FinTech

Lecture 5. Demystifying blockchain and cryptocurrency

Luping Yu (俞路平)

Xiamen University

October 21, 2022

Learning outcomes

- Identify the key principles of blockchain technology
- Articulate the uses of blockchain and cryptocurrency

Overview

1. **Introduction**
2. What is blockchain
3. How blockchain can disrupt and transform the financial industry
4. Bitcoin as the original peer-to-peer currency
5. Global adoption of cryptocurrencies
6. Conclusion

Introduction I

- Transfer of financial information
  - Require a trusted third party verifies the claims made by individuals
  - A complex system of contract verifications using lawyers and other third-party systems to confirm non-fraudulent payment.
- Centralized system: incorruptibility of third parties
  - Government regulatory bodies were established to confirm the identities of individuals and the validity of legal contracts
  - Organizations like Visa were also established to confirm fund availability for card transactions to prevent fraudulent payments
    - Charge a percentage of the transaction to fund their operations

Introduction II

- Byzantine Generals' Problem
  - Other generals cannot be certain of the loyalty of their peers or the trustworthiness of the messengers

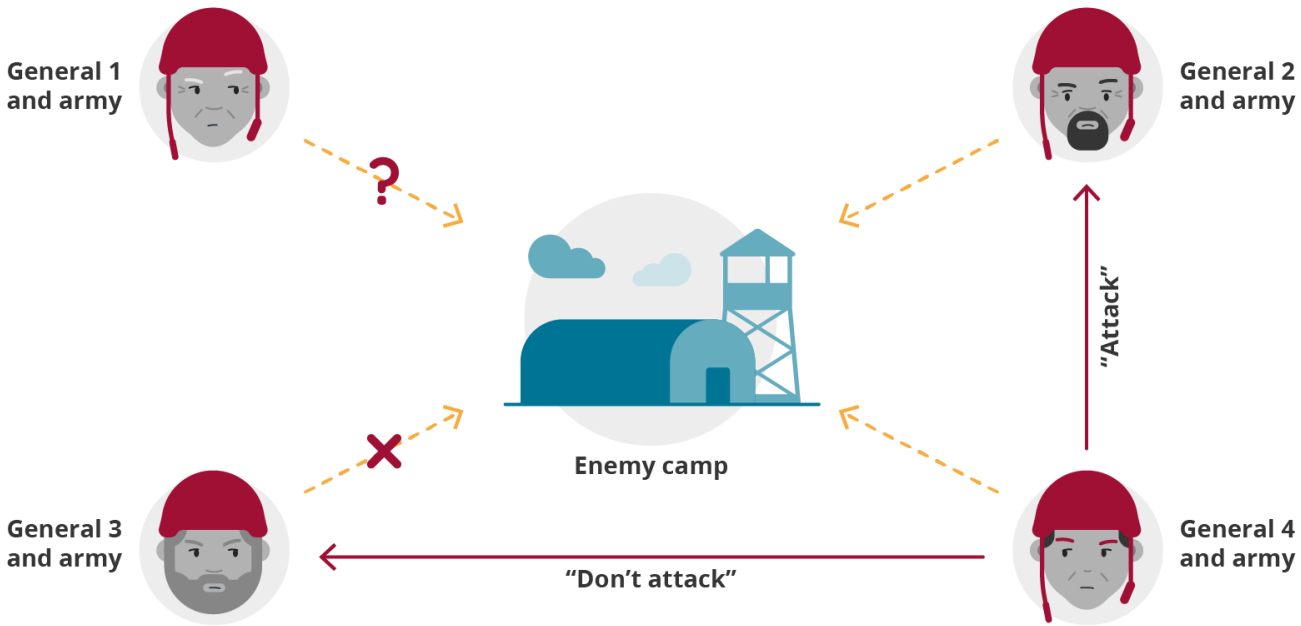

Fig. The Byzantine Generals' Problem.

Introduction III

- Why decentralized networks are difficult to operationalize?
  - Untrustworthy member of the network falsify information
  - Byzantine failure $\rightarrow$ Establishment of traditional/trustworthy third parties
- Blockchain: revolutionize decentralized information sharing networks' ability to operate securely
  - Distributing the information throughout a network
  - Each member of the network then cooperating to verify the data given
- This module outlines what blockchain is and how it operates:
  - Resolve the issue of trust between two parties in a transaction
  - Possible financial applications of this revolutionary technology
  - Concerns regarding its longevity

Overview

1. Introduction
2. **What is blockchain**
3. How blockchain can disrupt and transform the financial industry
4. Bitcoin as the original peer-to-peer currency
5. Global adoption of cryptocurrencies
6. Conclusion

Blockchain I

- Blockchain:
  - Self-sustaining, peer-to-peer ledger technology with an integrated set of computer codes for managing and recording transactions without the involvement of any central authority
- Blockchain technology is a digital infrastructure
  - Upon which applications such as bitcoin are built
  - A secure and transparent way to track the ownership and transaction
  - Distributed ledger:
    - Each transaction is recorded as a block and linked to the previous transaction, forming a chain
    - The chain is open to all its members, who can view each transaction (which are permanently recorded)

Blockchain II

- Distributed network
  - Information is dispersed among members of the network
  - All transactions are made transparent and auditable
  - All members of the network can examine each transaction and agree that it took place

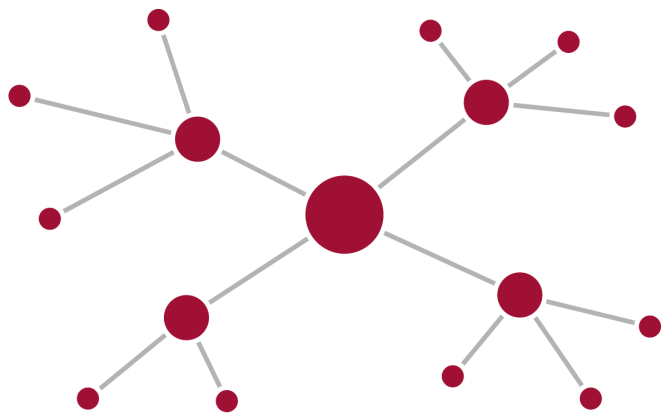

Fig. Blockchain and the distributed network

Blockchain III

- Secure and private transactions
  - No personal data is visible in the transaction
  - No third party is required to house this information
  - Limit opportunities for data breaches
    - e.g. there are no banks storing account balances that can be hacked

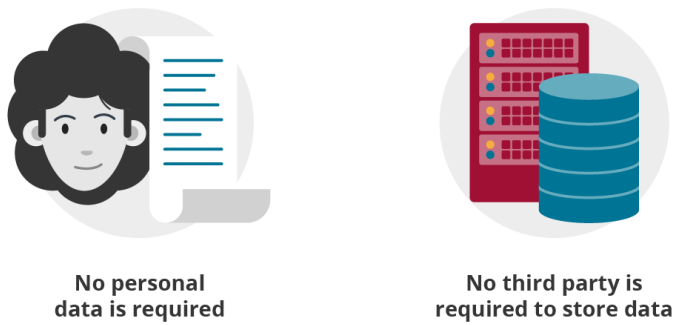

Fig. How security and privacy are secured in the blockchain

Securitization of blockchain transactions I

- Security of transactions:
  - Authorize the process: solving a mathematical puzzle (a proof of work)
    - This process $\rightarrow$ mining
    - Individuals who complete this process $\rightarrow$ miners
  - Miners are incentivized through payment
    - In the case of a bitcoin transaction, miners are compensated for their work by receiving a payment in bitcoin

Securitization of blockchain transactions II

- What is a proof of work?
  - A proof of work is how consensus is achieved in a blockchain network
  - It follows this series of steps:
    1. A transaction is proposed by two parties
    2. Miners verify the transaction by ensuring that the accounts can complete the transaction
    3. To add a new block to the chain, miners complete a complex mathematical puzzle
    4. The puzzle can only be solved by computational power, resulting in the production of a hash function
    5. This hash function then confirms the authenticity of the transaction

Securitization of blockchain transactions III

- Hash function: cryptographic key
  - Once this calculation is complete, a HF is produced
  - It acts as a cryptographic key that unlocks the information and allows for confirmation of the transaction.
- Hash function: digital fingerprint to validate the new transaction
  - A cryptographic hash function is designed to be a one-way function
    - Easy to verify, but requires expensive brute-force be generated
  - If the network verifies HF is correct, the block is added to the chain
    - If HF is incorrect, validation process will not be accepted by the network
  - Each block is linked by including the HF from the previous block in the chain, along with the data of the most recent transaction
    - To fraudulently alter the chain, every single block needs to be altered

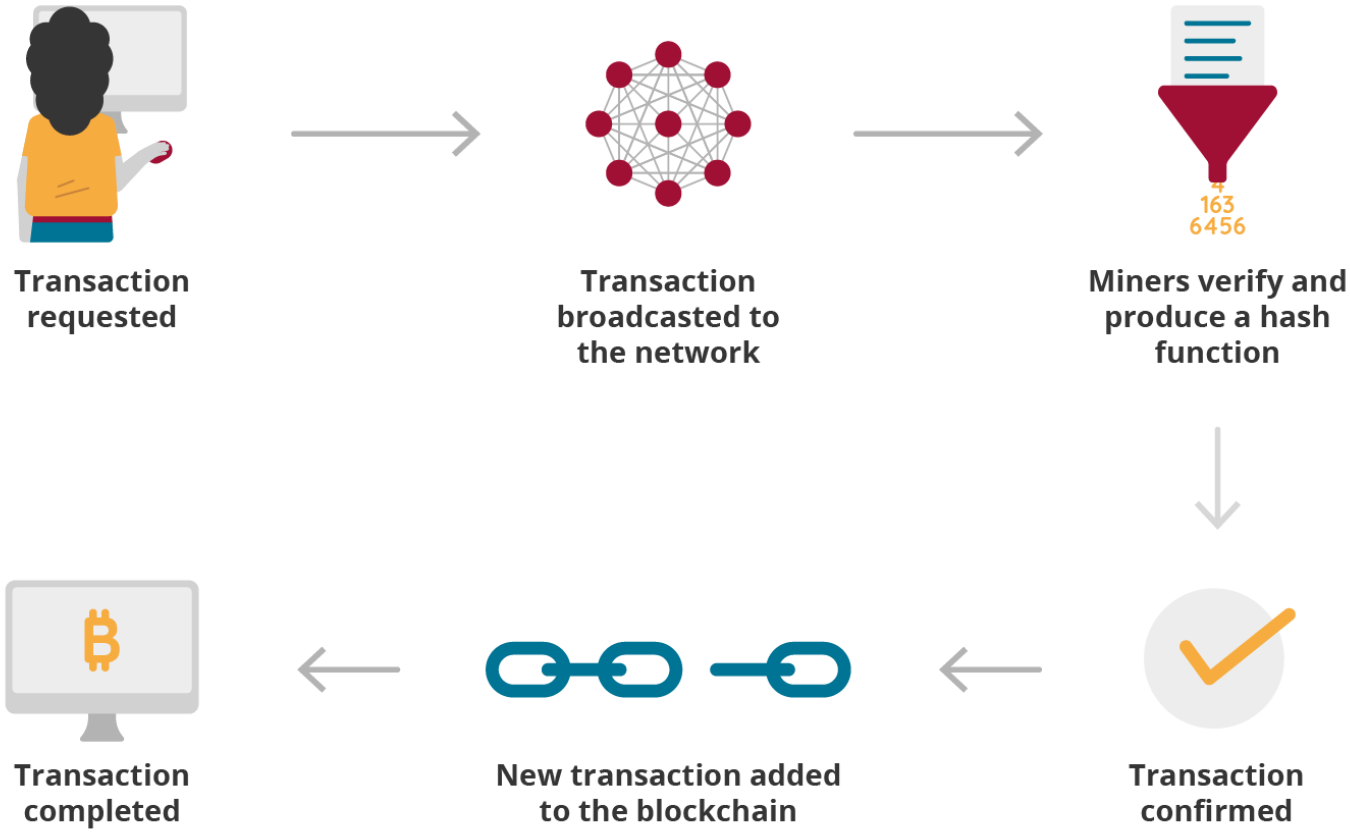

Fig. Completing a blockchain transaction

Overview

1. Introduction
2. What is blockchain
3. **How blockchain can disrupt and transform the financial industry**
4. Bitcoin as the original peer-to-peer currency
5. Global adoption of cryptocurrencies
6. Conclusion

Potential of blockchain to disrupt financial industries

- Ptential of blockchain
  - Resolve issues of trust in decentralized networks
  - How to apply this technology to the financial industry?
- Benefits of blockchain
  - One ledger detailing multiple transactions
  - Each member can view any changes to contracts or balances in real time
  - No coordination (third party) is required to update the system
  - Dramatically lower transaction costs (no additional fees on transactions)
  - The system is highly secure and any changes must be verified by consensus

Potential applications I

- Decentralized Finance (DeFi)
  - DeFi: Financial applications that are developed on blockchain systems
  - DeFi has grown at a fast pace during the past few years.
- Major categories of use:
  - Clearing and payments
  - Digital identification
  - Smart contracts

Applications - Clearing and payments

- Clearing and payments
  - Popularized by the use of bitcoin as a method of payment
  - Blockchain could be used to efficiently process payments
  - e.g. cross-border payments
    - Currently, cross-border payments involve a long and costly process and require a variety of different intermediaries
    - This process can increase costs by around 10%, which will not be finalized until the funds are received
    - With blockchain, the payment could happen in real time without intermediaries and at a much lower cost

Applications - Digital identification

- Digital identification
  - Require the development of a block to store personal data
  - Could be used in government records or for financial services businesses
    - e.g. speeding up of applications for insurance and banking products
  - The block storing this data would be consistent and secure
    - Relatively easy to update
  - A block storing personal data could revolutionize governmental functions
    - e.g. house ownership could be easily transferred, and voter IDs could be verified quickly

Applications - Smart contracts

- Smart contracts
  - Powered by the code that creates the block
    - Once a certain set of obligations has been fulfilled and detected by the code, a transaction is triggered
  - e.g. revolutionize dividend payments to shareholders
    - Transaction should take place once a share price reaches a certain level
  - e.g. logistics industry
    - Processing of shipping documentation

Potential applications II

- Explore further [link]
  - How Barclays bank is using these three major applications of blockchain

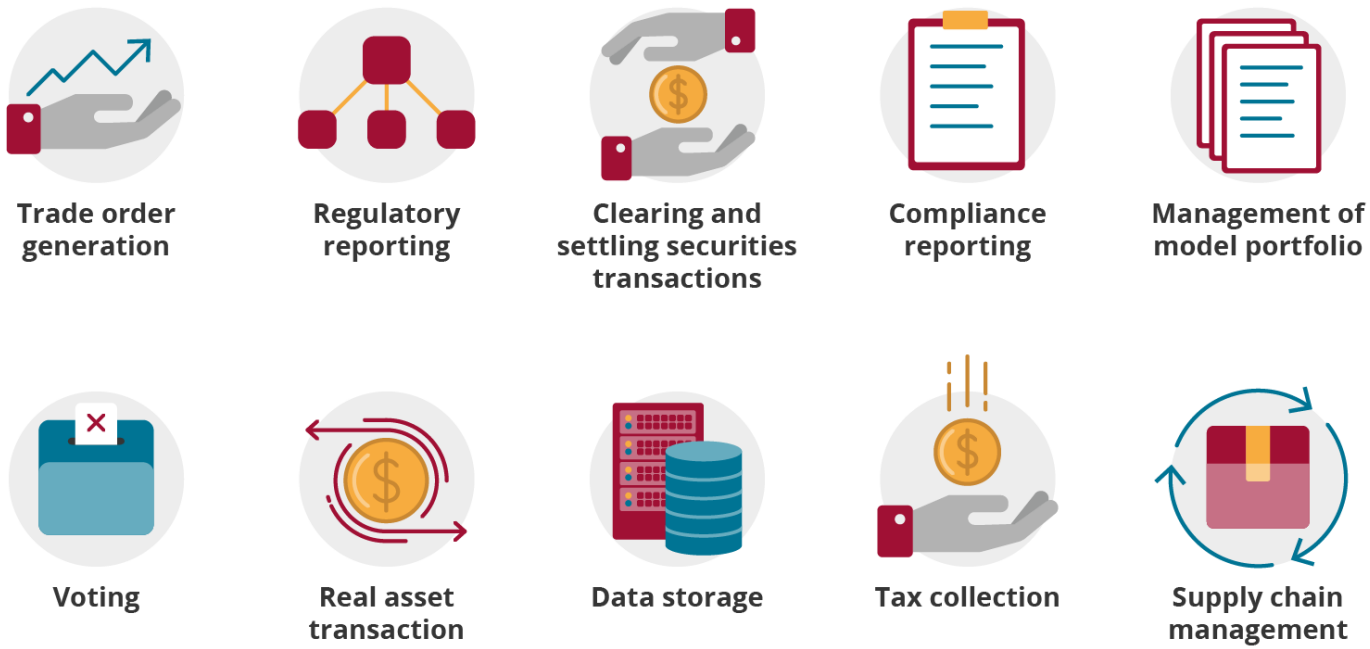

Fig. The potential uses of blockchain

Overview

1. Introduction
2. What is blockchain
3. How blockchain can disrupt and transform the financial industry
4. **Blockchain technology and cryptocurrencies**
5. Global adoption of cryptocurrencies
6. Conclusion

What is money?

- Evolution of money
  - Money evolved from the need to formalize traditional barter economies
  - Money made processes efficient (accurate and centralized pricing systems)
  - Today, bank notes and currency are used as a medium of exchange
    - Assign value to goods
- Identifiable properties of money:
  - Medium of exchange
    - e.g. RMB can be used to purchase a product or service
  - Unit of account
    - Money allows for the pricing of goods and services
  - Store of value
    - Money can be saved for a later date, usually without the worry of it losing its value dramatically

Bitcoin as the original peer-to-peer currency

- Bitcoin
  - Bitcoin and blockchain technology were introduced to the world in 2008
    - Satoshi Nakamoto: an unidentified individual or a collective of developers
  - Bitcoin is limited to 21 million coins
    - Its value is linked to scarcity
    - Rewards for miners halve for every 210,000 coins added to the block
    - This may end up undermining the fee advantage inherent in the system
    - As the chain becomes longer, greater computing power is required to solve the proof of work
    - As rewards decrease, miners are paid less and may require further incentives to continue this process

Benefits of Bitcoin

- Benefits from using bitcoin as a method of payment:
  - Bitcoin transactions are transparent.
    - All parties in the transaction are aware of the balances involved
  - Bitcoin is impossible to counterfeit
    - The unalterable nature of the blockchain
  - Bitcoin is immune to government monetary policy
    - Assisted by the limited number of coins available, the value of bitcoin is not vulnerable to deflationary pressures

Potential drawbacks of Bitcoin I

- Issues in utilizing bitcoin
  - No nation in the world recognizes bitcoin as a legal tenure of exchange
    - It's difficult to use bitcoin as a medium of exchange, and everyday consumer products are not exchanged or priced in bitcoin
  - Bitcoin is non-refundable
  - Bitcoin's value is extremely volatile
  - Bitcoin is not a viable method of storing value
- These drawbacks undermine some of the characteristics of money
  - Explore further: threats to bitcoin and cryptocurrency [link]

Potential drawbacks of Bitcoin II

- Illegal transaction
  - Bitcoin is also linked to the trading of illicit goods on the black market
  - Critic: Bitcoin is a tool for criminals with no real value as a currency
- Waste of energy
  - Complete a proof of work demand a substantial amount of energy
- Slow transaction
  - Length of the chains increase $\rightarrow$ slow transaction speeds

- Do you think that bitcoin can be considered money?
  - Yes, bitcoin satisfies the definition of money
  - No, bitcoin does not fulfill the definition of money

The value of bitcoin

- CoinDesk website
  - The market has been speculated as a prototypical bubble
- How the value of bitcoin will change over the next year?
  - An increase in price of bitcoin due to its usefulness
  - A stable price as bitcoin was overvalued
  - A decrease in price as bitcoin is not a currency
  - A volatile price due to speculation and poor regulation

Other cryptocurrencies

- Bitcoin was the first cryptocurrency, now there are countless others
  - 2,000 cryptocurrencies by the end of 2018
  - 7,000 cryptocurrencies by the end of 2020, market value of $350 billion
- Cryptocurrencies vary in their security protocols
  - Ethereum: Bitcoin's largest competitor
  - Ethereum operates as a smart contract to transfer assets.
  - Ethereum is not simply a coin, but rather allows for a variety of applications to be built on the underlying code
    - e.g. a decentralized file sharing system

Initial coin offerings (ICOs)

- The rise of ICOs
  - These coins or tokens were created by startups to raise capital
  - The hope was that the tokens would then be redeemable for products and services offered by these startups
  - In 2017, ICOs raised US$1.8 billion
- Legality of ICOs
  - Some governments and financial service companies became worried about the legality of this funding method
  - In 2017, Chinese government ruled ICOs as illegal

Overview

1. Introduction
2. What is blockchain
3. How blockchain can disrupt and transform the financial industry
4. Blockchain technology and cryptocurrencies
5. **Global adoption of cryptocurrencies**
6. Conclusion

Global adoption of cryptocurrencies

- Developing countries paving the way in cryptocurrency adoption
  - Explore further: impact of cryptocurrencies on developing nations [link]

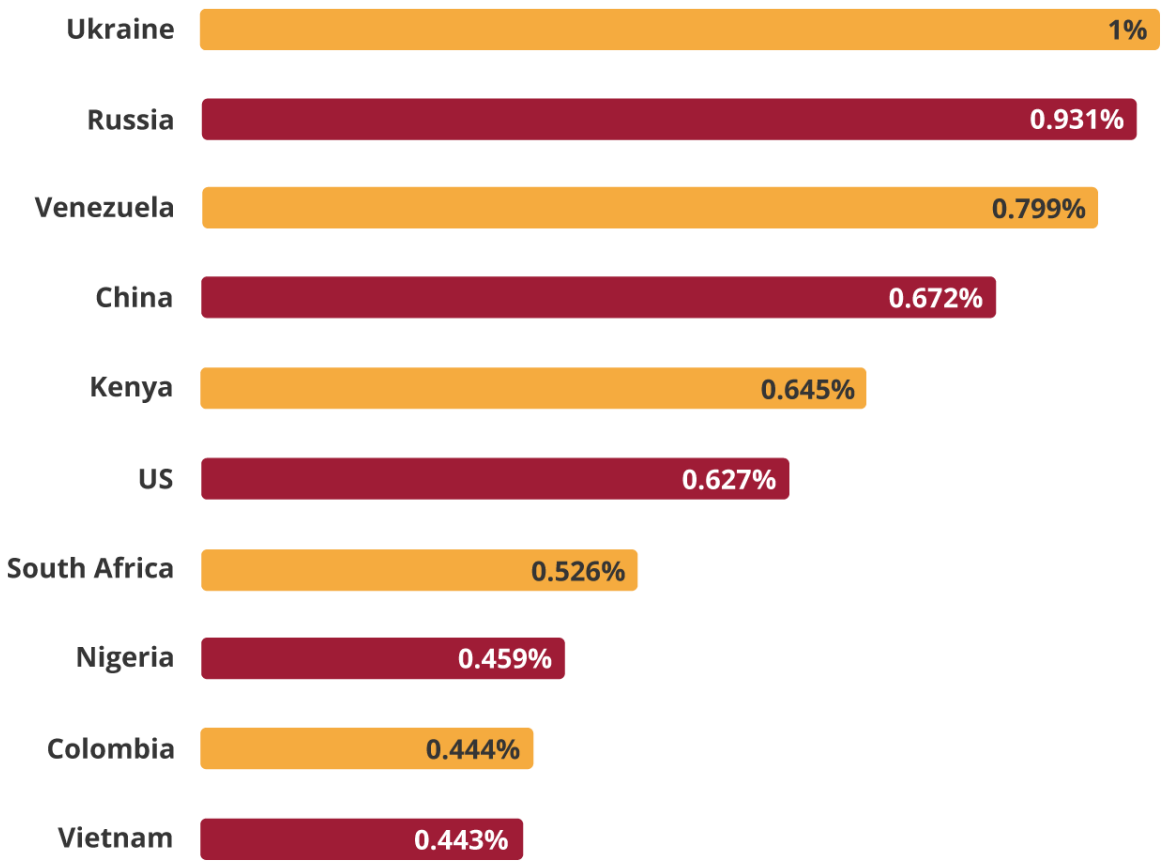

Fig. Global adoption index (Adapted from Chainanalysis, 2020)

Overview

1. Introduction
2. What is blockchain
3. How blockchain can disrupt and transform the financial industry
4. Blockchain technology and cryptocurrencies
5. Global adoption of cryptocurrencies
6. **Conclusion**

Conclusion I

- Growing popularity of blockchain and potential applications:
  - Led to a growing interest in it in the FinTech sphere
  - Blockchain could revolutionize how business is conducted across the globe
- This module explains how blockchain works and the problems it could solve:
  - Overcome issues of trust when transferring data between strangers
  - Possible applications of blockchain and the rates of adoption globally
  - Benefits and drawbacks of cryptocurrencies as means of exchange

Conclusion II

- An interview with Jeff Bussgang (HBS)
  - Video 5-1
    - The value of blockchain and cryptocurrencies
    - The rise of blockchain
    - The potential future growth of cryptocurrencies
- Discussion:
  - Will cryptocurrencies see more widespread adoption over the coming years? Or will the hype around these platforms eventually die down?
  - What do you think is the fundamental force that could lead to the acceptance of cryptocurrencies moving forward?
  - What are some of the obstacles that might prevent the widespread adoption of cryptocurrencies?
- **Quiz**