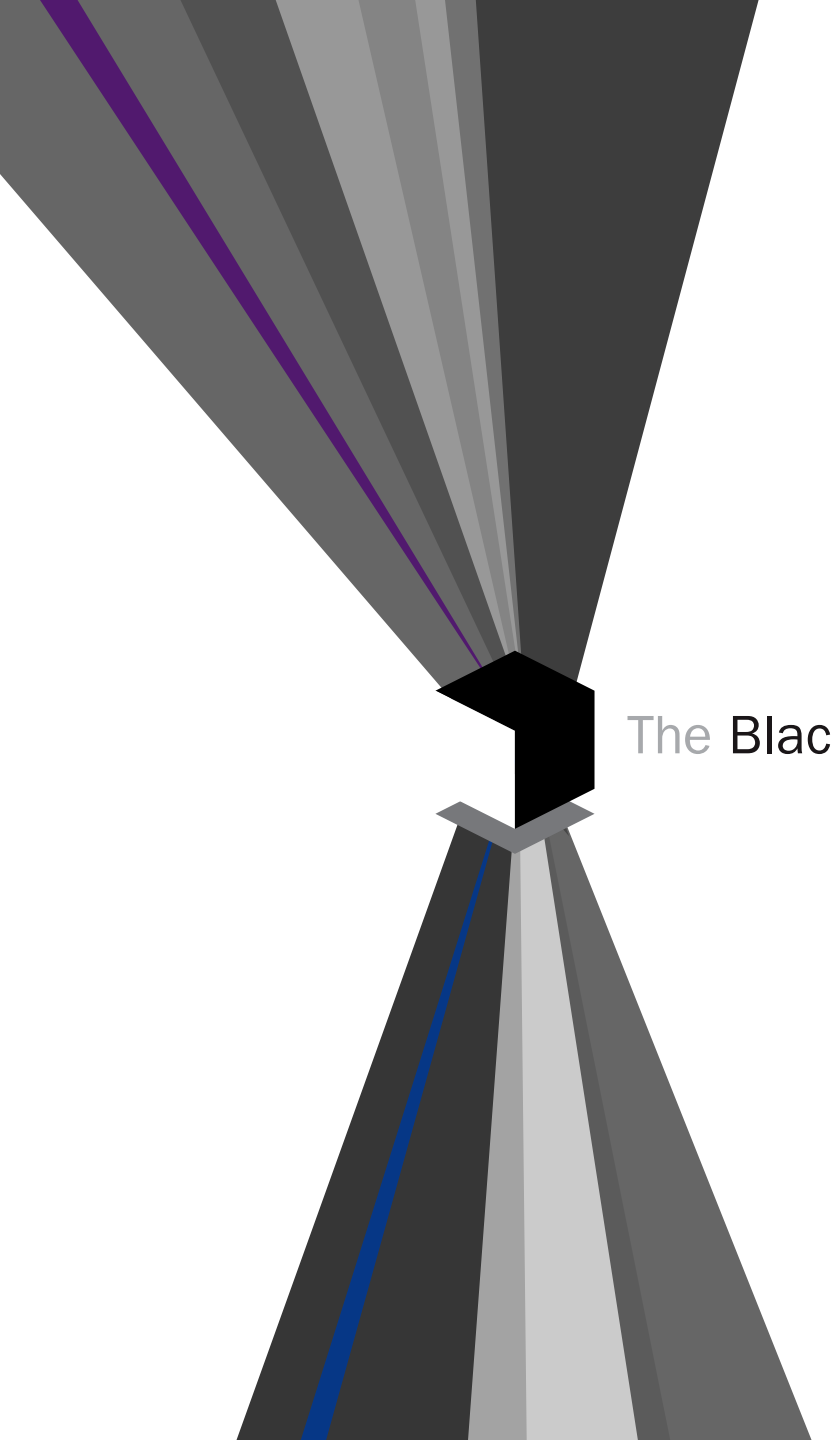


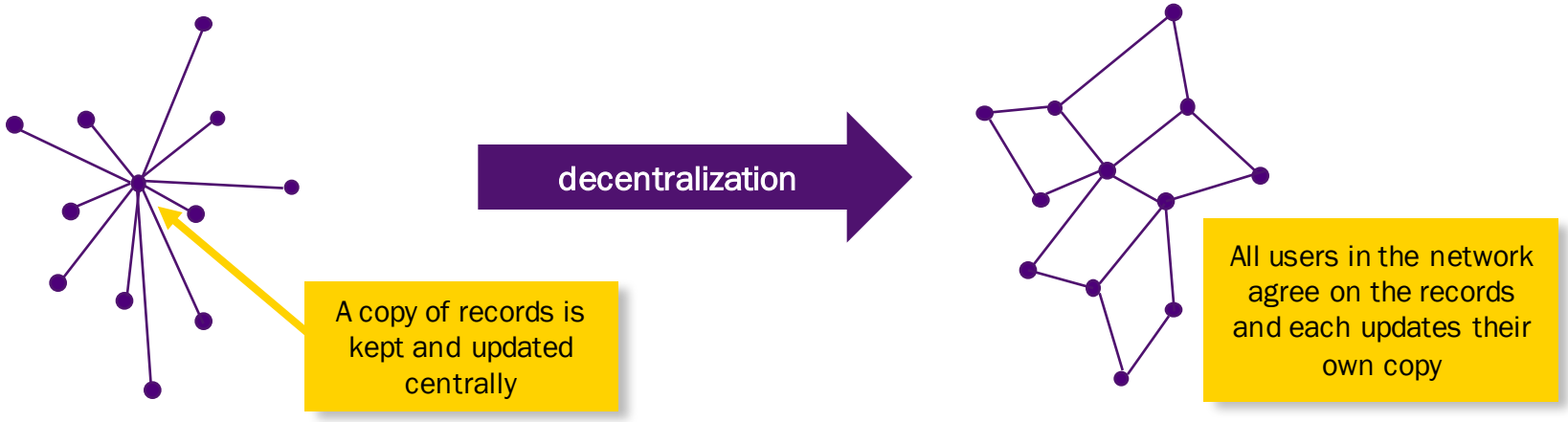
The Black Box Institute

Reimagining Trust with Blockchain

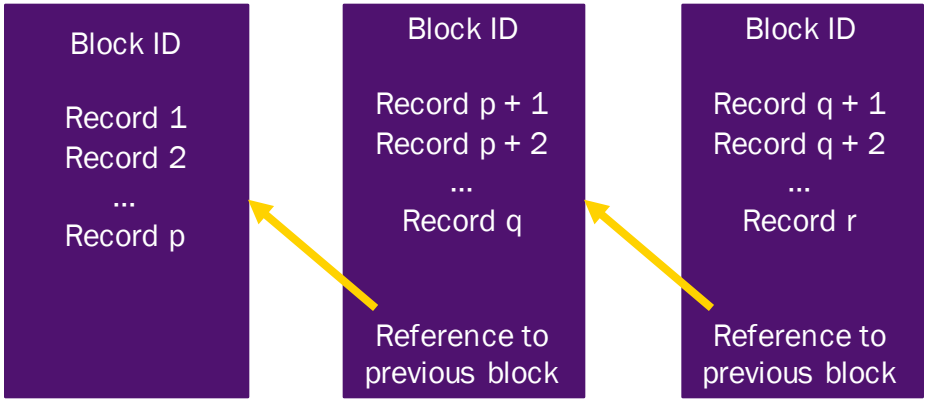
Table of contents

Blockchain is a decentralized ledger which organizes records using a sequence of blocks

Blockchain is a decentralized system of record-keeping. Instead of a central authority keeping track of records, every participant in the network keeps their own copy of the records, and based on consensus, all users update their copy of the records.



The records are kept in the form of a chain of blocks. Each block contains a set of records, and a reference to the previous block in the chain.

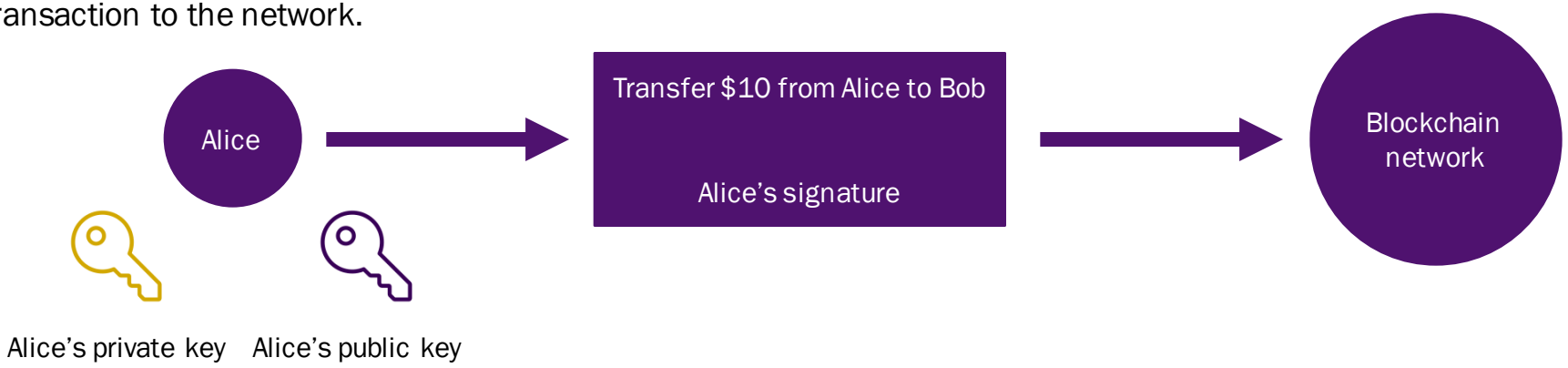


Due to the lack of central oversight, blockchain requires cryptography as a method to verify transactions

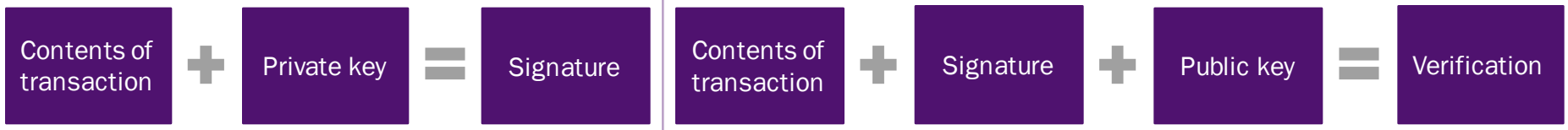
Blockchain uses cryptography, a branch of mathematics, to construct the blockchain and verify records.

In particular, in order to verify a record or transaction, public-key cryptography is commonly used. In public-key cryptography, each user in the network has a private and a public key. The public key is shared with all other users, while the private key is kept secret.

Suppose Alice wants to send $10 to Bob. Using her private key and the contents of the transaction, Alice creates a digital signature, which she include with the contents of the transaction. She then broadcasts her signed transaction to the network.



Everyone in the blockchain network can then verify that Alice is the real sender of the message. Using Alice's signature, her public key, and the contents of the message, the network can verify that the sender indeed used Alice's private key, thus confirming that the sender really is Alice.



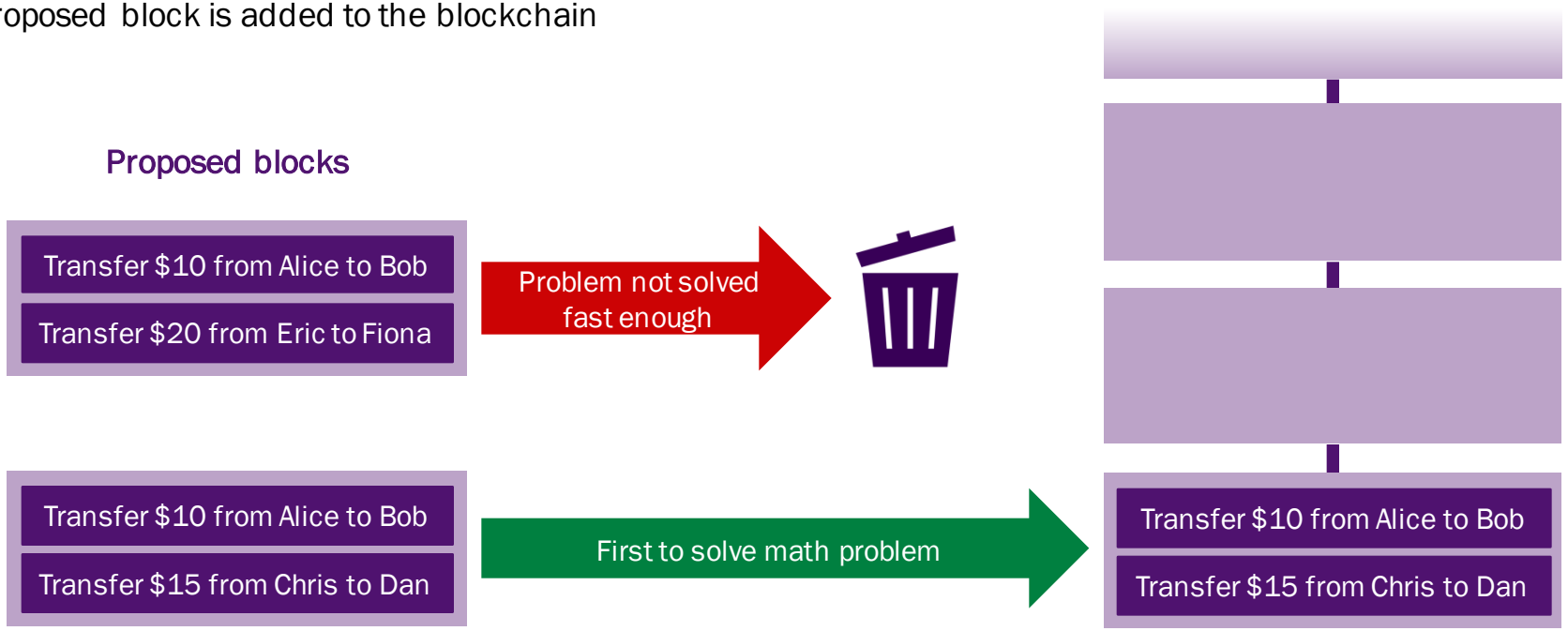
Source: Michele D'Aliessi

The sequence of new data being added to the blockchain is determined using mathematics

For Alice's money transfer to go through, the transaction needs to be added to the blockchain. However, multiple transactions like Alice's occur across the network. Since the network is decentralized, there must be a system to decide in which order transactions are added to the blockchain.

A commonly used system is proof-of-work:

- Anyone across the network can group some transactions into a block and suggest that their block should be the next one in the blockchain
- However, blocks can only be added to the blockchain if they contain the answer to a complex mathematical problem, which can only be solved by trial-and-error
- The first person in the network to correctly guess the answer to the mathematical problem is the one who's proposed block is added to the blockchain



Source: Michele D'Aliessi

Blockchain's cryptographic nature and decentralized structure presents both advantages and challenges

Advantages

- No need for third-party to moderate transactions
- Full transparency
- No single point of failure
- Fast and secure information transfer
- Single ledger results in simple information storage system

Challenges

- Large energy consumption required to determine order of blocks in blockchain
- Loss or theft of private key presents security concerns
- Requires participation of entire network of users to function
- High initial cost to set up

Blockchain technology is most advantageous when an information transfer process requires enhanced security, more transparency, and simplification of transactions.

Blockchain's advantages translate to various use cases in finance

Smart contracts

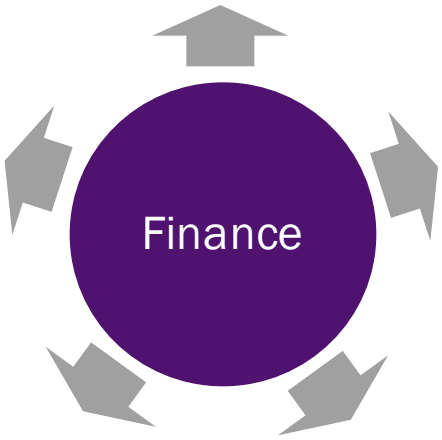
- Contracts such as those governing insurance policies and mortgage agreements can be securely stored in a blockchain
- Contracts can be programmed to be self-executing or self-enforcing

Digital identity

- Processes such as know your customer (KYC) could be simplified
- Identity verified via private key
- Combined with internet of things (IoT), consumers could securely add IoT devices to their identity

Smart assets

- In trade finance, traders can keep track of ownership of assets, in real-time
- Smart asset technology can be combined with smart contracts to fully automate trade transactions



Payments

- Fees associated with global transfers and other transactions could be greatly reduced
- Security, speed, and bookkeeping of payment could be improved

Clearing and settlement

- Blockchain could eliminate the need for clearing transactions
- Transactions would complete quickly and without the oversight of a third-party

Source: Finyear

Some of blockchain's use cases from finance also apply specifically to the insurance industry

Insurer value chain

Product design	Pricing	Distribution and underwriting	Claim management
• By combining IoT capabilities with Blockchain, new products can be designed to automatically trigger and approve claims	• The single ledger design of Blockchain could provide a single point of access for data needed for actuarial analysis (used to price new products)	• Smart underwriting – client's digital identity could be leveraged to automatically obtain the information necessary for the underwriting process	• Smart contracts could automate and simplify claims processing, at the same time reducing fraud

Customer value chain

• Smart underwriting – retrieval of customer information is easier and more automated

• Smart contract – when customers accept their policy, their contract is added to the blockchain

• Smart contract – premium payments and claims processing is faster and more automated

Purchase

Use

Blockchain technology can optimize and automate operations across the entire insurance value chain, giving the insurer a competitive advantage.

New players in the insurance market are leveraging blockchain's use cases

DYNAMIS

- Uses blockchain to create smart contracts in the peer-to-peer insurance industry
- Technology is based on the crypto-currency Ethereum

ChainThat
Blockchain Innovation

- Provides decentralized solutions for insurers and reinsurers
- Services include proof-of-concept and pilot projects, and implementation of a blockchain framework to improve processes along the value chain

safe share

- Develops insurance products for start-ups in the sharing economy
- Service is based on blockchain technology developed by the Z/Yen Group, a British commercial think-tank

everledger

- Using a blockchain, maintains a ledger for diamond certification and transaction history
- As such, it aims to reduce insurance fraud related to diamonds

Healthcare industry can leverage a distributed ledger to collect and transact data from various sources

Demographic Data

An individual's age, gender, location, ethnicity, etc.

Bio Data

Height, weight, blood pressure, cholesterol levels and other basic medical information

Patients

Patients have a private key to their transactions to keep their information secure and confidential

IoT Devices

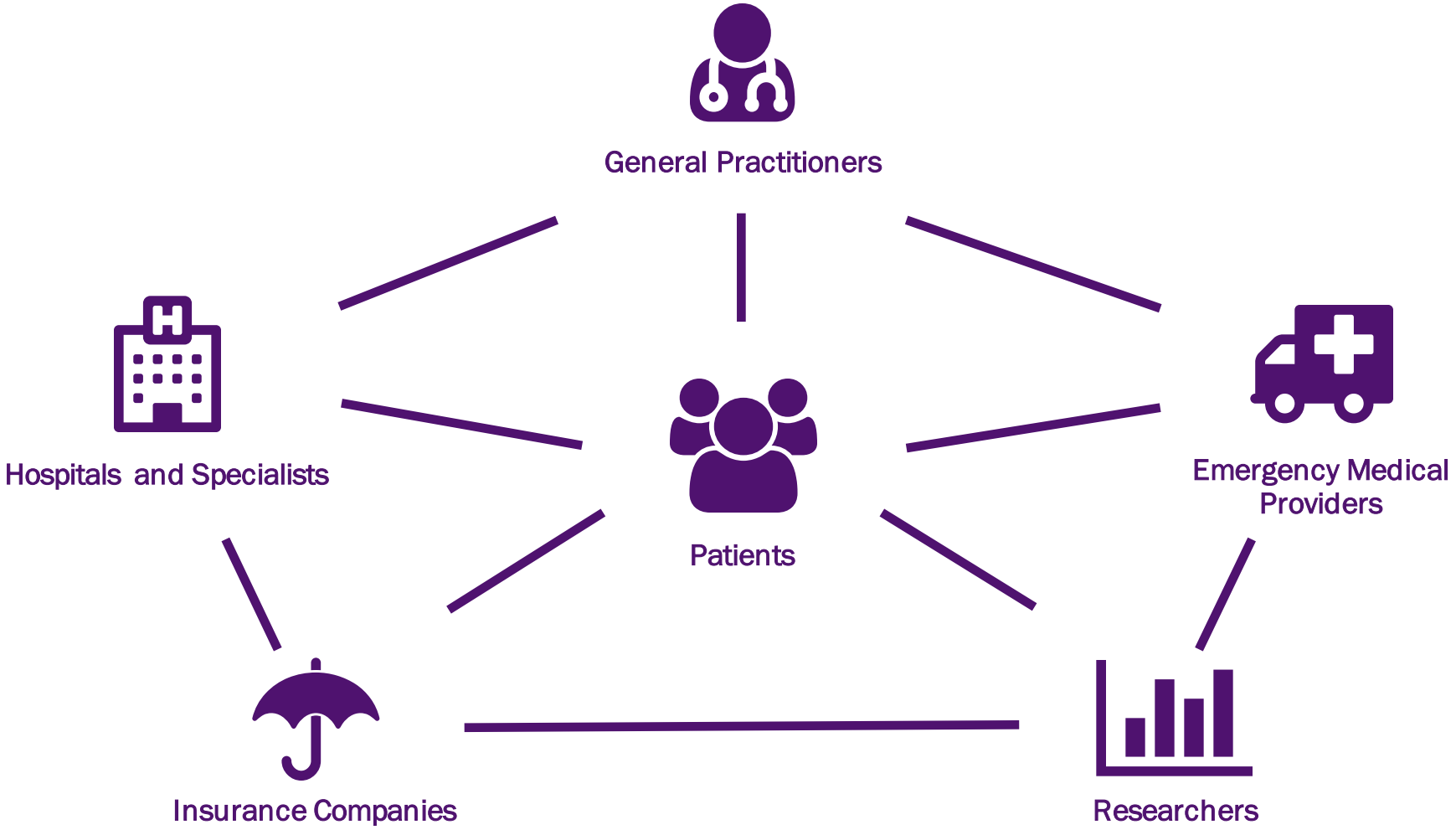
Wearable devices and home health monitoring technology provide rich patient health data

Medical Records

Family medical history and records of medical procedures and results

Blockchain technology can maintain a secure ledger of various transactions between patients and an ecosystem of health information.

A distributed ledger improves interoperability across a network of health organization



Interoperability is the potential for computer systems and software to collaborate and exchange information.

Interoperability of blockchain opens many opportunities and challenges to the healthcare system

Opportunities:

Healthcare providers will be able to provide better service with the patient's permission to access to complete and accurate health information at reduced costs

Research institutions will be able to mine public population data from the distributed ledger without having personal identification to the information

Blockchain will be able improve the security and privacy of patient data as it is distributed across the chain of health organizations

Smart contracts enable the automatic processing of insurance claims and prior authorization forms

Challenges:

Internet connectivity and increased processing power is required across the chain

Organizations must consider the ownership of patient data and who has the right to access certain information

Certain personal health information along with geographic data can lead to privacy concerns for patients living in less densely populated regions

To improve efficiency and reduce the processing power required, the ledger is only able to record basic data and will have to create links to more complicated information (X-rays, MRI scans, etc.)

Does not replace the need for a secure database of patient information

Improving transparency and security is the main application of blockchain in the manufacturing sector

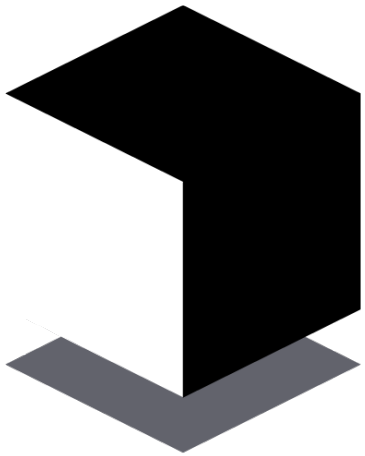
Private blockchain networks used across supply chain partners will leverage IoT applications and smart contracts to verify transfer of legitimate goods and increase transparency to all parties

- The cost of transferring data and information is reduced and the speed and accuracy is increased
- Blockchain improves trust amongst partners and increases the security of transactions across multiple parties
- Smart contracts can ensure the appropriate partners are receiving the right goods and are updating the chain accordingly
- Modern supply chains can leverage existing internet connectivity on all access points to facilitate the implementation on blockchain technology

Industry incumbent and new players that are developing blockchain for supply chain use:

IBM and Maersk are working on developing a blockchain-based shipping and logistics company

Provenance is a startup that uses blockchain technology for supply chain tracking



The Black Box Institute

200 King Street West, Suite 1301, Toronto, Canada
www.theblackboxinstitute.com
+1.416.862.5487