KPMG

Crypto Insights

#1. An introduction to Decentralised Finance (DeFi)

October 2021

Foreword: Why DeFi matters

For a long time dismissed as speculation, the crypto economy has turned heads over the past year as institutions are publicly committing to digital assets. While the Bitcoin price has captured the news, the real story has been Decentralised Finance (or 'DeFi') and the rise of the creator crypto economy, embodied by trading of crypto collectable images and adoption of play-to-earn gaming ('P2E').

In this report we focus on DeFi. "Value locked" in Ethereum, the blockchain underlying most of the DeFi ecosystem, has grown 60-fold in the past year to USD >90b*.

DeFi consists of financial services enabled by public blockchains and smart contracts executing rules set by developers and governance token-holders, with no ability for a central party to intervene or manipulate users' assets.

This is a radical new way of building, based on new and constantly developing technologies pushed forward by a large community of passionate and tech-savvy market participants. This innovation and competitive combination attracts two potentially opposing forces – accelerated innovation and regulatory attention.

Innovation has been rapid: It seems that not a day goes by without a new DeFi lending, exchange, insurance, trading, aggregation, or stablecoin project being announced. Smart contracts innovation may hold the key to overhauling a lot of the inefficient processes within traditional financial services.

Regulators are beginning to grapple with DeFi. Compliance risks and challenges working with unregulated open source code has long inhibited direct institutional capital allocation into DeFi (i.e. who do you call if you lose your capital?). Investing in DeFi apps is also not yet very user friendly, which may be the reason why many may not have heard as much about Uniswap or dYdX – currently the largest Decentralised Exchanges (or 'DEX') for spot and futures, respectively – both handle similar daily trading volumes to Coinbase**.

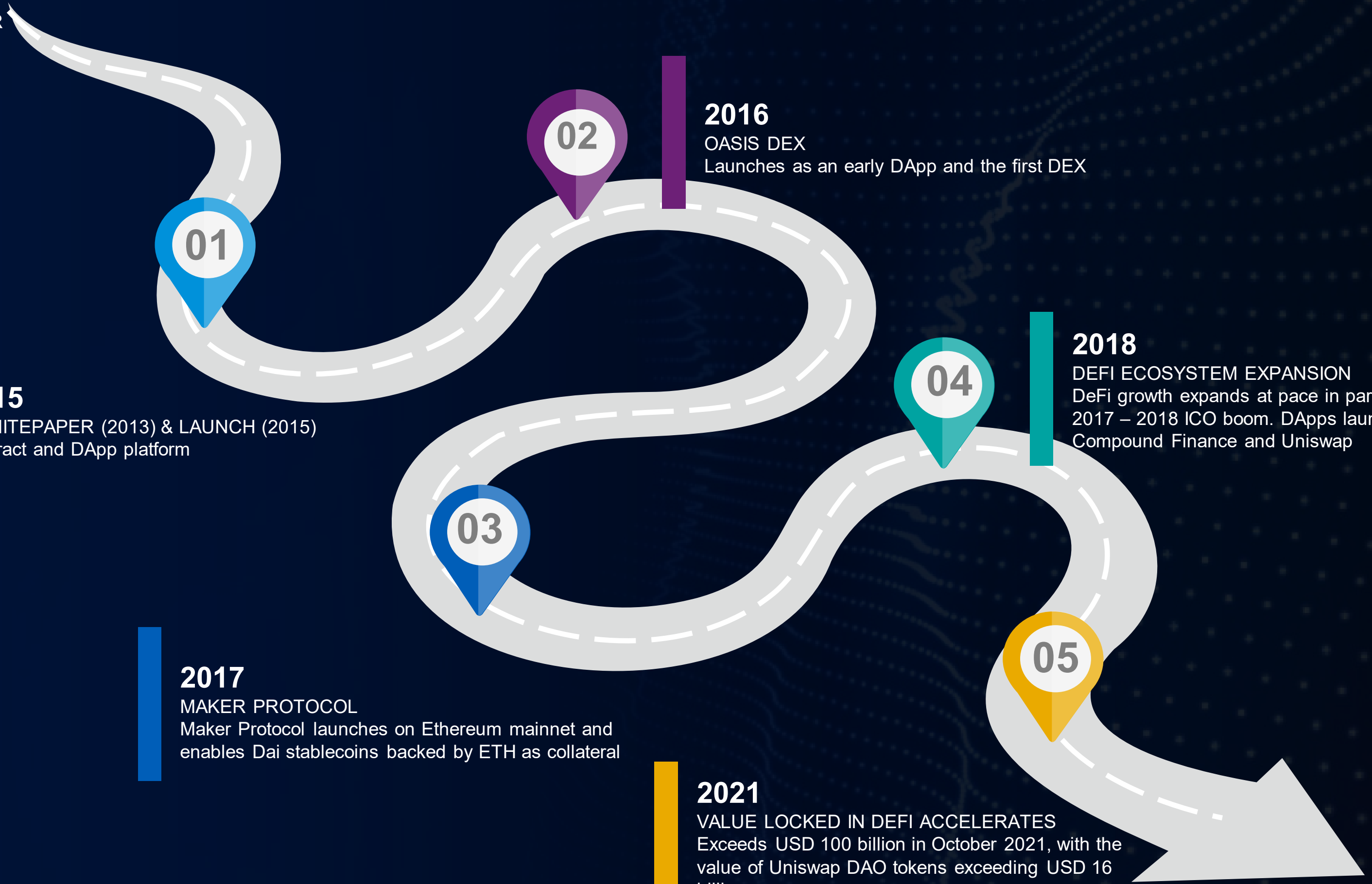
In 10 years, we may look back and remember the DeFi boom as an interesting anecdote told as part of the overall maturation of the crypto industry. It's possible that these early days of DeFi are similar to the early days of the internet - growing pains, but heralding a fundamental shift in business models, social interactions and politics.

This paper pulls together KPMG's in-market insights from working with regulators, financial investors, and the crypto industry, and sets out the background to DeFi and key factors which we believe will impact its evolution. The following papers in this series will be companion pieces that go into detail on how DeFi protocols are structured as well as other cutting edge crypto use cases. We hope you find this first report on DeFi useful.

Source: * DeFi Pulse, accessed 06/09/2021; ** Coinmarketcap.com 19/10/2021: Coinbase: USD 4.9bn, dYdX USD 4.1bn, Uniswap USD 1.3bn

Content

The DeFi movement is accelerating its use-cases, building on prior waves of innovation



START

2008
BITCOIN WHITE PAPER
P2P Electronic cash with guaranteed cap on supply

2013 - 2015
ETHERIUM WHITEPAPER (2013) & LAUNCH (2015)
First smart contract and DApp platform

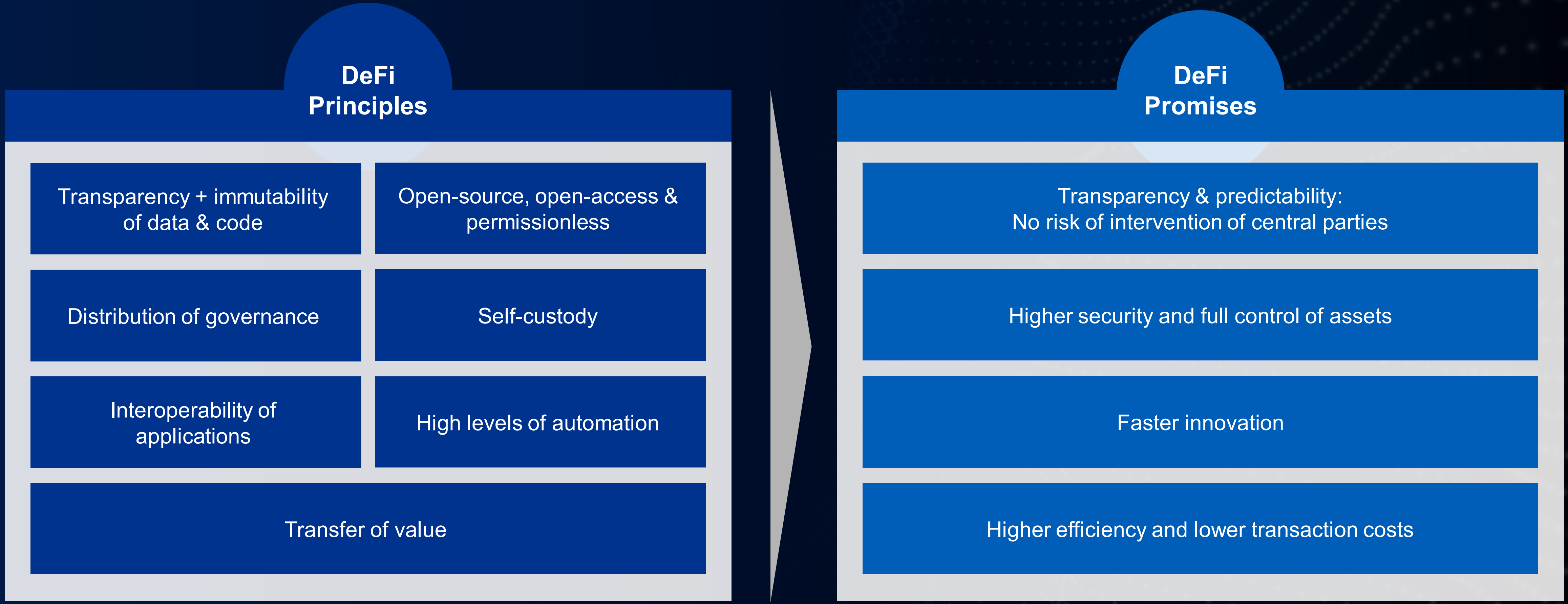
2016
OASIS DEX
Launches as an early DApp and the first DEX

2017
MAKER PROTOCOL
Maker Protocol launches on Ethereum mainnet and enables Dai stablecoins backed by ETH as collateral

2018
DEFI ECOSYSTEM EXPANSION
DeFi growth expands at pace in part funded by the 2017 – 2018 ICO boom. DApps launched include Compound Finance and Uniswap

2021
VALUE LOCKED IN DEFI ACCELERATES
Exceeds USD 100 billion in October 2021, with the value of Uniswap DAO tokens exceeding USD 16 billion

DeFi is trust-minimised finance on the blockchain without intermediaries



DeFi Principles

- Transparency + immutability of data & code
- Open-source, open-access & permissionless
- Distribution of governance
- Self-custody
- Interoperability of applications
- High levels of automation
- Transfer of value

DeFi Promises

- Transparency & predictability: No risk of intervention of central parties
- Higher security and full control of assets
- Faster innovation
- Higher efficiency and lower transaction costs

The Wharton & WEF principles: There are significant differences in principles between TradFi, CeFi, and DeFi

	Fiat	Crypto	
Principles	**Traditional Finance (TradFi)**	**Centralised Crypto Finance (CeFi)**	**Decentralised Finance (DeFi)**
Custody of Assets	Held by a regulated service provider or custodian on asset owners' behalf.		Held directly by users in non-custodial wallets or via smart contract-based escrow.
Units of Account	Typically denominated in fiat currency.	Denominated in digital assets or stablecoins (which may themselves be denominated in fiat money).	
Execution	Intermediaries or institutional counterparties process transactions between market participants.		Via smart contracts operating on the user's assets.
Clearing and Settlement	Processed by service providers, clearinghouses, or centralised exchange typically after a period of time.		Writing transactions to the underlying blockchain completes the settlement process.
Governance	Specified by the rules of the service provider, marketplace, regulator and/or self-regulatory organisation.		Managed by protocol developers or determined by users holding tokens granting voting rights.
Auditability	Authorised third-party audits of proprietary code or potential for open-source code that is publicly verified.		Open-source code and public ledger allows auditors to verify protocols and activity.
Collateral Requirements	Transactions may involve no collateral, or collateral less than or equal to the funds provided.		Overcollateralisation generally required, due to digital asset volatility and absence of credit scoring.
Cross-service Interaction	Limited movement, interoperability enabled via application programming interfaces or dedicated intermediaries.	Venues often integrate with other providers (e.g. for custody), allow for on-chain asset migration to wallets	Any service may integrate with any other service on the same blockchain, and potentially across chains.
Access and Privacy	Identity checks conducted by service providers. Personal data subject to national privacy laws.		Identity verification requirements under discussion by AML regulators. User balances and transaction activity are generally public.
Security	Vulnerable to hacks and data breaches in software systems controlling assets.		Vulnerable to hacks and other technical and operational risks of smart contracts or personal wallets.
Investor Protection	Government-mandated disclosure and consumer protections, anti-fraud enforcement, exposure limits, and insurance schemes.		Users assume all risks as a default, although private arrangements such as DeFi insurance offer some protection.

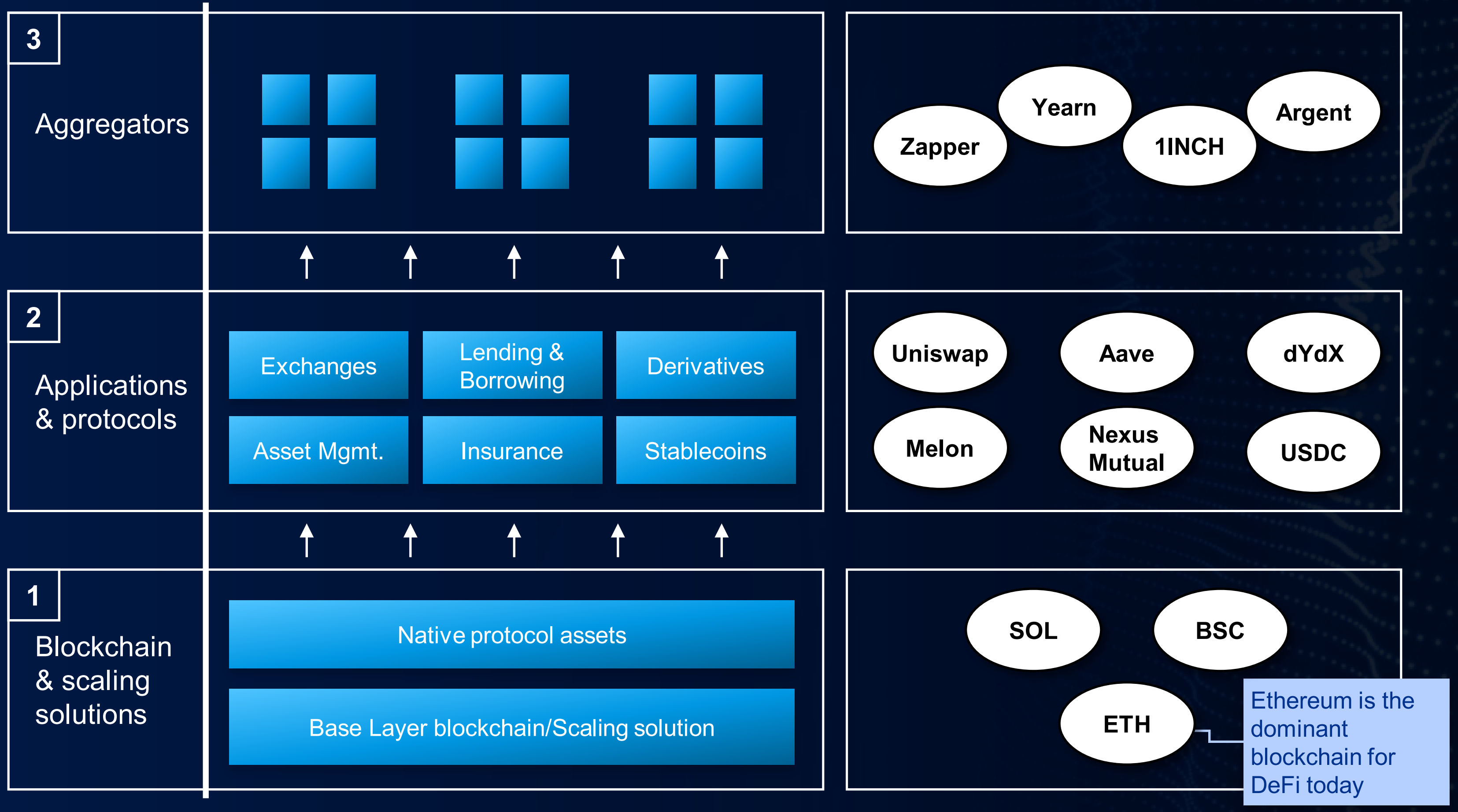
Source: "DeFi Beyond the Hype The Emerging World of Decentralized Finance", produced by the Wharton Blockchain and Digital Asset Project, in collaboration with the World Economic Forum. May 2021
Note: Centralized Finance column added to original Traditional Finance/ Decentralized Finance model

DeFi offers financial services through Decentralised applications (DApps) which potentially compete with TradFi and CeFi services

	Fiat			Crypto					
	Traditional Finance (TradFi)			Centralised Finance (CeFi)			Decentralised Finance (DeFi)		
Currencies	USD	CNY	EUR	USDT	USDC	BNB	DAI	BTC	ETH
Commercial banking/ lending	ICBC	BAML	HSBC	BlockFi	Nexo	Celsius	Compound	Maker	AAVE
Exchanges	NYSE	HKEX	NDAQ	Binance	Coinbase	Kraken	dYdX	Uniswap	Curve
Payment & Wallet	Stripe	Alipay	Paypal	KuCoin	FTX	Huobi	Metamask	Phantom	Portis
Insurance	AXA	AIG	Ping An	AON	Coincover	KASE	Opyn	Nexus Mutual	Etherisc
Asset management	BlackRock	Amundi	Vanguard	Bitwise	Greyscale	Crescent	Melon	TokenSets	Zapper

The DeFi stack relies on native blockchains, dApps & protocols, and protocols built on top of dApps

The DeFi tech stack



3 Aggregators

Zapper · Yearn · 1INCH · Argent

2 Applications & protocols

Exchanges · Lending & Borrowing · Derivatives · Asset Mgmt. · Insurance · Stablecoins

Uniswap · Aave · dYdX · Melon · Nexus Mutual · USDC

1 Blockchain & scaling solutions

Native protocol assets

Base Layer blockchain/Scaling solution

SOL · BSC · ETH

Ethereum is the dominant blockchain for DeFi today

LAYER 3: Aggregation layer: On top of the dApp layer, another layer of applications can exist and integrate with dApps. For example, Yearn Finance aggregates protocols to provide competitive liquidity offers across applications. This is possible due to the composability (like bricks, but for DeFi) enabled through shared interoperability standards.

LAYER 2: Applications & protocols: Protocols are autonomous programs that run on the underlying blockchain. Applications are the interfaces through which users interact with these protocols.

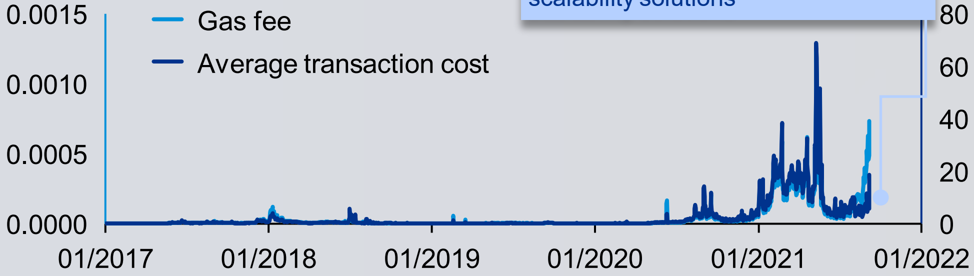
LAYER 1: Blockchain & tokens: Each network's base layer. Ethereum is the most commonly used blockchain in DeFi. Alternative chains in this layer include Solana, Binance Smart Chain and Ethereum scaling solutions environments (e.g. Polygon). These base layers have native tokens used to pay for operations performed on-chain, and usually have the ability to create and transfer other tokens, fungible or non-fungible.

Source: Based on Schaer, 2021, "Decentralized Finance: on Blockchain- and Smart Contract-based Financial Markets"

Ethereum is the dominant chain for DeFi, but transaction costs are high and throughput (transactions per second) is low compared to other Layer 1 blockchains

Ethereum mainnet transaction cost growth

Ethereum mainnet gas & transaction fee
USD , 2017-21



Increase in gas fees from high NFT demand. Offset by network improvements, sidechains & scalability solutions

Why are gas fees so high?

- Gas fees are paid by users to miners to fuel the completion of transactions on the Ethereum blockchain. They can rise with prices of ETH, increased transaction complexity, and based on network traffic.
- ETH price and demand for transactions have exploded over the past year, in part due to the rise of DeFi.

The Ethereum mainnet exploit issues

Front- and backrunning

- On Ethereum, users broadcast their transactions in a public 'queue' (mempool) to be handled by miners. Each transaction is accompanied by a gas fee offer, based on which miners prioritise which transactions to complete first
- Malicious actors (miners or other traders) can take advantage of their place as arbitrators in how blocks are packaged and use this information to 'frontrun' and 'backrun' transactions, extracting value from users ('miner extracted value'), increasing token prices on exchanges and gas fees
- Exchanges are estimated to incur >95% of total miner extracted value damage

Total cost incurred due to Miner Extracted Value in past 30 days:**

USD 27m

Scams and exploits

- Scams such as "rug-pulls" (i.e. suddenly removing liquidity from a liquidity pool) are still common in DeFi but not limited to ETH
- Flash loan exploits have also been prominent in the past: They refer to smart-contract based unsecured loans that can be used to exploit vulnerable DeFi protocols. These are used to manipulate price 'oracles' and extract value from DApps that depend on these price oracles

The community is looking at ways to **overcome Ethereum mainnet challenges.**

Ethereum v2 (expected 2022) is aiming to lower gas fees, increase transaction capacity through 'sharding' and move to Proof of Stake (PoS) verification (from Proof of Work (PoW)).

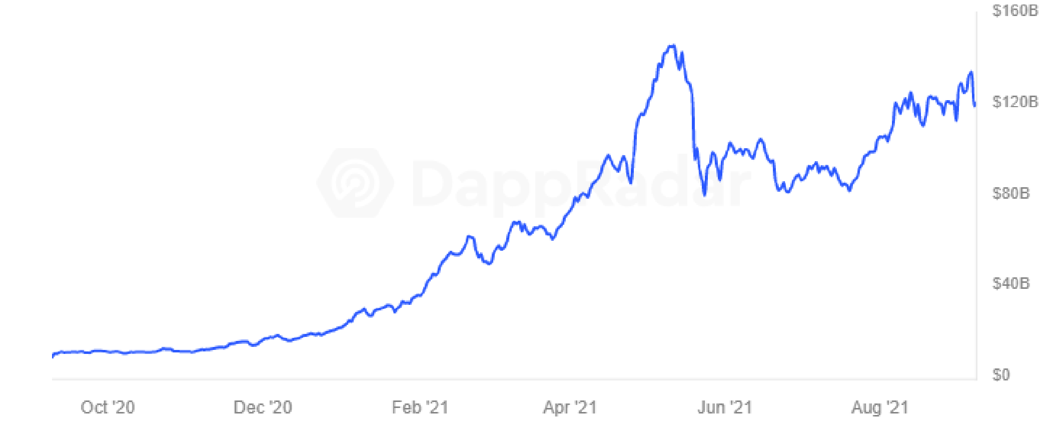
Meanwhile, DeFi ecosystems built on **Layer 2 Ethereum** (e.g. xDai, Optimism, Polygon) and **other smart contract blockchains** (Binance Smart Chain, Solana, Terra, Avalanche) are gaining prominence – several rounds of innovation are still necessary to establish best practices and liquidity at scale

Source: *Etherscan.io **Flashbots tool (explore.flashbots.net), accessed on 09/2021

Still, value locked in DeFi has grown 14-fold to over USD 119B in the past year. Exchanges are a key component and a great example of the innovative power of DeFi

Total Value Locked in DeFi (on ETH, BSC, and Polygon) has grown 14-fold between Sept 2020 to 2021 to USD 119.3B*

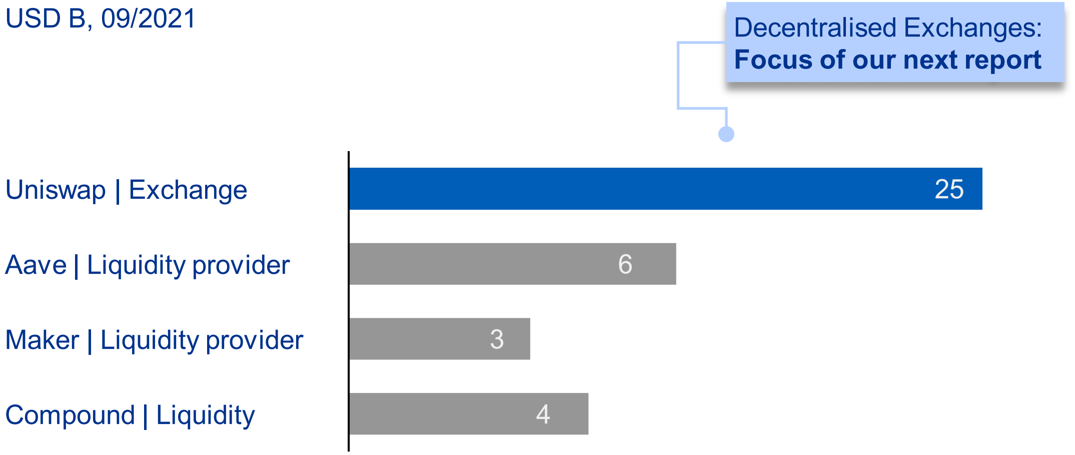
Total Value Locked in DeFi*
USD, 2020-'21



- While there are potential issues calculating total value of wrapped tokens added into DeFi, 'total value locked' (TVL) has been a directionally popular indicator for participation in DeFi protocols and markets.
- Depending on the platform, this may refer to the total value of tokens that the protocol has available for market participants to affect trades.

Exchanges are an integral part of the DeFi ecosystem

Top DAO tokens by fully diluted market capitalisation**
USD B, 09/2021



Decentralised Exchanges: **Focus of our next report**

- In the centralied crypto space, the most valuable organisations are exchanges like Coinbase, FTX, Huobi, and OkEX. As expected in DeFi, the most popular application by DAO token market cap is a decentralised exchange.
- Trading tokens is a core element in DeFi, which allows liquidity to flow into the most productive and in-demand protocols. Decentralised Automomous Organisations (DAOs) run on tokens, which provide holders with rewards and/or governance rights.

Source: *DappRadar, accessed on 07/09/2021; **Coinmarketcap 07/09/2021

The rapid growth of DeFi has caught regulators off-guard. We believe regulation is inevitable

DeFi does not fit neatly into existing regulatory frameworks

DEXs like Uniswap operate without license or KYC/ AML provisions. Some regulators have made statements on DeFi, but are not enforcing it consistently

- EtherDelta, a closed limit order-book (CLOB) DEX, was fined USD 388k in 2018 for facilitating the transfer of unspecified tokens that were securities, and not registering with the SEC
- The SEC has clarified that tokens without protocol utility are securities, but slow and inconsistent enforcement puts builders in a holding pattern as others rush to accumulate sufficient capital to cover fines.

This is the case as regulating DeFi is challenging

- Most capital markets regulatory regimes rest on holding intermediaries accountable
- This is an issue in DeFi, which eliminates intermediaries and distributes governance and accountability

KYC/ AML applicable?

- KYC/AML requirements (BSA, FinCEN) in the US hinge on intermediaries, i.e. hosted wallets, which don't exist in DeFi
- Without privacy tech, transparently marking a wallet on-chain presents privacy issues

This has prevented institutional investors from deploying capital

> "I think DeFi is really exciting […] We do not use any DeFi services. We don't have the capacity to audit code on AMMs. I am managing my investors' money, the tail risk of total loss is not acceptable. At the end of the day, I want someone to sue."
>
> **- MD of a USD >100m crypto hedge fund**

- Institutional money has been a major driver behind digital asset growth
- Lack of regulation can lead to heightened risk of scams/ exploits and subsequent regulatory crackdown
- This, and the inability to contact a central intermediary in case of conflict, inhibits institutional money flow. DeFi growth primarily relies on retail and crypto-native funds and investor volumes
- Institutional money, however, has exposure to and drives DeFi through investments in associated services (e.g. mining, equity/token investments in DeFi protocols or teams) purchase of DeFi tokens on regulated exchanges

How DeFi might be regulated

The non-conducive fit of existing regulation does not diminish the need for capital markets regulation. With its potential scale, DeFi poses risks relevant to regulators (financial crime, consumer protection, financial stability).

New regulatory frameworks relying on concepts like substituted compliance will need to be developed in order to match the cross-border nature of DeFi with the spirit of capital markets oversight, which are difficult to forecast.

How would you regulate a DAO?

While corporate law may apply to actors in DAOs, protocols can run autonomously with pseudonymous wallets. Forcing protocols to shut down may be challenging for regulators – especially if governance is distributed among many pseudonymous holders, or if the operations are automated.

DeFi market fragmentation risk

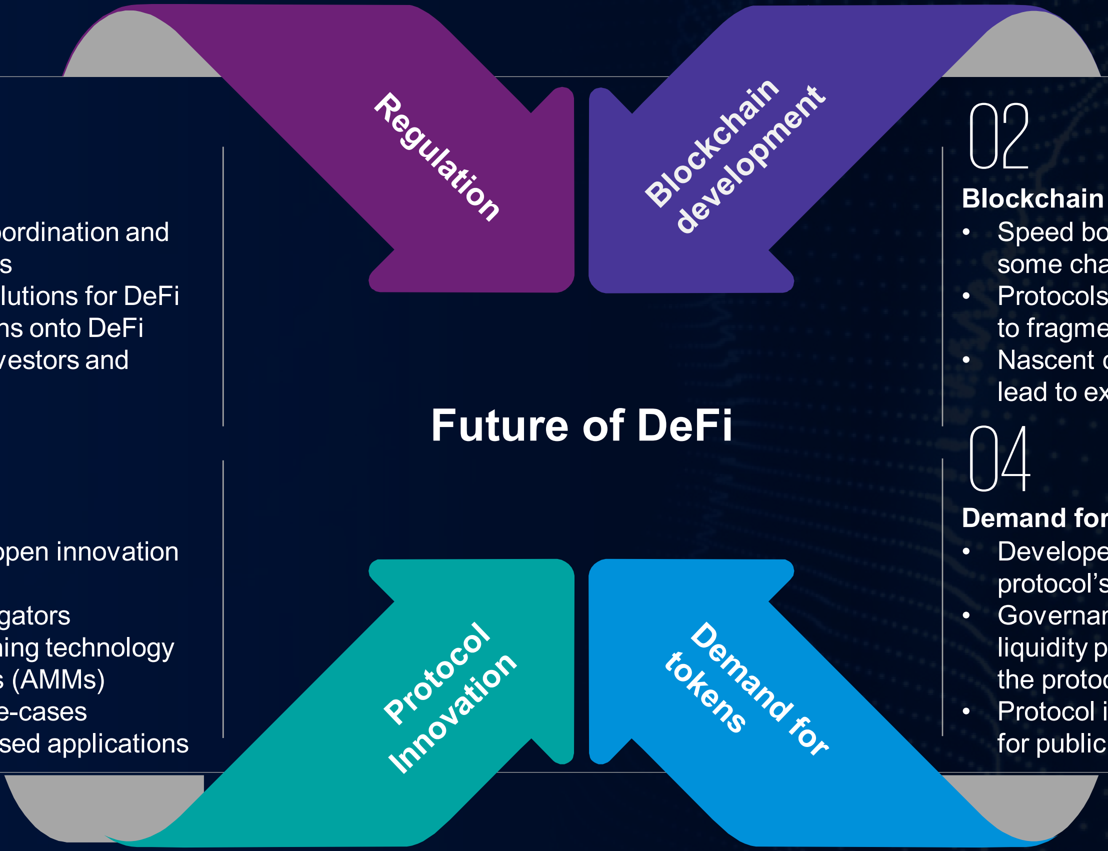
Should legislation not be considered beneficial by the community, we may see a **fragmentation of liquidity:**

- Parts of DeFi compliant with regulation and potentially more centralised. These venues may offer institutional liquidity, but lower yields.
- Non-institutional DeFi with higher yields and higher risk, mostly servicing retail

A split could also be seen along geographical lines, as is the case today for CEXs.

Source: Massari, Catalini (2021), "DeFi, Disintermediation, and the Regulatory Path Ahead", World Economic Forum & Wharton Blockchain and Digital Asset Project (2021), "Decentralized Finance (DeFi) Policy-Maker Toolkit"

We see four broad themes which will drive the future of DeFi



01

Regulation

- The design, extent of global coordination and impact of regulation on markets
- Development of AML / KYC solutions for DeFi
- Transposing existing regulations onto DeFi protocols in order to protect investors and encourage conducive markets

02

Blockchain development

- Speed bottlenecks and high transaction fees on some chains present adoption challenges
- Protocols built on other blockchains may lead to fragmentation of liquidity
- Nascent cross-chain design implications may lead to exploits

03

DeFi innovations

- Extent to which open-source, open innovation culture remains in DeFi
- Growth and role of DEX aggregators
- Innovation in DEX order matching technology and Automated Market Makers (AMMs)
- Development of blockchain use-cases
- User-friendliness of Decentralised applications

04

Demand for governance tokens

- Developers often align incentives through the protocol's governance tokens
- Governance tokens issued can also influence liquidity provision and yield farming activities on the protocols
- Protocol interaction for tokens can be a proxy for public interest in participating in the protocol

KPMG has experience across the full spectrum of crypto needs

Consulting

Planning

- Strategy and revenue models
- Product management & pricing
- Leadership & governance

Onboarding

- Customer on-boarding, KYC & investor qualification
- Asset provenance
- Account creation & funding
- Cryptographic key provisioning & exchange integration
- Custody operations and physical security
- Cyber threat defense
- Privacy
- Market Surveillance & Fraud Monitoring
- Third party risk management
- Regulatory compliance, integration, and reporting
- Proof of reserves

Service and Deliver

- Order management, booking & settlement
- Anti-money laundering, counter terrorist financing & sanctions
- Fork management & network governance
- Market and network data
- Customer and account servicing
- Resiliency and disaster recovery
- Blockchain network optimisation & risk management
- Finance, P&L and Tax reporting
- Internal audit, external audit and attestation

Deal Advisory

- Financial, tech, operating, HR, tax, and commercial due diligence
- Valuation & modelling
- Fund raise
- Target identification & lead advisory
- Deal strategy and equity value story development

Your contacts & contributors

Hong Kong

Authors of this report

Barnaby Robson
Partner, Deal Advisory
T: +852 6548 4923
E: barnaby.robson@kpmg.com

Karl Koch
Manager, Deal Advisory
T: +852 6576 8097
E: karl.koch@kpmg.com

James O'Callaghan
Head of Technology Enablement and Technology Consulting
T: +852 2143 8866
E: james.ocallaghan@kpmg.com

Paul McSheaffrey
Partner, Financial Services
T: +852 2978 8236
E: paul.mcsheaffrey@kpmg.com

Jianing Song
Head of Advisory, Hong Kong
T: +852 2978 8101
E: jianing.n.song@kpmg.com

Nigel Hobler
Partner, Tax
T: +852 2978 8266
E: nigel.hobler@kpmg.com

Matthew Sung
Partner, Asset Management
T: +852 3927 3008
E: matthew.sung@kpmg.com

Adam Bobrowski
Contributor

United States

(Cryptoasset Products and Services)

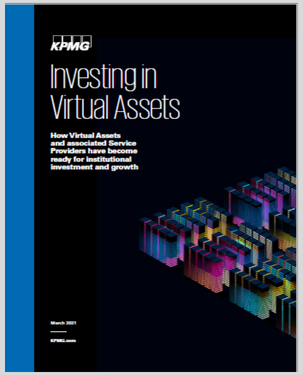
Arun Ghosh
Principal, Advisory
T: +1 617 988 1628
E: arunghosh@kpmg.com

Sam Wyner
Director, Advisory
T: +1 212 954 4903
E: swyner@kpmg.com

Patrick O'Kain
Manager, Advisory
T: +1 212 758 9700
E: pokain@kpmg.com

Okiki Famutimi
Jillian Johannes
Contributors

KPMG regularly publishes thought leadership in the digital asset space


KPMG

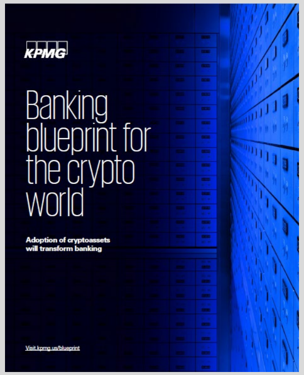
Investing in Virtual Assets

How Virtual Assets and associated Service Providers have become ready for institutional investment and growth

March 2021

KPMG.com

Investing Virtual Assets
2021

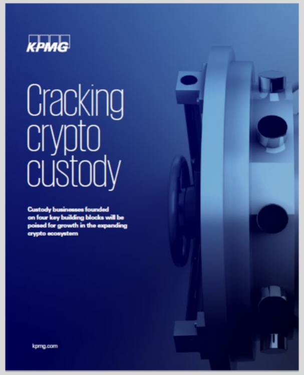

KPMG

Banking blueprint for the crypto world

Adoption of cryptoassets will transform banking

Visit kpmg.us/blueprint

Banking blueprint for the crypto world
2021


KPMG

Cracking crypto custody

Custody businesses founded on four key building blocks will be poised for growth in the expanding crypto ecosystem

kpmg.com

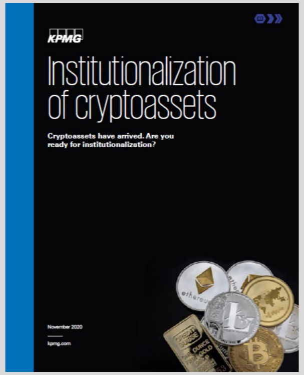
Cracking crypto custody
2020

KPMG

Six blockchain and cryptoasset predictions for 2020

kpmg.com

Six blockchain and cryptoasset predictions
2020


KPMG

Institutionalization of cryptoassets

Cryptoassets have arrived. Are you ready for institutionalization?

November 2020

kpmg.com

Institutionalization of cryptoassets
2020

KPMG

Pulse of Fintech H2 2019

February 2020

Pulse of Fintech H2’19
2020

Our Thought Leadership

Our global team of blockchain and virtual asset professionals share their ideas with our clients and the marketplace through the regular publication of thought leadership and other materials on industry.

These publications range from white papers and surveys through to opinion pieces and regulatory analyses.

Appendix

Glossary

Term	Definition
AML	Anti-Money Laundering; processes and policies put in place to prevent and/or detect money laundering
Aggregator	Web applications/systems which allow users to access a wider range of liquidity pools via one single platform
Automated Market Making (AMM)	A DeFi protocol allowing digital assets to be traded in a permissionless and automatic way via Liquidity Pools rather than a traditional CLOB (Closed Limit Order Book)
Blockchain	A cryptographically secure digital ledger that maintains a record of all transactions that occur on the network and follows a consensus protocol for confirming new blocks to be added to the blockchain
Centralised exchange (CEX)	A type of cryptocurrency exchange that holds users' funds in custody
CeFi	Short for Centralised Finance; financial services organised through centralised corporations that hold users' funds in custody
Cryptocurrency (or crypto)	Tokens on a cryptographically secured ledger, including Bitcoin and 'altcoins', (tokens launched after Bitcoin). This category of cryptoasset is designed to work as a medium of exchange, store of value or to power applications, and typically excludes security tokens. "Crypto" is often used as a term for any cryptography-based market, system, application, or decentralised network
Crypto asset (or 'token')	Any digital asset built using blockchain technology, including cryptocurrencies, NFTs, stablecoins, and security tokens
Decentralised exchange (DEX)	A type of cryptocurrency exchange which functions without a central intermediary party holding users' funds in custody
DeFi	Short for Decentralised Finance. Peer-to-peer software-based network of protocols that can be used to facilitate traditional financial services like borrowing, lending, trading derivatives, insurance, and more through smart contracts
Ethereum (ETH)	A decentralised global computing platform that supports smart contract transactions and peer-to-peer applications. The native crypto asset is called "Ether" (ETH)

KPMG

Glossary

Term	Definition
Fiat money/currency	A type of currency which is government issued and is not backed by any physical commodity, such as gold and silver
Fork	A fundamental change to the software underlying a blockchain which results in two different blockchains.
Gas	A term used on the Ethereum blockchain, which refers to the required cost when making transactions on the blockchain
HODL	Hold On for Dear Life; holding a crypto asset through ups, downs and times of volatility rather than selling it
KYC	Know Your Client/Customer
Liquidity Pool	A smart contract holding two or more tokens or cryptoassets for the purposes of facilitating transactions performed by market participants
Miner/Validator	Individuals or entities who operate a computer or group of computers that add new transactions to blocks, and verify blocks created by other miners. Miners collect transaction fees and are rewarded with new tokens for their services
Mining	The process by which new blocks are created, and thus new transactions are added to the blockchain. This is done by 'miners'
Oracle	A service, entity, or smart contract that provides information outside of the context of a given smart contract. This can include data found on-chain (price feeds) and data found off-chain (weather, sports events). It queries, verifies, and authenticates external data sources via trusted APIs and then relays that information to other nodes in a network
Protocol	A type of algorithm or software that governs how a blockchain operates
Proof of Stake (POS)	Consensus mechanism/algorithms used by blockchain networks to prevent users from invalid transactions and provide a distributed consensus by giving validators the ability to add transactions to a block based on pro rata proportion of tokens held
Proof of Work (POW)	Consensus mechanism/algorithms used by blockchain networks to prevent users from invalid transactions and provide a distributed consensus by giving validators the ability to add transactions to a block based on computational energy

Glossary

Term	Definition
Smart contract	Software that digitally facilitates or enforces a rules-based agreement or terms between transacting parties
Stablecoin	Crypto assets designed to minimise price volatility. A stablecoin is designed to track the price of an underlying asset such as fiat money or an exchange-traded commodity (such as precious metals or industrial metals). Stablecoins can be backed by fiat money or other crypto assets
Total Value Locked (TVL)	The amount of assets in dollar value which are locked in a smart contract at a given decentralised protocol
TradFi	Traditional, i.e. non-cryptocurrency finance. This mostly refers to finance based on fiat currency
USD Coin or USDC	A USD stablecoin that is issued through the Centre Consortium (co-founded by Coinbase and Circle Internet Financial Limited, or Circle)
USD Tether or USDT	A USD stablecoin that is issued through the Tether organisation
Yield Farming	A strategy, also known as liquidity mining, of providing liquidity in turn for rewards. Yield farming especially refers to moving funds around between decentralised applications in the shorter term

kpmg.com/cn/socialmedia

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.