2023/2024 S2

DeFi & RWA

Dr. Hui Gong (h.gong1@westminster.ac.uk)

UNIVERSITY OF WESTMINSTER

What is DeFi?

What is DeFi?

Decentralized Finance

DeFi is short for “decentralized finance”, **an umbrella term for a variety of financial applications** in cryptocurrency or blockchain geared toward disrupting financial intermediaries.

DeFi draws inspiration from blockchain, the technology behind the digital currency bitcoin, which allows several entities to hold a copy of a history of transactions, meaning it isn’t controlled by a single, central source. That’s important because centralized systems and human gatekeepers can limit the speed and sophistication of transactions while offering users less direct control over their money. **DeFi is distinct because it expands the use of blockchain from simple value transfer to more complex financial use cases.**

Bitcoin and many other digital-native assets stand out from legacy digital payment methods, such as those run by Visa and PayPal, in that they remove all middlemen from transactions.

When you pay with a credit card for coffee at a cafe, a financial institution sits between you and the business, with control over the transaction, retaining the authority to stop or pause it and record it in its private ledger. With bitcoin, those institutions are cut out of the picture.

Direct purchases aren’t the only type of transaction or contract overseen by big companies; financial applications such as loans, insurance, crowdfunding, derivatives, betting and more are also in their control. Cutting out middlemen from all kinds of transactions is one of the primary advantages of DeFi.

Before it was commonly known as decentralized finance, the idea of DeFi was often called “open finance.”

Applications

Applications

Decentralized exchanges (DEXs)/Swap

A swap is simply the exchange of one type of token to another. The key benefit of swapping in DeFi is that it is atomic and noncustodial. Funds can be custodied in a smart contract with withdrawal rights that can be exercised at any time before the swap is completed. If the swap does not complete, all parties involved retain their custodied funds. The swap only executes when the exchange conditions are agreed to and met by all parties, and are enforced by the smart contract. If any condition is not met, the entire transaction is cancelled.

Decentralized exchanges or DEXs are autonomous decentralized applications (DApps) that allow cryptocurrency buyers or sellers to trade without having to give up control over their funds to any intermediary or custodian.

This type of infrastructure is entirely different from centralized exchanges where users hand over their crypto assets to the exchange, which acts as a custodian and essentially issues IOUs for users to trade with on the platform.

DEXs were initially conceptualized to eliminate the need for any authority to supervise and approve trades made within a particular exchange. Through the help of smart contracts, DEXs operate automated order books (or automated market makers) and trades. This makes them “truly peer-to-peer.”

On-Chain Order Books
In a DEX that uses on-chain order books, there are network nodes that are assigned to maintain the record of all orders. It also requires the operation of miners to confirm each transaction. E.g. Bitshares and StellarTerm exchanges.

Off-Chain Order Books
As opposed to on-chain order books, records of transactions in off-chain order books are hosted in a centralized entity. They utilize “relayers” to help manage these order books. In this respect, off-chain order book DEXs are only quasi-decentralized, unlike other types of DEXs. E.g. Binance DEX, 0x and EtherDelta.

Applications

Decentralized exchanges (DEXs) mechanisms

Order Book Matching

Order-book matching is a system in which all parties must agree on the swap exchange rate. Market makers can post bids and asks to a DEX and allow takers to fill the quotes at the pre-agreed-upon price. Until the offer is taken, the market maker retains the right to remove the offer or update the exchange rate as market conditions change. A leading example of a fully on-chain order book is Kyber.

The order-matching approach is expensive and inefficient because each update requires an on-chain transaction. We will explore a solution to this problem when we discuss Ox. An insurmountable inefficiency with an order-book matching is that both counterparties must be willing and able to exchange at the agreed-upon rate for the trade to execute.

Automated Market Makers (AMMs)

An Automated Market Maker (AMM) is a smart contract that holds assets on both sides of a trading pair and continuously quotes a price for buying and for selling. Based on executed purchases and sales, the contract updates the asset size behind the bid and the ask and uses this ratio to define its pricing function. The contract can also take into account more complex data than relative bid/ask size when determining price.

A naive AMM might set a fixed price ratio between two assets. With a fixed price ratio, when the price shifts between the assets, the more valuable asset would be drained from the AMM and arbitraged on another exchange where trading is occurring at the market price. The AMM should have a pricing function that can converge on the market price of an asset so that it becomes more expensive to purchase an asset from the trading pair as the ratio of that asset to the others in the contract decreases.

Applications

Stablecoins

A cryptocurrency that's tied to an asset outside of cryptocurrency (the dollar or euro, for example) to stabilize the price.

A crucial shortcoming to many cryptocurrencies is excessive volatility. This adds friction to users who wish to take advantage of DeFi applications but don't have the risk-tolerance for a volatile asset like ETH. To solve this, an entire class of cryptocurrencies called stablecoins has emerged. Stablecoins are intended to maintain price parity with some target asset, USD or gold for instance. Stablecoins provide the necessary stability that investors seek to participate in many DeFi applications and allow a cryptocurrency native solution to exit positions in more volatile cryptoassets. They can even be used to provide on-chain exposure to the returns of an off-chain asset if the target asset is not native to the underlying blockchain (e.g., gold, stocks, ETFs). The mechanism by which the stablecoin maintains its peg varies by implementation. The three primary mechanisms are **fiat-collateralized**, **crypto-collateralized**, and **non-collateralized stablecoins**.

Now the largest class of stablecoins are **fiat-collateralized**. These are backed by an off-chain reserve of the target asset. Usually these are custodied by an external entity or group of entities which undergo routine audits to verify the collateral's existence. The largest fiat-collateralized stablecoin is Tether (**USDT**) with a market capitalization of $19 billion dollars, making it the 4th largest cryptocurrency behind Bitcoin, Ethereum and Ripple at time of writing.

The second largest class of stablecoins are **crypto-collateralized**. These are stablecoins which are backed by an overcollateralized amount of another cryptocurrency. Their value can be hard or soft pegged to the underlying asset depending on the mechanism. The most popular crypto-collateralized stablecoin is **DAI**, created by MakerDAO and it is backed by mostly ETH with collateral support for a few other cryptoassets. It is soft pegged with economic mechanisms that incentivize supply and demand to drive the price to $1. DAI's market capitalization is $1 billion as of writing.

Applications

Lending platforms/Flash Loan

These platforms use smart contracts to replace intermediaries such as banks that manage lending in the middle.

Collateralized Loans
Debt and lending are perhaps the most important financial mechanisms that exist in DeFi, and more generally, in traditional finance. On the one hand, these mechanisms are a powerful tool for efficiently allocating capital, increasing return-bearing risk exposure, and expanding economic growth. On the other hand, excess debt in the system can cause instability, leading to large economic and market contractions. These benefits and risks are amplified in DeFi, because the counterparties share an adversarial and integrated environment. Platforms are increasingly interdependent, and a debt-fueled collapse in one part of the system can quickly contaminate all connected protocols—and expand outward.

Flash Loan (Uncollateralized Loan)
A financial primitive that uniquely exists in DeFi and dramatically broadens certain types of financial access is a flash loan.

In traditional finance, a loan is an instrument designed to efficiently allocate excess capital from a person or entity who wishes to employ it (lender) to a person or entity who needs capital to fund a project or to consume (borrower). A lender is compensated for providing the capital and bearing the risk of default by the interest amount charged over the life of the loan. The interest rate is typically higher the longer the duration of the loan, because the longer time to repay exposes the lender to greater risk that the borrower may default.

Reversing the concept leads to the conclusion that shorter-term loans should be less risky and therefore require less compensation for the lender. A flash loan is an instantaneous loan paid back within the same transaction. A flash loan is similar to an overnight loan in traditional finance, but with a crucial difference—repayment is required within the transaction and enforced by the smart contract.

Applications

Prediction markets/Oracles

Markets for betting on the outcome of future events, such as elections. The goal of DeFi versions of prediction markets is to offer the same functionality but without intermediaries.

An interesting problem with blockchain protocols is that they are isolated from the world outside of their ledger. That is, the Ethereum blockchain only authoritatively knows what is happening on the Ethereum blockchain, and not, for example, the level of the S&P 500 or which team won the Super Bowl.

This limitation constrains applications to Ethereum native contracts and tokens thus reducing the utility of the smart contract platform and is generally known as the oracle problem. An oracle, in the context of smart contract platforms, is any data source for reporting information external to the blockchain.

How can we create an oracle that can authoritatively speak about off-chain information in a trust-minimized way? Many applications require an oracle, and the implementations exhibit varying degrees of centralization.

There are several implementations of oracles in various DeFi applications. A common approach is for an application to host its own oracle or hook into an existing oracle from a well-trusted platform. One Ethereum-based platform known as Chainlink is designed to solve the oracle problem by using an aggregation of data sources. The Chainlink whitepaper includes a reputation-based system, which has not yet been implemented. We discuss the oracle problem later in more depth. Oracles are surely an open design question and challenge for DeFi to achieve utility beyond its own isolated chain.

Applications

Others

"Wrapped" bitcoins (WBTC)

A way of sending bitcoin to the Ethereum network so the bitcoin can be used directly in Ethereum's DeFi system. WBTCs allow users to earn interest on the bitcoin they lend out via the decentralized lending platforms described above.

Yield farming

For knowledgeable traders who are willing to take on risk, there's yield farming, where users scan through various DeFi tokens in search of opportunities for larger returns.

Liquidity mining

Liquidity mining is a process in which crypto holders lend assets to a decentralized exchange in return for rewards. These rewards commonly stem from trading fees that are accrued from traders swapping tokens.

Composability

DeFi apps are open source, meaning the code behind them is public for anyone to view. As such, these apps can be used to "compose" new apps with the code as building blocks.

Problem DeFi Solves

Problem DeFi Solves

Inefficiency & Limited Access & Opacity

Inefficiency
The first of the five flaws of traditional finance is inefficiency. DeFi can accomplish financial transactions with high volumes of assets and low friction that would generally be a large organizational burden for traditional finance. DeFi creates reusable smart contracts in the form of dApps designed to execute a specific financial operation. These dApps are available to any user who seeks that particular type of service, for example, to execute a put option, regardless of the size of the transaction. A user can largely self-serve within the parameters of the smart contract and of the blockchain the application lives on.

Limited Access
As smart contract platforms move to more-scalable implementations, user friction falls, enabling a wide range of users, and thus mitigates the second flaw of traditional finance: limited access. DeFi gives large underserved groups, such as the global population of the unbanked as well as small businesses that employ substantial portions of the workforce.

Opacity
The third drawback of traditional finance is opacity. DeFi elegantly solves this problem through the open and contractual nature of agreements. We will explore how smart contracts and tokenization improve transparency within DeFi.

- Smart Contracts
  DeFi participants are accountable for acting in accordance with the terms of the contracts they use. One mechanism for ensuring the appropriate behavior is staking. Staking is escrowing a cryptoasset into a contract, so that the contract releases the cryptoasset to the appropriate counterparty only after the contract terms are met; otherwise, the asset reverts to the original holder. Parties can be required to stake on any claims or interactions they make. Staking enforces agreements by imposing a tangible penalty for the misbehaving side and a tangible reward for the counterparty. The tangible reward should be as good as or even better than the outcome of the original terms of the contract. These transparent incentive structures provide much securer and more obvious guarantees than traditional financial agreements.

Problem DeFi Solves

Centralized Control

The fourth flaw of traditional finance is the strong control exerted by governments and large institutions that hold a virtual monopoly over elements such as the money supply, rate of inflation, and access to the best investment opportunities. DeFi upends this centralized control by relinquishing control to open protocols having transparent and immutable properties. The community of stakeholders or even a predetermined algorithm can control a parameter, such as the inflation rate, of a DeFi dApp. If a dApp contains special privileges for an administrator, all users are aware of the privileges, and any user can readily create a less-centralized counterpart.

The open-source ethos of blockchain and the public nature of all smart contracts assures that flaws and inefficiencies in a DeFi project can be readily identified and “forked away” by users who copy and improve the flawed project. Consequently, DeFi strives to design protocols that naturally and elegantly incentivize stakeholders and maintain a healthy equilibrium through careful mechanism design.

Naturally, trade-offs exist between having a centralized party and not having one. Centralized control allows for radically decisive action in a crisis, sometimes the necessary approach but also perhaps an overreaction. The path to decentralizing finance will certainly encounter growing pains because of the challenges in pre-planning for every eventuality and economic nuance. Ultimately, however, the transparency and security gained through a decentralized approach will lead to strong robust protocols that can become trusted financial infrastructure for a global user base.

➢ Decentralized Autonomous Organization
Traditional financial products are difficult to integrate with each other. DeFi solves this lack-of-interoperability aspect of traditional finance. The product possibilities in DeFi are substantial and innovations are growing at a nonlinear rate. Putting the concept "composability" another way, DeFi apps are like Legos, the toy blocks children click together to construct buildings, vehicles and so on. DeFi apps can be similarly snapped together like "money legos" to build new financial products.

Problem DeFi Solves

Lack of Interoperability

We will now touch on the lack-of-interoperability aspect of traditional finance that DeFi solves. Traditional financial products are difficult to integrate with each other, generally requiring at minimum a wire transfer, but in many cases cannot be recombined. The possibilities for DeFi are substantial and new innovations continue to grow at a non-linear rate. This growth is fueled by the ease of composability of DeFi products. Once one has some base infrastructure to, for example, create a synthetic asset, any new protocols allowing for borrowing and lending can be applied. A higher layer would allow for attainment of leverage on top of borrowed assets. Such composability can continue in an increasing number of directions as new platforms arise.

➢ Tokenization
Tokenization is a critical way in which DeFi platforms integrate with each other. Take for example a percentage ownership stake in a private commercial real estate venture. In traditional finance to use this asset as collateral for a loan or as margin to open a levered derivative position would be quite difficult. Because DeFi relies on shared interfaces, applications can directly plug into each other's assets, repackage, and subdivide positions as needed. DeFi has the potential to unlock liquidity in traditionally illiquid assets through tokenization. A simple use case would be creating fractional shares from a unitary asset such as a stock. We can extend this concept to give fractional ownership to scarce resources such as rare art. The tokens can be used as collateral for any other DeFi service, such as leverage or derivatives. We are able to invert this paradigm to create token bundles of groups of real-world or digital assets and trade them like an ETF. **Imagine a dApp similar to a real estate investment trust (REIT), but with the added capability of allowing the owner to subdivide the REIT into the individual real estate components to select a preferred geographic distribution and allocation within the REIT. Ownership of the token provides direct ownership of the distribution of the properties. The owner can trade the token on a decentralized exchange to liquidate the position.**

➢ Networked Liquidity
Any exchange application can leverage the liquidity and rates of any other exchange on the same blockchain.

Case Studies

Case Studies

MakerDAO (MKR & DAI)

Traditional Finance Problem	MakerDAO Solution
Centralized Control: Interest rates are influenced by the US Federal Reserve and access to loan products controlled by regulation and institutional policies.	MakerDAO platform is openly controlled by the MKR holders.
Limited Access: Obtaining loans is difficult for a large majority of the population.	Open ability to take out DAI liquidity against an overcollateralized position in any supported ERC-20 token. Access to a competitive USD-denominated return in the DSR.
Inefficiency: Acquiring a loan involves costs of time and money.	Instant liquidity at the push of a button with minimal transaction costs.
Lack of Interoperability: Cannot trustlessly use USD or USD-collateralized token in smart contract agreements.	Issuance of DAI, a permissionless USD-tracking stablecoin backed by cryptocurrency. DAI can be used in any smart contract or DeFi application.
Opacity: Unclear collateralization of lending institutions.	Transparent collateralization ratios of vaults visible to entire ecosystem.

MakerDAO (DAO is decentralized autonomous organization) is often considered an exemplar of DeFi. In order for a series of applications to build on each other, there must necessarily be a foundation. The primary value-add of MakerDAO is the creation of a crypto-collateralized stablecoin, pegged to USD. This means the system can run completely from within the Ethereum blockchain without relying on outside centralized institutions to back, vault and audit the stablecoin.

MakerDAO is a two-token model where a governance token **MKR** yields voting rights on the platform and participates in value capture. The second token is the stablecoin, called **DAI**, and is a staple token in the DeFi ecosystem with which many protocols integrate - including a few we will discuss later.

Case Studies

Uniswap

Traditional Finance Problem	Uniswap Solution
Centralized Control: Exchanges that control which trading pairs are supported.	Allows anyone to create a new trading pair if it does not already exist and automatically routes trades through the most efficient path if no direct pair exists.
Limited Access: The best investment opportunities and returns from liquidity providing are restricted to large institutions.	Anyone can become a liquidity provider and earn fees for doing so. Any project can list its token on Uniswap to give anyone access to an investor.
Inefficiency: Trades generally require two parties to clear.	An AMM that allows constant access for trading against the contract.
Lack of Interoperability: Ability to exchange assets on one exchange is not easily used within another financial application.	Any token swap needed for a DeFi application can utilize Uniswap as an embedded feature.
Opacity: Unknown if the exchange truly owns all user's entire balance.	Transparent liquidity levels in the platform and algorithmic pricing.

The primary example of an AMM on Ethereum is Uniswap. Uniswap uses a constant product rule to determine the trading price, using the formula k = x*y, where x is the balance of asset A, and y the balance of asset B. The product k is the invariant and is required to remain fixed at a given level of liquidity. To purchase (withdraw) some x, some y must be sold (deposited). The implied price is x/y and is the risk-neutral price, because the contract is equally willing to buy or sell at this rate as long as invariant k is constant.

Deep liquidity helps minimize slippage. Therefore, it is important that Uniswap incentivizes depositors to supply capital to a given market. Anyone can become a liquidity provider by supplying assets on both sides of a market at the current exchange rate.

Risks

Risks

Smart-Contract & Governance & Oracle Risk

Smart Contract risk
Smart Contract risk can take the form of a logic error in the code or an economic exploit in which an attacker can withdraw funds from the platform beyond the intended functionality. The former can take the form of any typical software bug in the code. For example, let's say we have a smart contract which is intended to be able to escrow deposits from a particular ERC-20 from any user and transfer the entire balance to the winner of a lottery. The contract keeps track of how many tokens it has internally, and uses that internal number as the amount when performing the transfer. The bug will belong here in our hypothetical contract. The internal number will, due to a rounding error, be slightly higher than the actual balance of tokens the contract holds. When it tries to transfer, it will transfer "too much" and the execution will fail. If there was no failsafe put into place, the tokens are functionally locked within the protocol. Informally these are known as "bricked" funds and cannot be recovered.

Governance Risk
Protocol governance refers to the representative or liquid democratic mechanisms To participate in the governance process, users and investors must acquire a token that has been explicitly assigned protocol governance rights on a liquid marketplace. Once acquired, holders use these tokens to vote on protocol changes and guide future direction. Governance tokens usually have a fixed supply that assists in resisting attempts by anyone to acquire a majority (51%), nevertheless they expose the protocol to the risk of control by a malicious actor.

Oracle Risk
Oracles represent significant risks to the systems they help support. If an oracle's Cost of Corruption is ever less than an attacker's potential Profit from Corruption, the oracle is extremely vulnerable to attack.
To date, three types of oracle solutions have been introduced, developed, and used.

Risks

Scaling & DEX & Regulatory Risk

Scaling Risk
Vertical scaling centralizes all transaction processing to a single large machine. This centralization reduces the communication overhead (transaction/block latency) associated with a PoW blockchain such as Ethereum 1.0, but results in a centralized architecture in which one machine is responsible for a majority of the system's processing. Some blockchains, such as Solana, follow this approach and can achieve upward of 50,000 TPS.

Horizontal scaling, however, divides the work of the system into multiple pieces, retaining decentralization but increasing the throughput of the system through parallelization. Ethereum 2.0 takes this approach in combination with a Proof of Stake consensus algorithm. Ethereum 2.0's technical architecture differs drastically from vertically scaled blockchains such as Solana, but the improvements are the same. Ethereum 2.0 uses horizontal scaling with multiple blockchains and can achieve upward of 50,000 transactions per second.

DEX Risk
Uniswap is perhaps the best-known example of an AMM, also known as a Constant-Function Market Maker (CFMM). Uniswap relies on the product of two assets to determine an exchange price. The amount of liquidity in the pool determines the slippage when assets are exchanged during a transaction.

CFMMs such as Uniswap optimize for user experience and convenience, but sacrifice absolute returns. CFMM liquidity providers (LPs) earn yield by depositing assets into a pool, because the pool takes a fee for every trade (LPs benefit from high trading volume). This allows the pool to attract liquidity, but exposes LPs to smart contract risk and impermanent loss.

Regulatory Risk
As the DeFi market increases in size and influence, it will face greater regulatory scrutiny. Major centralized spot and derivatives exchanges, previously ignored by the CFTC, have recently been forced to comply with KYC/AML compliance orders, and DEXs appear to be next.

RWA (Real World Assets)

RWA

What Exactly is RWA (Real World Assets)?

Crypto Perspective on RWA

The RWA logic in crypto primarily revolves around how to transfer the income rights of assets that generate revenue, such as **U.S. Treasuries**, **fixed income**, and **stocks**, onto the blockchain.

It also involves placing off-chain assets on the blockchain for mortgage loans to obtain liquidity for on-chain assets, as well as moving **various tangible assets**, such as **gravel**, **minerals**, **real estate**, and **gold**, onto the blockchain for trading. This reflects the crypto world's unilateral demand for real-world assets, and there are many obstacles in terms of compliance.

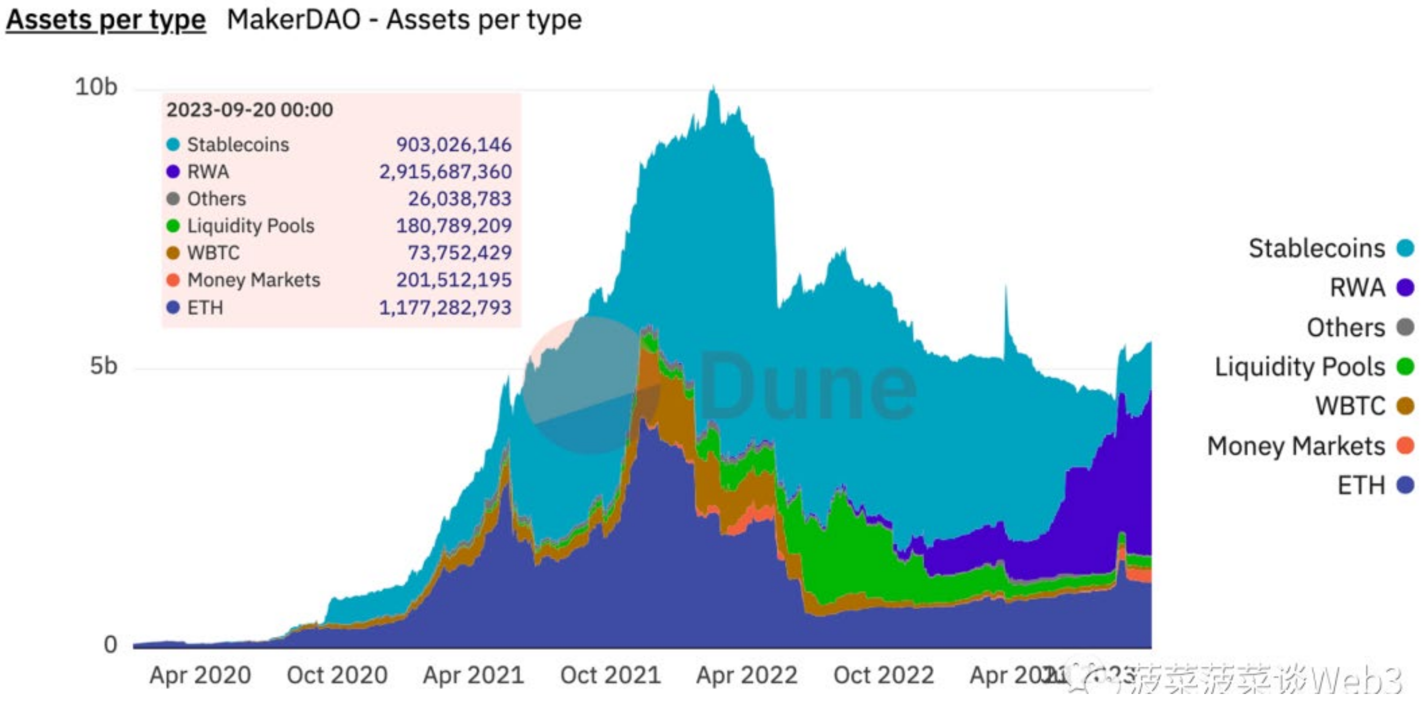
TradFi Perspective on RWA

The future focus of RWA will be driven by **authoritative institutions** such as **TradFi institutions**, **regulatory bodies**, and **central banks**. They aim to establish a new financial system on a blockchain using DeFi technology. To realise this system, a comprehensive system is required, including **computational systems** (blockchain technology), **non-computational systems** (such as legal frameworks), **on-chain identity systems**, **privacy protection technologies**, **on-chain legal tender** (**CBDCs**, tokenized deposits, legal stablecoins), and **a robust infrastructure** (low-threshold wallets, oracles, cross-chain technologies, etc.).

RWA

Crypto Perspective on RWA

The RWA in the crypto world as the crypto world's unilateral demand for the yield of real-world financial assets. The main context is set against the backdrop of the Federal Reserve's continuous interest rate hikes and balance sheet reduction, which significantly affects the valuation of risk markets. The reduction in the balance sheet substantially withdraws liquidity from the crypto market, leading to a continuous decline in the yield of the DeFi market.

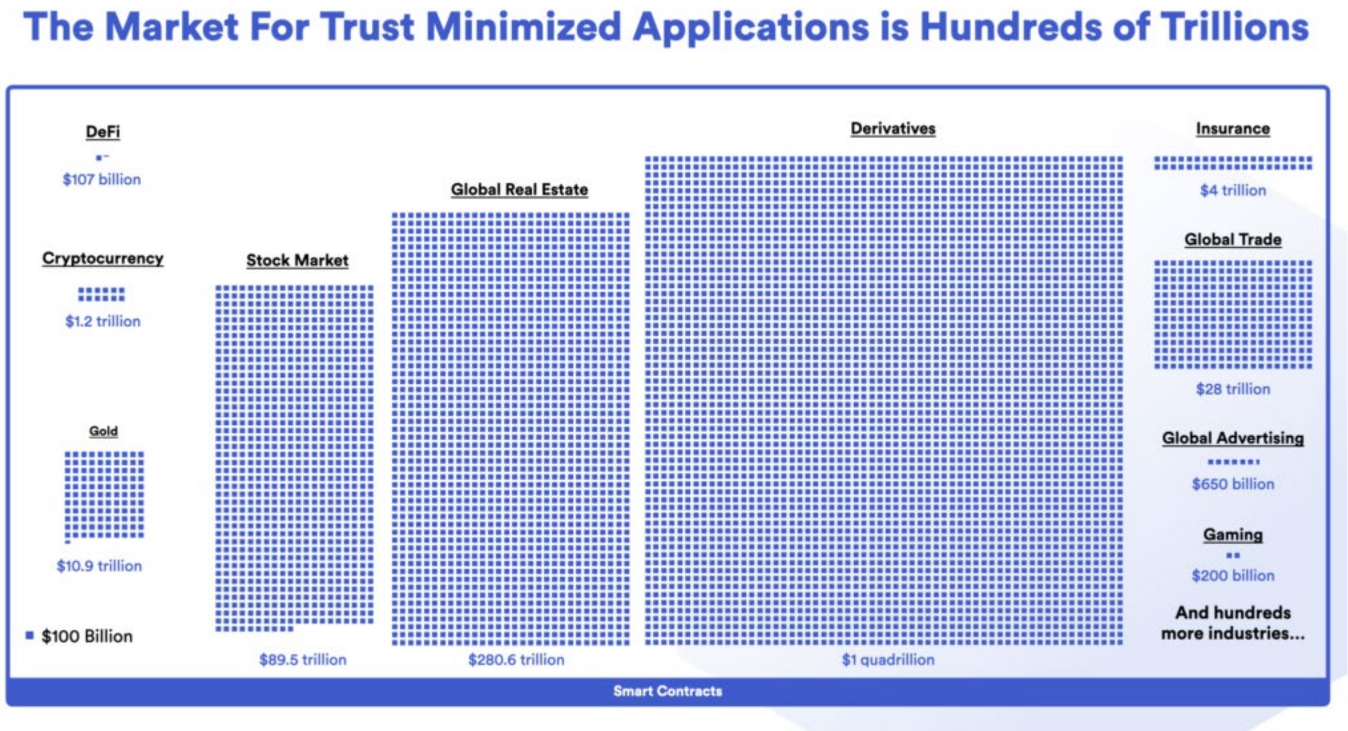


At this time, the risk-free yield of U.S. Treasuries, which is around 5%, has become highly sought after in the crypto market. The most notable instance of this is MakerDAO’s significant purchase of U.S. Treasuries this year. As of September 20, 2023, MakerDAO has purchased over 2.9 billion dollars of U.S. Treasuries and other real-world assets.

RWA

TradFi Perspective on RWA

From the perspective of TradFi, RWA represents a bidirectional journey between TradFi and DeFi. For the TradFi world, DeFi financial services, which are automatically executed based on smart contracts, represent a revolutionary fintech tool. RWA in the TradFi sector focuses more on how to combine DeFi technology to tokenize assets, empowering the TradFi system, reducing costs, increasing efficiency, and addressing the pain points existing in TradFi.



The focus is on the benefits that tokenization brings to the TradFi system, rather than just finding a new channel for asset sales. From the visual comparison chart of market sizes provided above, we can see the scale difference between the crypto market and the TradFi market.

RWA

Blockchain - Infrastructure for Asset Tokenisation

The internet enables the rapid, low-cost, lossless, and convenient transmission of information, providing unprecedented possibilities for global knowledge and information sharing. However, the internet faces challenges **when dealing with contracts/instruction systems, especially in scenarios involving authority and trust, such as business operations, government decision-making, and military command**.

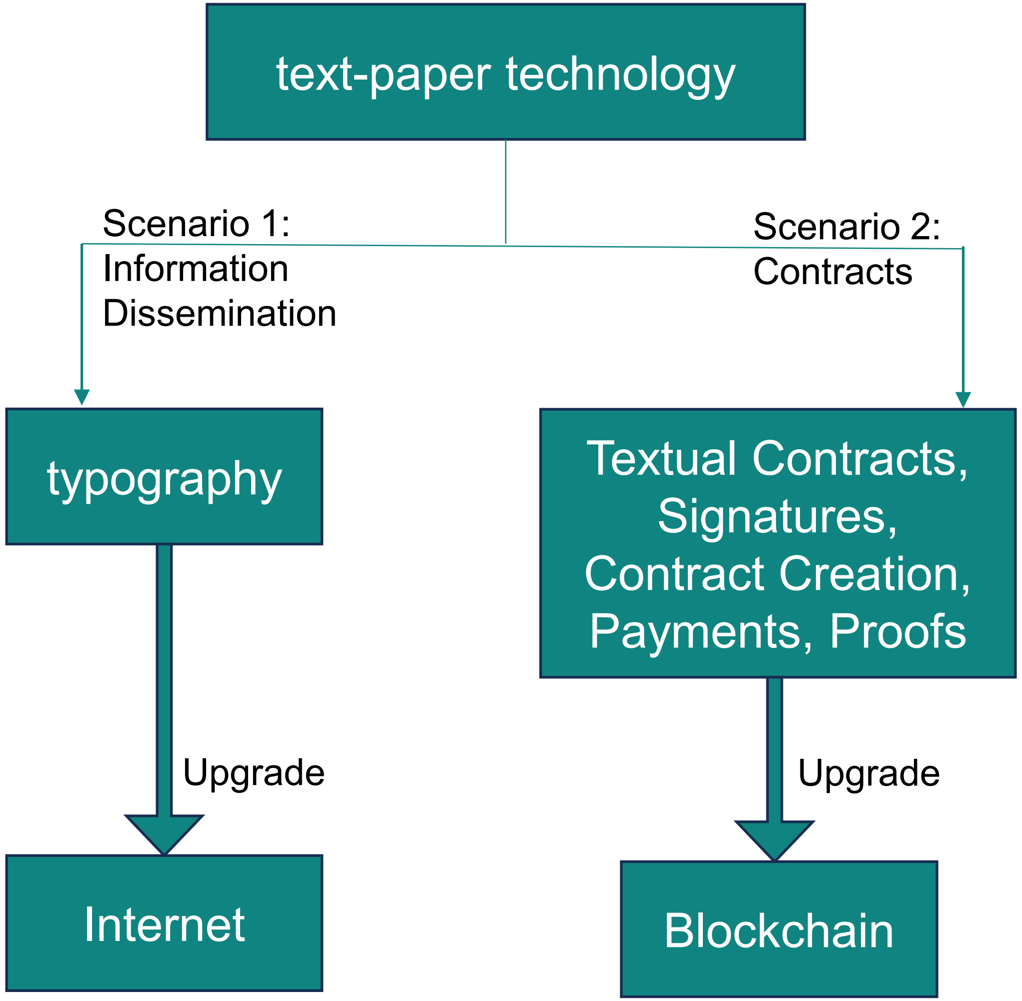
Centralised power structures may lead to the concentration and abuse of power, making information transmission opaque and unfair. The involvement of trusted third parties may introduce additional security risks and trust issues, as these third parties could also become unreliable sources of information.

Blockchain, as a decentralised, transparent, and immutable distributed ledger, ensures the authenticity and reliability of information. This means that people no longer need to rely on centralised institutions or third parties to establish trust. This innovative technology offers a new perspective and solution to the problems of information transmission in contract and instruction systems, ensuring the truthfulness, integrity, and consistency of information without the need for centralized verification.

Therefore, since blockchain is inherently a platform for digital contracts, and contracts are the basic expression of assets, **tokens** are the digital carriers of assets formed by smart contracts. Thus, blockchain becomes the ideal infrastructure for digital assets/tokenised assets.

Internet vs Blockchain

If we consider the internet as the digital upgrade of text-paper technology in the context of information dissemination, then blockchain undeniably serves as the digital advancement of text-paper technology supporting contracts/instructions. Thus, blockchain can be recognised as a distributed system maintained collectively, facilitating the creation, verification, storage, circulation, and execution of digital contracts along with other associated operations. Post the evolution of computers and the internet, blockchain stands out as the first effective means to digitise contracts.


text-paper technology
Scenario 1: Information Dissemination
Scenario 2: Contracts
typography
Textual Contracts, Signatures, Contract Creation, Payments, Proofs
Upgrade
Upgrade
Internet
Blockchain

Humanity's Demand for “Computability”

Distinguishing between “computational systems” and “non-computational systems” is crucial for understanding the problem-solving capabilities of blockchain.

- Blockchain addresses issues within “computational systems”, which are transactions characterized by “repeatable processes and verifiable results”.
- “Non-computational systems” include transactions influenced by human cognition, where processes cannot be reliably repeated and results are not consistently verifiable.

Since ancient times, humans have had computational needs, but were limited to primitive tools and human cognition for simulating computational processes.

In a centralized “computational system” like the internet, the infusion of subjective human consciousness can disrupt the “repeatable processes and verifiable results”, affecting the reliability and authenticity of information transfer and hindering the establishment of trust.

The emergence of blockchain introduces a new tool for addressing “computational” demands, providing a decentralised computational system less susceptible to human interference. In this decentralised system, it becomes significantly more challenging for hackers to manipulate results, as they would need control more than 50% of the network’s nodes to alter the output of smart contracts, an attack that is typically not cost-effective.

DeFi - A “Computational” Financial Innovation

- DeFi represents a novel financial paradigm that utilises **distributed ledger technology** to offer a variety of financial services, such as lending, investment, and the exchange of cryptocurrency assets, all **without relying on traditional centralised financial institutions**.
- These financial services in DeFi are implemented through **smart contracts**, which are programmed to autonomously execute the logic of TradFi operations. Users interact with these programs, which aggregate assets from other DeFi users, maintaining control over their funds.
- DeFi, facilitated by blockchain's “computational system”, can be seen as a “computational” innovation in finance. Smart contracts can replace certain “computational” elements in TradFi that depend on manual or mechanical processes for achieving deterministic results, such as **clearing**, **settlement**, **transfers**, and other repetitive tasks that do not rely on human cognition.
- In short, DeFi automates time-consuming and manual steps in TradFi activities through smart contracts, significantly reducing transaction costs, eliminating settlement delays, and achieving automation and programmability.

RWA

DeFi - A “Computational” Financial Innovation

- DeFi lending protocols, according to Jake Chervinsky from Compound, do not facilitate actual loans but operate as **interest rate protocols**, relying on **over-collateralisation and liquidation**, rather than creating credit or relying on borrower‘s future payment promises, e.g. Borrowers must first provide collateral exceeding the loan amount, such as depositing $100 in ETH to borrow $65-70 in USDT. This form of lending is essentially "computational leverage," and does not create any credit, as it does not rely on any promises of future payment, trust, or reputation on the part of the borrower.

- Blockchain as a computational system enables repeatable processes and verifiable results, positioning DeFi as a computational innovation in finance, automating and optimising cost and efficiency while allowing programmability.
- However, the current DeFi system does not encompass credit, and unsecured lending based on credit has not yet been realized in the current DeFi ecosystem. This is due to blockchain's current lack of an identity system that expresses “**relational identity**” and the absence of a legal system to protect the rights and interests of both parties.

RWA

DeFi - A “Computational” Financial Innovation

- TradFi services are based on **trust** and **empowered by information**, relying on financial intermediaries to maintain and verify the integrity of records covering ownership, liabilities, conditions, and contracts, which are usually scattered across various systems.
- The financial system requires extensive post-transaction coordination to reconcile and settle transactions, ensuring consistency across all relevant financial data, a process that is complex, time-consuming, and particularly challenging in cross-border transactions due to differing regulations and involvement of multiple financial institutions.
- Blockchain, as a distributed ledger technology, shows immense potential in addressing these efficiency issues in the TradFi system, offering a unified and shared ledger that resolves the fragmentation caused by multiple independent ledgers, significantly improving **transparency**, **consistency**, and **real-time updating capabilities**.
- The application of smart contracts further enhances these advantages, allowing transaction conditions and contracts to be encoded and automatically executed upon meeting specific criteria, significantly improving transaction efficiency, and reducing settlement times and costs, especially in **complex**, **multi-party**, or **cross-border** transactions.

What is Required for the Mass Adoption of RWA?

- **Robust Legal Framework**: Establishing a comprehensive legal system is crucial to protect asset tokenization, and implementing suitable blockchain networks ensures secure and regulated operations.
- **Identity Systems and Privacy Protection**: Developing identity systems that prioritize user privacy is essential, safeguarding personal information while facilitating asset tokenization.
- **W3C Standard DID+VC Identity System**: Adopting the World Wide Web Consortium (W3C) standards for Decentralized Identifiers (DID) and Verifiable Credentials (VC) enhances the security and interoperability of identity verification processes.
- **On-Chain Fiat Currency**: Integrating legal tender on the blockchain enables smoother transactions and increases the accessibility of asset tokenization.
- **Oracles and Cross-Chain Protocols**: Implementing oracles and cross-chain protocols is vital for ensuring data accuracy and enabling interoperability between different blockchain networks.
- **Low-Threshold Wallets**: Providing easy-to-use wallets with low entry barriers encourages wider adoption of asset tokenization among the general public.

DeFi

References to read

[1] Consensys-Codefi, 2020, DeFi Report Q4 2020.

[2] MakerDao, 2020, The Maker Protocol: MakerDAO's Multi-Collateral Dai (MCD) System.

[3] Uniswap, 2020, Uniswap v2 Core.