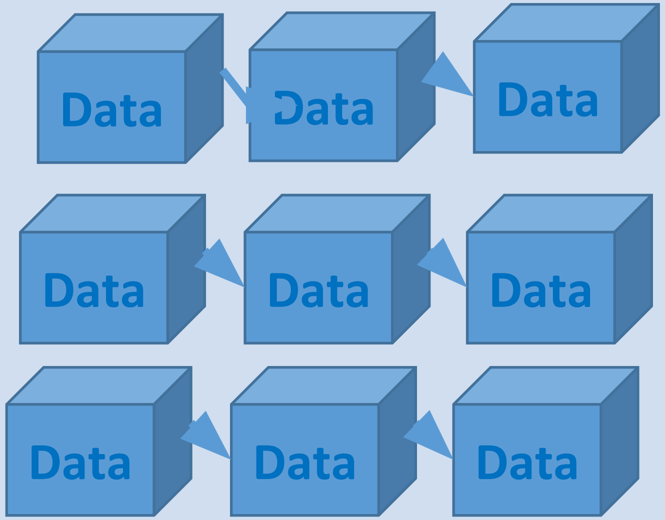
Cryptography

- Hash funktion
- Merkle tree, Digial Signature



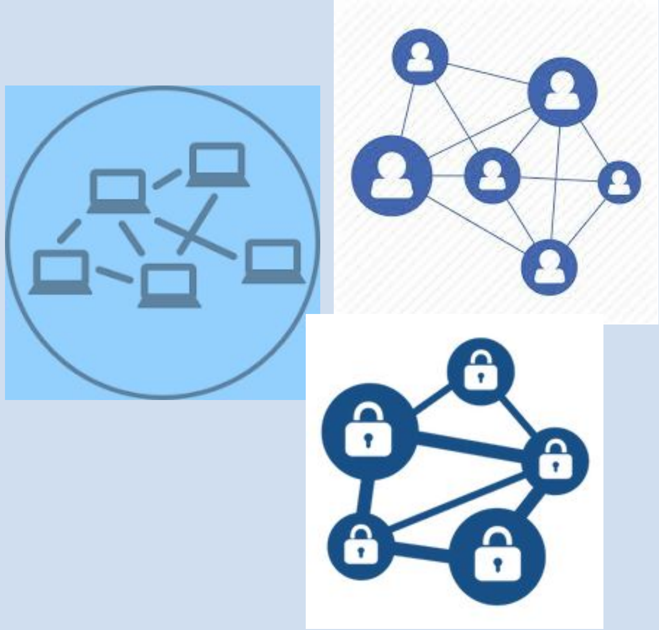
Software

- Protocol
- Virtual Machine

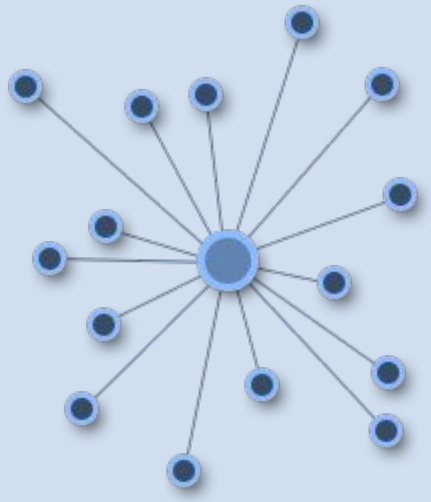
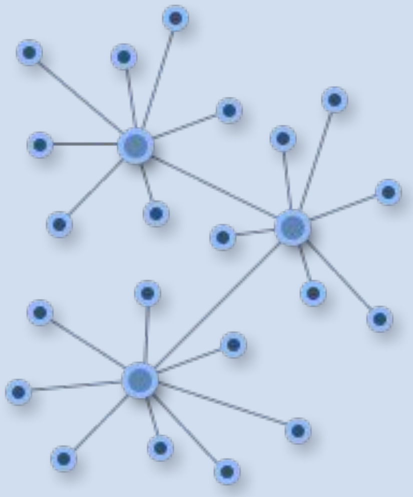
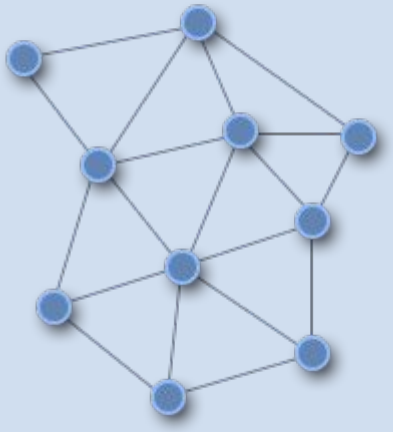


Network

- Internet
- P2P



Blockchain

Centralized	Decentralized	Distributed
- Database - Past 	- Distributed DB - Present 	- DLT, direct - Future 

Information Security

Confidentiality	Integrity	Availability
❑ Un-authorizations	❑ Un-modifications	❑ Un-interruptions
✔ Unique addresses	✔ Unchangeable, forever	✔ Uncounted saving
✔ Private keys	✔ Protections hash	✔ Proof protocols

Information Security

Non repudiation	Authenticity	Accountability
✔ Signed digital signature ✔ No cancel	✔ Real time check ✔ No fraud	✔ Transparent, pseudonym ✔ No disappear
🚫	🚫	🚫

Blockchain in Mongolia

Blockchain is the Future of Internet.

Thank your for your Attention.

uuganbayar.t@icn.mn