

Information Security in Blockchain

T.Uuganbayar /www.icn.mn/

2018.10.05

The Corporate Hotel & Convention Centre


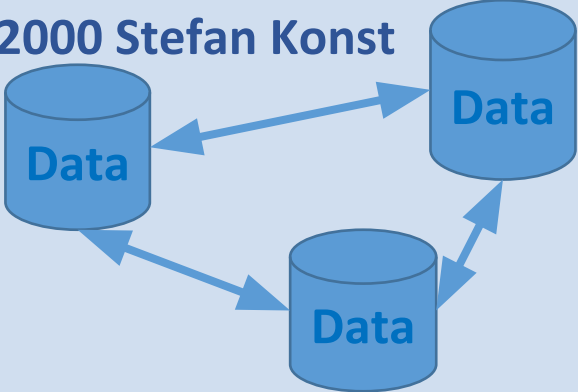
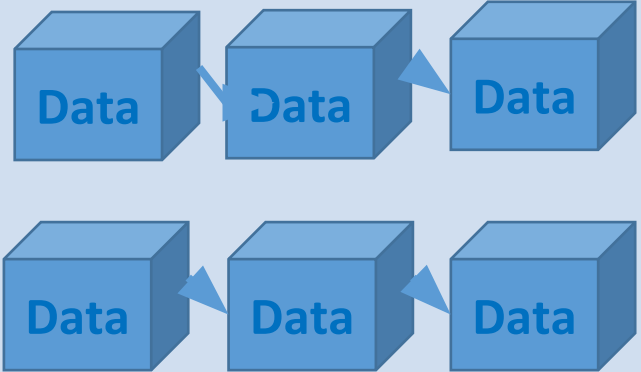
Information

Citizens	Company	Government
<ul style="list-style-type: none">• Ability• Data 	<ul style="list-style-type: none">• Assets• Money 	<ul style="list-style-type: none">• Authority• Power 

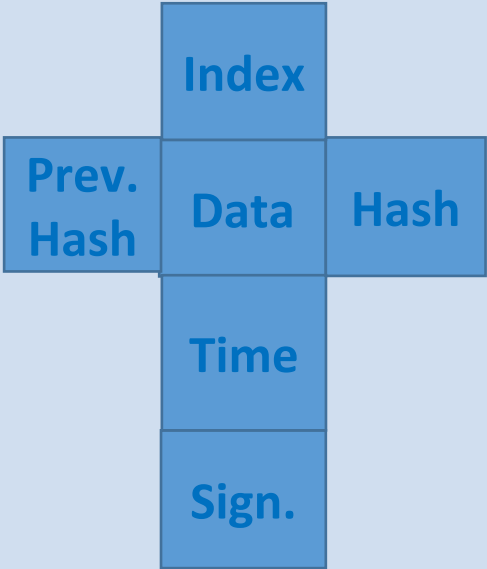
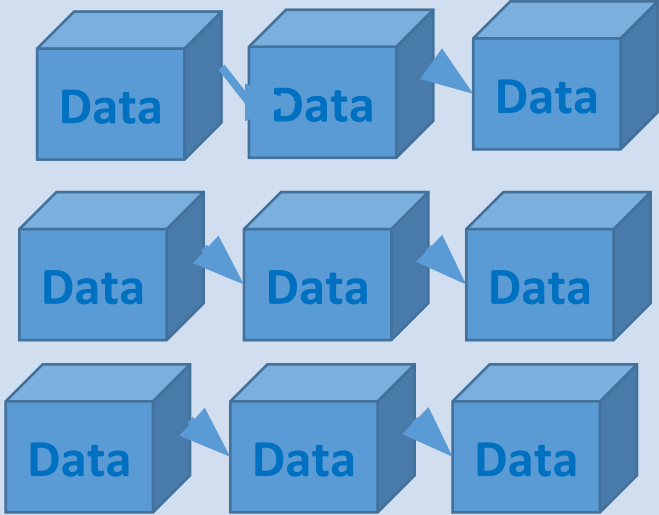

Information

Action	Trust	Risk
<ul style="list-style-type: none">• Collection / Saving• Transmission / Sharing• Proccession / Computing 	<ul style="list-style-type: none">• Person• System• 3rd Party 	<ul style="list-style-type: none">• Threat• Vulnerability• Value 

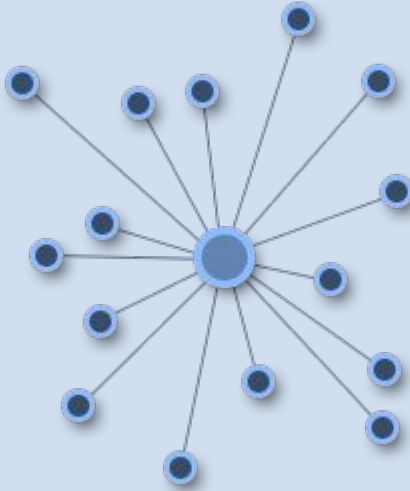
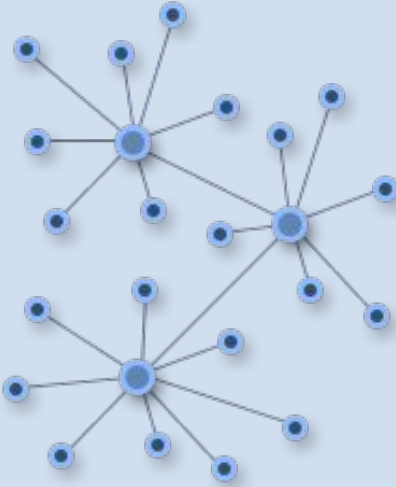
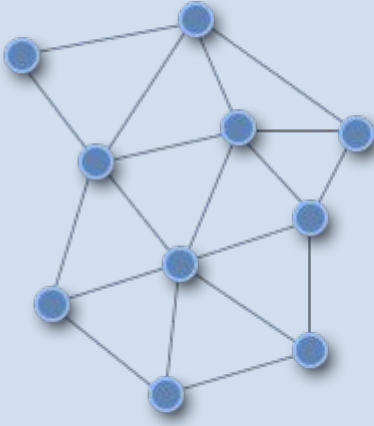
Blockchain

Database	Distributed DB	Blockchain
<ul style="list-style-type: none">• Software• Hardware• Network• Physikal• Personal• Procedural 	<ul style="list-style-type: none">• 1991 Stuart Haber, W. Scott Stornetta (DDB)• 1996 Ross J. Anderson• 1998 Bruce Schneider, John Kelsey, Nick Szabo (Bit Gold)• 2000 Stefan Konst 	<ul style="list-style-type: none">• 2008 Satoshi Nakamoto (?) (Bitcoin)• 2013 Vitalik Buterin (Ethereum) 




Blockchain

Cryptography	Software	Network
<ul style="list-style-type: none">• Hash funktion• Merkle tree, Digital Signature  <p>The diagram shows a central blue box labeled 'Data'. To its left is a box labeled 'Prev. Hash', to its right is 'Hash', above it is 'Index', below it is 'Time', and at the bottom is 'Sign.'. All boxes are connected by lines, forming a cross shape.</p>	<ul style="list-style-type: none">• Protocol• Virtual Machine  <p>The diagram shows three rows of three blue boxes labeled 'Data'. Each box in a row is connected to the next by a right-pointing arrow. Additionally, each box in a row is connected to the box directly above it in the previous row by a downward-pointing arrow, illustrating a chain of data blocks.</p>	<ul style="list-style-type: none">• Internet• P2P  <p>The network section contains three diagrams. The first is a circular network of five laptops connected by dashed lines. The second is a network of six person icons connected by solid lines. The third is a network of five padlock icons connected by solid lines, representing a secure or locked network.</p>

Blockchain

Centralized	Decentralized	Distributed
<ul style="list-style-type: none">• Database• Past  A diagram of a centralized network. It features a single large blue circular node at the center, with approximately 20 smaller blue circular nodes arranged around it. Each of the smaller nodes is connected to the central node by a thin grey line, forming a star topology.	<ul style="list-style-type: none">• Distributed DB• Present  A diagram of a decentralized network. It consists of three distinct clusters of nodes. Each cluster has a larger blue circular node at its center, which is connected to several smaller blue circular nodes. The three clusters are positioned in a triangular arrangement relative to each other, but there are no connections between the clusters.	<ul style="list-style-type: none">• DLT, direct• Future  A diagram of a distributed network. It shows a single, interconnected mesh of nodes. There are 10 blue circular nodes of varying sizes connected by a network of thin grey lines, forming a complex, non-hierarchical web structure.

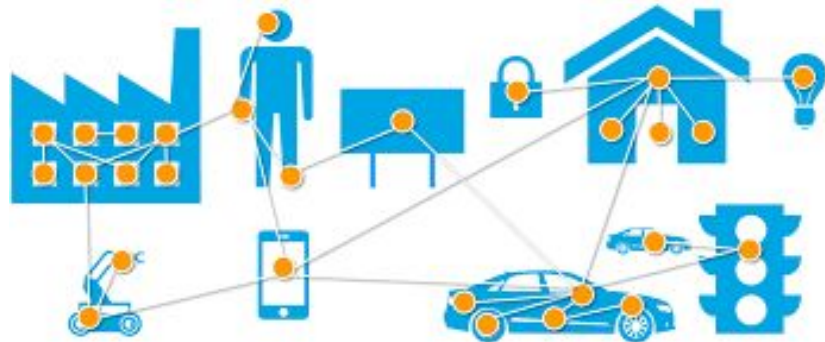
Information Security

Confidentiality	Integrity	Availability
<ul style="list-style-type: none"><input type="checkbox"/> Un-authorizations<input checked="" type="checkbox"/> Unique addresses<input checked="" type="checkbox"/> Private keys	<ul style="list-style-type: none"><input type="checkbox"/> Un-modifications<input checked="" type="checkbox"/> Unchangeable, forever<input checked="" type="checkbox"/> Protections hash	<ul style="list-style-type: none"><input type="checkbox"/> Un-interruptions<input checked="" type="checkbox"/> Uncounted saving<input checked="" type="checkbox"/> Proof protocols
		

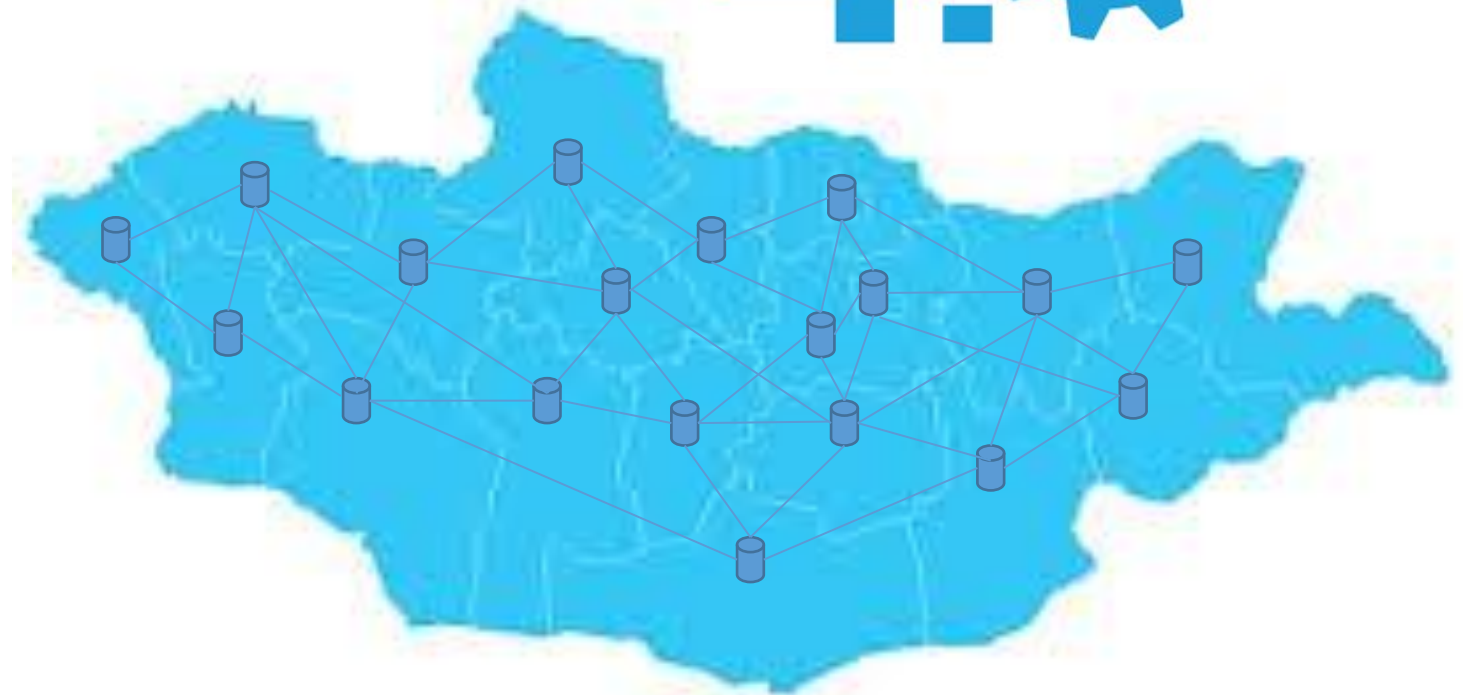
Information Security

Non repudiation	Authenticity	Accountability
<ul style="list-style-type: none">✓ Signed digital signature✓ No cancel	<ul style="list-style-type: none">✓ Real time check✓ No fraud	<ul style="list-style-type: none">✓ Transparent, pseudonym✓ No disappear
		

Blockchain in Mongolia



4. 



Blockchain is the Future of Internet.

**Thank you for your
Attention.**

uuganbayar.t@icn.mn