


# Blockchain in a Nutshell

Prof. David (Duc) Tran, PhD  
University of Massachusetts, Boston (USA)



1

## Let's play a game

Consider a simple example: Alice and Bob each bet \$100 on a coin flip

1. Alice calls the outcome of the coin flip
2. Bob flips the coin
3. Alice wins \$200 if her guess was correct

Now, what if Alice and Bob are **separated** and **don't trust one another**?  
*Bob may cheat. Alice can run away if losing*


2

... is an example of a **big real-world problem**.

That is, how to **quickly** process **transactions** for everybody, possibly **involving multiple people**, in an environment **not always honest**, where people may **not trust** one another?

3

### Conventional Method: Intermediary



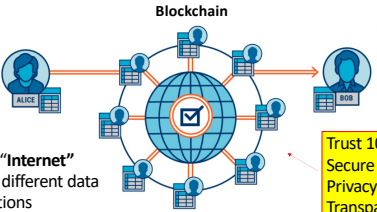
- E.g., banks (central management)
- Servers (central IT processing)
- **Attacks, errors** by human
- **High cost, complex** to scale

Trust 100%? **NO**  
Secure 100%? **NO**  
Privacy 100%? **NO**  
Transparency 100%? **NO**

4

### With Blockchain

- Data replicated in **many computers**
- All **autonomously** process transactions
- Consensus even with **uncooperative** computers

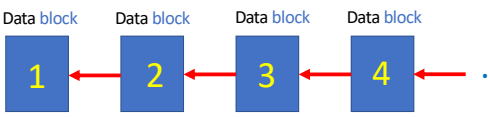


Like an **"Internet"** serving different data applications

Trust 100%? **YES**  
Secure 100%? **YES**  
Privacy 100%? **YES**  
Transparency 100%? **YES**

5

### Why the name "Blockchain"? Crypto?



Data storage is structured as a **chain** of data **blocks** which are linked by **cryptographic** methods ("locks")

6

### Blockchain and AI

Intelligent  
→ Future Human

Data Computer  
→ Future Internet

Blockchain

7

"How seriously should we take **Blockchain**? I would take it as **seriously** as we should have taken the concept of the **Internet** in the 1990s."

**Blythe Masters**

- Chairman of the Governing Board of the [Linux Foundation](#)'s open source [Hyperledger](#) Project
- Advisory Board Member of the US [Chamber of Digital Commerce](#)

8

Harvard Business Review

**"Blockchain is not a disruptive technology... Blockchain is a foundational technology: It has the potential to create new foundations for our economic and social systems."**

— Harvard Business Review

**The Truth About Blockchain**  
by Marco Iansiti and Karim R. Lakhani  
FROM THE JANUARY/FEBRUARY 2017 ISSUE

9

### Is Blockchain right for you?

Answer yes 4 out of 6

- Multiple parties share data?
- Intermediaries add complexity?
- Multiple parties update data?
- Interactions are time-sensitive?
- Requirement for verification?
- Transactions interact?

Doc No: Prof. Duc (Duc) Tran - duc.tran@humb.edu 10

10

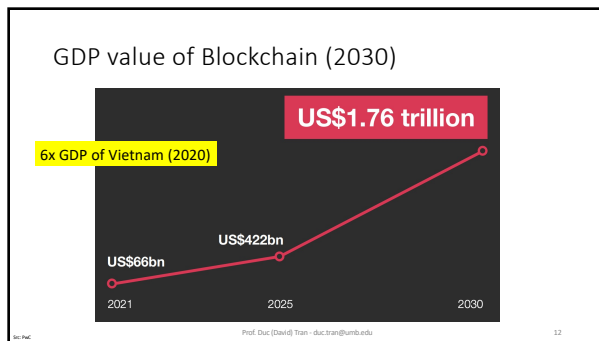
### Beneficiary Sectors

Top applications:

1. Financial services
2. Product manufacturing
3. Energy and utilities
4. Healthcare
5. E-government
6. Retail and consumer
7. Entertainment and media

Prof. Duc (Duc) Tran - duc.tran@humb.edu CREATED BY 101BLOCKCHAINS.COM

11



12

### Deloitte Report (2020)

- Survey of 1488 business leaders from 14 countries
- **39%** applied Blockchain, 23% increase from 2019
- **55%** consider Blockchain a **top-5** priority of company
- **82%** will hire blockchain staff within 12 months

Prof. Duc (David) Tran - duc.tran@umb.edu 13

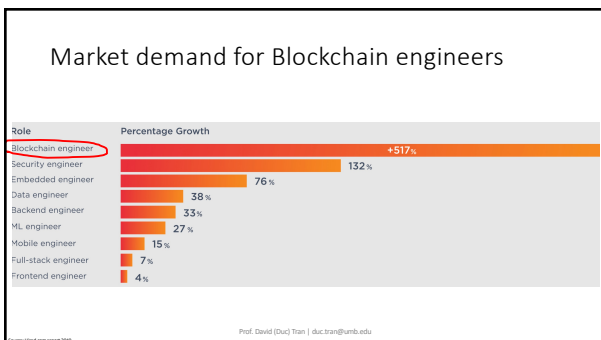
13

### 2030

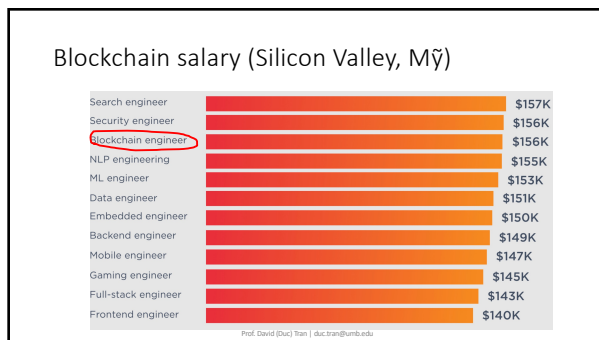
- Create **40 million** new jobs
- **10% - 20%** global business infrastructure will run technological systems with **blockchain** in it

Source: Gartner, Inc. Prof. Duc (David) Tran - duc.tran@umb.edu 14

14



15



16

## What is Blockchain?

Prof. Duc (David) Tran - duc.tran@umb.edu 17

17

## Blockchain

A computing technology for **data storage** and **transacting** that is

- safe** (no loss or change of data possible),
- transparent** (easily verify and trace),
- trust-less** (confidently transact without any intermediary)

Prof. Duc (David) Tran - duc.tran@umb.edu 18

18

Another way to define Blockchain

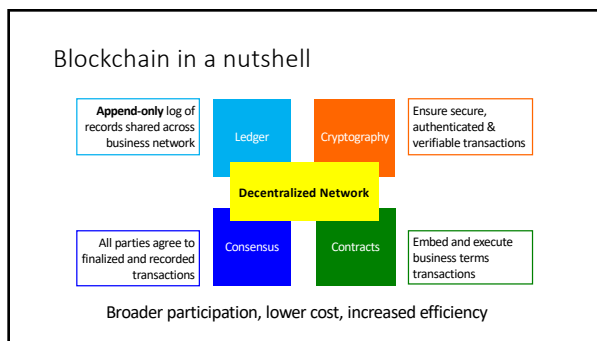
A computing technology for **data storage** and **transacting**

that stores data **chronologically** in **blocks** which are added in an **append-only** manner

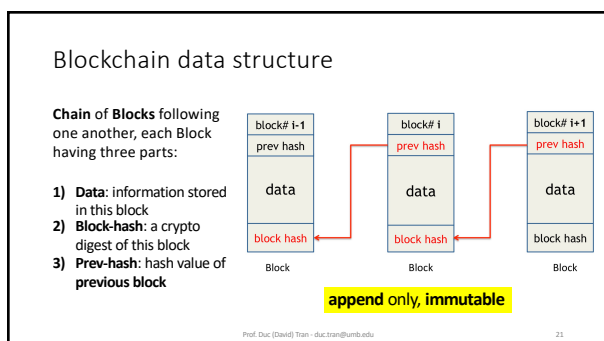
and operates as a **decentralized** digital ledger where participants must reach **CONSENSUS** to record any new input.

Prof. Duc (David) Tran | duc.tran@umb.edu 19

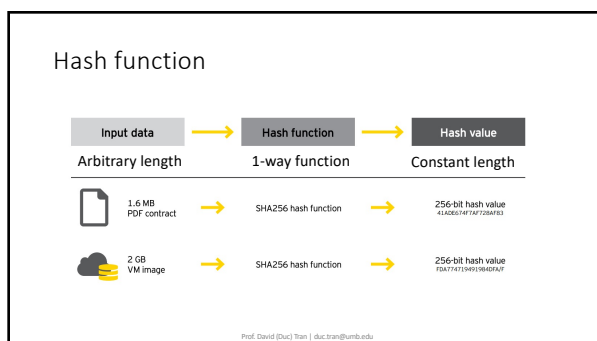
19



20



21



22

### Crypto hash function

- H** = hash function (length of output is **“fixed”** n bits)
- Crypto hash function = Hash function with 2 properties:**
  - Collision-resistant**
    - Cannot find  $x \neq y$  such that  $H(x) = H(y)$
  - Puzzle-friendly** (difficulty to solve is as hard as Sudoku-like puzzle)
    - Even if we know  $C = H(r || x)$  and  $x$ , **cannot find r** in time faster than  $2^n$

Prof. David (Duc) Tran | duc.tran@umb.edu 23

23

### Let's play this game!

Consider a simple example: Alice and Bob each bet \$100 on a coin flip

- Alice calls the outcome of the coin flip
- Bob flips the coin
- Alice wins \$200 if her guess was correct

Now, what if Alice and Bob are **separated** and **don't trust one another**?

**... Bob may cheat!**

Prof. Duc (David) Tran | duc.tran@umb.edu 24

24

### Solution: Commitment Scheme

1. Alice **predicts** outcome: **B**
2. Alice chooses a **large random number: R**
3. Alice **sends** Bob an encrypted "**commitment**": **C = H (R, B)**
4. Alice **sends C** to Bob
5. Bob **tosses** coin, sends **outcome** to Alice
6. Alice knows whether her prediction is correct
7. If correct, Alice sends Bob her prediction **B** and the number **R**
8. Bob verifies if **C = H(R, B)**?
9. Both agree who win

**Bob cannot lie due to not knowing Alice's prediction**

**Alice cannot lie due to commitment to Bob**

Prof. David (Duc) Tran | duc.tran@umb.edu 25

25

### Why does Alice need big random number R?

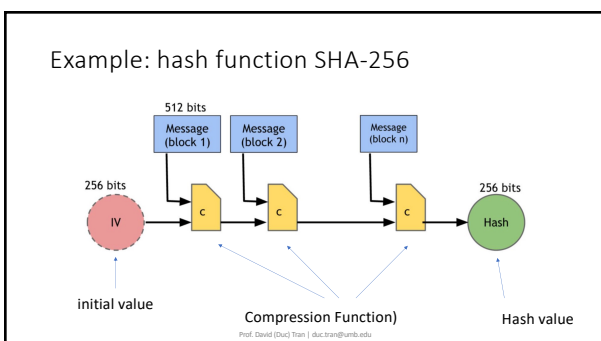
- If Alice's commitment is **C = H (B)**, Bob can precompute hash value for **B = 0** and **B = 1**.
  - $H(B = 0) = 0x67ebbd370daa02ba...22360240a42fe922e$
  - $H(B = 1) = 0xc04b5bb1a5b2eb3e...b5474c4adae9faa80$

By comparing **C** to **H(0)** and **H(1)**, Bob can tell the answer **B** of Alice

- Using large random **R**, Alice enlarges the value range of **R||B** so that Bob cannot find **B** ("puzzle-friendly" property of crypto hash H)

Prof. David (Duc) Tran | duc.tran@umb.edu

26



27

### Crypto Hash: Used in Bitcoin Blockchain

#### ELLIPTIC CURVES

INTRODUCTION

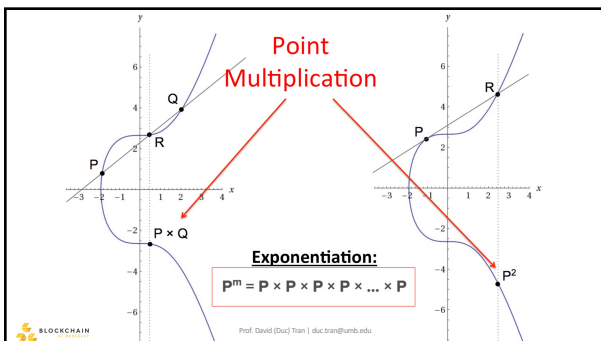
Defined by the following short Weierstrass form:

$$E: Y^2 = X^3 + aX + b$$

- For cryptographic purposes, we use elliptic curves over a **finite field**.
- We define an operation analogous to multiplication using points on the curve (called a group law).
- This group law provides a **finite abelian group** where the **discrete logarithm problem** is hard.
- (non-math speak) We can do "multiplication" with points on this funky elliptic curve thing.

Prof. David (Duc) Tran | duc.tran@umb.edu

28



29

### Elliptic Curve Cryptography

- Knowing  $P^m$

$$P^m = P \times P \times P \times P \times \dots \times P$$

- Impossible in practice to find  $m$  such that

$$\log_P (P^m) = m ?$$

Prof. David (Duc) Tran | duc.tran@umb.edu

30

### Why is data immutable?

If this block is altered → its hash will change

not same as prev\_hash of this block → detected và not accepted

Prof. Duc (David) Tran - duc.tran@umb.edu 31

31

### Where is Blockchain data stored?

- Traditionally: central server (**centralized**)
  - Not safe, can be attacked (internally or from outside)
  - Error possible (maybe intentional by internal people)

**Blockchain: decentralized**

- **Many computers** join, auto-connect, cooperate to process transactions
- **Peer-to-peer** model: autonomous, avoid putting power on a single participant (weakest link)
- **Solution:** each computer store a **Full Copy** of the whole blockchain data

Prof. Duc (David) Tran - duc.tran@umb.edu 32

32

### How a transaction works?

Someone requests a transaction.

The requested transaction is broadcast to a peer-to-peer network consisting of nodes.

Nodes: They verify the transaction and the user's status using known algorithms.

A verified transaction can involve cryptocurrencies and other digital tokens, records, or other information.

The transaction is complete.

The new block is then added to the existing blockchain, in a way that is permanent and unalterable.

Once verified, the transaction is combined with other transactions to create a new block of data for the ledger.

Prof. Duc (David) Tran - duc.tran@umb.edu 33

33

### Consensus Problem

- Each transaction is sent to all nodes. The same transaction may be added to different blocks at different nodes. But, a transaction can only be added to the blockchain **once**
  - Question: how to avoid **transaction duplication**?
- Only one block can append to the existing blockchain. But different blocks are independently created at different nodes.
  - Question: which **block should be the next block on the blockchain**?
- The blockchain network is fully **decentralized**, nodes independently add blocks to their respective local blockchain
  - Question: which **blockchain version is correct**?

→ We need a **consensus mechanism**

Prof. David (Duc) Tran | duc.tran@umb.edu

34

### Consensus Problem: 30 years of study

- Back in the 1970s: Aircraft control
  - Computers were being used in aircraft control. As a mission-critical system, it was important to replicate it on multiple machines to tolerate faults
  - NASA sponsored the *Software Implemented Fault Tolerance (SIFT)* project to build a resilient aircraft control system
  - In this project, Lamport et al. (1982) introduced the well-known "**Byzantine Generals Problem**" and **laid the foundation** of distributed consensus
- Since 2000: Industry adoption
  - Companies like Google and Facebook have adopted distributed consensus for mission-critical services such as Google Wallet and Facebook Credit.
- 2009: Bitcoin
  - A **new breakthrough** in distributed consensus, showing that consensus is viable in a decentralized, permissionless environment where anyone is allowed to participate

Prof. David (Duc) Tran | duc.tran@umb.edu

35

### 1991: First Blockchain

Trusted  
timestamping  
of documents

How to Time-Stamp a Digital Document\*

Stuart Haber  
stuart@bellcore.com

W. Scott Stornetta  
stornetta@bellcore.com

Bellcore  
445 South Street  
Morristown, N.J. 07960-1910

Abstract

The prospect of a world in which all text, audio, picture, and video documents are in digital form on easily modifiable media raises the issue of how to certify when a document was created or last changed. The problem is to time-stamp the data, not the medium. We propose computationally practical procedures for digital time-stamping of such documents so that it is infeasible for a user either to back-date or to forward-date his document, even with the collusion of a time-stamping service. Our procedures maintain complete privacy of the documents themselves and require no authentication by the time-stamping service.

36

## 1992: Tree Hash

Put multiple documents in a block, using Merkle tree hash

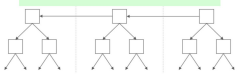
Improving the Efficiency and Reliability of Digital Time-Stamping

Dave Bayer\*  
Barnard College  
Columbia University  
New York, N.Y. 10027 U.S.A.  
dab@math.columbia.edu

Stuart Haber  
Bellcore  
445 South Street  
Morristown, N.J. 07960 U.S.A.  
stuart@bellcore.com

W. Scott Stornetta  
Bellcore  
445 South Street  
Morristown, N.J. 07960 U.S.A.  
stornetta@bellcore.com

March 1992



Abstract  
To establish that a document was created after a given moment in time, it is necessary to report events that could not have been predicted before they happened. To establish that a document was created before a given moment in time, it is necessary to state an event based on the document, which can be observed by others. Cryptographic hash functions can be used both to report events accurately, and to cause events based on documents without revealing their contents. Haber and Stornetta have proposed two schemes for digital time-stamping, which will be described in this paper.

Prof. David (Duc) Tran | duc.tran@umb.edu

37

## Blockchain = Super Safe Computer

- A computer = a machine that automates processing of applications
- **Once upon a time (Desktop Computing):** applications run on a desktop near you (home, office)
- **Yesterday and today (Cloud Computing):** run on a server in the computing cloud (of a cloud provider, some organization)
- **Today and future (Blockchain Computing):** run on a super computer – the blockchain computer, an autonomous network of computers not in any “cloud”, collectively contribute to process, detect errors, ensure security, forming a strong wall against all data attacks

### Blockchain = next big tech only after the Internet

Prof. Duc (David) Tran | duc.tran@umb.edu

38

## Blockchain “computer” architecture

Bitcoin

**3. Logic:** what specific application is served (dApp)

**2. Consensus:** how Nodes agree with each other

**1. Networking:** how Nodes P2P message with each other

Smart Contract

Ethereum

Specific-purpose Blockchain

Universal Blockchain: can run any-purpose applications

Prof. David (Duc) Tran | duc.tran@umb.edu

39

## Software Tools to build a Blockchain/Application

Solidity, Rust, C++, etc.

**3. Logic:** what specific application is served (dApp)

**2. Consensus:** how Nodes agree with each other

**1. Networking:** how Nodes P2P message with each other

Substrate (Polkadot SDK)

Tendermint (Cosmos SDK)

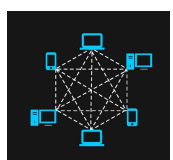
Build an application atop of a blockchain network

Build a blockchain network from scratch


Prof. David (Duc) Tran | duc.tran@umb.edu

40

## Permissionless vs. Permissioned Blockchain?



**Permissionless:** allow anybody to join freely, participate in the autonomous decision making with fair power (based on resource or stake contribution)



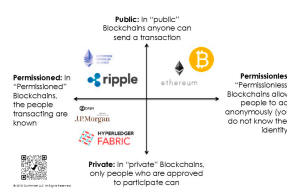
**Permissioned:** maintain an access control layer to allow certain actions to be performed only by certain identifiable participants (such as an organization, a government, a bank).

Prof. Duc (David) Tran | duc.tran@umb.edu

41

## Public vs. Private Blockchain?

- **Public blockchain:** service available to everybody
- **Private blockchain:** available to certain permitted participants



**Case by case basis:** can build “permissionless/permissioned” and “public/private”

Prof. Duc (David) Tran | duc.tran@umb.edu

42

## 2008: First Operational Blockchain

- Bitcoin payment transactions

### Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto  
satoshi@igmp.com  
www.bitcoin.org

**Abstract.** A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

Prof. Duc (David) Tran - duc.tran@umb.edu

43

43



## Use by Businesses

Prof. Duc (David) Tran - duc.tran@umb.edu

44

44

## Copyright violation, product frauds

<p><b>MICROSOFT</b></p> <p>Blockchain solution for managing xbox managing content rights and royalties</p> 	<p><b>LVMH</b></p> <p>AURA ensures tracking of products to reduce counterfeit luxury items</p> 
--	--

Prof. Duc (David) Tran - duc.tran@umb.edu

45

45

## Environment and Foods

<p><b>DAIMLER</b></p> <p>Tracks and reduces CO2 emission in their Cobalt supply chain process</p> 	<p><b>WALMART</b></p> <p>Food Traceability Initiative helps in ensuring proper food safety standards</p> 
--	--

Prof. Duc (David) Tran - duc.tran@umb.edu

46

46

## Healthcare



<p><b>IBM</b></p> <p>Digital Health Pass helps organizations with verifying COVID-19 tests of individuals</p> 	<p><b>NOVARTIS</b></p> <p>PharmaLedger offers use cases in clinical trials, patient data and pharma supply chain</p> 
---	--

Prof. Duc (David) Tran - duc.tran@umb.edu

47

47

## Supply chain

<p><b>MAERSK</b></p> <p>TradeLens helps in digitalizing supply chain information</p> 	<p><b>SHELL</b></p> <p>Features a decentralized passport system for authenticating all parts, equipment and products</p> 
---	--

Prof. Duc (David) Tran - duc.tran@umb.edu

48

48



### Financial

**VISA**

Visa B2B Connect offers a faster and secured financial solution in cross-border payments

**METLIFE**

Vitana offers health insurance for gestational diabetic pregnant women

Prof. Duc (David) Tran - duc.tran@umb.edu 49

49

### Aerospace

**BOEING**

SkyGrid helps in tracking and communications with drones

**HONEYWELL**

GoDirect Trade features a blockchain-based marketplace for aerospace products

Prof. Duc (David) Tran - duc.tran@umb.edu 50

50

## Use by Governments

Prof. Duc (David) Tran - duc.tran@umb.edu 51

51

### Estonia (started first)

- First government in the world (2012) adopted Blockchain for government operations
- Ministry of Justice: Succession registry, later digital court system
- Healthcare registry, property registry, business registry, state gazette

Prof. Duc (David) Tran - duc.tran@umb.edu 52

52

### China (going fast)

- 2016: China's 5-year economic development plan (2016-2020) considered **Blockchain** development a **national key goal**
- 2019: President **Xi Jinping** urged China not to lose the opportunity to lead the world in blockchain technology
- Invested billions of USD** in blockchain R&D
- The top country in the world in submission of **Blockchain patents**

Prof. Duc (David) Tran - duc.tran@umb.edu 53

53

### CCP Politburo organized a study session on Blockchain - 24/10/2019

Source: Xinhua

WITH CHINESE CHARACTERISTICS

Beijing unveils plan for blockchain-based government

China's state-owned news outlet Xinhua reports that the government will lead in blockchain adoption.

Xinhua News Agency, July 2019

Prof. Duc (David) Tran - duc.tran@umb.edu 54

54

USA (cautiously)

**CHAPTER 9: BUILDING A SECURE FUTURE, ONE BLOCKCHAIN AT A TIME**

- The Report estimates the substantial direct costs and longer-term indirect loss incurred to the economy and critical infrastructure from cyberattacks and threats. The Report suggests blockchain as a potential tool for securing America's digital infrastructure.

**In 2018, the US congress recommended the potential of Blockchain for securing America's digital infrastructure**

Prof. Duc (David) Tran - duc.tran@umb.edu

55

US State-level Blockchain Adoption

Example: blockchain for digital transformation (Delaware), birth certificates (Illinois), voting and election (West Virginia)

Prof. Duc (David) Tran - duc.tran@umb.edu

56

Blockchain adoption by other governments

- Australia: sharing import/export documents in cross-border trades
- Russia: government document management, health systems
- Dubai: e-passport, government documents, transportation
- Ghana, Georgia, Honduras, Thụy Điển: Land registry
- Switzerland: electronic identity
- Ukraine: Elections
- UK: social programs (Ministry of Labor), inter-ministry services

Prof. Duc (David) Tran - duc.tran@umb.edu

57

Let's talk crypto!

Prof. Duc (David) Tran - duc.tran@umb.edu

58

Watch out!

- US Gov. Budget **\$3.5 trillion**
- Crypto market cap **\$1.9 trillion**
- Bitcoin market cap **\$868 billion**

**August 11, 2021**

Prof. Duc (David) Tran - duc.tran@umb.edu

59


Fidelity's 2021 Institutional Investors

**70+% plan to invest in digital assets in the near future**

Digital Asset survey of 1,800+ investors in the US, Europe and Asia. It included institutions, high net worth individuals, family offices and hedge funds

Prof. Duc (David) Tran - duc.tran@umb.edu

60



Speaking about BTC, Damodaran – also known as “the Dean of Valuation” – described it as “millennial gold.” In his opinion, the yellow metal is an obsolete investment instrument for most of the youngsters who now find the digital currency as an attractive solution:

“If you are 35-years-old, and you have lost faith, you are no longer going to buy gold. That was for your parents and your grandparents. You are going to buy Bitcoin.”

61

### Digital Tokens and Cryptocurrency

- **Digital tokens** = digital representations of assets, securities, and currencies, based on **blockchain** technology
- **Cryptocurrency** = an example of **digital tokens**
  - Represent **digital money** (in the form of a “coin” or “token”)
  - “Crypto” because it is based on blockchain cryptography
  - Work without border, without intermediaries
- **Bitcoin, Ethereum** = most popular cryptos

Prof. Duc (David) Tran - duc.tran@umb.edu 62

62





### Main functions of “money”

- A **medium of exchange**: widely accepted for transactions
- A **store of value**: hold value over the time
- An **unit of account**: common measure of the value of goods and services being exchanged

Prof. Duc (David) Tran - duc.tran@umb.edu 63

63

### Types of Digital Tokens

			
<b>Currency tokens</b> Like Bitcoin and Ether, these are payment consideration similar to traditional fiat currencies.	<b>Utility tokens</b> Right to goods or services, such as data storage, advertising rights, or energy propositions.	<b>Commodity tokens</b> Rights to the value of an underlying commodity, such as oil or coffee beans.	<b>Security tokens</b> Investment interest in a company, including entitlement to profits or rise in company value.

**NON-FUNGIBLE TOKEN (NFT)** = represent a digital asset that is **unique** and **non-interchangeable**; e.g., photos, videos, audio, and other digital contents

Prof. Duc (David) Tran - duc.tran@umb.edu 64

64

### Non-Fungible Tokens (NFT)

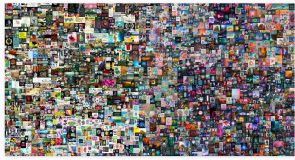
- **Fungible tokens**: tokens are identical
  - E.g., BTC, Ether: every one unit of BTC is identical to another unit of BTC
  - Fungibility is a fundamental property of traditional currencies, like the USD
- **Non-fungible tokens (NFT)**: a digital representation of a unique asset
  - E.g., digital art or any asset that wants to be traded digitally
  - used as digital proof-of-ownership of underlying assets
- ERC-20 is Ethereum standard for Fungible Token
- ERC-721 is Ethereum standard for Non-Fungible Token

Prof. David (Duc) Tran | duc.tran@umb.edu

65

NFTs

### ‘Beeple’ NFT sold for \$69 million is the fourth most expensive artwork sold by a living artist



Is money even real anymore? The NFT sector is making it seem so.

SHALINA MUKHERJEE | MARCH 10, 2021 AT 2:58 PM UTC - 2 MIN READ

#### NFT Steps

1. Create an **NFT token** with necessary descriptions about the painting, ownership
2. The NFT has an attribute to store the **blockchain addresses of the artist and owner**
3. List the NFT for **sale** on some NFT marketplace (e.g., OpenSea)
4. When a buyer buys this NFT, the **owner address will be changed to the new owner**

66

### In theory, anything can be NFT

**Musician sells rights to deepfake her voice using NFTs**

*"Creating work with the voices of others is something to embrace," said Holly Herndon.*

Fans who want to make their own deepfakes using her unique voice will have the opportunity to sell their minted creations NFT. Fans can **submit** their digital copies to be approved by the project's DAO and would receive 50% of any auction profits.

**Holly Herndon** (born 1980) is an American composer, musician, and sound artist based in [Berlin, Germany](#). Studied composition and completed PhD at [Stanford University](#).

67

### Many "coin" projects today

- **Application-specific** (payment, video app, file storage, finance, NFT)
  - Bitcoin, Theta, Filecoin, Chainlink, Chiliz, etc.
- A **universal platform** to deploy applications (smart contracts)
  - Ethereum, Cardano, Polkadot, Cosmos
- **Design differs** in how they address the following problems:
  - **Consensus:** make decision in a decentralized manner
  - **Scalability:** fast & efficient in processing more transactions
  - **Spamming:** present or discourage attacks
  - **Incentive:** encourage good participation

68

### Cryptocurrencies

#	Name	Price	24h %	7d %	Last 7 Days
1	Bitcoin BTC Buy	\$56,757.90	-4.13%	-4.12%	
2	Ethereum ETH Buy	\$3,421.26	-4.44%	+25.06%	
3	Binance Coin BNB Buy	\$637.84	-1.30%	-12.05%	
4	Dogecoin DOGE	\$0.6085	+10.26%	+91.50%	

Ranking based on Market Cap (May 6, 2021) Prof. Duc (David) Tran | duc.tran@umb.edu 69

69

### DeFi Coins (DeFi = Decentralized Finance)

#	Name	Price	24h %	7d %	Last 7 Days
11	Uniswap UNI	\$41.50	-4.20%	+1.99%	
12	Chainlink LINK	\$46.76	-8.12%	+29.91%	
21	Wrapped Bitcoin WBTC	\$56,739.10	-4.34%	-4.20%	
27	Terra LUNA	\$17.09	-1.47%	-3.46%	

Ranking based on Market Cap (May 6, 2021) Prof. Duc (David) Tran | duc.tran@umb.edu 70

70

### NFT Coins (NFT = Non-Fungible Token)

#	Name	Price	24h %	7d %	Last 7 Days
17	THETA THETA	\$11.03	-3.31%	+2.85%	
53	chiliz CHZ	\$0.5066	-2.84%	+12.51%	
61	Decentraland MANA	\$1.39	-5.65%	+5.84%	
63	Enjin Coin ENJ	\$2.49	-4.63%	+6.69%	

Ranking based on Market Cap (May 6, 2021) Prof. Duc (David) Tran | duc.tran@umb.edu 71

71

### Fundraising: ICO, IEO, IDO, STO

- **ICO = Initial Coin Offering**
  - Like a crowdfunding campaign. Tokens will be issued and sold to investors
  - Money is used to develop the project
- **IEO = Initial Exchange Offering**
  - Similar to ICO but tokens can only be sold on a crypto exchange
- **IDO = Initial Decentralized Exchange Offering**
  - Similar to IEO but the exchange is a decentralized exchange (dEX)
- **STO = Security Token Offering**
  - A fundraising campaign that sells tokens that represent shares of ownership of some asset (similar to "stocks")
  - The token issuance must respect the regulations that apply to all securities

72

## Asset Tokenization

- **Asset** = physical/virtual thing or investment fund
  - The value or **revenue** of asset is sliced into **shares**
  - Shares are issued on blockchain as **security tokens**
  - Investors buy/trade tokens on **crypto exchange**
- Advantages**
- **simplify** investments
  - **attractive** fractional investment
  - reduce the operational **cost**
  - increase asset **liquidity**
  - **secure** thanks to blockchain
  - eliminate **intermediaries**
  - transaction **transparency**

73

## Crypto Staking

- A blockchain network needs a **consensus mechanism**
- If the consensus is based on **Proof-of-Stake (PoS)**, the chance of a node being chosen to validate a transaction is proportional to its financial stake in the consensus protocol
- By staking crypto in a PoS network, you **earn** transaction fees if your node (or the node you delegate your staking to) is chosen
- If a node commits **fraudulent** transactions, the cryptocurrency staked can be seized as **punishment**
- This way, stakers are financially **incentivized** to act **honestly**

74

## Example

- **Ethereum (ETH) 7%**: [Ethereum](#) has the most validators. To run a node independently, you'll need 32 ETH. Coinbase and Gemini let you stake Ether (without running a node) with no minimum required
- **DAI (DAI) 6% to 8%**: DAI is a stablecoin pegged to USD dollar. To stake DAI, you'll need to use a platform like [Gemini](#) or [BlockFi](#)
- **Cardano (ADA) 4.6%**: Cardano is a leading PoS blockchain founded by Charles Hoskinson, a co-founder of Ethereum
- **Cosmos (ATOM) 9%**: Although higher interest rates for staking, it's more volatile than Ethereum and Cardano
- **Algorand (ALGO) 6%**: Yet another PoS blockchain network, founded by MIT Professor and Turing Award Winner Silvio Micali

75

## Let's play this game!

Consider a simple example: Alice and Bob each bet \$100 on a coin flip

1. Alice calls the outcome of the coin flip
2. Bob flips the coin
3. Alice wins \$200 if her guess was correct

Now, what if Alice and Bob are **separated** and **don't trust one another**?

**... Bob may cheat!**

Prof. Duc (David) Tran - duc.tran@umb.edu

76

76

## Solution: Commitment Scheme

1. Alice **predicts** outcome: **B**
2. Alice chooses a **large random number: R**
3. Alice **sends** Bob an encrypted "**commitment**":  $C = H(R, B)$
4. Alice **sends C** to Bob
5. Bob **tosses** coin, sends **outcome** to Alice
6. Alice knows whether her prediction is correct
7. If correct, Alice sends Bob her prediction **B** and the number **R**
8. Bob verifies if  $C = H(R, B)$ ?
9. Both agree who win

**Bob cannot lie due to not knowing Alice's prediction**

**Alice cannot lie due to commitment to Bob**

Prof. Duc (David) Tran - duc.tran@umb.edu

77

77

What if Alice runs away?

Prof. Duc (David) Tran - duc.tran@umb.edu

78

78

... and **that is why** we need **Blockchain**

The next big thing after the Internet, Blockchain enables a digitalized society where people can **fairly** and **easily** contribute, collaborate, and transact without having to **second-guess** trust and transparency

Prof. Duc (David) Tran - duc.tran@umb.edu

79