Information Technology Law in the Global Society

Faculty of Law, University of Latvia

Class 11

28 April 2020

Shawn Sullivan

Chapter 17: Electronic payments & cryptocurrency

Payments

- Electronic commerce has made possible trade in a digital environment.
- Improving the process by which online purchasers pay for their purchases has been key to the expansion of e-commerce.
- Today we look at how online payments are carried out & the legal regimes that have made payment transactions more secure & efficient.

Token payments

- A token is money that has little intrinsic value in comparison to its face value. For example:
  - Banknotes;
  - Coins.
- Some characteristics:
  - **Portable**: Can be easily and economically transported from one place to the other.
  - **Storable**: Capable of being stored for considerable time without loss of freshness or usability.
  - **Fungible**: Each individual token (or fraction of a token) is interchangeable for another. Money is fungible because there is no difference between one Euro and another Euro.
  - **Divisible**: Tokens can be divided into small increments that can be used in exchange for goods of varying values.
  - **Acceptable/transferable**: Government guarantees your right to use official currency to pay bills.
- Enable commerce beyond barter in commodities.
- Most tokens are guaranteed by a central bank or currency.

Alternative Payment Systems -- Debt Substitution

- When a depositor opens a savings or checking account, the bank owes the depositor the balance on that account.
- A checking or savings account in fact is a debt owed by the financial institution to the depositor.
- When the depositor writes a check, the depositor is instructing the bank to pay someone else a part of the money that the bank owes to the depositor.
- When a person pays for goods or services with a check, s/he is substituting the bank’s debt to him/her for the debt s/he owes the seller.
- Debt transactions using checks or debit cards are a substitute for money, but—
  - Not fungible.
  - Not as widely accepted or as easily transferable as money.
  - High transaction costs for debit cards.

Alternative Payment Systems - Credit Cards

- When a consumer uses a credit card, the financial institution becomes indebted to the seller, and the consumer becomes indebted to the financial institution.
- High transaction costs.
  - Merchant's cost for processing a payment card is usually a combined percentage plus a flat fee.
  - Processing charge = financing risk charge + computer network costs.

Alternative Payment Systems -- Various Kinds of Fund Transfers

- Automated Clearing House (ACH) payments: made through a computer-based electronic network for processing transactions between participating financial institutions. An ACH network may support both credit transfers and direct debits.
- All these systems have become widely used, but in some ways they're not as efficient as cash.
- These systems generally depend upon the participation of a trusted central party that verifies the value of the payment instrument (e.g., with cash, a central bank; with debt instruments, a financial institution).

Payment Services Directive II – Directive (EU) 2015/2366

- Supports innovation and competition in retail payments and enhances the **<u>security of payment transactions</u>** and the protection of consumer data.
- Requires payment service providers to—
  - Issue & use strong customer authentication solutions, allowing for authorization to be dynamically linked to the specific amount and payee;
  - Offer transaction and device monitoring to identify unusual payment patterns;
  - Provide a standardized and reliable access interface to payment accounts (i.e. an application programming interface, API) which makes it possible to identify third-party payment service providers in a secure way and secures all related communication between all parties involved.
- Where there is payment fraud in a transaction in which the payment instrument isn't present at point of sale, the payment service provider can only shift the loss to the customer where the service provider can prove the customer was negligent.

E-Money

Since Internet usage became widespread, there have been many attempts to create different kinds of "electronic cash" for use in consumer transactions.

- Mondex
- Digicash

Desire to simplify the process.

- Reduce or eliminate transaction costs.

These were attempts to create digital tokens.

- Fungible.
- Divisible.
- Anonymous.

Early attempts to create "electronic cash" were not very successful.

- Lack of trust in the companies—Electronic Money Issuers (EMIs)—behind the tokens.
- More certainty with debit & credit transactions – legal protection against certain kinds of fraud.

Original E-Money Directive (2000)

- Effort to stimulate development of electronic money & provide customer protection.
  - E-money institutions were required to have an initial capital of € 1 million.
  - E-money institutions were prohibited from engaging in other businesses.

E-Money Directive II – Directive 2009/110/EC

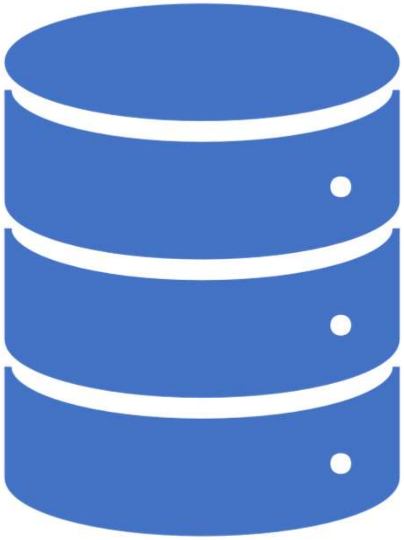
- Aims to enable new and secure electronic money services and to foster effective competition between all market participants.
  - "E-money" means "electronically, including magnetically, stored monetary value as represented by a claim on the issuer which is issued on receipt of funds for the purpose of making payment transaction, and which is accepted by a natural or legal person other than the electronic money issuer".
  - Includes prepaid cards and electronic wallets.
- Establishes requirements for obtaining a license as an e-money institution.
- Prohibits anyone who is not an electronic money issuer from issuing electronic money.
- E-Money Directive II sets initial capital requirement for EMIs at €350,000.
- Allows EMIs to engage in a wide range of payment functions AND to carry on other lines of business.

Cryptocurrency

- A digital asset designed to work as a medium of exchange that uses strong cryptography to secure financial transactions, control the creation of additional units, and verify the transfer of assets.
- Cryptocurrencies have arisen independently of legal systems.
- Replaces the role of a trusted central party (e.g. a central bank in the case of official currency or a financial institution in the case of checks) that authenticates the value of the money or money substitute, with a peer-to-peer network.

Blockchain (distributed ledger) technology

- The blockchain is a decentralized, distributed public ledger that records transactions anonymously and securely. By recording all transactions made within the cryptocurrency network, blockchain technology removes the need for a middle-person like a central bank, payment app such as PayPal, or any other central authority.
- The decentralized nature of blockchain technology means that cryptocurrencies have no central point of control, as with most traditional currencies, and is sustained by individuals in the widespread cryptocurrency community.
- This creates a trustless payment system, where parties participating in bitcoin transactions can be sure of the information displayed on the blockchain.

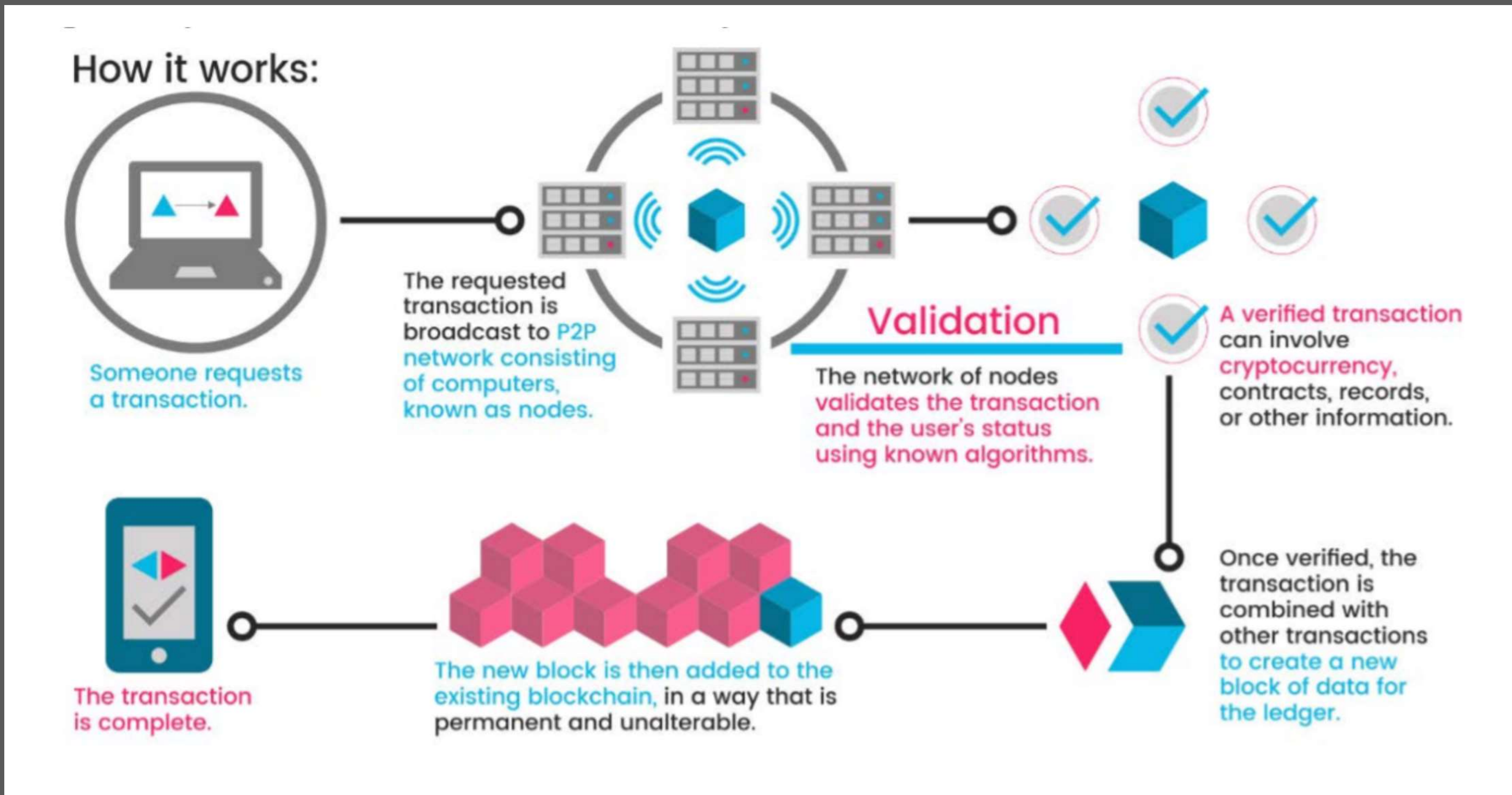


How Blockchain Works

A blockchain is a distributed ledger that does the following:

- Records any transaction or information chronologically, permanently and unalterably.
- Uses one-way hash cryptography that is computationally impractical to break.
- Is visible to all permissioned users.
- Uses Peer-to-Peer transmission, with each node forwarding new transactional information to all others.
- Can trigger transactions automatically, based on business logic and custom algorithms.
- Verifies transactions through node consensus with no reliance on third-party intermediaries (e.g., clearinghouses).

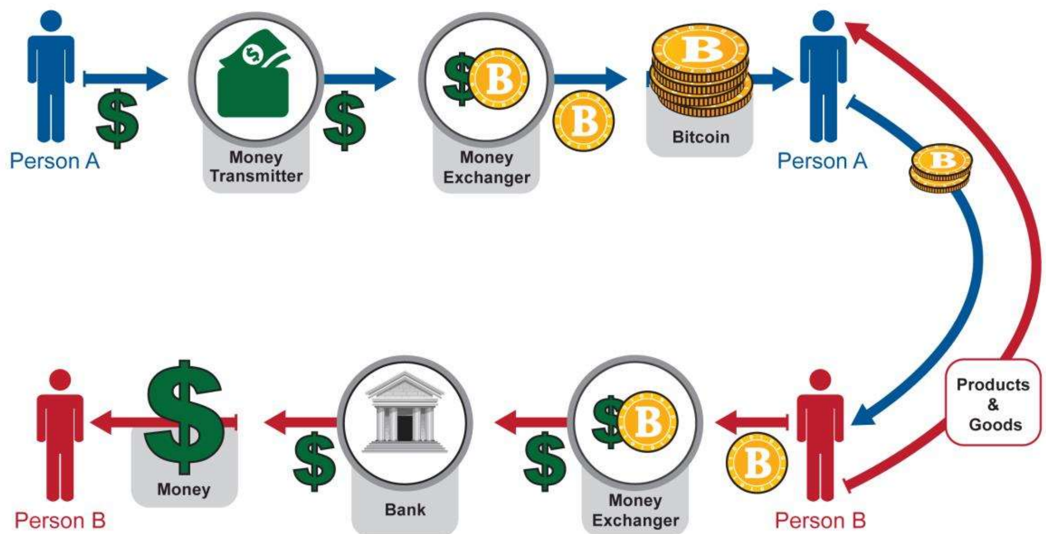
M. Swan, Blockchain: Blueprint for A New Economy. Sebastopol, CA: OReilly Media, Inc., 2015


How it works:
Someone requests a transaction.
The requested transaction is broadcast to P2P network consisting of computers, known as nodes.
Validation
The network of nodes validates the transaction and the user's status using known algorithms.
A verified transaction can involve cryptocurrency, contracts, records, or other information.
Once verified, the transaction is combined with other transactions to create a new block of data for the ledger.
The new block is then added to the existing blockchain, in a way that is permanent and unalterable.
The transaction is complete.

Bitcoin: A decentralized virtual currency

- Bitcoins exist in the virtual world as snippets of code.
- New bitcoins are created through a process called bitcoin mining, in which powerful computers solve complex equations.
- Bitcoin mining creates a new “block” on the blockchain where transactions are recorded, verified & saved.
- Part of bitcoins’ value is created through supply & demand, because there is a limited number of bitcoins to be mined.

A Series of Transactions When Bitcoin is Used in a Purchase



Cryptocurrency and the law

- Because cryptocurrencies arose outside regulated payment channels, the law is still catching up to their existence and use.
- Rights of consumers and commercial payors who use cryptocurrencies to pay merchants & other businesses.
- Income tax, value added tax (VAT).
- Use of cryptocurrencies in criminal transactions.

Limitations in Use of Cryptocurrencies

- Fluctuating currency – volatile values require that the merchant assumes the exchange risk.
- Some exchangers don't require identification of customers, some don't require a bank account.
- Exchangers don't always follow anti-money laundering (AML) compliance rules & thus banks may consider them to be high risk.

Cryptocurrencies Now Often Used by Criminals

- Can be used anonymously (not face-to-face).
- Can use it on dark web for unlawful transactions (weapons, illegal drugs, etc.)
- Can be used to launder money.
- Decentralized currency with little government oversight or regulation
- Can be transferred rapidly.

Anti-Money Laundering Laws Are Now in Effect in Many Countries

- Multi-jurisdictional investigations involving authorities from European Union, United States, and other bodies.
- Extraterritorial reach of US AML laws:
  - Exchangers of convertible virtual currency are “money transmitters” as defined at 31 C.F.R § 1010.100(ff)(5) and “financial institutions” as defined at 31 C.F.R § 1010.100(t). A foreign-located business qualifies as an MSB if it does business as an MSB “wholly or in substantial part within the United States.”

Russian national arrested in Greece. Operated unregistered cryptocurrency exchange with US customers.

UNITED STATES OF AMERICA
DEPARTMENT OF THE TREASURY
FINANCIAL CRIMES ENFORCEMENT NETWORK

IN THE MATTER OF:	)	
	)	
	)	
	)	**Number 2017-03**
BTC-E a/k/a Canton Business Corporation	)	
and Alexander Vinnik	)	
	)	

ASSESSMENT OF CIVIL MONEY PENALTY

I. INTRODUCTION

The Financial Crimes Enforcement Network (FinCEN) has determined that grounds exist to assess a civil money penalties against BTC-E a/k/a Canton Business Corporation (BTC-e) and Alexander Vinnik, pursuant to the Bank Secrecy Act (BSA) and regulations issued pursuant to that Act.[1]

FinCEN has the authority to impose civil money penalties on money services businesses (MSBs) and individuals involved in the ownership or operation of MSBs.[2] Rules implementing the BSA state that "[o]verall authority for enforcement and compliance, including coordination and direction of procedures and activities of all other agencies exercising delegated authority under this

BRIAN J. STRETCH (CABN 163973)
United States Attorney

BARBARA J. VALLIERE (DCBN 439353)
Chief, Criminal Division

WIL FRENTZEN (LABN 24421)
Assistant United States Attorney
450 Golden Gate Avenue, Box 36055
San Francisco, California 94102-3495
Telephone: (415) 436-6959
Fax: (415) 436-7234
William.Frentzen@usdoj.gov

Attorneys for the United States

FILED
2017 JAN 17 P 4:38
CLERK, U.S. DISTRICT COURT
NO. DIST. OF CA.

SEALED BY COURT ORDER

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN FRANCISCO DIVISION

UNITED STATES OF AMERICA, Plaintiff, v. BTC-E, A/K/A CANTON BUSINESS CORPORATION, and ALEXANDER VINNIK. Defendants.	CASE NO: CR 16-00227 SI UNITED STATES' MOTION TO SEAL SUPERSEDING INDICTMENT, ARREST WARRANTS AND ~~[PROPOSED]~~ ORDER UNDER SEAL

FinCEN Guidance on Cryptocurrencies

- U.S. Department of the Treasury Financial Crimes Enforcement Network, or FinCEN.
- 2013 - FinCEN issued Bitcoin and virtual currency guidance regarding creating, obtaining, distributing, exchanging, accepting or transmitting virtual currencies.
- Companies providing cryptocurrency-related services must report all data to US government so that it can prevent money laundering.

2013 FinCen Guidance on Virtual Currencies

FinCEN Guidance (2013) covers convertible cryptocurrencies that either have “an equivalent value in real currency, or act as a substitute for real currency” https://www.fincen.gov/sites/default/files/shared/FIN-2013-G001.pdf

Money Services Businesses (MSBs) are subject to on-site examination by US Internal Revenue Service (IRS), the tax collection agency of US government.

MSBs are subject to civil and criminal penalties for non-compliance with laws.

2013 FinCen Guidance continued

- Requires cryptocurrency MSBs to have an anti-money laundering (AML) program and treats them as "money transmitters" – exchangers and administrators:
  - An exchanger is a person engaged as a business in the exchange of virtual currency for real currency, funds, or other virtual currency.
  - An administrator is a person engaged as a business in issuing (putting into circulation) a cryptocurrency, and who has the authority to redeem (to withdraw from circulation) such cryptocurrency.
- Although administrators and exchangers are treated as MSBs engaged in money transmission, users who buy & sell goods or services aren't covered by FinCEN guidelines.

Consolidated with other guidance in 2019 Guidelines: Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies (CVC)

Like other MSBs, Virtual Currency Exchangers Are Required to Have an Anti-Money Laundering (AML) Program with 4 Elements

- Written policies, procedures and controls (PPCs) based on a written risk assessment
- Designation of an AML Compliance Officer
- Periodic independent AML reviews (i.e., audits)
- Training of appropriate personnel, including, inter alia, Board of Directors, senior management, AML compliance officer (AMLCO) and client-facing staff

Other Requirements for Exchangers

- Also an electronic registration requirement for MSBs within 180 days after establishment of business.
- Recordkeeping requirement for customers sending over $3,000.
- Filing of suspicious activity reports (SARs) and CTRs (i.e. acceptance of or provision of more than US$10,000 in cash)
- Must be on guard against suspicious transactions
- Must monitor customers & transactions.

Reading for Next Week

- Chapter 18 – Consumer Protection
- Chapter 19 – Computer Misuse