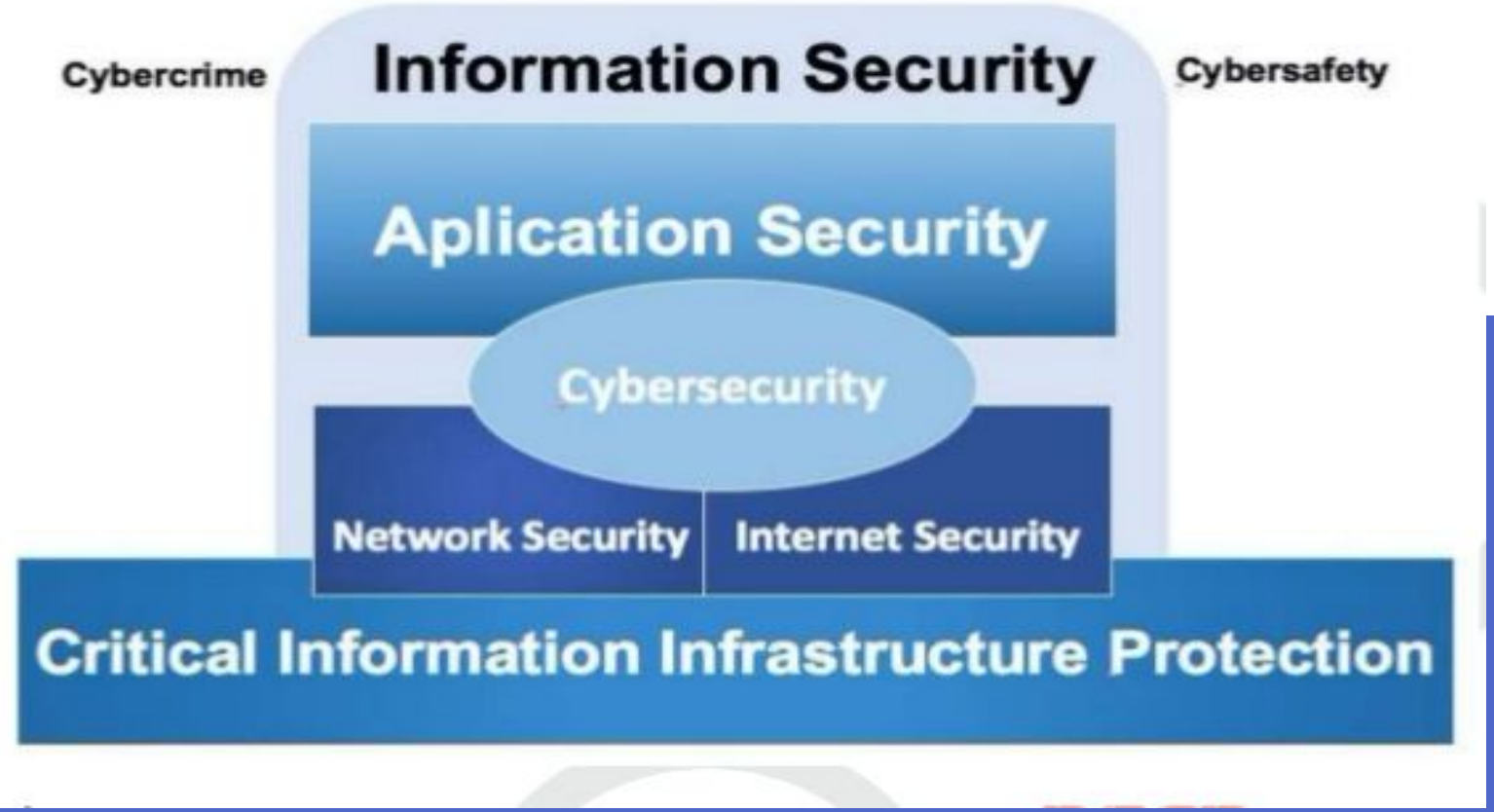
USE OF BLOCKCHAIN FOR ENSURING CYBER SECURITY IN THE ARCTIC.

Nasteka Aleksei
Graduate student
PUKHOV INSTITUTE FOR MODELING IN ENERGY ENGINEERING NAS of UKRAINE

RELEVANCE

HOW THE BLOCKCHAIN TECH WILL ENSURE CIIP SAFE ?

CYBERSECURITY RELATIONSHIPS BETWEEN OTHER TYPE OF SECURITY



BLOCKCHAIN

Decentralized

Peer-to-peer network

Distributed ledger

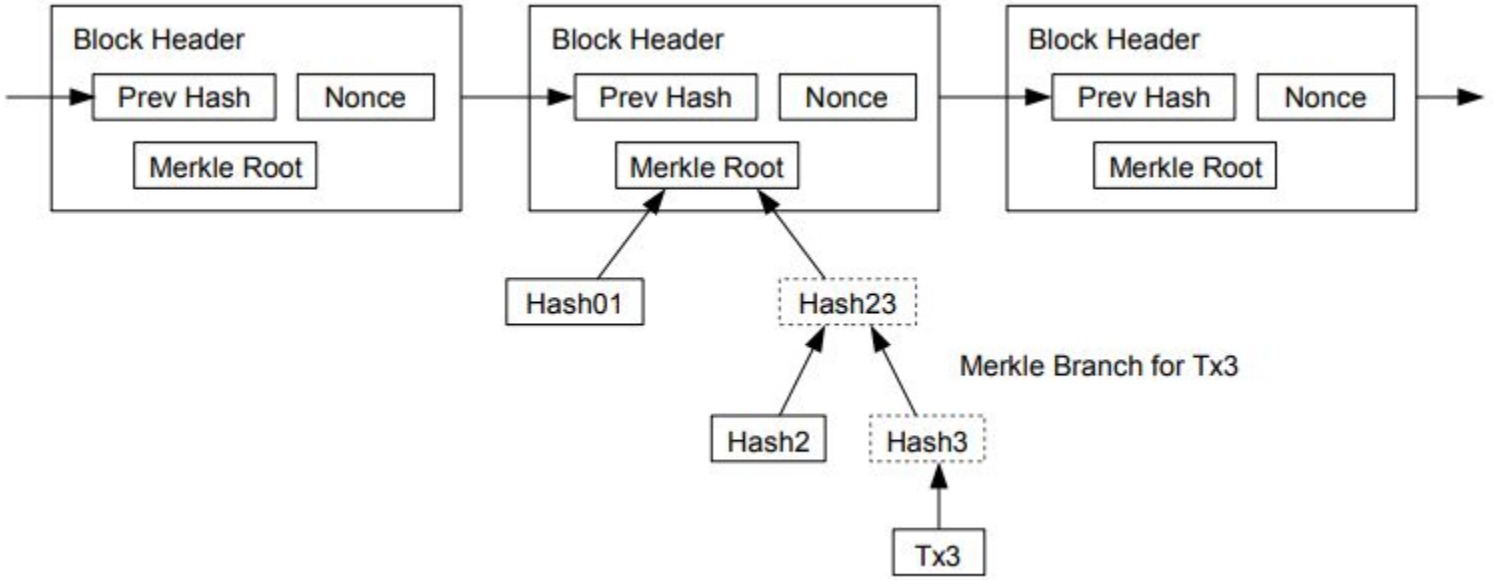
Data safe- no possible to change
Add new Data
Timestamp
Honesty and transparency
Security (identification, authentication, authorization)
Integrity

Blockchain In Crypto	Programming languages
Bitcoin	C++
Etherium	Solidity, Java Scrypt, Python, Golang
XRP	C++
Bitcoin Cash	C++
EOS	C++
Stellar	C++
Litecoin	C++
Monero	C++
IOTA	C#, Java

CRYPTOGRAPHIC HASH FUNCTION

A **hash function** is any function that can be used to map data of arbitrary size to data of a fixed size.

A **cryptographic hash function** is a special class of hash function that has certain properties which make it suitable for use in cryptography. It is a mathematical algorithm that maps data of arbitrary size to a bit string of a fixed size and is designed to be a one-way function, that is, a function which is infeasible to invert.



SHA-256	Bitcoin, Bitcoin Cash, Namecoin, NuBits, Peercoin, SHACAL-2, DSA, IPSEC, PGP	**SHA-2** (**Secure Hash Algorithm 2**) is a set of cryptographic hash functions. The SHA-2 family consists of six hash functions with digests (hash values) that are 224, 256, 384 or 512 bits: **SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224, SHA-512/256**.	United States National Security Agency. 2001	Merkle–Damgård construction with Davies–Meyer compression function.
Ethash (DaggerHashimoto)	Etherium, Etherium Classic, OmissGO	Ethash is the proof-of-work function in Ethereum-based blockchain currencies.It uses Keccak, a hash function eventually standardized to SHA-3. Ethash has been designed to be ASIC-resistant via memory-hardness and easily verifiable.It also uses a slightly modified version of earlier Dagger and Hashimoto hashes to remove computational overhead.	Vitalik Buterin 2015	Ethash uses an initial 1 GB dataset known as the Ethash DAG and a 16 MB cache for light clients to hold. These are regenerated every 30,000 blocks, known as an epoch. Miners grab slices of the DAG to generate mix-hashes using transaction and receipt data, along with a cryptographic nonce to generate a hash below a dynamic target difficulty.
Scrypt	Litecoin, Dogecoin, Gulden, Potcoin	**scrypt** is a password-based key derivation function originally for the Tarsnap online backup service.	Colin Percival 2009	The scrypt function is designed to hinder such attempts by raising the resource demands of the algorithm. Specifically, the algorithm is designed to use a large amount of memory compared to other password-based KDFs
X11	Dash	a proof of work algorithm with a hash function called "X11", with eleven rounds of hashing, and the average time to mine a coin was around two a half minutes		
Crypto Night	Monero, Monero	**CryptoNote** is an application layer protocol that powers several decentralized privacy-oriented digital currencies.	2012	
Equihash	Bitcoin Private, Zcash, Zcoin, Bitcoin Gold	**Equihash** is a memory-oriented Proof-of-Work algorithm	Alex Biryukov and Dmitry Khovratovich, 2016	
X11 Gost	Sibcoin			
BLAKE2b	Zcash, FreeBSD Ports, OpenSSI, Crypto++, Libsodium, Botan			
Keccak (SHA-3)		**SHA-3** (**Secure Hash Algorithm 3**) is the latest member of the Secure Hash Algorithm family of standards. SHA-3 is a subset of the broader cryptographic primitive family **Keccak.**	Guido Bertoni, Joan Daemen, Michaël Peeters, and Gilles Van Assche. 2015	Keccak is based on a novel approach called sponge construction.

TYPES AND OBJECTS OF ATTACK

- *51% Attack*
- *Attack on network nodes*
- *Attack Black holes*
- *Attacks on users wallets*
- *Denial-of-service (DoS) and distributed denial-of-service (DDoS) attacks*
- *Man-in-the-middle (MitM) attack*
- *Phishing and spear phishing attacks*
- *Password attack*
- *Cross-site scripting (XSS) attack*
- *Birthday attack*
- *Malware attack*
- *Hacking Crypto Exchanges*

CHRONOLOGY OF ATTACKS

2010-2015		2015		2016		2017		2018	
Bitcoin *Vulnerability source code*	**$184M**	Bitstamp *Hacking Crypto Exchanges*	**$5.1 M**	BitFinex *Attacks on users wallets*	**$72M**	CoinDash *Attack on network nodes*	**$7M**	Coincheck Japan *Hacking Crypto Exchanges*	**$500 m**
Mt. Gox *Hacking Crypto Exchanges*	**$473M**			The DAO *Vulnerability source code*	**$50 M**	Parity *Vulnerability source code*	**$32M**	Coinrail South Korea *Hacking Crypto Exchanges*	**$40 m**
				Steem.mit.com *Hacking private account*	**$85K**	Veritasium *Attacks on users wallets*	**$8M**		
						Tehter *Attacks on company's servers*	**$30,9 M**		

INFORMATION SECURITY PARADIGM: CONFIDENTIALITY, INTEGRITY, ACCESSIBILITY, OBSERVATION PROTECTION ACORDING TO ND TPI 2.5-004-99

- **Confidentiality**
- **Integrity**
- **Accessibility**
- **Observation**

CONCLUSION

PROBLEMS THAT CAN BE SOLVED BY USING THE BLOCKCHAIN TECHNOLOGY ARE:

- Transparency and Trust. It's immutable and append-only – records can only be added to that database and never removed or changed. It's updateable only via consensus or agreement on the state of the data among peers
- Decentralization. Blockchain databases are distributed among multiple computers (nodes) that store full or partial copies of that database. Remove monopoly and single point of authority and keep trust between parties
- Security and Fraud prevention. The records on blockchain are secured through cryptography. Every transaction is signed with a personal digital signature. If a record is altered, the signature will become invalid and the peer network will know right away that something has happened. Blockchain don't have a single point of failure and can't be changed from a single computer
- Value Exchange & Micropayments. Cryptocurrencies allow transferring value between parties without banks, governments. Transaction cost is almost zero comparing to Visa/Mastercard payments (600,000 transactions for $0.01 in Stellar)