Wharton
University of Pennsylvania
ONLINE

Cryptocurrency and Blockchain: an Introduction to Digital Currencies

Module Introduction

Sarah Hammer, Adjunct Professor of Law, University of Pennsylvania Law School

In this Module

- Blockchain technology
- Blockchain ecosystem
  - The community of developers, producers, suppliers, and consumers

Wharton
University of Pennsylvania
ONLINE

Cryptocurrency and Blockchain: an Introduction to Digital Currencies

What is an Ecosystem

Sarah Hammer, Adjunct Professor of Law, University of Pennsylvania Law School

Understanding the Blockchain Ecosystem

- The dynamics of the blockchain are rooted in its ecosystem
  - Consists of producers, suppliers, customers, stakeholders and competitors
  - Many smaller ecosystems also comprise blockchain
  - Blockchain companies do not always easily fit into one area of the ecosystem
- The blockchain ecosystem is a living map, exhibiting constant change

What is Blockchain

- Blockchain technology arose with the invention of the digital currency Bitcoin in 2009
  - A shared, immutable ledger that facilitates the recording of transactions in a network
  - Provides the means for recording any transaction or track the movement of any asset, not just a digital currency
  - Assets recorded on blockchain can be tangible (cash, gold, or real estate), or they can be intangible (intellectual property, copyrights, or licenses)

What is Blockchain

- Stores data in blocks that are linked together in a chain
  - As the number of transactions grows, so does the blockchain
- Each block contains a “hash,” or digital fingerprint, a timestamped batch of valid transactions, and the hash of the previous block in the chain
- The previous block hash links the blocks together and prevents any block from being altered or a change in order
- Blocks are added to the blockchain based on a set of rules agreed on by the network participants
  - Each block strengthens the verification of the previous block

Key Attributes of Blockchain

1. Decentralized nature of the network
2. Increase in transparency since copies of the ledger are stored on every block
3. Security through public and private keys for encryption
4. Lower likelihood of hacking given immutable nature of blockchain

Wharton
University of Pennsylvania
ONLINE

Cryptocurrency and Blockchain: an Introduction to Digital Currencies

Building the Blockchain

Sarah Hammer, Adjunct Professor of Law, University of Pennsylvania Law School

Building the Blockchain

- The blockchain begins with the “stack”
  - Has projects with multiple layers of protocols
    1. Base layer
    2. Application protocol
    3. Application layer at the top of the “stack”
- By replicating and storing user data across a decentralized network rather than individual applications controlling access to silos of information, blockchain does two things
  1. Reduces barriers to entry
  2. Creates a potentially more competitive ecosystem of products and services

Mining and Staking

- Bitcoin's process requires the continuous validation of new transactions and recording of them on the blockchain
  - Called "mining the blocks"
    - Each block contains a timestamp, a "nonce," a reference to the previous block (i.e., a hash), and a list of all transactions that have taken place since the previous block
- Currently, a new Bitcoin block is mined approximately every 10 minutes
- To produce blocks, miners compete to solve difficult mathematical problems based on a cryptographic hash algorithm
  - Called Proof of Work (POW)

Mining and Staking

- POW provides that the miner spent time and resources to solve the problem
- Once the block is solved, the transactions in it are considered confirmed
- Blockchain mining companies perform this function

Mining and Staking

- To address concerns over the speed of mining, Proof of Stake (POS) was developed
  - Serves as an alternative to the POW process
- POS is a process whereby the amount held in a particular cryptocurrency determines the amount that can be mined by the holder of the cryptocurrency
  - An individual that holds 3% of a cryptocurrency can mine 3% of the blocks
- POS is premised on the assumption that individuals with an economic stake in the cryptocurrency would not want to devalue their holdings, so they will act in the best interests of the network

Interoperability

- Refers to standards that ensures that different blockchain implementations can work with each other
- Currently, the only way to move value across blockchains is to
  - Move tokens into a centralized exchange
  - Trade on the exchange's in-house ledger
  - Withdraw the net asset on a different blockchain
- Interoperability standards could potentially speed up this process and drive creation of value

Interoperability

- Two types of blockchain interoperability
  1. **Cross chain messaging:** relays messages about the state of one blockchain to another
  2. **Cross chain atomic swaps:** facilitates the exchange of tokens between users and across blockchains, without using a third party
- Companies are working to build bridges between blockchains, offering interoperability between them

Other Development Efforts

- Scalability
- Forks
- Efficiency improvements

Smart Contracts and Oracles

- Smart contract: A set of digital promises, including protocols within which the parties perform on the promises
  - A computerized algorithm which performs the terms of a contract
  - Can be written on and off blockchain
- Oracle: An agent that finds and verifies real-world occurrences and submits the information to a blockchain to be used by smart contracts
  - A data feed, provided by a third party data service
  - Types: software, hardware, inbound, outbound, and consensus-based

Security, Legal and Audit, Privacy

- Security
  - Two elements make blockchain tamperproof
    1. A cryptographic fingerprint unique to each block (the hash), which proves that the miner did the computational work to add the block to the chain
    2. A consensus protocol, which is the process by which the nodes in the network agree on a shared history
  - In order to change an entry in the distributed ledger retroactively, a new hash would have to be created not only for the block that it is in but also for every subsequent block

Security, Legal and Audit, Privacy

- Blockchain security companies conduct security audits of decentralized applications
  - They might review a system's architecture and code, then provide a report on action items for issues discovered
- Legal and Audit
  - Audit the compliance of a company's use of the blockchain
- Privacy
  - Distributed data privacy platforms
  - If an individual stores data on the blockchain, they can delegate access to another individual using a privacy company
  - The data is then rekeyed to the second individual's key in storage, who can download the data and decrypt it

Sovereignty and Communications

- Communication
- User-controlled internet
- Security/cybersecurity

Wharton
University of Pennsylvania
ONLINE

Cryptocurrency and Blockchain: an Introduction to Digital Currencies

Crypto Finance

Sarah Hammer, Adjunct Professor of Law, University of Pennsylvania Law School

Crypto Finance

- Crypto finance includes:
  - Cryptocurrency payments
  - Cryptocurrency privacy
  - Cryptocurrency wallets
  - Cryptocurrency exchanges
  - Stable coins
  - Hardware wallets and storage
  - Cryptocurrency merchants

Cryptocurrency Payments

- Manage ownership and transfer of cryptocurrencies
- The payments companies effectuate real-time, non-cash payments
- Blockchain is particularly attractive, because it is decentralized and avoids a single point of failure
- Eliminates the role of third parties and delays

Cryptocurrency Privacy

- Creates privacy by obscuring the identity of the sender
  - Uses ring signatures – digital signatures that can be performed by any member of a group
- Transactions cannot be linked to a real identity

Cryptocurrency Wallets

- A “soft” wallet is a pseudonym (nothing is in a physical wallet)
  - It is a software program that stores the public and private keys
  - Interacts with the blockchain to enable the holder to send and receive digital currency
  - Can support a single currency or multiple currencies

Cryptocurrency Exchanges

- Online trading platforms
- Cryptocurrencies can be exchanged for fiat currency
- Similar to a traditional stock exchange, where buyers and sellers trade based on the current market price
- The security of the exchange is vital
- Liquidity is also crucial – the higher the volume of transactions, the better

Stable Coins

- A cryptocurrency with price stable characteristics
- Pegged to something else, like the U.S. dollar
- Can also be linked to a basket of currencies, or even an index (like the CPI)
- Can potentially avoid price volatility

Hardware Wallets

- Physical devices that store private keys in a protected area within an actual device
- Similar to a paper wallet
- Intended to reduce incidents of large-scale vulnerabilities
- Provide some resistance to viruses

Blockchain Merchants

- A merchant that accepts Bitcoin or another cryptocurrency as payment
- There are now many blockchain merchants
  - Major retailers now accept cryptocurrency like Bitcoin

Crypto FinTech

- Trading – trading platforms as discussed previously
- Insurance – insurance against theft of digital assets
  - The challenge is that they don’t know much about customers
  - There is little data in this space, as compared to traditional insurance
    - Harder to do actuarial analysis
  - Crypto insurance companies spend time scrutinizing security and storage procedures for digital assets
  - The type of coverage varies – it may be for theft of payments, but not cover hacking

Crypto FinTech

- Lending
  - Allow individuals to lend against digital assets as collateral
    - For example, a $10,000 loan, with an interest rate of 15%
    - Loan to value is important, they often require 50% (so $20k down for a $10k loan)
- Investment funds
  - Cryptocurrency trading
    - May include just cryptocurrency or mix cryptocurrency with other assets

Wharton
University of Pennsylvania
ONLINE

Cryptocurrency and Blockchain: an Introduction to Digital Currencies

Business Use Cases

Sarah Hammer, Adjunct Professor of Law, University of Pennsylvania Law School

Business Use Cases

- Value exchange
- Shared data
- Authenticity
- Diversified financial

Business Use Cases – Value Exchange

- Value exchange
  - Content monetization
    - Hasn’t changed much over time
    - Extensive and largely offline
    - Involves creators, distributors, and many formats
      - Mobile, TV, cable, cinema, etc.
    - Consumers of content are global
    - Costs of content distribution are high
    - Content rights are tied up for long periods of time
    - Blockchain can improve the world of content
    - It can move more marketplaces onto the blockchain

Business Use Cases – Value Exchange

- Value exchange
  - Content monetization
    - Drives content trading between producers and buyers
    - Facilitates funding of creative ideas
    - Offers increased transparency in sharing of rights

Business Use Cases – Value Exchange

- Marketplaces
  - Offer exchange of goods, services, and even jobs
  - These marketplaces face trust challenges
  - Allows buyers and sellers to transfer their reputation from one marketplace to another
- Energy
  - Blockchain energy companies are decentralized energy data exchange platforms
  - May include smart grid management
  - Provide data transparency and integrity solutions
  - Enable forecasting for smart grids and provide for trading and investment

Business Use Cases – Shared Data

- Shared data
  - Internet of Things (IoT)
  - Supply chain/logistics
  - Attribution for collaboration
  - Reputation systems
  - Healthcare information

Business Use Cases – Shared Data

- Internet of Things
  - Combines blockchain technology and the Internet of Things
  - Blockchain creates secure and optimized IoT applications
  - Leverage blockchain to change how devices communicate with each other
  - Both new and existing companies focus on IoT

Business Use Cases – Shared Data

- Supply chain and logistics
  - Supply chain of any one product can span hundreds of stages
    - Multiple geographies
    - Invoices and payments
    - Thousands of individuals may be involved
    - Very non-transparent
  - Blockchain technology can transform supply chain
    - Every transaction can be recorded on a block and distributed across many nodes
    - Increased transparency and security
    - Efficient and scalable
  - Examples: vehicle production, food, diamonds

Business Use Cases – Shared Data

- Attribution for collaboration
  - Allows collaboration in an area like music or writing
  - Artists can generate immutable and timestamped titles
  - Can register assets to a network
  - Verify and authorize content
  - Can also create terms for licensing
- Reputation systems
  - Address counterparty risk
  - Encourages and rewards accurate information about all parties
  - Creates a reputation “score”

Business Use Cases – Shared Data

- Healthcare information
  - Also ripe for disruption
  - Data is highly fragmented
  - Can use blockchain to allow individuals to own and control their own information
  - Patients can decide who gets access to their information
    - Patients can sell their data to a drug trial

Business Use Cases – Authenticity

- Authenticity
  - Data and title
    - Such as real estate
      - Facilitates storage of data that was once on paper
      - Secure integrity of customer's data
      - Can create an audit trail for business processes or create proof of an event or transaction

Business Use Cases – Authenticity

- Authenticity
  - Ticketing
    - Current problem with counterfeiting event tickets
    - Blockchain solution - can facilitate the transfer of ownership
    - Create tickets and validate them on the blockchain
    - Registration prohibits fraud

Business Use Cases – Diversified Financial

- Diversified financial
  - Legal
  - Accounting
  - Middle and back office
  - Other diversified financial services

Business Use Cases – Diversified Financial

- Legal
  - Leverages smart contracts
    - Offers an alternative to direct execution between parties
    - No written contracts, and less real lawyer involvement
    - Secure property, IP, and replace notary public
- Accounting
  - Blockchain can create a new type of accounting ledger
    - Continuous verification and updating
    - Lower threat of alteration or corruption
- Middle and back office functions
- Other diversified financial (payroll, lending and trading, market analytics)

Wharton
University of Pennsylvania
ONLINE

Cryptocurrency and Blockchain: an Introduction to Digital Currencies

Blockchain in Gaming

Sarah Hammer, Adjunct Professor of Law, University of Pennsylvania Law School

Gaming

- Gaming and esports
- Gambling and prediction markets
- Virtual reality

Gaming

- Gaming and esports
  - Gaming companies have been creating digital assets for a long time
  - Blockchain is a natural step in their evolution
    - Gamers can create their own virtual characters, profiles, items and resources
    - Gives users a new way to monetize
    - Players may buy digital assets to use across games

Gaming: Gambling and Prediction Markets

- Blockchain casinos allow anyone to be a member of their casino
- Users can share funding of the casino and profit shares
- Some blockchain companies even use oracles to create a prediction market about the outcome of an event

Gaming: Virtual Reality

- Virtual reality companies are working to power an economy of tradeable digital assets
- Blockchain can be leveraged to create holographic avatars

Wharton
University of Pennsylvania
ONLINE

Cryptocurrency and Blockchain: an Introduction to Digital Currencies

Investing in Blockchain

Sarah Hammer, Adjunct Professor of Law, University of Pennsylvania Law School

Other Stakeholders

- Investors
- Government and regulation
- Media and advocates

Other Stakeholders

- Investors
  - Pour their resources into different components of the blockchain community
- Government and regulation
  - Sets rules and regulations around the development and use of blockchain technology
- Media and advocates
  - Important sources of information and influence

Investors

- Types of investments
  - Initial coin offerings (ICOs)
  - Venture capitalists
  - Corporate investors
  - Consortia

Investors

- ICOs:
  - A fundraising mechanism for a new project
  - Cryptocurrencies are sold in the form of coins (tokens)
    - Sold to investors in exchange for some item or another token

Investors

- Venture capitalists
  - Provides active investment in blockchain companies
  - Support and incubate new businesses
  - There are many ways VCs can invest
    - Directly into ICOs
    - Cryptocurrency companies, such as token exchanges
    - Companies exploring blockchain payments
    - Other use cases
    - Private companies that are building enterprise blockchain solutions

Investors

- Corporate investment
  - Investments by traditional companies into blockchain companies
  - More than $1 billion has been invested by corporations since 2012
- Private blockchains and public blockchains
  - Private - a few companies
  - Public - everyone
  - Consortia fall between private blockchains and public blockchains
    - Brings organizations from the same vertical onto a distributed database
    - Creates a middle option
      - Security of a private blockchain with the network effects of a public blockchain

Wharton
University of Pennsylvania
ONLINE

Cryptocurrency and Blockchain: an Introduction to Digital Currencies

Government and Regulation

Sarah Hammer, Adjunct Professor of Law, University of Pennsylvania Law School

Government and Regulators

- Securities and Exchange Commission
- Commodity Futures Trading Commission
- FinCEN and TFI
- Internal Revenue Service
- States
- International Standard-Setting Bodies

Government and Regulation

- Securities and Exchange Commission
  - Governs the offer and sale of securities as set forth in the Securities Act of 1933
    - Seeks to reduce risks to investors from poor or inadequate information
  - Very active in the blockchain space
  - Issued reports about the issue and sale of tokens
  - Uses a test known as the Howie Test related to whether or not something is a security
  - SEC cyber unit

Government and Regulation

- Commodity Futures Trading Commission
  - Charged with establishing a regulatory environment for investors and market participants
  - In 2014, the CFTC declared cryptocurrencies to be a commodity subject to its oversight
  - Has taken action against unregistered futures exchanges
  - Has taken an approach to responsible regulation and promote innovation

Government and Regulation

- FinCEN and TFI
  - Financial Crimes Enforcement Network
  - Office of Terrorism and Financial Intelligence
    - Relates to the Bank Secrecy Act
    - Virtual currency exchanges and administrators may be subject to the BSA
    - May have to register with FinCEN as a money service business

Government and Regulation

- Internal Revenue Service
  - Collects and manages revenue of the United States
  - Sets forth the principles that apply to transactions using virtual currency
  - It's possible the IRS may treat virtual currency as property and therefore subject to those tax principles

Government and Regulation

- States
  - State governments have begun to recognize the transformative power of blockchain
  - Some states, such as Delaware Illinois and Wyoming, have launched blockchain initiatives
  - Other states, such as New York, have specific laws that may apply if the company is located there

Government and Regulation

- Non-U.S. regulators
- International standard setting bodies

Government and Regulation

- Non-U.S. regulators
  - Global regulators are in the process of building rules and regulations
  - The European Union has implemented a data protection guidance
  - Harmonization of data and laws across countries is important
- International standard setting bodies
  - The Financial Stability Board consist of the G20 countries
  - Works on monitoring cryptocurrency markets
  - Bank for International Settlements also published a chapter of the risks of cryptocurrency

Wharton
University of Pennsylvania
ONLINE

Cryptocurrency and Blockchain: an Introduction to Digital Currencies

Media and Advocacy

Sarah Hammer, Adjunct Professor of Law, University of Pennsylvania Law School

Media and Advocacy

- The media has played an increasing role in mainstream discussion
  - Disseminating information
  - Hosting conferences on blockchain and cryptocurrencies
  - Advocacy organizations actively working in Washington, D.C. to promote or amend rules and regulations that positively enhance the development in blockchain technology

Wharton
UNIVERSITY of PENNSYLVANIA

ONLINE