# Dissecting Decentralization: An in Depth Look at Blockchain Technology and its Applications

Alec Shackett & Frank Breitinger, Ph.D.

University of New Haven
TAGLIATELA COLLEGE OF ENGINEERING

## Objective

Compile an interactive lecture to help bring an understanding to our students by exploring the expansive blockchain literature and its applications.

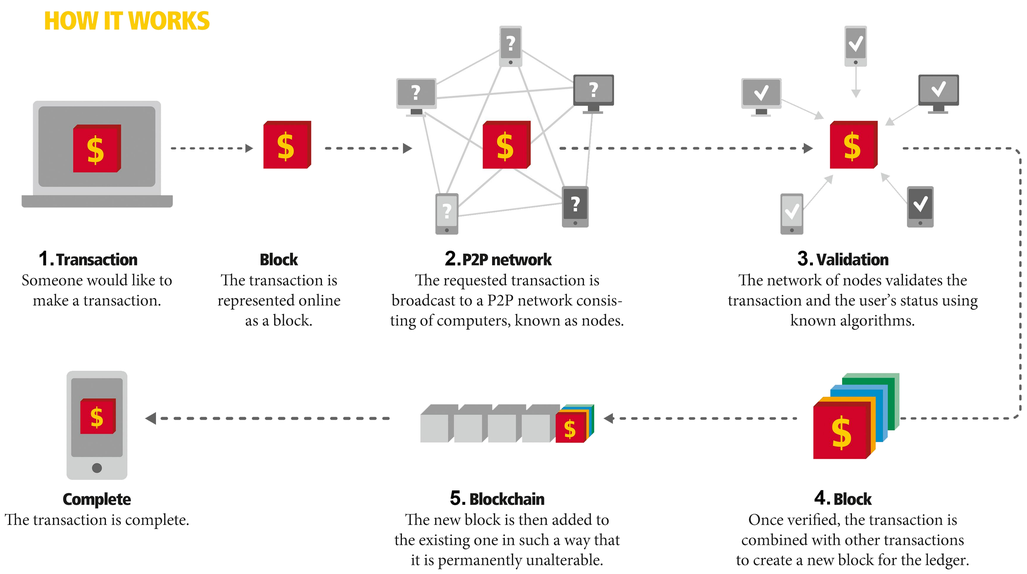
**Adjustment:**
The project's original title was *How To Use Blockchain Technology To Protect Personally Identifiable Information* and focused on proposing a novel concept for handling personally identifiable information. Due to the later discovery of a paper titled *Decentralizing Privacy: Using Blockchain to Protect Personal Data* by Zyskind et al the project goal was revised as such.

## Problem Statement

In order for Alice to send money to Bob, in the current system, she will have to go through a financial institution, such as a bank. Banks are in place to ensure people actually have the money they claim to be spending and do not **double spend** it. It is usually time consuming for transactions to go through as most often the money will have to transfer banks and this can take multiple business days.

In 2008, Bitcoin introduced a way to eliminate this slow process and provide a way for the peer-to-peer transfer of money between parties. The technology now coined **blockchain** was introduced alongside Bitcoin to serve as a digital ledger. Blockchain is a write only data structure that each participant node in the network can store on their computer.

## Blockchain Technology





http://www.delivered.dhl.com/en/articles/2017/06/explained-blockchain.html

1. A **transaction** occurs between parties.
2. That transaction is then broadcasted to each **node** on the **peer-to-peer** network.
3. Nodes validate the transaction by ensuring the sender has the available funds.
4. Special nodes called **miners** collect valid transactions and work to solve a **hash** problem by trial and error provided by the **proof-of-work** algorithm.
5. Once a miner finds a correct hash they **append** the new block of transactions to the blockchain and broadcast it to each other node on the network.

## Applications



Storj

ChainPrint
PUBLISHING BLOCKCHAIN

MedRec

Decentralizing Privacy

## Future Work

- Develop a highly technical presentation for use in lecture.
- Expand on this gathered information to develop a future class at the University of New Haven.

## References

- Nakamoto, Satoshi. "Bitcoin: A Peer-to-Peer Electronic Cash System." Bitcoin.org, bitcoin.org/bitcoin.pdf.
- Buterin, Vitalik. "Ethereum White Paper: A Next Generation Smart Contract & Decentralized Application Platform." ethereum.org.
- "Explained: Blockchain." Delivered. The Global Logistics Magazine., www.delivered.dhl.com/en/articles/2017/06/explained-blockchain.html.

**Acknowledgements**: We would like to thank Carol Withers and the SURF team for running the program and giving us this wonderful opportunity to learn and grow as researchers.