

Reviews of the decentralized Internet

1. Decentralized Networks: The future Internet
2. Blockchain and the future of the Internet:
A comprehensive review

Iveta Kremenova, et. Al., Mobile Networks and Applications 2019

Fakhar ul Hassan, et. Al., Under review in IEEE COMST

Outline

- Introduction
- Blockchain (short overview)
- Applications
- Challenges
- Conclusion

Introduction

- Paradigm shift is entailed by blockchain's premise of decentralization
- A user should ideally have complete control over trust decisions
- However, Internet applications remain centralized
 - Email and Domain Name System (DNS)

Main focus of the presentation

- Introducing various decentralized applications
- Discussing remaining challenges

Blockchain overview (1/2)

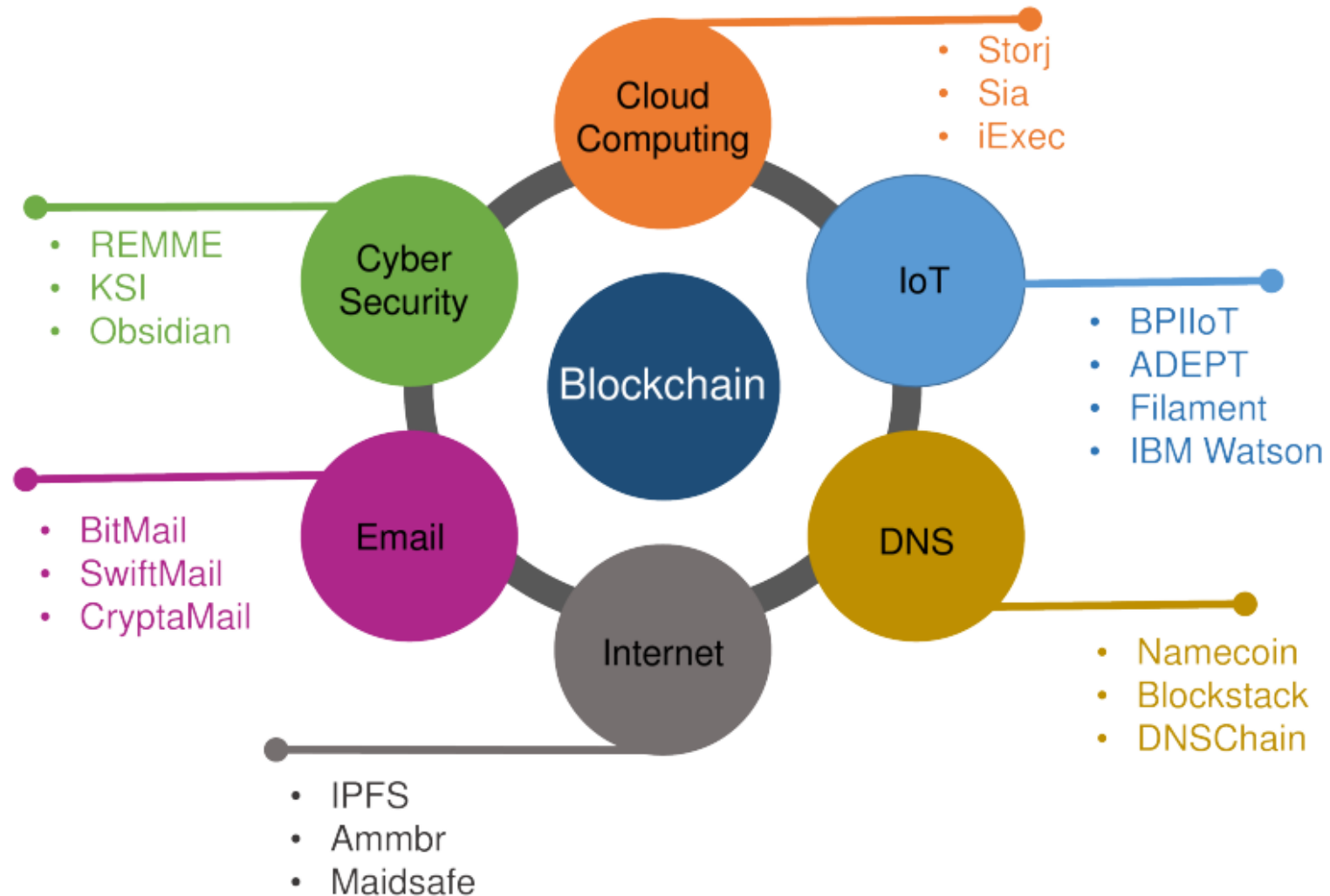
- A record of transactions among the peers are stored in a chain of a series of a data structure – *blocks*
- Each peer of a blockchain network maintains a copy of blocks
- A consensus is also established on the state of the blockchain that all the peers of the network store
 - Taking into consideration the majority of the network peers

Blockchain overview (2/2)

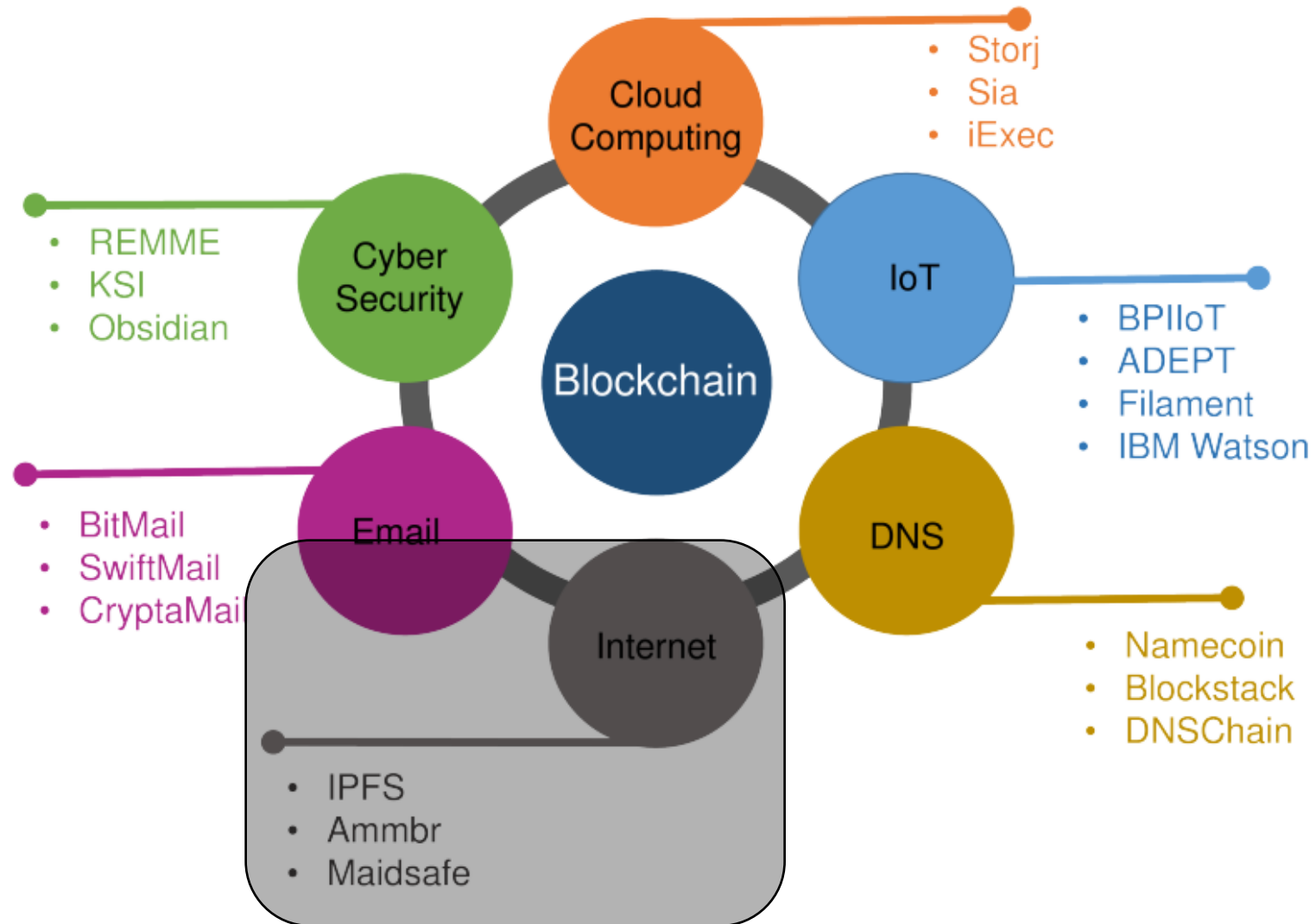
- Blockchain is also referred to as Distributed Ledger Technology (DLT)
- Establishing trust in a P2P network circumventing the third managing parties
- A trust is in the form of verifiable mathematical evidence
- Integrity, tamper-free, decentralization

Network applications

Applications overview



The decentralized Internet



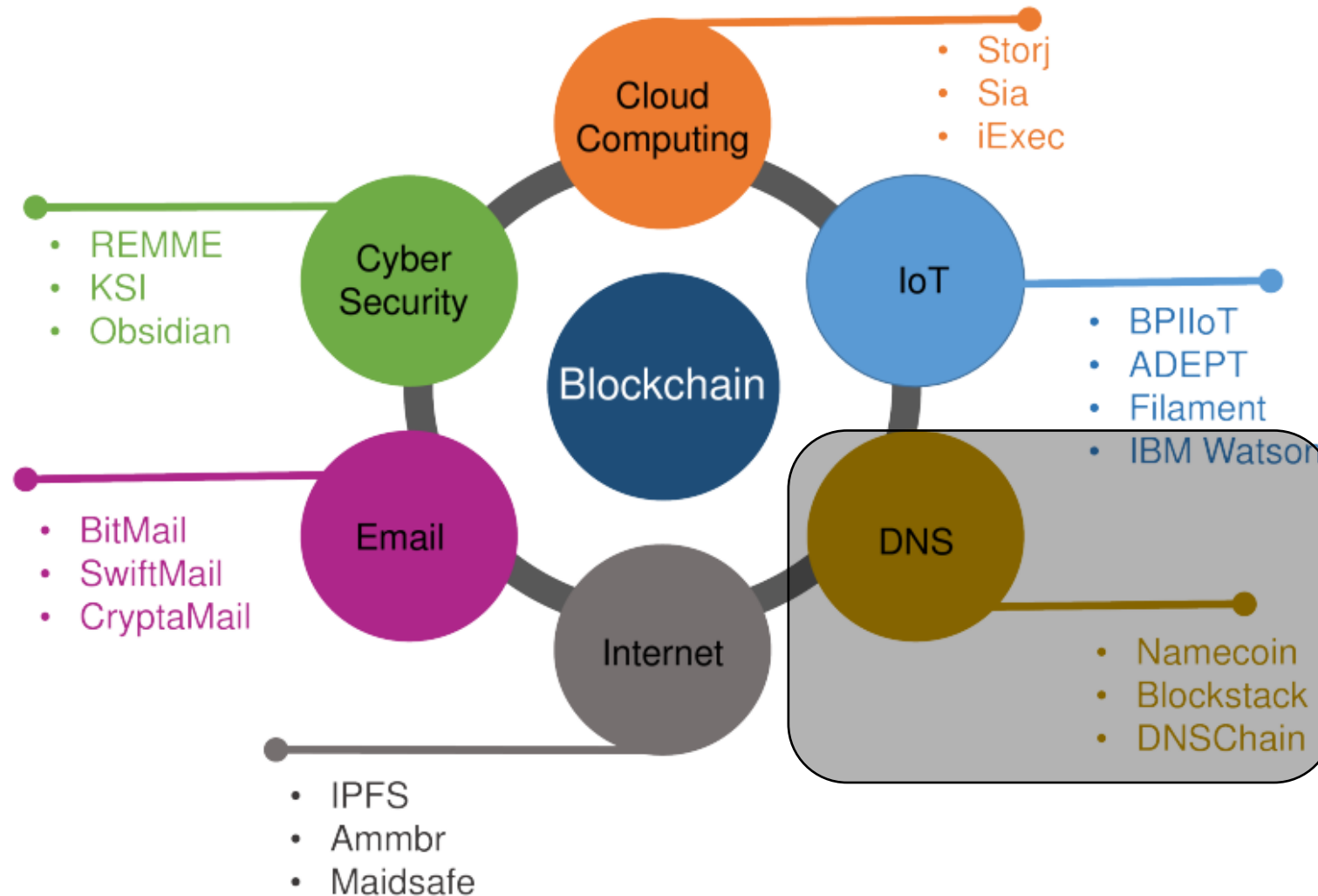
The decentralized Internet (1/2)

- Existing Internet infrastructure is predominantly centralized
 - Centralized infrastructure has vulnerabilities of the single point of failure inherently
 - DDoS attacks on DNS servers
 - Certificate authority compromises
- ➔ Decentralization of the infrastructure can mitigate such attacks

The decentralized Internet (2/2)

- Decentralized approach to the online service provisioning gives more control to the users
- Decentralization also ensures fair participation and sharing of the resources

Decentralized naming system



Decentralized naming system

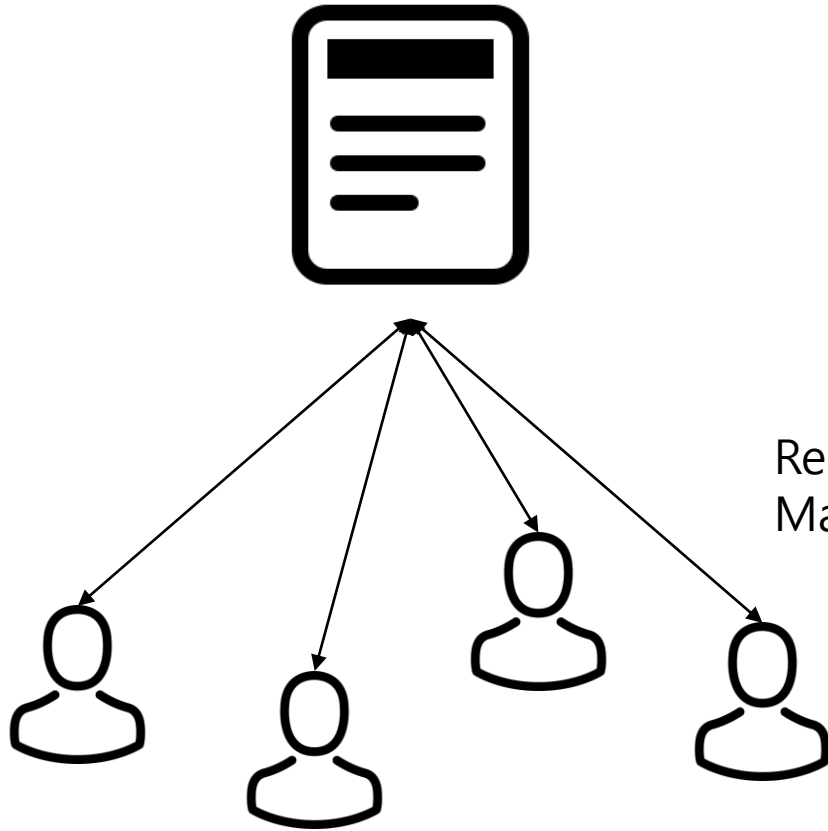
- Domain Name System (DNS) is representative example of centralized Internet infrastructure
- Blockchain can enable a decentralized namespace system
 - Using global, tamper-resistant, and append-only ledgers
 - Guaranteeing the integrity, availability, uniqueness, and security of name-value pairs

Example: Namecoin

- Namecoin is designed to work on top of a blockchain, as an alternative to the existing conventional DNS root servers
- “.bit” top-level domain is handled by Namecoin infrastructure
- Namecoin is immune to censorship or seizure of the registered domain name accounts

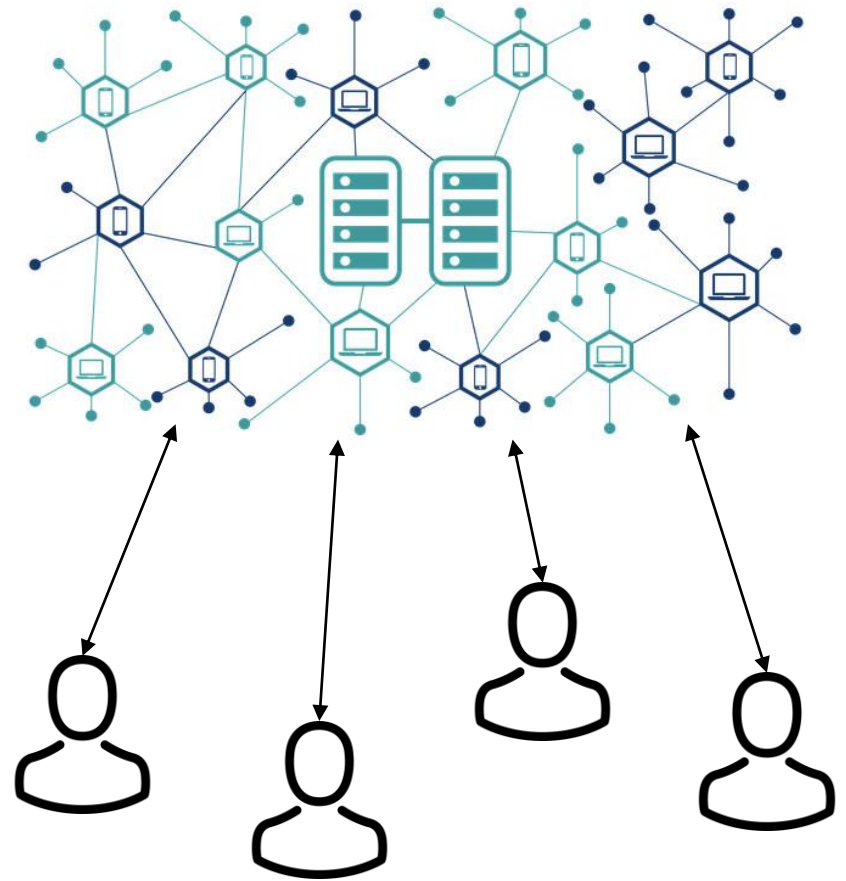
Example: Namecoin

Centralized authority (might be replicated)

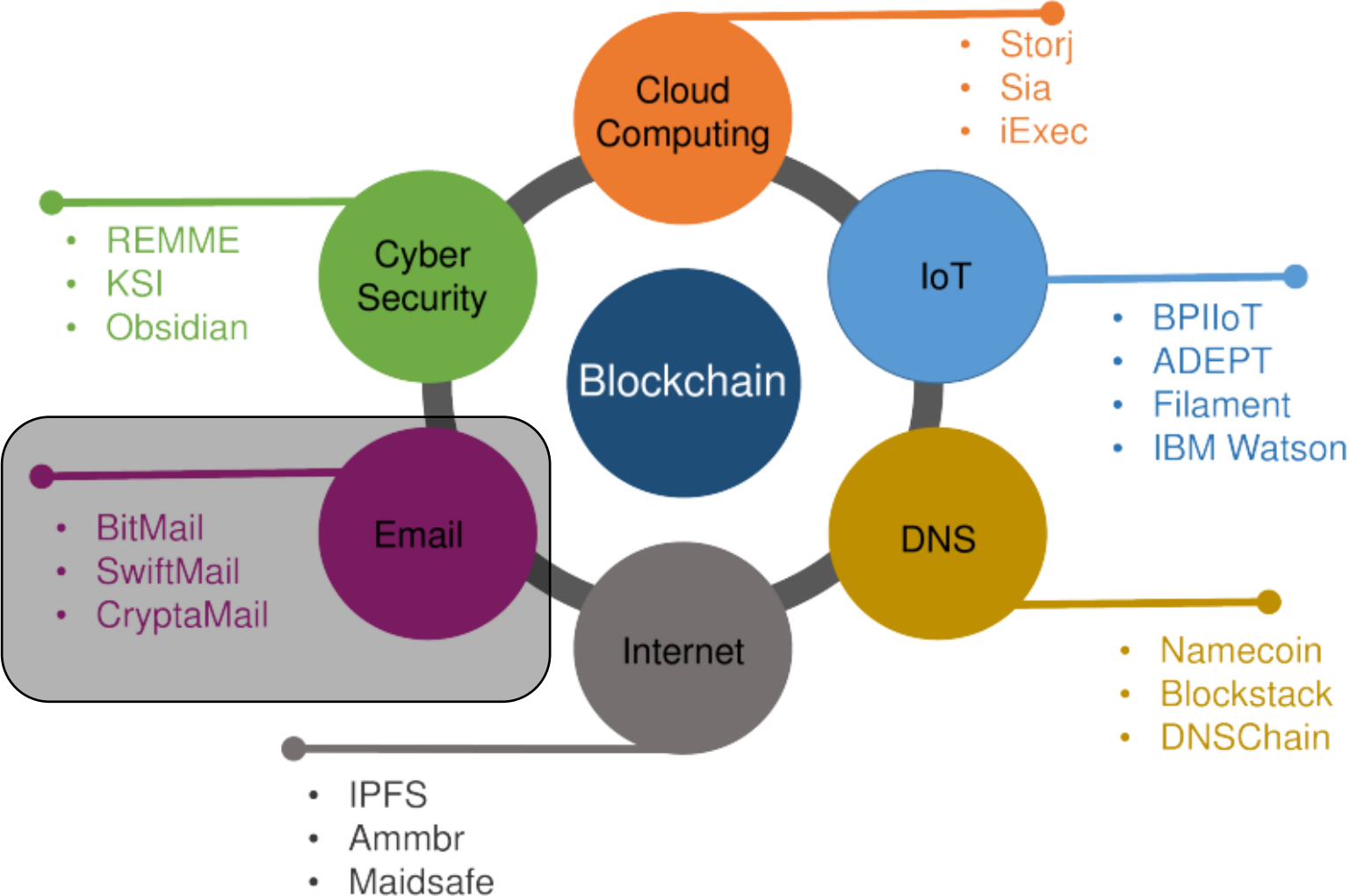


Request domain:IP address
Mapping information

Namecoin network (blockchain)



Decentralized email



Decentralized email

- Email is a common form of communication
 - Various protocols such as SMTP, ESMTP, POP, and IMAP
 - The security of an email system relies on a continuous process of planning and management
 - Without appropriate security safeguards, email can potentially be read, modified, and copied at any point along their path
- ➔ Blockchain-powered decentralized and distributed email system

Blockchain-based email



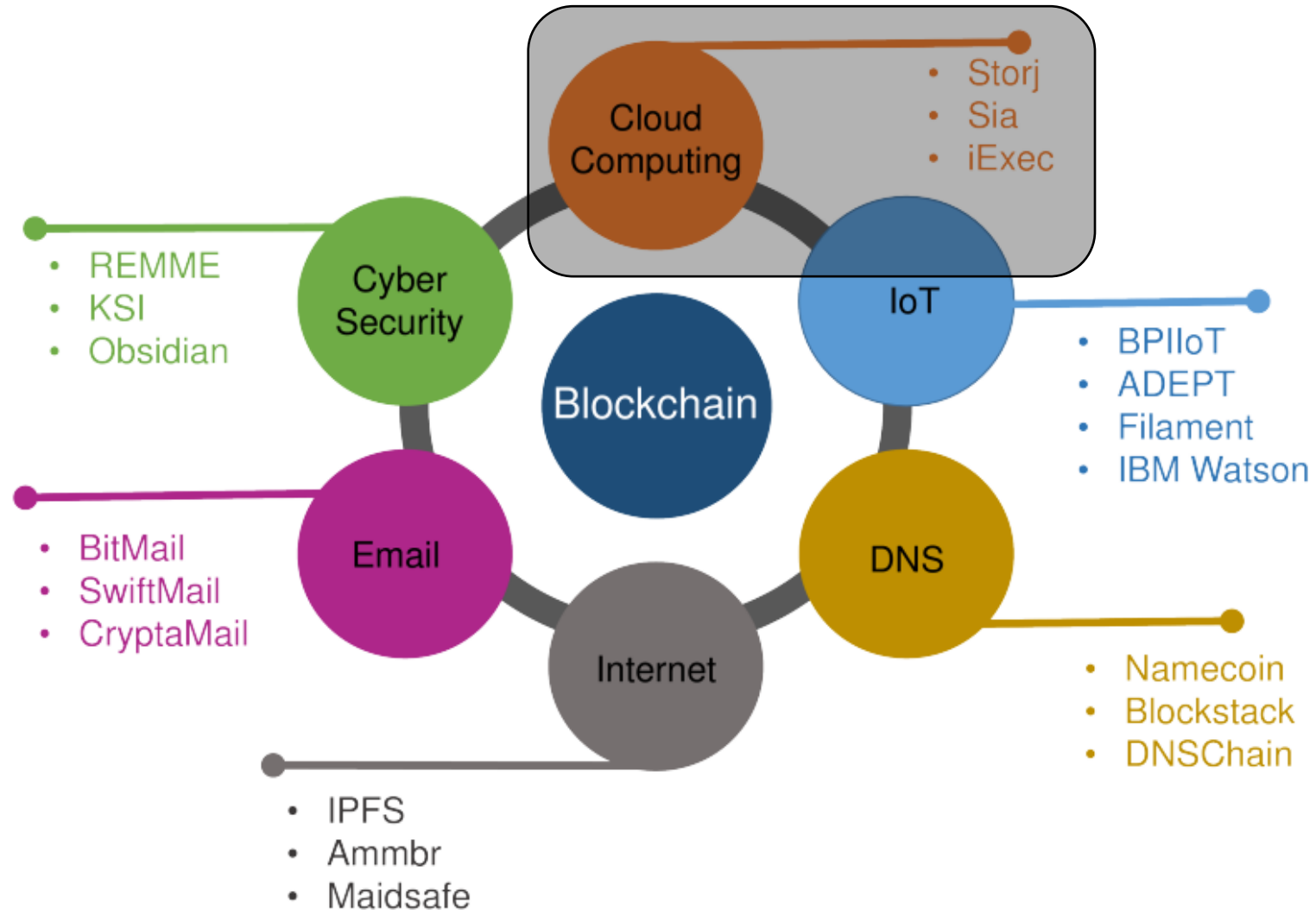
John McAfee Swiftmail



Cryptamail

- Email addresses can be assigned to the users over blockchain technology
- No centralized controlling server in order to gain access to personal data and records
- No influence of centralized authorities
 - Government authorities, ISPs and technology giants such as Google, Amazon, and Facebook, etc

Decentralized cloud storage



Decentralized cloud storage

- Consumers and enterprises face the storage and management problems
 - Ever-increasing volume of data on non-volatile data storage systems
 - Existing cloud storage solution can address the problem
 - E.x) Dropbox, Google Drive, iCloud, etc.
 - However, control, security, and privacy of data remain major concerns
 - Information thieves, censorship agencies, spies, etc.
- ➔ Decentralized cloud storage can potentially solve the problem

Sia



- Blockchain-based cloud storage platform
- Automating trusted service level agreements (SLAs) between a user and storage provider using smart contracts
- Splitting users' data into encrypted fragments and distributing them across a P2P network

Filecoin



- Realizing the concept of distributed storage network in terms of an algorithmic marketplace for storage
- Being built as an incentive layer on top of another distributed file system called Inter-Planetary File System (IPFS)
- Brief operation
 - The miners: Hosting the storage space with the mining capability
 - Filecoin: Enabling verifiable markets, which dictates how and where data is written to and read from
 - Read/write transaction: Powered by the underlying cryptocurrency called Filecoin

Decentralized content distribution

- Content distribution networks (CDNs) are an effective approach to improve Internet service quality
 - Replicating the content at different strategic geographic locations in the form of data centers
 - BitTorrent is well-known P2P content distribution protocol, however it is
 - Hard to manage traffic
 - Hard to keep copyrights of content creators
- ➔ Blockchain technology can stabilize the rights management related issues

Blockchain-based CDN

- Participants can verify a record and its origin without the need for a centralized authority
- Blockchain can store and share all the record related to the content (e.g., its origin)
- By utilizing them, blockchain-based CDN can enable a monetization system to empower the content creators

Decentralized CDN example

- DECENT
 - Blockchain-based CDN providing secure content distribution
 - Maintaining the reputations of the content creator with a mechanism for the payment between authors and client nodes
 - Content (e.g., ebooks, videos, and audio) is released cryptographically over the global DÉCENT network
 - Other nodes can then purchase them with DECENT tokens
- SingularDTV
 - Right management solution initiated by Ethereum-based entertainment studio
 - Enabling rights management as well as P2P distribution to empower artists and creators

Decentralized online social networks

- The engagement of people with online social networks (OSNs) has increased greatly in recent years
 - Privacy and security concerns however still remain an issue with many OSNs
 - E.x) Cambridge Analytica: got the access to personal information of more than 50 million Facebook users during 2016 US presidential campaign
- ➔ Decentralization, transparency, and P2P consensus gives blockchain the potential to address security and privacy concerns prevalent in OSNs

Steem



- Blockchain-based social media platform
- Enabling users to earn rewards on the basis of votes received by the community
- Encouraging honest participations of community peers in maintaining the quality of the overall network
- Such OSN systems can further be made self-healing by a blockchain-based reputation system

Other applications: IoT

- Blockchain is applied to IoT ecosystem
 - Fast development of blockchain networks + rapid growth in smart devices
- DLT ensures critical preconditions for safe and effective IoT ecosystems
 - Trust, transparency and decentralized communication, secure transactions storage, timestamped records, smart contracts

IoT industrial use-cases (1/2)

- Industrial manufacturing
 - Potential to record all manufacturing tasks in DLT
- Connected and driverless vehicles
 - Recording the route on automated vehicles
- Transportation
 - Tracking records in logistics and objective recording

IoT industrial use-cases (2/2)

- Financial services and insurance
 - Recording banking and insurance transaction
- Home and commercial real estate management
 - Recording all relevant household records
- Retail
 - Tracking of goods and delivery, etc.

Challenges

Scalability issues

- One of the major concerns in the way of wide spread adoption of blockchain-based technological solutions
 - Blockchain-based Internet service can be used by millions or trillions of individuals
 - The number of transactions would increase drastically
- ➔ Transaction throughput, storage issues

Regulatory issues

- European General Data Protection Regulation (GDPR) includes “right to be forgotten (deletion)”
 - A user must be able to make a company delete all the information pertaining to her whenever she chooses
- This right may be at odds with the blockchain’s characteristics
 - Can be mitigated by hashing, however, GDPR conflicts with integrity of blockchain in principle

Anonymity

- Users utilize generated addresses for identification over the blockchain network
 - Mostly in the form of public keys
 - The transaction amount details and the blockchain-based cryptographic keys along with their respective balances are publicly visible
- ➔ The movements of blockchain-based transactions are traceable and thus do not possess enough anonymity
- Proved in [1]

Conclusion

- Various blockchain-based decentralized applications are suggested
- Decentralized applications can potentially solve single point of failure, tamper and integrity problem
- Blockchain shares large portion of challenges with the general decentralized Internet