itworldcanada.com

Understanding Cybersecurity Management in DeFi (UCM-DeFi) – The Origin of Modern Decentralized Finance (Article 1) - IT World Canada

Sepideh HajiHosseinKhani and Arash Habibi Lashkari

18-23 minutes

The modern financial system has become more decentralized, moving away from the centralized system used by banks in the past. Decentralized finance (DeFi) eliminates intermediaries from transactions, allowing for two or more users to execute financial transactions without a central authority.

Understanding Cybersecurity Management in DeFi (UCM-DeFi), a five article series, aims to discuss decentralized finance and explore a range of cybersecurity issues that impact DeFi and blockchain-based financial solutions. The articles in this series are based on the recent book titled *Understanding Cybersecurity Management for DeFi*, published by Springer this year. This first article discusses the origin of decentralized finance and the problems facing centralized financial systems. It also introduces cryptocurrencies and blockchains like Bitcoin, Cardano, Ethereum, and Solana, among others.

Contents

A Brief History of Finance

Let's start by checking out a brief history of finance by highlighting some key moments, starting way back during the earliest civilizations:

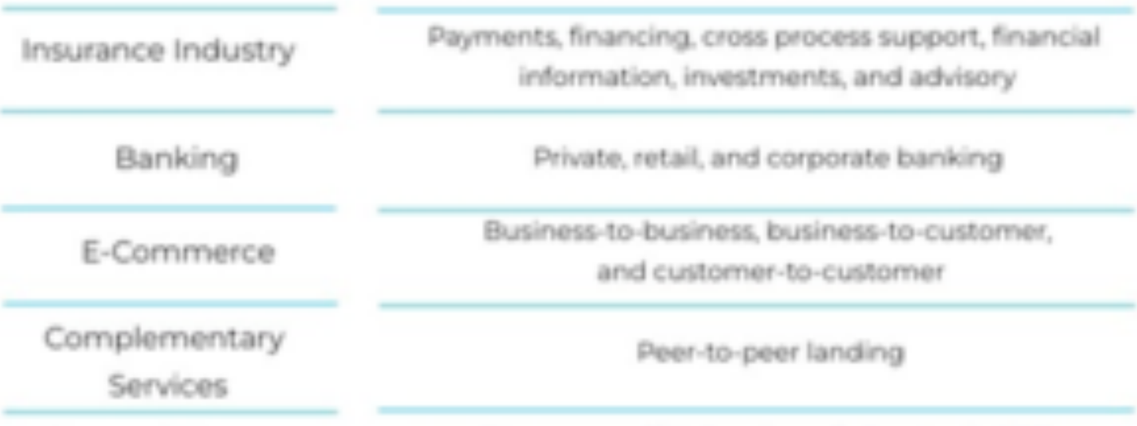
- Finance originated in ancient times when the Sumerians used grains and valuable commodities for transactions.
- The Babylonian Code of Hammurabi established the foundation for loans and credit.
- Coined money was introduced in Greece, and bills of exchange were developed in the Middle Ages for long-distance payments.
- European trading centers performed financial exchanges that involved currency conversions.
- The Dutch established the Bank of England, and the first modern stock market was established in 1611.
- Italy played a lead role in developing the international banking system.

- In the 18th century, the first mutual fund was launched after a financial crisis.
- In the 19th century, England experienced rapid growth due to the industrial revolution, while the United States was also growing. There were no centralized, generally accepted currencies, so various jurisdictions produced their own.
- In the 20th century, there were significant changes in credit forms, resulting in the development of vast investment structures.
- The U.S. Federal Reserve Act paved the way for the United States' central bank.

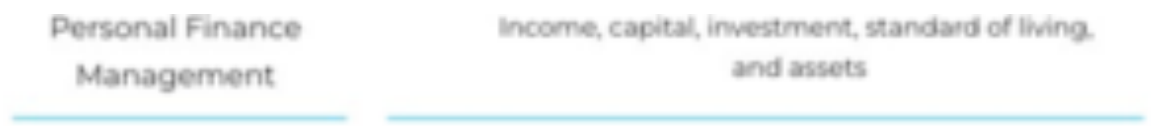
Introduction to FinTech

FinTech, or financial technology, uses technology in financial services such as payments, lending, and stock market activities. It was first used in 1866 and has evolved significantly since then.

FinTech covers five essential areas: insurance, banking, e-commerce, lending, and personal finance management. Transfers and payments are the most used FinTech services globally. On average, one-third of digitally active consumers use two or more mobile and cloud-based FinTech services. Big companies have invested heavily in FinTech in recent years.



Insurance Industry	Payments, financing, cross process support, financial information, investments, and advisory
Banking	Private, retail, and corporate banking
E-Commerce	Business-to-business, business-to-customer, and customer-to-customer
Complementary Services	Peer-to-peer landing



Personal Finance Management	Income, capital, investment, standard of living, and assets

The FinTech ecosystem comprises startup companies, financial regulators, consumers, technology developers, and traditional financial institutions. It includes various technologies such as peer-to-peer transfers, crowdfunding, blockchain-based services, artificial intelligence, and mobile banking.

The growth of FinTech has been driven by new technologies, investor interest following the 2008 financial crisis, and economic factors. FinTech is transforming financial institutions by moving towards digital and customer-centric models.

Key Problems of Centralized Financial System

Centralized financial systems (CeFi) are financial structures that a central decision-making committee governs, and that process orders through a central exchange, which decides exchange rates.

Centralized financial systems offer transparency, but they also have many challenges, including:

- lack of control over personal information
- high transaction fees
- security vulnerabilities
- forgery and reversal of transactions
- slow international transactions
- global inequality

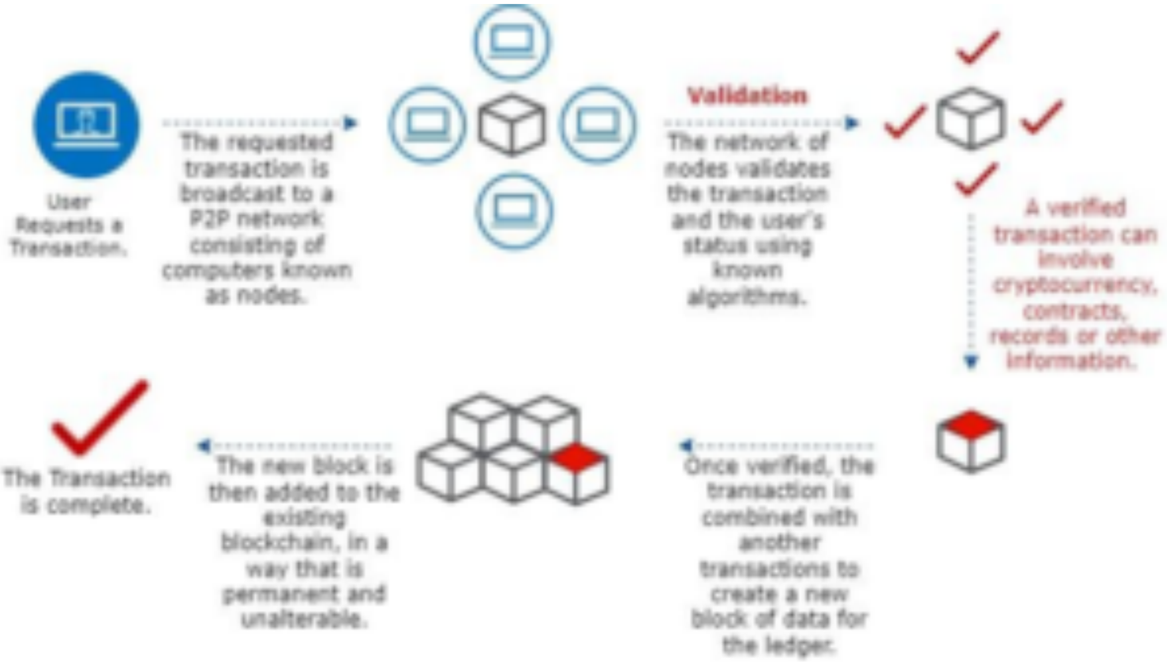
These issues have contributed to a shift towards decentralized finance.

Introduction to Crypto-based Finance

DeFi is a decentralized financial technology based on the secure distributed ledgers used by cryptocurrencies. It eliminates intermediaries and allows people, merchants, and businesses to conduct financial transactions over peer-to-peer networks using specialized security protocols, hardware, and software. DeFi uses blockchain technology to handle financial transactions through dApps, which are secured through the encryption of blocks.

Blockchain technology stores and verifies user information using closed and encrypted blocks once the information is verified. The subsequent block stores information related to previously closed and encrypted blocks, forming a chain of blocks called the blockchain. The blockchain is secure since all blocks are encrypted and linked, making it a suitable technology for secure financial transactions.

The figure below provides an overview of how the blockchain stores, verifies, and processes data.


User Requests a Transaction.
The requested transaction is broadcast to a 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 another 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.

Blockchain technology allows for secure and unalterable storage of transaction information. DeFi uses this technology to create an open and permissionless financial infrastructure built on top of smart contract platforms such as Ethereum.

Compared to traditional centralized finance (CeFi), DeFi allows transactions to be completed through a decentralized application that ingests user needs and searches for peers to fulfill those needs. All transaction details are stored in the blockchain, providing secure and transparent record-keeping for both the borrower and lender.

Roots of DeFi

DeFi is rooted in the emerging technologies of AI, Blockchain, Cloud, and Data, known by the acronym 'ABCD'. Blockchain includes distributed ledgers and smart contracts, which enable secure, decentralized transactions without intermediaries. Cloud services are utilized to store data in distributed servers, while data, including Big Data, is at the core of all DeFi.

Examples of DeFi

DeFi has disrupted traditional finance and is used in various sectors. DeFi protocols include:

- cryptocurrency exchanges like Uniswap
- flash loans such as Aave
- decentralized insurance protocols like InsurAce
- asset management tools like MetaMask
- Know your customer (KYC) and identity management tools such

as Civic.

There are also other protocols used for decentralized lending, payment solutions, marketplaces, prediction markets, and stablecoins.

Advantages of DeFi Ecosystem

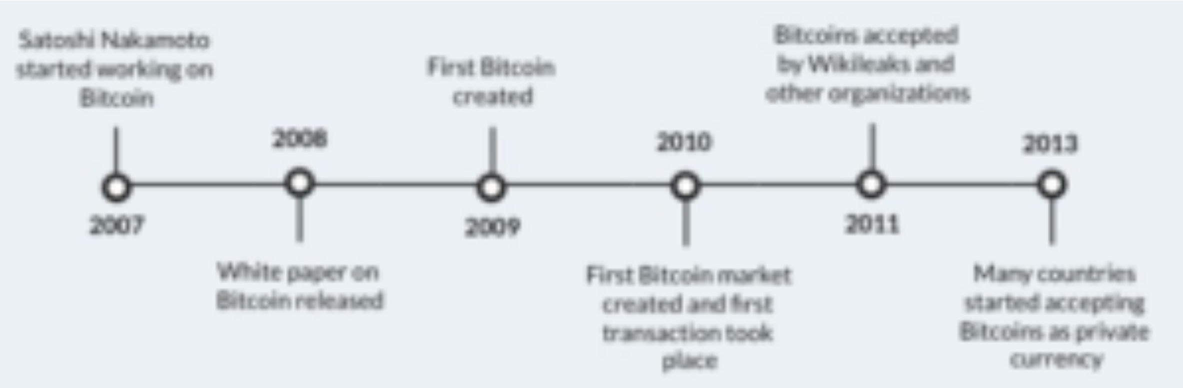
DeFi offers several advantages over traditional financial systems. These include transparency, trustlessness, permissionlessness, interconnectedness, decentralization, and self-sovereignty. DeFi applications use smart contracts for distributed governance, allowing easy connectivity with existing applications without complex requirements. Users have full control and access to their data since there is no central control.

Bitcoin

Bitcoin is a digital currency that operates on a distributed ledger without the support of a centralized authority. It comprises digital currency, communication protocol, and digital network.

History of Bitcoin

Bitcoin was created by Satoshi Nakamoto in 2007 and introduced to the public in 2008 through a whitepaper. The first 50 bitcoins were created and documented in 2009, and the first version of the Bitcoin software was released. The first bitcoin exchange, “The Bitcoin Market,” was created in February 2010, followed by organizations like Wikileaks accepting bitcoins as donations in the following year. By 2013, many European and western countries recognized bitcoin as a private currency.


Satoshi Nakamoto started working on Bitcoin
2007
2008
White paper on Bitcoin released
First Bitcoin created
2009
2010
First Bitcoin market created and first transaction took place
Bitcoins accepted by Wikileaks and other organizations
2011
2013
Many countries started accepting Bitcoins as private currency

Characteristics of the Bitcoin Ecosystem

Bitcoin is a distributed, trustless, peer-to-peer, cryptographically secure, and immutable electronic payment system that uses digital tokens. Users have full control over their transactions, and there is no centralized authority. Every user possesses a public and private key, and transactions are stored in encrypted blocks that cannot be undone.

Purchasing With Bitcoin

Users in the bitcoin ecosystem have digital wallets with a public-private key pair to encrypt and store transactions. Transactions inform the digital network of the transfer of bitcoins between users, resulting in changes to ownership.

A user scans a QR code provided by a retailer, which includes the payment request in physical currency and the corresponding rate in bitcoins. The user sends the authorized payment to the retailer using their digital wallet and private key. The transaction involves public-key cryptography, with each user having a public-private key pair used to encrypt and decrypt the transaction. The transaction is validated and added to a new block using blockchain technology.

Smart Contract-based Blockchains

Smart contracts are computer programs that automate contractual agreements between parties in a transaction. They are coded with “if-else-if” statements that execute certain actions when conditions are met, and they are deployed on top of blockchains to ensure immutability.

Smart contract life cycles include creation, deployment, execution, and completion. The use of smart contracts has led to the development of various platforms for smart contract-based blockchains. Continue reading to learn about specific smart contract-based blockchains:

Algorand

Algorand is a cryptocurrency that utilizes a new Byzantine Agreement protocol to achieve transaction consensus. It uses a gossip protocol for communication and cryptographic sortition to select users to propose new blocks randomly. Algorand faces challenges such as Sybil attacks, scalability, and resiliency to denial-of-service attacks.

Avalanche

Avalanche is a blockchain platform that is scalable, secure, and customizable. It aims to build, transfer, and trade complex digital assets through application-specific blockchains. Avalanche is massively scalable, secure against attacks, decentralized, and interoperable. Its architecture consists of multiple subnets for validation, offering advantages such as reduced network traffic and trusted validations.

Binance Smart Chain

Binance Smart Chain was launched in 2019 as a parallel blockchain to Binance Chain to provide decentralized trading and support smart contracts. It is compatible with Ethereum and offers fast block times and cheap transaction costs. BSC provides security, compatibility, interoperability, and strong community involvement through a Proof-of-Staked Authority consensus algorithm. Its dual-chain architecture allows for building decentralized apps and digital assets on one chain while performing fast trading on the other.

Cardano

Cardano is a project that aims to improve the design and development of cryptocurrencies through modular and interdisciplinary approaches, multiple asset accounting, metadata manipulation, and improved design. It started with extensive cryptocurrency research, producing a library of white papers. The findings include the importance of social consensus, the use of Proof-of-Stake, and the need for room for future modifications. Cardano aims to capitalize on these findings to improve the current state of cryptocurrencies.

Celo

The current banking system’s wire transfers are slow and costly, and cryptocurrencies provide a more secure and efficient solution. However, there are obstacles to wide cryptocurrency adoption, including the need for public key cryptography and price instability due to deterministic supply. The Celo protocol addresses these issues through a cryptographic scheme that uses cell phone numbers to map public keys and a verification method to prevent forgery. The protocol uses elastic supply rules and a variable-value reserve to stabilize asset value and introduces a governance structure with stable-value coins.

Cosmos

Cosmos is a unique blockchain network that consists of multiple parallel blockchains linked together through an inter-blockchain communication protocol. The first blockchain in this network is the Cosmos hub, which can transfer tokens between different blockchains quickly and securely. This architecture solves problems related to interoperability, scalability, and seamless upgradability. The Cosmos hub acts as a single distributed ledger.

Elrond

Elrond is a blockchain platform that is designed to be secure, efficient, scalable, and interoperable. It uses a state sharding scheme and secures a Proof of Stake (POS) consensus mechanism. Users hold public/private key pairs and sign transactions using their private key. The network is divided into smaller units called shards, and each shard contains a randomly selected consensus group. Validators are responsible for running consensus and adding blocks to the blockchain. Elrond is designed to provide security from various attacks, including Sybil, Nothing at Stake, long-range, and distributed denial of service attacks.

Ethereum

Ethereum is an open-source blockchain technology that enables developers to create consensus-based applications using smart contracts. It has two types of accounts: externally owned accounts controlled by private keys and contract accounts controlled by their contract code. Ethereum messages are similar to bitcoin transactions, but can be created by external or contract accounts, can contain data, and can respond back using functions.

Fantom

Blockchain technology faces challenges with real-time settlement and scalability. Fantom is a DAG-based smart contract platform that uses the Lachesis Protocol to maintain consensus, allowing instant transactions and low transaction costs. The platform aims to create an ecosystem for real-time transactions and data sharing while providing high reliability and breaking the sequential processing of transactions.

Harmony

Harmony is a sharding-based blockchain that is fully scalable, secure, and energy-efficient. It uses a Distributed Randomness Generation process to provide scalable, unbiased sharding and has a fast and efficient Proof of Stake consensus algorithm. Harmony also supports cross-shard transactions and has a scalable network infrastructure for propagating blocks.

Polkadot

Polkadot allows specialized blockchains to communicate with each other through a Parachain Slot Auction, providing shared security, consensus, and cross-chain interoperability. Parachains are individual blockchains for specific projects, while bridges connect parachains and parathreads to external networks. Validators secure the network by confirming transactions, and the Relay Chain is the main blockchain responsible for shared security and cross-chain interoperability. Collators maintain a full node of their parachain and the relay chain to collect transactions and author Proof of Work blockchain.

Kusama

Kusama is a platform created in 2019 to advance experimental development and deployment for Polkadot, often called its “canary network” to forecast issues before implementing on Polkadot. It uses Parachain Slot Auctions, which can involve crowdloans, to secure a parachain slot. Kusama also has the potential to serve as a home network for underfunded crypto projects that cannot compete for a parachain slot in the Polkadot ecosystem.

Neo

Neo is a potential alternative to Ethereum, commonly known as Chinese Ethereum. Its main objective is establishing a smart economy with features like identity management and cross-chain compatibility. Neo provides two types of tokens, NEO and NeoGas. NEO manages the network and participates in on-chain governance, while NeoGas needs to be well-documented. Neo supports Java or C# programming languages and uses a delegated BFT algorithm for consensus. However, it has limited support outside the Chinese community, and energy consumption is a concern.

Polygon

Polygon is a protocol and framework that connects Ethereum-compatible blockchain networks, combining the best features of Ethereum and sovereign blockchains to offer scalability, flexibility, security, and developer experience. Its architecture has four layers, including the Ethereum layer, security layer, Polygon network layer, and execution layer. Polygon uses Ethereum and a specialized security layer to provide validators that periodically check the validity of its blockchains. In contrast, the network layer provides consensus and block production, and the execution layer interprets and executes transactions.

Solana

Solana is a new blockchain architecture that uses Proof of History (PoH) to verify the order and passage of time between events. PoH encodes a trustless passage of time into a ledger and can be used with other algorithms to reduce messaging overhead. A node is designated as a leader to generate a PoH sequence, and transactions are executed and confirmed by replicator nodes, which act as votes for the consensus algorithm.

Terra

Terra is a pricing protocol that uses elastic monetary policy to stabilize pricing while retaining the censorship resistance of bitcoin. Terra, which is both price-stable and growth-driven, achieves price-stability via an elastic money supply, enabled by stable mining incentives. It also uses seigniorage created by its minting operations as transaction stimulus, thereby facilitating adoption.

Tezos

Tezos is a public blockchain and smart contract platform that uses a PoS consensus algorithm and Michelson as its smart-contract language. It can instantiate any crypto ledger and supports meta upgrades by amending its code through a seed protocol that allows stakeholders to approve amendments to the protocol.

Tron

Tron is a content platform that offers security, scalability, and privacy. It allows users to contribute to a user registration network while incentivizing positive contributions. Tron is scalable and allows legally binding contracts, certificates, and audio and video files to be stored in the blockchain database. It is decentralized, operates in a trustless environment, and has consistent data information between nodes. The system can also tolerate one-third of node Byzantine failure.

xDai

xDai is an Ethereum-compatible sidechain that supports Dai and its native currency. The xDai Stake is a multi-chain staking token and the first-ever USD-stable blockchain. It is designed for fast, inexpensive, and stable transactions, making it ideal for everyday payments. Transactions occur on a bridge sidechain with extremely low fees and fast payments. The xDai chain is a neutral network that allows for the transfer of stable value free from speculation, volatility, or FUD. Validators on the xDai chain produce random numbers, providing true on-chain randomness without needing centralized services or third-party applications.

What’s next

This article introduced some essential foundational building blocks of decentralized finance. It digs into the roots of the origin of decentralized finance and critical problems faced by centralized financial systems. It also introduced bitcoins and cryptocurrencies to set up the base for upcoming chapters. The next article of the series, entitled “Understanding cybersecurity management on DeFi: Introduction to Smart Contracts and DeFi” will introduce the fundamentals of smart contracts and decentralized finance. It brings forward the technical and operational process of smart contracts and how they are programmed to replace traditional paper-based legal agreements.