EDUCATIONAL
MATERIAL

DEX® FINANCIAL DIGITAL EXCHANGE

VQ32022

A LOOK LATERAL GROUP COMPANY

LOOK LATERAL

BACK TO BASICS : BARTER, MONEY AND TRUST

- Before money existed, people used other systems to perform exchanges, such as bartering (a direct trade of goods/services for other goods/services). **BARTER** is effective only when (i) there is a limited set of goods/services to be traded, as it is very complex to continuously recalculate the exchange ratios of every trade pair, and when (ii) both parties are interested in receiving what the other has to offer, otherwise, even knowing the correct exchange ratio, the transaction would not occur.

- In order to let more complex commercial systems work, a special instrument is needed: **MONEY**. Therefore, the origin of money comes from the specialisation of people's activities, as societies became more structured, and from the related necessity to facilitate the exchange of many different products and services between individuals.

- Money is an «intermediate tool», which allows to (i) quantify the value of a wide set of goods/services using the same metric, and (ii) facilitate transactions using money itself as matter of exchange. Instead of having to know the exchange ratios of every trade pair, you can now see the value of every good/service in terms of «something trasversal» which is commonly used. Finally, being now part of every transaction, everyone wants it, as it can be translated in a second moment in any other good/service. This way, transactions can always take place, as both counterparts always want/accept money instead of another good/service directly.

- At the beginning, money was represented by food or useful objects, followed by metals, banknotes and finally electronic data, with a progressive improvement of its performance (ease of storage/accumulation and transportation) and security.

SOURCE: SAPIENS, A BRIEF HISTORY OF MANKIND (YUVAL NOAH HARARI) / WHY TRUST MATTERS ((BENJAMIN HO)

BACK TO BASICS : BARTER, MONEY AND TRUST

Money is nothing more than a system of mutual **TRUST** between individuals, as well as a collective convention/ belief around one object: everyone believes in it because others believe in it (positive network effect), belief which is reinforced and advertised by the reference authorities in charge of societies' organization. At the beginning, in order to induce trust, money had to show an instrinsic value/utility. Since then, it progressively dematerialized and become a largely shared belief, underpinned by a complex system of political, social and economic relations, in which a key role is played by the central, trusted, authority (at the beginning the king/emperor, and subsequently governments and central banks). Thanks to money, individuals who don't know each other can easily cooperate through the exchange of goods and services.

The evolution we are seeing today with permissionless cryptocurrencies (digital money) is the existence of trust between individuals who don't know each other even without trusting a central authority. How? Having trust in the process that governs the overall monetary system (a blockchain-based protocol, i.e. set of functioning rules, which – if universally accepted – is immutable and transparent). The trust is into the mechanics of a specific techical infrastructure, not into a central authority. Furthermore, generally the quantity of digital money supply is fixed and that cannot be changed (deflationary characteristic). This is the logic behind many protocols who wants to have their token become the next reference asset to be collectively recognized as «money». It is yet to be seen if this vision will become reality, and who the winner will be. It is also fair to highlight that many other protocols don't have this monetary goal, but they instead want to become the reference infrastructure for the development of blockchain-based software applications (i.e. they want to use the blockchain for «industrial» applications in real life).

Having another look at the token economy in light of the above, it is now easier to understand how the introduction of stablecoins (and in the near future CBDCs) represents the invention of money in the blockchain-based world, while until then only bartering (exchange of tokens) was available.

SOURCE: SAPIENS, A BRIEF HISTORY OF MANKIND (YUVAL NOAH HARARI) / WHY TRUST MATTERS ((BENJAMIN HO)

DECENTRALIZED FINANCE (“DEFI”): THE NEXT STEP IN THE DIGITALIZATION OF FINANCE

- Decentralized Finance (“De-Fi”) is an ecosystem of applications where smart contracts automate/govern manual processes of traditional finance, in order to (i) remove the need of relying on traditional financial institutions, and at the same time (ii) replicate existing financial offerings (such as lending, borrowing, insurance, investing/trading etc) with a higher level of security and efficiency. These financial services are accessible via Dapps (decentralized applications), based on blockchain. Smart contracts are the heart of the decentralized finance movement because they allow De-Fi protocols to function based on code and logic without the need of a trusted intermediary. **USERS RETAIN THE FULL CONTROL/CUSTODY OF THEIR ASSETS WHILE INTERACTING WITH THE DE-FI ECOSYSTEM.**

- The concept of decentralization stands in contrast with the traditional financial services that are generally centralized, and more prone to errors, frauds, costs and inefficiencies.

- De-Fi applications are a fast-growth segment of the digital asset ecosystem (on a parabolic rise since mid-2020), with the goal of expanding the access to financial services using more efficient, trustless protocols. There are multiple products and services that are aiming to emulate or augment traditional financial industries, which can also be combined together:

1. Lending / farming, in order to gain an interest from your tokens (for example liquidity mining, i.e. getting rewards for contributing to liquidity pools)
2. Borrowing, using your tokens as collateral
3. Trading on decentralized exchanges (DEXs), which let users’ wallets interact (swap their tokens) directly on the blockchain without the need of central intermediaries
4. Insurance
5. Margin trading
6. Derivatives
7. Other emerging uses (lotteries, flash loans etc)

SOURCE: SAPIENS, A BRIEF HISTORY OF MANKIND (YUVAL NOAH HARARI) / WHY TRUST MATTERS ((BENJAMIN HO)

DECENTRALIZED FINANCE ("DE-FI"): THE NEXT STEP IN THE DIGITALIZATION OF FINAN-

- Stablecoins have become key assets in the De-Fi ecosystem, enabling investors to borrow, lend, trade and make plans without the adverse effect of volatility. They represent the bridge between centralized finance and decentralized finance, allowing you to switch/convert your tokens with fiat-like tokens (stablecoin themselves), always remaining on-chain. They effectively represent "money" in the token economy.

- The main risks associated with De-Fi are bugs in smart contracts, shutdown procedure feasibility (linked to the level of decentralization), systemic risks due to the interconnection of different De-Fi protocols ("De-Fi lego") and network fees/congestion altering economics and user experience.

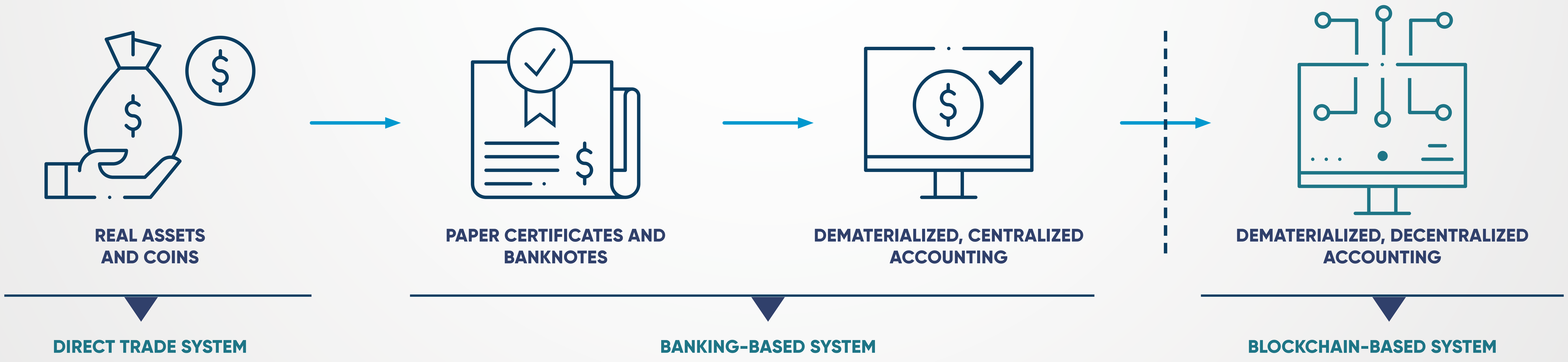
- One of the biggest problems of traditional, crypto-related, De-Fi protocols is how to attract sticky liquidity from the outside, in particular at the beginning, when the value added is still not consolidated and well-known to market participants. DEXs for example, aim to have a deep liquidity, so that users can always trade at the best prices. Many protocols give away a big chunk of their native token as an incentive, but LPs are still mainly opportunistic, and might switch for another project easily ("mercenary capital"). Vesting of incentives can be added to slowdown the manifestation of this risk. Aim is to grow fast and establish/retain a positive network effect. De-Fi 2.0 identifies a new wave of protocols trying to tackle this problem in a more sustainable way (such as bonding mechanisms and liquidity redirecting mechanisms).

BLOCKCHAIN AND SMART CONTRACTS: THE NEXT INFRASTRUCTURAL LEAP

- **BLOCKCHAIN:** an innovative type of register that allows to certify ownership and record events in a decentralized, incorruptible and efficient manner. This flexible and ingenious technology can be leveraged to run a wide array of applications, including issuance/trading/clearing-settlement/custody of securities, enabling faster and cheaper transactions, automating and streamlining the whole financial security value chain.

- **SMART CONTRACTS:** programmable instructions executed using the blockchain, with the aim to automatically enforce certain contractual obligations upon the occurrence of certain situations. They can essentially automate any kind of process or operation. This allows "trustless protocols", where random users can interact knowing that contractual actions will be executed only if certain events occur, with no room for interference or frauds and reducing costs (no more intermediaries needed). Back to our business case, through Smart Contracts it is possible to create digital securities paying coupons, executing capital calls etc. on an automated basis, reducing to zero risks of fraud, mistakes and delays.

JUST LIKE DEMATERIALIZATION HAS REPLACED PAPER SECURITIES, THIS NEW MARKET PROTOCOL HAS BUILT THE FOUNDATIONS OF THE NEXT EVOLUTIONARY STEP IN FINANCIAL MARKETS. AS OF TODAY, ABOUT A THIRD OF ALL GLOBAL BLOCKCHAIN-RELATED INVESTMENTS HAVE BEEN DONE WITHIN THE FINANCIAL INDUSTRY:


REAL ASSETS AND COINS
PAPER CERTIFICATES AND BANKNOTES
DEMATERIALIZED, CENTRALIZED ACCOUNTING
DEMATERIALIZED, DECENTRALIZED ACCOUNTING
DIRECT TRADE SYSTEM
BANKING-BASED SYSTEM
BLOCKCHAIN-BASED SYSTEM

SOURCE: DELOITTE – ARE TOKEN ASSETS THE SECURITIES OF TOMORROW? 2020. LIQUEFY/BNP/CAIA – TOKENISATION OF ALTERNATIVE INVESTMENTS 2020. INVESCO – GLOBAL BLOCKCHAIN BENCHMARKING STUDY, CAMBRIDGE CENTER FOR ALTERNATIVE FINANCE 2017.

SECURITY TOKENS: THE FUTURE OF FINANCIAL INSTRUMENTS

- **Tokens** are digital certificates/contracts representing a unit of an underlying asset, just like a stock represents a share of a company.
- **Tokenization** is the contractual process by which ownership and / or property rights relating to any underlying asset are split and transported on a blockchain-based digital infrastructure, which allows them to be held and transferred in a transparent, efficient and secure manner.
- There are three types of tokens, treated differently from an operational and regulatory perspective:
  - Payment/currency tokens (such as cryptocurrencies, accepted as payment and unit of account, whose value depends exclusively on the value that users place in them),
  - Utility tokens ("vouchers" that provide rights to use a specific product/service/protocol offered by the token issuer). Tokenization of services and goods fall into this category,
  - Security tokens (securitizations / digital representations of an asset or financial instrument providing rights and entitlements, such as ownership or future cash flows). Tokenizations of equity, debt, assets, funds etc fall into this category.
- "Hybrid tokens" can combine various of these aspects, and one further classification is between "Fungible" and "Non-Fungible" tokens (being the former interchangeable with each other and the latter not interchangeable and valued uniquely).
- For investment purposes, **our focus is on Security tokens only. These tokens are regulated, and are linked to underlying assets, unlike payment and utility tokens. Security tokens represent the evolution of traditional financial instruments.**
- Why? Because they facilitate the record of ownership and the safekeeping of assets, by providing a single source of truth and by making ultimate beneficial ownership transparent through the life of an asset and through the custody chain. Furthermore, they open-up a wider array of investment opportunities and allow to reduce illiquidity and concentration risks for end investors, while at the same time fostering efficiency and speed (tokens can be traded 24/7 and settled almost instantaneously, shortening settlement time to minutes compared to the usual T+2 or T+3 standards). Finally, tokens are also very flexible, as they can be customized with unlimited share classes and fee structures at low operational costs.
- This is why **regulators have well-received this innovation**, which has already been formally regulated in multiple jurisdictions (Switzerland in primis), equating security tokens to traditional financial securities, i.e. using a "substance over form" approach and application of existing laws. Within the EU, the regulation which applies to security tokens is MIFID 2, while additional details are expected to be formalized over the next couple of years.
- The expectation is that this paradigm **will become mainstream within the next 5-10 years,** progressively replacing old-fashioned, non-digital financial securities.

CENTRALIZED/TRADITIONAL EXCHANGES (CEXS) VS. DECENTRALIZED EXCHANGES (DEXS)

	CEXS	DEXS	
WHAT THEY ARE	A TECHNOLOGY PLATFORM RUN BY A CENTRAL MARKET OPERATOR	A SMART CONTRACT (SOFTWARE RUNNING ON BLOCKCHAIN)	→ **MORE TRANSPARENCY AND TRUST**
TYPE OF INTERACTION	USERS INTERACT THROUGH THE PLATFORM (INTERMEDIARY + EVENTUAL BROKERS)	USERS INTERACT DIRECTLY OR WITH THE SMART CONTRACT (PEER-TO-PEER VS. PEER-TO-CONTRACT)	→ **LOWER COSTS**
EASE OF USE	HIGH. NO NEED OF A WALLET OR TOKENS TO START.	MEDIUM. NEED OF A WALLET AND TOKENS TO START.	
CUSTODY	CENTRALISED (THE MARKET OPERATOR HOLDS YOUR TOKENS)	DECENTRALISED (USERS HOLD THEIR TOKENS IN THEIR OWN WALLETS)	→ **MORE SECURE**
ON-CHAIN / OFF-CHAIN	TRANSACTIONS OCCUR OFF-CHAIN, MANAGED BY THE CENTRAL MARKET OPERATOR DIRECTLY	TRANSACTIONS OCCUR ON-CHAIN	→ **MORE TRANSPARENCY**
TRADE EXECUTION MODEL	CENTRALIZED ORDER BOOK (CLOB)	PEER-TO-PEER / CENTRAL LIMIT ORDER BOOK (CLOB) OR AUTOMATED MARKET MAKER	→ **NEW LIQUIDITY MECHANISMS**
TRADES SUPPORTED	TOKEN VS. TOKEN, TOKEN VS. FIAT	TOKEN VS. TOKEN ONLY (BEING FULLY ON-CHAIN)	
TRADE COUNTERPARTS	EITHER YOU TRADE WITH A COUNTERPART (IF THERE IS A NATURAL BID/ASK PRICE CONVER-GENCE) OR YOU TRADE WITH A MARKET MAKER	EITHER YOU TRADE WITH A COUNTERPART (IF THERE IS A NATURAL BID/ASK PRICE CONVERGENCE) OR YOU TRADE WITH A LIQUIDITY POOL	→ **NEW LIQUIDITY MECHANISMS**
COUNTERPARTY RISK	YES	NO	→ **MORE SECURE**
CYBER-ATTACK AND DOWNTIME RISK	YES	NO	→ **MORE SECURE**

LIQUIDITY POOLS 101

What are they?

Each liquidity pool is a smart contact (software) which orchestrates a secondary market for a particular pair of tokens, as it aggregates liquidity for both sides of that trading pair. Such smart contract is like a “decentralized” market maker, whose stock of assets is composed by several small contributions made by “liquidity providers”, sitting across various wallets. The various tokens provided are said to be “locked” into the smart contract / liquidity pool.

How do they work?

Each trade occurs against the pool (“peer-to-contract”), and each token swap determines a price adjustment in the pair price within the pool (the ratio of the tokens in the pool determines the trade price as a consequence of an algorithm). In our case, liquidity pools are made of (i) a certain amount of security tokens and (ii) a corresponding amount of stablecoin; the proportion among the two is given by the initial price of the security token expressed in stablecoin.

Why are they needed?

Liquidity pools are a useful tool to provide liquidity / facilitate trading (just as real external market makers), in situations where there is a bid/ask impasse. Depending on the technical features of the DEX (network fees, transaction speed etc), liquidity pools might be the only viable alternative to real external market makers, in order to always allow trades to occur.

What advantages do they provide?

They allow investors to always be able to trade immediately, at a price decided by an algorithm. The liquidity pool never dries up of quantities, it just changes the price users have to pay.

What are the disadvantages?

In order to function properly (i.e. transactions execute with low slippage), liquidity pools rely on a large number of liquidity providers to join and supply tokens for that specific trade pair. In fact, the more the trade alters the pool equilibrium (i.e. the larger it is compared to the dimension of the pool), the more the price investors will have to pay will be distant (“slippage”) from the reference/initial price of the underlying asset. In case of pools containing assets which are highly volatile, “impermanent loss” come into play, i.e. a liquidity provider will automatically incur losses when the price ratio of the pooled asset deviates from the price at which he deposited funds. The higher the shift in price, the higher the loss incurred (a 25% change in price equals to a 0.6% impermanent loss, while a 100% change in price equals to a 5.7% impermanent loss). However, this loss is impermanent because there is a probability that the price ratio will revert. The loss only becomes permanent when the liquidity provider withdraws the funds before the price ratio reverts. In normal conditions, impermanent loss is more than offset by LP rewards. Liquidity pool hacks are another risk, and, finally, like any blockchain-based application, smart contract risk should be a consideration.

CRYPTOGRAPHY AND WALLETS 101

- **CRYPTOGRAPHY** has several possible applications. Within a blockchain protocol, cryptography is being used as "certification system" in order to avoid functioning frauds. In fact, it allows to certify that a certain token has been transferred from one user to another, that a certain token is unique and that everything on-chain remains immutable (thanks to the digital signature using the private key, and thanks to hash functions). Therefore, within the blockchain world, cryptography is not being used for its main use of protecting/hiding sensible information.

- The cryptographic systems utilized in the blockchain world is the asymmetric one, which foresees a **couple of keys**: a private one (used to sign/certify transactions) and a public one (which everyone can use to verify the authenticity of that transaction). The receiver can indeed check the authenticity of the transaction using the public key of the sender.

- If cryptography were used to protect/hide sensible information instead, the public key of the receiver would be used by the sender to encrypt the message, and the private one of the receiver would be used by the receiver to decode it.

  A pair of keys is mathematically linked but it's extremely difficult to discover the private key starting from the public key. Today, quantum computing is not a threat either in this respect ("post-quantum cryptography").

- One **wallet** can be seen as the security custody service offered by a bank

- One wallet can work with multiple **"accounts"** (pair of keys), even if generally 1 wallet = 1 account. The generation of a pair of keys is therefore not linked to the fact of having a wallet, but generally a wallet automatically creates one pair of keys for the new user

- For each account:
  - The user has (i) private key, (ii) public key, (iii) public address (0x…)
  - The public address (derived as the hash function of the public key) is like the IBAN
  - The public address can receive multiple tokens (if compatible with the wallet)
  - It is essential not to lose the private key, as it's the only one granting access to the account. Users can recover the lost private key thanks to a 12-words secret phrase (easier to remember) which is generated by the wallet

INDUSTRY AND DE-FI DATA: 2021

INDUSTRY OVERVIEW

2021 was a defining year for the blockchain and cryptocurrency, maturing from a nascent industry. The institutionalization of the sector also flowed over to the private markets, in which historic levels of venture capital were allocated to crypto/blockchain companies: approx. $25 billion (> 700% YoY, more than the previous six years combined) across 1700 deals.

One of the leading indicators that quantify the maturation of the crypto/blockchain sector in 2021 is the occurrence and frequency of mid to later-stage deals. Nevertheless, in 2021 there have been more than five times the amount of seed deals than 2020 (approx. 2/3 of the 1700 deals occurred in 2021). Like for mid to later-stage deals, as 2021 progressed, the valuations for firms at the seed & series A stage continued to increase as investors crowded to increase their exposure to the sector.

The most dominant investment trends in 2021 included Decentralized Finance (De-Fi), NFTs/Gaming and Web3. Approximately a quarter of all funding rounds has involved the De-Fi vertical and it has been the most popular deal type with over 400 raises.

M&A transaction volumes have surpassed $6 billion in 2021 (> 700% YoY) across over 200 transactions, another record high for the sector.

At least 65 companies in the crypto/blockchain sector now have the unicorn status; over the last two years there has been nearly a 500% increase in the number of companies reaching unicorn status.

DE-FI OVERVIEW

Decentralized Finance (De-Fi) had a stellar rise and the ecosystem continued to mature. The total value locked (TVL*) in De-Fi protocols skyrocketed from $16 billion to almost $100 billion this year, with most crypto assets allocated to lending protocols and DEXs.

Top 20 De-Fi token market caps of approx. $37 billion as of 31.12.2021.

Decentralized exchange (DEX) volume grew at a breakneck pace >500% increase year-on-year. Overall, top 20 DEXs trade volume has been over $1.1 trillion in 2021. Nevertheless, DEX trade volume still accounts for just over 10% of the CEX volume, as of 31.12.2021. UniSwap has been leading in trading volumes during the year, while Curve became the largest DEX by TVL.

While crypto as an asset class has matured into a two-and-a-half-trillion-dollar market, it remains comparatively siloed and disconnected from other economies. As the token-based economy advances, everything that carries value, financial or cultural, will somehow be tokenized. Bridging the gap between real-world assets and De-Fi could bring a vast pool of "old wealth" into the new digital economy and enormously augment the nascent De-Fi ecosystem. The European Union's proactive approach and relatively more welcoming attitude in addressing legal concerns surrounding stablecoins and other crypto assets could bring greater De-Fi adoption in Europe.

SOURCE: THE BLOCK RESEARCH – 2022 DIGITAL ASSET OUTLOOK, DEFI PULSE.

* A MEASURE OF GROWTH IN THIS MARKET IS THE AMOUNT OF TOKENS (USUALLY ETHER) COMMITTED TO SMART CONTRACTS KNOWN AS TOTAL VALUE LOCKED (TVL).

GLOSSARY

Decentralized Finance ("De-Fi"): ecosystem of smart contract-powered applications that aim to replicate traditional financial product/services leveraging the blockchain, removing the need for intermediaries, reducing overall costs, and greatly improving security and automation.

Blockchain: "special" register recording ownership/transactions ("who has what") and events, which gets updated by its mining/user community (distributed) in exchange of a reward. Such register, certified by its community/network, is immutable, and it works thanks to a collective effort.

Smart Contracts: series of programmable instructions (software code) which get executed on the blockchain, with the aim to automatically enforce certain contractual obligations upon the occurrence of certain situations. They can essentially automate any kind of process or operation using the blockchain, this way opening the world of blockchain to industrial adoption.

Trustless protocol: a safe system in which random users can interact knowing that contractual actions will be executed only if certain events occur, with no room for interference or frauds (users trust the system/environment, not someone in particular such as intermediaries, authorities or other users).

Tokens: "units" of value/account of a specific blockchain register, which can represent many things and get an evolving economic value, based on demand and offer.

Security tokens: digital certificates/contracts representing a unit of value of an underlying financial asset (therefore compliant with the relevant financial regulations).

Tokenization: the contractual process by which ownership and / or property rights relating to any underlying asset are split and transported on a blockchain-based digital infrastructure, which allows them to be held and transferred in a transparent, efficient and secure manner.

Wallet: the instrument the user needs in order to interact with a blockchain network (send/receive), and where tokens are safely stored (hold).

Liquidity pool: essentially made of (i) a certain amount of tokens and (ii) a corresponding amount of FIAT currency or stablecoin, it represents a "synthetic" counterpart able to execute trades. The pool can be created by one single counterpart as well as by multiple counterparts joining forces.

Stablecoin: a cryptocurrency whose value is linked 1:1 to a major FIAT currency, like USD. Backed by "stable" assets such as the US dollar, were created to address digital asset volatility. These are the closest example of digital FIAT currencies and will likely be replaced by "official" Central Bank Digital Currencies ("CBDC") over the next few years.

DEX® FINANCIAL DIGITAL EXCHANGE

Contacts: info@dexx.finance

THANK YOU

A LOOK LATERAL GROUP COMPANY

LOOK LATERAL