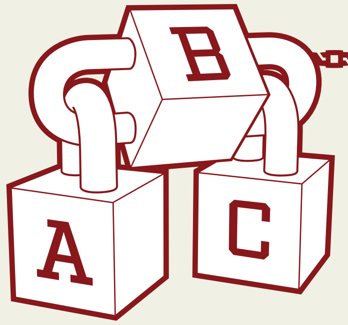
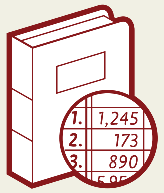
GOVERNMENT BLOCKCHAIN

BY PETER STOYKO



BLOCKCHAIN BASICS

Traditionally, the stock and flow of assets are tracked in a ***ledger*** book. These days, digital ledgers are stored on computers.



Those who control access need to be trusted to not make self-serving changes and to protect the ledger. Whenever you make a simple transaction, such as wire someone money or charge a credit card, the ledgers of intermediary organizations are updated. What might appear simple is, behind the scenes, a cumbersome and rickety coordination process.

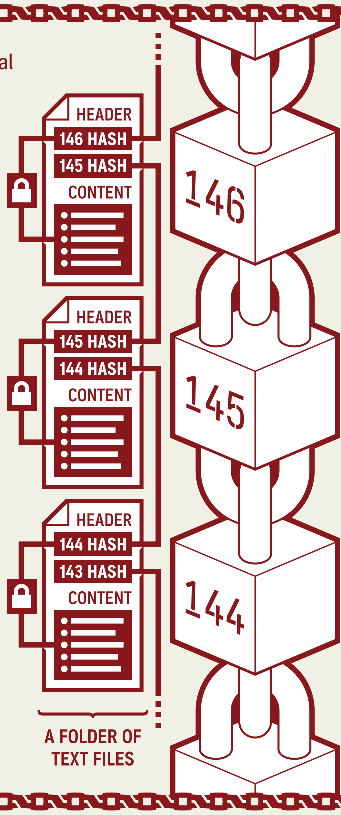
A ***blockchain*** is a decentralized digital ledger that tries to overcome these problems. It has five defining parts.

A THE BLOCK

A block is a page in the ledger. Unlike with a paper ledger, these pages can store thousands of transactions (up to a set limit), are added regularly, and cannot be changed once fully established in the chain.

B THE CHAIN

The header section of each block links the blocks together. This is done with a ***hash chain***. A hash is a long string of numbers and letters made by an algorithm from an input. The input in this case is the content of the block. If any transaction is changed, the block's content no long matches its hash. A block's hash is copied in the next block, so that no block can change without invalidating the chain.



C DISTRIBUTED

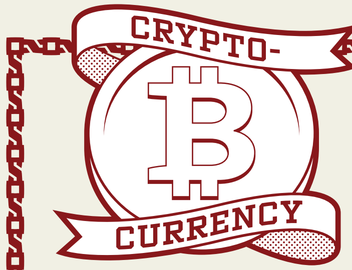
Copies of the blockchain are distributed throughout a decentralized network via ***peer-to-peer file sharing*** technology for safe keeping and openness.

D ENCRYPTED

Anyone in the network can read the ledger but ***public-key cryptography*** protects accounts by encoding them. Each account is controlled with a long number called a private key kept secret in a trusted software ***wallet***. Moving items between accounts involves using the private keys to generate sharable codes (including a public key) needed to conduct a transaction (see below).

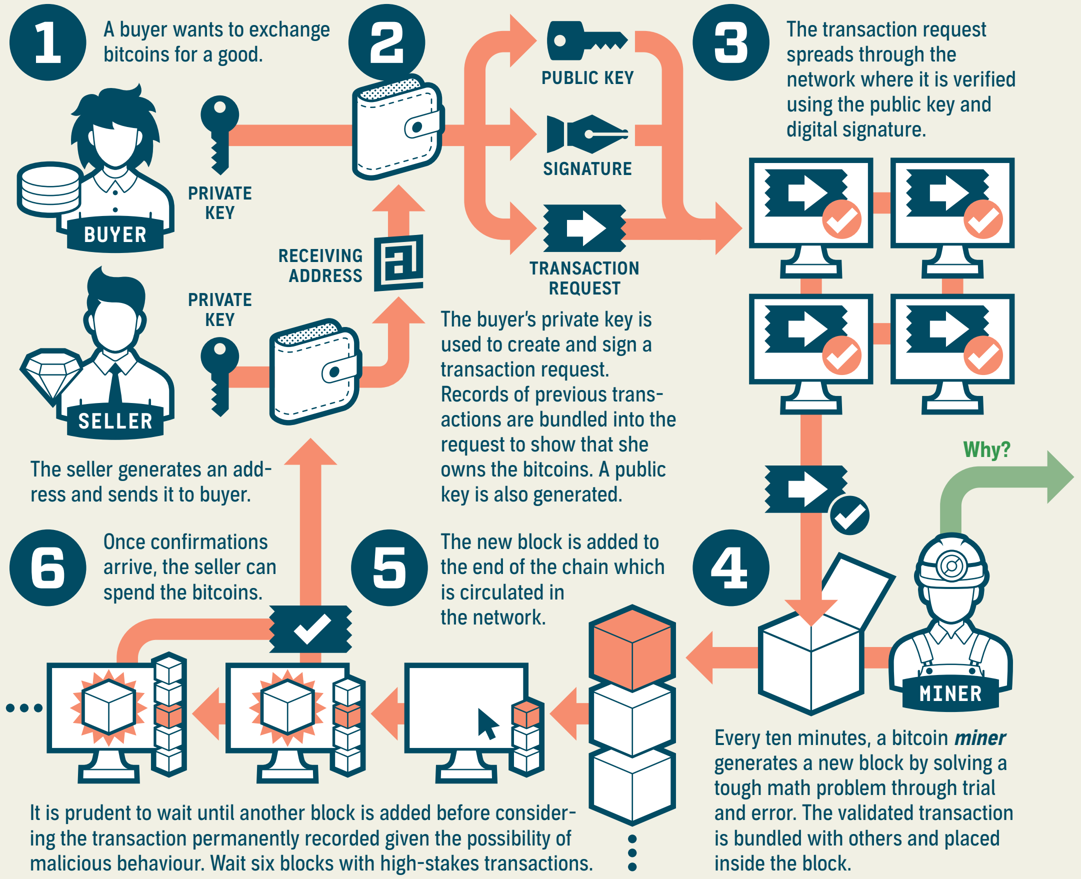
E RECONCILED

A ***consensus mechanism*** sets how blocks are added and transactions verified so everyone in the network gets the right version of the chain.



HOW BLOCKCHAINS CURRENTLY WORK

Decentralized digital money (cryptocurrency) is the typical application of blockchains. Bitcoin (฿) is the most successful example—how successful is up for debate. As a method of payment, the Bitcoin system is only able to process a few transactions a second due to design limitations that prevent the system from scaling. As a store of value, Bitcoin is subject to exchange rate volatility and is not easily exchanged into a fiat currency, such as the one you use everyday. Hacks and scams remain a threat. Nonetheless, Bitcoin is a prosperous market (worth 21 billion Canadian dollars) that demonstrates the promise of blockchain technology. Consider the basic stages of a Bitcoin transaction.



1 A buyer wants to exchange bitcoins for a good.

The seller generates an address and sends it to buyer.

2 The buyer's private key is used to create and sign a transaction request. Records of previous transactions are bundled into the request to show that she owns the bitcoins. A public key is also generated.

3 The transaction request spreads through the network where it is verified using the public key and digital signature.

4 Every ten minutes, a bitcoin ***miner*** generates a new block by solving a tough math problem through trial and error. The validated transaction is bundled with others and placed inside the block.

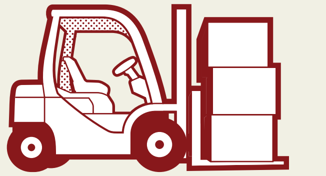
5 The new block is added to the end of the chain which is circulated in the network.

6 Once confirmations arrive, the seller can spend the bitcoins.

It is prudent to wait until another block is added before considering the transaction permanently recorded given the possibility of malicious behaviour. Wait six blocks with high-stakes transactions.

WHY GOVERNMENTS SHOULD CARE

Central banks are investigating the potential of cryptocurrencies. There are many more promising use cases for governments, which rely heavily on ledgers to manage their affairs. Note that most of these applications are merely theoretical and are at the proof-of-concept or pilot stages of development. They fall into three general categories.

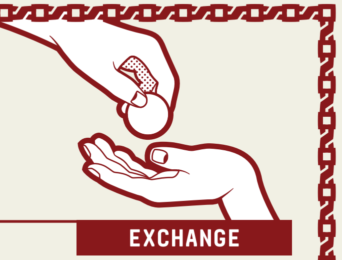


INVENTORY

- **Supply chains** can be managed on a common blockchain platform.
- **Sharing of property** (such as intellectual property) can be managed securely.
- Distributed ledgers can form backbone of new **record-keeping systems**.
- Copies of information can be secured and distributed to **prevent censorship**.

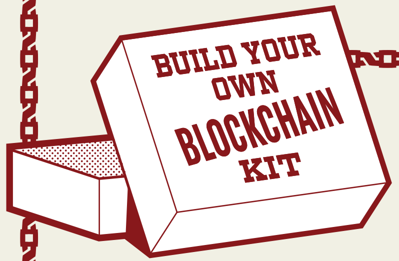
REGISTRY

- Access and entitlement can be verified with blockchain **identity systems**.
- **Asset ownership** and **provenance of valuables** can be tracked.
- A blockchain can make verification of **digital voting systems** more open.
- A **digital notary** is a trusted, inexpensive, immutable registry of historical facts.



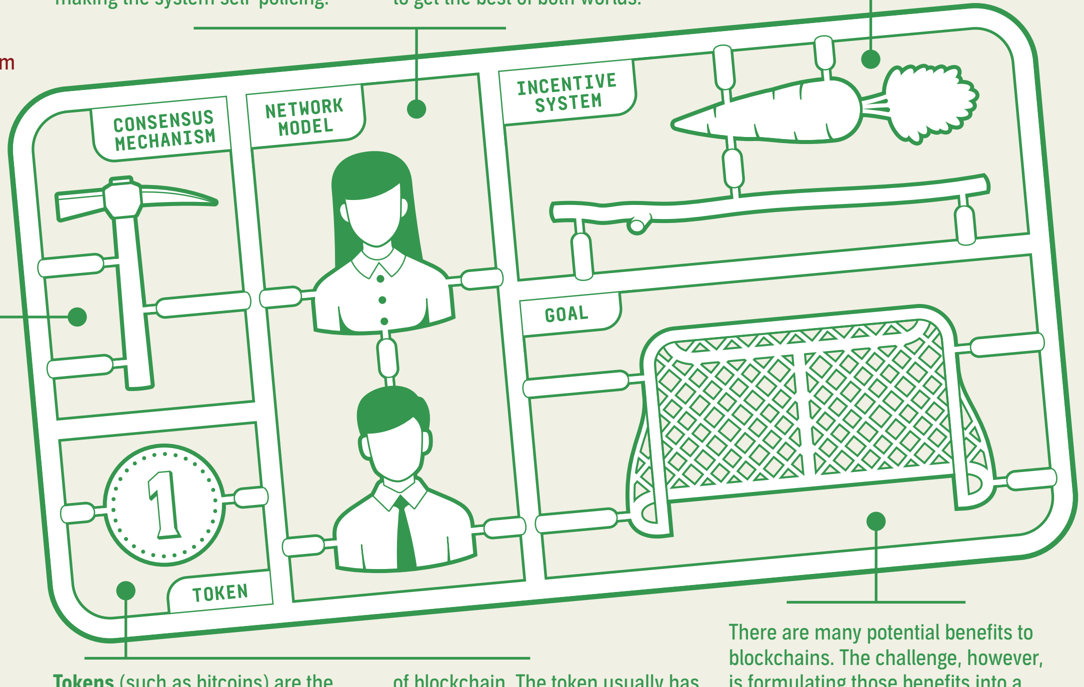
EXCHANGE

- **Smart contracts** govern economic relations in real time with coded terms.
- Blockchain tokens can be used for new digital **payment systems**.
- Projects can be funded using a blockchain as a **crowd-sourcing** platform.
- Blockchains can govern bidding in **blind auctions** and **tendering systems**.



COMPLEXITIES OF BUILDING ONE

Turning a theoretical benefit into reality means designing the system in which a blockchain operates. A few parts of that system deserve careful consideration.



Bitcoin's "mining" process controls the creation of new blocks and rewards those who validate transactions in good faith, all without the need of a central authority. A block is difficult to create (hence the math problem and a pay out) but easy to verify: a **consensus mechanism** called "proof of work." Other mechanisms exist for public blockchains. With "proof of stake", for example, certain nodes in the network are randomly selected to "mint" blocks. A node must first put up collateral which is forfeited if it does not abide by the consensus rules.

A cryptocurrency relies on a ***public blockchain***—a reference to the **network model**. Anyone can join the network. No one is required to trust one another. Members of the network may be anonymous (or pseudonymous). The trade-off, alas, is that a large amount of complexity and resources goes into making the system self-policing.

Members of the network may know each other and have a pre-existing basis for trust. It is possible to create a ***permission blockchain*** with controlled membership and conventional auditing, such as with enterprise or industry applications. A few schemes create a ***federated*** mix of public and permission models to try to get the best of both worlds.

Users need a compelling reason to use a blockchain. Networking, storage, and computing resources used by nodes in the network are costly, adding to the rationale for an **incentive system** that adequately rewards effort. Many peer-to-peer-sharing systems fail because of "free riders" who do not contribute.

Tokens (such as bitcoins) are the unit of value for a cryptocurrency. They also shape incentives for validating transactions and discouraging malicious behaviour in other types of blockchain. The token usually has no value separate from the system. That said, some blockchains (including non-public ones) will tie tokens to real-world assets.

There are many potential benefits to blockchains. The challenge, however, is formulating those benefits into a coherent and sustainable system with a clear **goal**. Blockchains fail when enthusiasm for the technology gets ahead of a compelling business model.

BATTERIES NOT INCLUDED

Bitcoin's mining uses a large city worth of energy for no productive purpose.

www.elanica.com/eye-cues

Citation: Peter Stoyko, "EyeCues: Government Blockchain," *Canadian Government Executive*, vol. 23, no. 2 (2017), pp. 12-13.