INTERNATIONAL INSURANCE SOCIETY

Affiliated with THE INSTITUTES

Decentralized Finance (DeFi) – Risks and Opportunities for Insurance Industry

ABSTRACT

Decentralized Finance (DeFi) or “open finance” is the automation of the financial industry sector based on exponential blockchain technologies, removing counterparties and shifting risk to technology. Currently $2 trillion USD in digital currency exists under management [i]. Insurance organizations will see new digital asset classes coming to market, bringing higher returns with a different risk landscape. This also brings a threat of new entrants, outside of the insurance industry, who may bring an alternative embedded risk approach, providing challenges as regulators align with this unfolding innovation across different jurisdictions.

The insurance industry has tailwinds to get higher investment returns from new asset classes in a deflationary environment and faces headwinds to protect against liability of failure of smart contracts, the software programs driving the transactions on the blockchain. DeFi is a substantial new line of business and will bring new premiums and protection products to market. This is a beneficial development for wholesale/retail consumers and regulators will look to strike a balance between automation of the financial sector and what human touchpoints remain in the process. It is early days but there are many moving parts leading to noteworthy changes over the next decade. This will reDeFine the way the world trades in business, makes payments, handles insurance claims and addresses financial inclusion in developing markets, all happening in parallel with central bank digital transformation which poses a balance between centralized and decentralized regulation.

The DeFi community is based on blockchain (digital ledger) focusing on principles of data integrity, digital identity, community consensus, mutuality, democratization, trust in data sharing and an immutable single version of the truth. Many applications or protocols exist and interoperability between them is paramount for mainstream adoption to increase demand in value of interchange of digital assets known as the INTERNET of VALUE (IOV) [ii].

Investment markets are being digitized using Automatic Market Maker (AMM) software using cryptocurrency and automation of banking functions using Digital Exchanges (DEX). In parallel Central Bank Digital Currencies (CBDCs) are being created by governments. DeFi and CBDCs are DeFining the “Future of Money” bringing more market trust and transparency.

INTRODUCTION

Evolution of cryptocurrencies after the 2008 Global Financial Crisis (GFC) triggered DeFi. BITCOIN (BTC) emerged in 2009 as a mechanism to create digital money outside of central bank control with blockchain as the underlying technology to avoid double spending. Many other cryptocurrencies inherited BTC properties and have evolved through a forking process [iii], an identified operational risk in DeFi. A significant development after BTC, was the emergence of Ethereum [iv] in 2015 when practitioners realized that blockchain was more than double spending control but a shift in the way we conduct business, adding to the IOV.

Ethereum also has digital currency, Ether (ETH), but expanded from decentralized payments to digital full stack architecture built on blockchain powering tamper-proof decentralized applications (dApps) which can run without potential downtime, fraud or interference from a third party. Like BTC, ETH is stored in electronic wallets and traded via online exchanges in the form of currency tokens. BTC was created as an alternative to national currencies as an exchange medium and store of value, Ethereum and peers are taking it to a new level to automate the financial industry via digital currencies using open source software.

Ethereum has been the platform of choice to date for the DeFi industry with entrants such as SOLANA now emerging. There are many strategically important operational platforms and distributed ledgers that are utilised in blockchain architecture which do not have currency tokens such as Hyperledger Fabric and R3 CORDA, so interoperability is a key factor.

It is burdensome to have 20th century regulation for 21st century technology but unregulated entities can create a “crypto wild west”, subject to arbitrage and abuse, so a balance is required between self-regulation and imposed regulation by government. BTC is gaining acceptance among regulators, government bodies and is formally recognized as a mode of payment and store of value in some countries. DeFi is regularly scrutinized based on events in cyberspace, seeking standardization and proof that the current financial system is not being replaced or disrupted by a libertarian ideal but is positively transforming cash and complex derivatives to a “tokenized” alternative with identity, trust, proof of ownership, data and cyber integrity. Regulation directs the financial services industry to create permissioned assets that have identity embedded for KYC (know your customer) compliance. Cash transactions can still remain incognito but auditors can reveal identities if required. This confluence between the anonymous, permissionless public blockchain used by DeFi and the permissioned identity based private industry blockchain, shows a need to interoperate to get acceptable open finance whilst preserving privacy at all times. The development of interoperability standards are paramount to take DeFi forwards and overcome challenges of ecosystems operating in silos.

Whether you are customer, provider or regulator the holy grail quest is the same namely asset classes with a higher rate of return and search for more yield within a proper risk framework. DeFi, which includes the Non Fungible Tokens (NFT) boom, is a source of these new asset classes. Using a process known as yield farming, investors and lenders lock up cryptocurrency tokens in exchange for trading fees to get higher returns at higher risk. This paper will not cover the in depth mechanics of DeFi and refer readers to an excellent primer by Wharton School [v]. It will however attempt to bring together the opportunities, risk, challenges and future possibilities of digital finance including the dovetailing of DeFi with emerging Central Bank Digital Currencies (CBDC).

Regulation technology (REGTECH) is the automation of regulatory compliance and reporting and needs to coexist with DeFi and CBDCs, so that regulation can be applied more on a real time basis, before rather than after the fact. This is a key requirement.

Volatility and market fluctuations in cryptocurrencies are barriers to entry. Stablecoins, which are cryptocurrencies pegged to fiat currency or other physical assets, address this volatility issue and also form the basis of the development of CBDCs, which could be on a collision course with DeFi in some juridictions rather than being complimentary. Whatever the future, from cryptocurrency, lending and borrowing, prediction markets, payments, insurance and NFT marketplaces, the DeFi landscape now represents an expansive network of protocols, IP and financial instruments worth at least $100 billion USD[vi].

DeFi is based on principles of decentralization and mutualisation which leads to community peer to peer transactions. Good behaviour is incentivised and bad behaviour, easily identified in a community, penalised. As mutual insurance companies and cooperatives are the roots of insurance plus the whole basis of Islamic Takaful insurance, this will have a notable effect on the future of protection. Community insurance is based on game theory, behavioural science, incentives, penalties and claims assessment voting. Given the importance of the IOV there is still a swathe of the world's population, the informal economy, that has no access to financial services but has access to INTERNET and mobile phones.

Where there are data driven functions and digitization there is systemic cybersecurity risk. In DeFi this is especially true for the external data pricing feeds and outside data influences that trigger smart contracts to trade, borrow, lend and pay claims. Emergence of bespoke parametric insurance acts as a safety net for DeFi ecosystem, network and protocol liability. Paying a premium to protect against smart contract risks, exploits and frauds creates mitigation for crypto investors who require real time, innovative, and scalable insurance. Smart contract approaches will transform insurance markets as they are not reliant on human involvement but initially there is likely to be hybrid versions of contract automation with human intervention before full adoption which requires legal and regulatory approval.

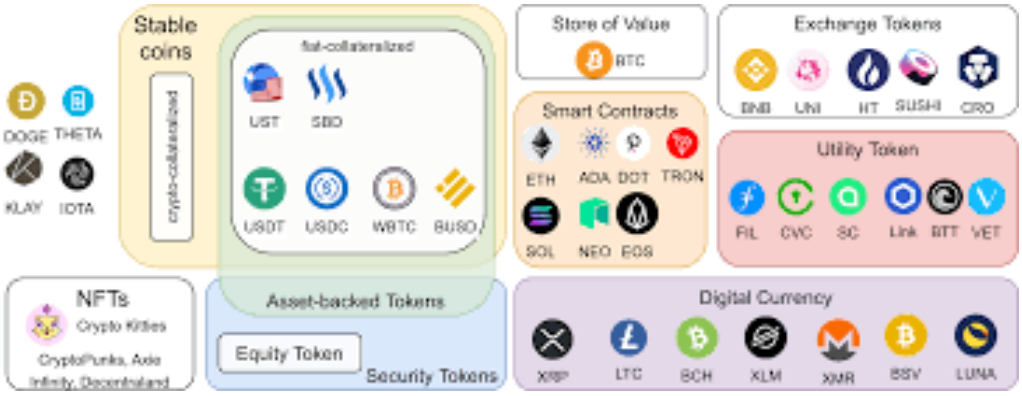
Hack attacks and accidental forks occur in protocols and users want a hedge to protect themselves. Traditional insurance offerings currently do not address this need, forcing the sector to self-insurance techniques beyond captives. Yield farming moves crypto assets frequently between different lending marketplaces, operating 24X7, to maximize returns and is currently unregulated, permissionless, no custodians/middlemen and open to anyone with a smart contract, internet connection and a wallet. Regulators are looking at this process and investors keep track of metrics using DEFI PULSE [vii] and DEFI LAMA [viii] dashboards.

Regulation has yet to fully enter the DeFi space. Intervention is expected on several components such as Stablecoins and scope of liability. Given their decentralised nature and potential global reach, DeFi insurance and alternative risk coverage dApps pose interesting legal and regulatory challenges on a jurisdictional basis. Several digital exchanges are under investigation and there is a possibility of political intervention as CBDCs may be seen as an alternative to DeFi instead of complimentary which would result in digital currency being centrally controlled and the current legacy financial system staying in existence a lot longer than consumers desire. This would be not be a good outcome from a technological innovation, which is now out of the lab environment, as the world, in the throes of pandemic, fiscal stimulus and a deflationary decade, looks to digital assets as the new money over old.

ROLE OF DIGITAL TOKENS. (TOKENOMICS)

Every day we use physical tokens such as paper money, air tickets, theatre tickets, door keys. We also have incentive tokens like air miles and loyalty points. These all have an equivalent in the digital world to tokens whose links to real world assets is the harbinger of change. DeFi consists of digital tokens which are programmable code (smart contracts), and there are many kinds of tokens existing with functions well beyond currency such as those which pass from device to device in the IoT [ix](Internet of Things). Tokens can embed insurance and as digital asset classes emerge for investment it is essential that risk management principles prevail. Token design properties can mitigate expenses, fraud, remove paper trails and third party touchpoints from the value chain. With

this enhanced profitability investors in the asset class will see a de-risking of liability with fresh global market places creating liquidity via digital asset exchanges. Tokens are tradable application programming interfaces which makes them work for purpose. Just to illustrate the varied token landscape the following diagram from Martin Thoma illustrates the diversity of tokens. [x]

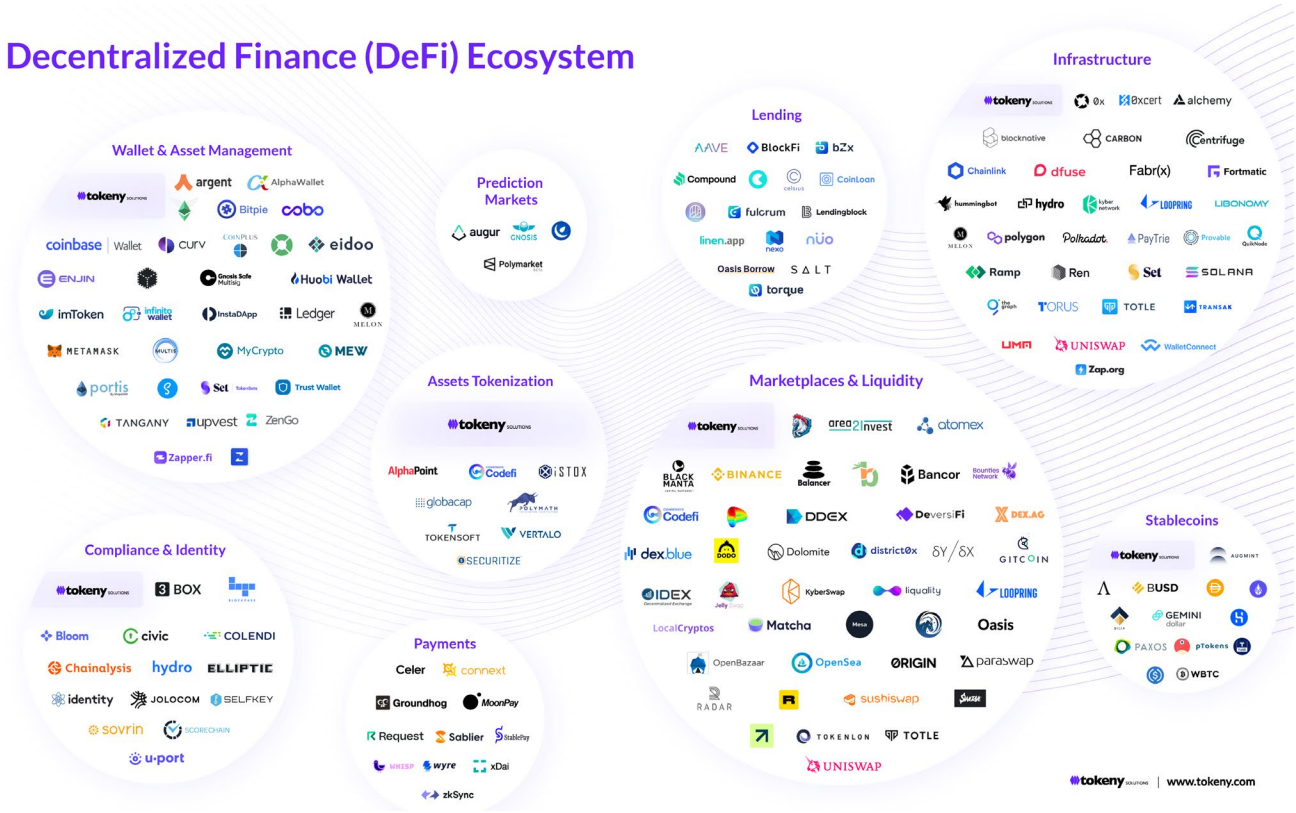


Incentives such as trading fees reside in DeFi to motivate investors to onboard, exchange tokens for rewards, farm yield and not hoard assets. Digital currency value increases on user acceptance. If paper money loses its belief it becomes just paper. BTC stores value but DeFi exchanges value where tokens are the digital money required for completing financial transactions and controlling governance of participants. Tokens are housed in electronic wallets, providing custody and reconciliation. Protocols designed on blockchain control issuance, supply, pricing, scope, consensus and governance whether it be borrowing, lending, trading, asset management, derivatives or insurance. Properties designed here shape the token amount issued, how they are deployed, destroyed or refreshed in an economic life cycle.

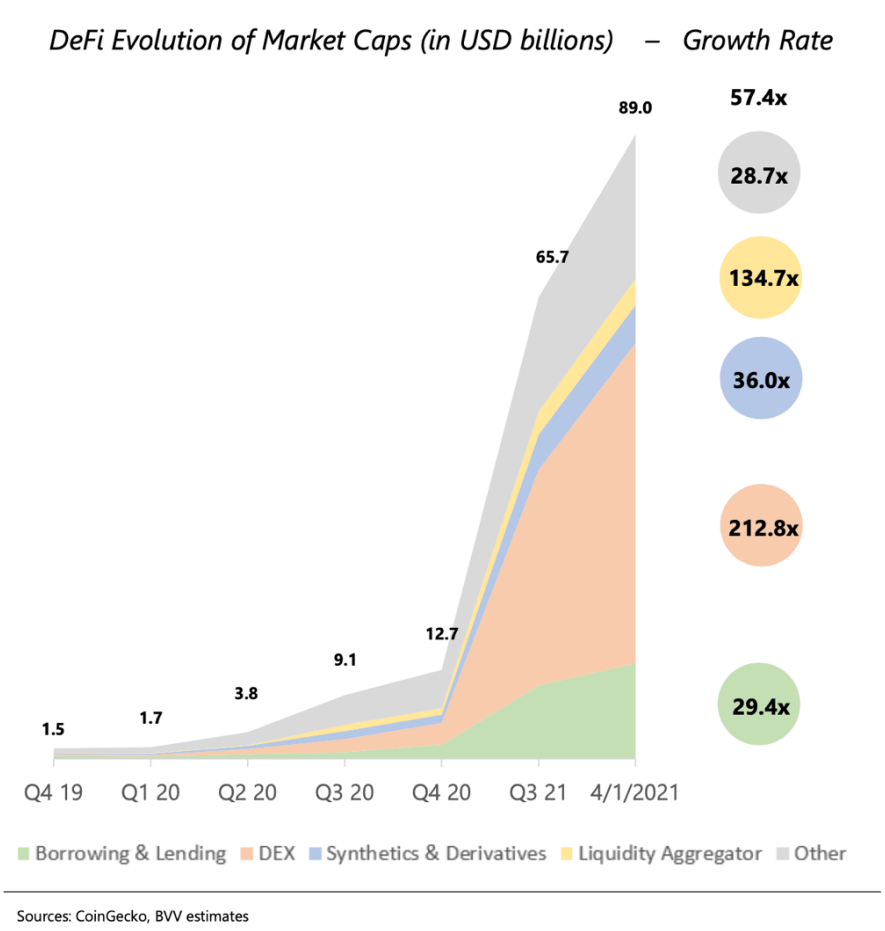
Digital currencies are volatile, changing in price dramatically and not directly linked to any geopolitical event or bull/bear market. Investors look for assets to give higher returns, up to 10X or more, especially in bear markets. Currency tokens that are limited addition are deflationary as they decrease in supply but increase in price, so investors will buy as the tokens store hedging value. Investors need incentives to trade them. Strong demand in BTC, ETH and others gives a strong future hedge for investors. Demand dictates the token's price. Conversely, they can be inflationary where unlimited tokens are issued (similar to quantitative easing). Overall, these currency tokens become interest bearing smart contract tokens based on supply and demand economics. Investors will look to long term yield to earn interest selected from the best protocols available. To achieve such value, reserving of digital tokens is required and collateralized Stablecoins fill that role. It is still to be decided how reserving is going to be achieved between over collateralization in DeFi or CBDCs.

OVERVIEW DEFI

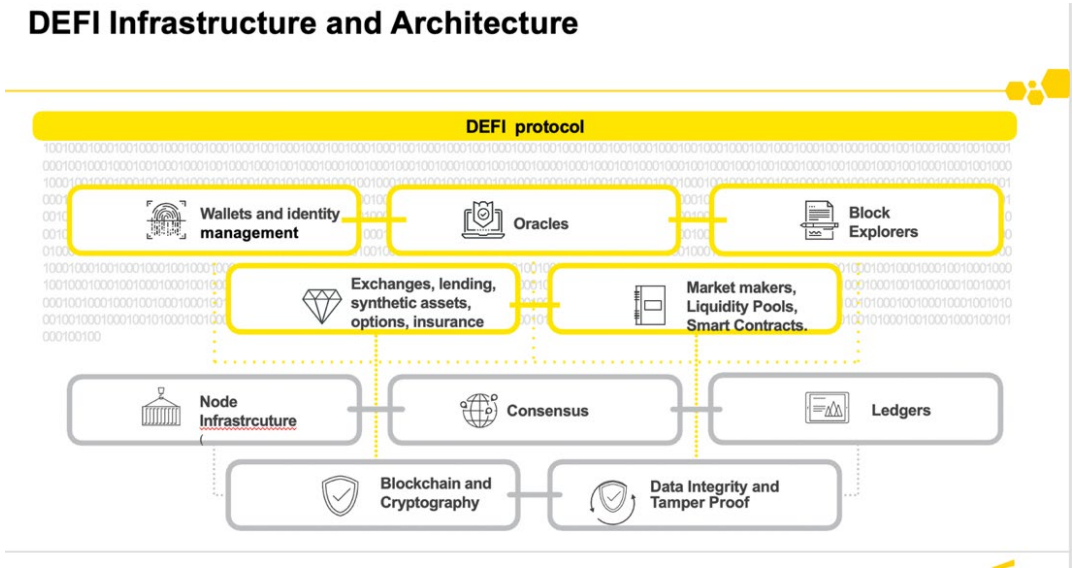
DeFi relates to a shift from centralized financial systems to peer-to-peer finance and fuelled by the pandemic digitisation acceleration. The Tokeny diagram below shows the growing protocol landscape. The functions of DEX, AMM, lending/borrowing platforms and Stablecoins, need to be understood in the context of yield generation within the realm of risk management. Custody of tokens moves to personal wallets and security to smart contract technology with less need for repetitive Know Your Customer (KYC) as everything is fully audited on the blockchain. Features shared by protocols are open source, transparency, interoperable and composable (programmable by plug points), and permissionless. So open and accessible to all on a public blockchain for audit/verification and non-custodial, which means users control of their wallets and also their own liability. All transactions are visible via blockchain explorer applications so reconciliation and clearing can be done in real time. Interest is calculated, paid and compounded continuously.



New markets are created via AMM with crypto assets traded through DEX. Holders of cryptocurrencies lend anonymously, generating interest returns in an automated manner via smart contracts for credit intermediation. Derivative trading markets for digital synthetic products can create positions held in cryptocurrencies. To compensate the risk, staking is accompanied by over collateralization. DEX match buyers and sellers of digital assets to allow an atomic swap of cryptocurrencies and DEX aggregators operate to offer the best possible deals across the whole landscape. Users then fund liquidity pools with owned crypto assets to facilitate trading on these protocol platforms while earning passive interest on deposits through liquidity aggregation. Insurance, asset management, external data flows and other functionalities complete the ecosystem giving high growth patterns shown below.



As new markets are made and digital assets created there has to be liquidity where yield can be farmed. Depositors who invest crypto assets into the pool automatically receive a liquidity provider token (LP) indicating their share of the pool. By linking markets and liquidity pools together a network effect is achieved [xi] as assets only have value to those who have access. Pools are not new and are the basis of traditional finance but with DeFi they are open and transparent to all whitelisted users. The diagram below shows a logical architecture.



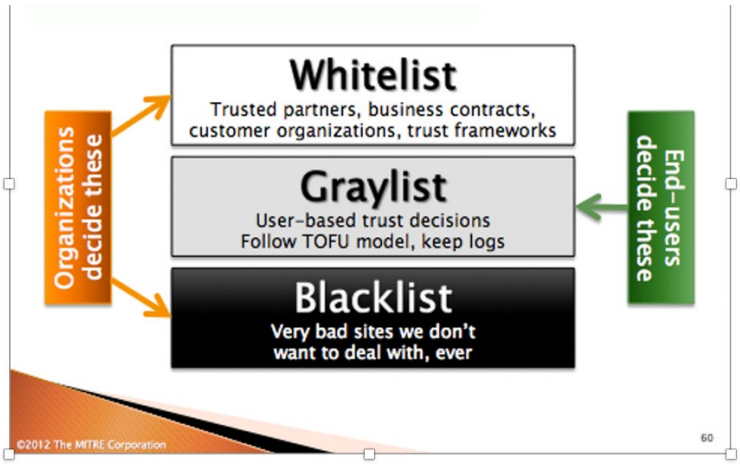
Creating liquidity, where anyone with funds can be a market maker, comes with a risk that the price of tokens deposited can drop and cause loss of value. This risk is mitigated by collateralized Stablecoins which peg back volatility in the trading pools. Collateralization is key to building out an insurance reserving infrastructure. Decentralized liquidity pools are a key innovation in DeFi as they maximize efficiency and lower costs while maintaining an open-source single version of the truth with blockchain security and immutability.

DeFi has its own metric to measure profitability, the Total Value Locked (TVL) and represents the number of digital assets that are staked (locked up) in a protocol for a specific period thus creating a stable, secure network in return for rewards. TVL ratios are calculated by multiplying the supply in circulation by the current price to get market cap and then divide by the overall total issued which determines over/under valuation tracked by DeFi Pulse.

Token holders perform self-governance on the network voting on issues that need resolution. One of these is known as “crypto mining”, a process where computational power is used to gain concensus to avoid double spending. This causes scalability issues and usage fees known as “gas” which are burdensome. The current process is a drawback to mainstream adoption of DeFi partly because of slow speed and high cost but also for the use of electricity, an antithesis for ESG in financial services, which needs immediate correction.

Flash loans are used by DeFi traders looking to profit from arbitrage opportunities when two markets price a cryptocurrency differently. The loan takes place within a single transaction so the difference can be collected in almost real time. If the lender and borrower do not follow the rules of engagement the loan is not issued and the smart contract will roll it back as the condition to transfer is not met, and the money will be returned to the lender. It is good to register this risk, for if the smart contract is breached the loan amount, often large, could be lost in the process and this has been a cybersecurity event in the past.

We are now at the crossroads of regulation and acceptability of permissionless trading and digital identity on how tokens are issued. The Initial Coin Offering (ICO) of 2017 have been mostly replaced by regulation to Security Token Offerings (STO) based on a litmus test on whether a token is considered a security and subject to security regulations. The DeFi landscape also has Initial DEX offerings (IDO) enabling tokens to be sold directly to the public creating a need for KYC and whitelist capabilities. Before banks and financial institutions can get involved in automatic anonymous lending, permissioned versions of DeFi will have to emerge and with it, a system of whitelisted and blacklisted wallet addresses as shown below from MIT Media Lab [xii]



DIGITAL SECURITIES AND DEFI

Today untokenized securities are held in electronic ledgers managed by financial institutions in a complex custody chain making it difficult to see all asset class holdings plus reconciling portfolios is done in a settlement process using SWIFT, but not in real time.

Security tokens and cryptocurrencies differ. The latter are decentralized with no issuer. Created on the network, held by investors in a wallet, they are permissionless tokens connected to smart contracts. If private keys become lost, then they are irretrievable unless put in an off chain cold storage hardware device [xiii] which can then be used to obtain insurance cover. Each investor gets a receipt token to show the assets they have locked into in the pool and regulators are questioning whether this receipt is a security.

Security tokens, by contrast, are permissioned digital representations of securities approved by regulators where security laws apply and are blockchain registered debt instruments with an issuer liable to investors and regulators. Dividends, stock splits and other management tools are embedded in smart contracts in order to change and manage the custody process.

Digital regulated securities need to be connected to DeFi markets to make these assets mutually available through market making, liquidity and collateral, as programmed interoperability creates connectivity. DeFi drives liquidity and arbitrage opportunities for digital securities which in turn must follow token rules to access DeFi protocols. Digital securities are regulated and have some centralized functions with intermediaries to their wallets. DeFi requires the digital securities to be placed in a smart contract to obey the pooling of assets. This raises identity concerns as capitalization tables maintaining the digital securities are held off chain and must be able to identify securities in the pool.

Here lies the horns of a dilemma. Public blockchains used by DeFi are open to all and the permissioned private blockchains are closed to business ecosystems. Blockchain was not designed to create API interoperability, rather to preserve integrity and privacy, but the value must be unlocked to the wider audience of investors to meet the yield and increase IOV as private blockchains, although secure, operate in silos which risks broader user acceptance.

The solution lies in properties of blockchain to secure digital identity and keep that identity cross chain and off chain. DeFi needs the capability to do security token issuance, meeting regulatory requirements and any centralized functions required. This oversight makes sure only eligible counterparties access the security token. Smart contracts hold the total number of shares issued in the various wallets so they can be reconciled on the blockchain. All the investor positions and compliance are visible on the same ledger. Proof of token ownership and visibility to other token holders is there to see if one member of the ecosystem moves to a sanctioned country. However, investors cannot be caught up in this centralized versus decentralized crossroads for long and regulators need to adapt to interoperability and move away from CSD's (Central Security Depositories) which fragment across jurisdictions.

Investors want more yield, transparency, proof of total supply, limit orders and trust especially as a global audience of investors is reached. Public blockchains seem high risk for financial institutions due to perceived loss of control. However, to achieve the IOV goal we need to accept that blockchain creates identity, integrity, trust, an attributable INTERNET and mutual auditability in a decentralized environment and when implemented correctly a blockchain is inherently more secure than centralized servers. In tandem bad actors must be mitigated from entering trades and move to blacklisted repositories. This mitigation will also address detractor concerns who say DeFi encourages terrorists and fraudsters.

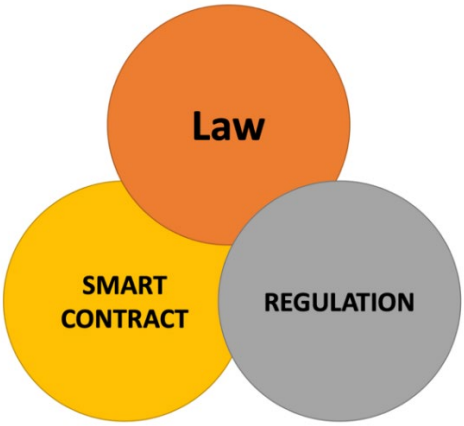
UNDERSTANDING SMART CONTRACTS

Smart contracts are irrevocable computer programs deployed on a blockchain that execute a set of pre-DeFined instructions. They are the basis of the DeFi ecosystem as tokens are themselves a smart contract. They operate with great similarity to an insurance parametric product where a pre-agreed policy event is triggered from an independent data source to pay a claim. These smart contracts can be simple with one condition or multiple conditions. A complete digital corporate entity can be built on the blockchain known as a Decentralized Autonomous Organization (DAO) consisting of multiple smart contracts and could comprise a digital mutual or cooperative organisation. The more complex the DAO the more risk of operational failure but as this is embedded on the blockchain all events are logged, immutable and provide a single chain of custody. DAO's make up the components of DeFi.

Smart contract failure due to program flaws is a major risk in DeFi and there is a good opportunity to address this risk with insurance solutions. This risk is mitigated by the open source nature where multiple developers and testers approve the code before release. Derivative platforms depend on well-functioning smart contracts governing the transaction. For this reason smart contracts must be frequently audited, tested and warranted.

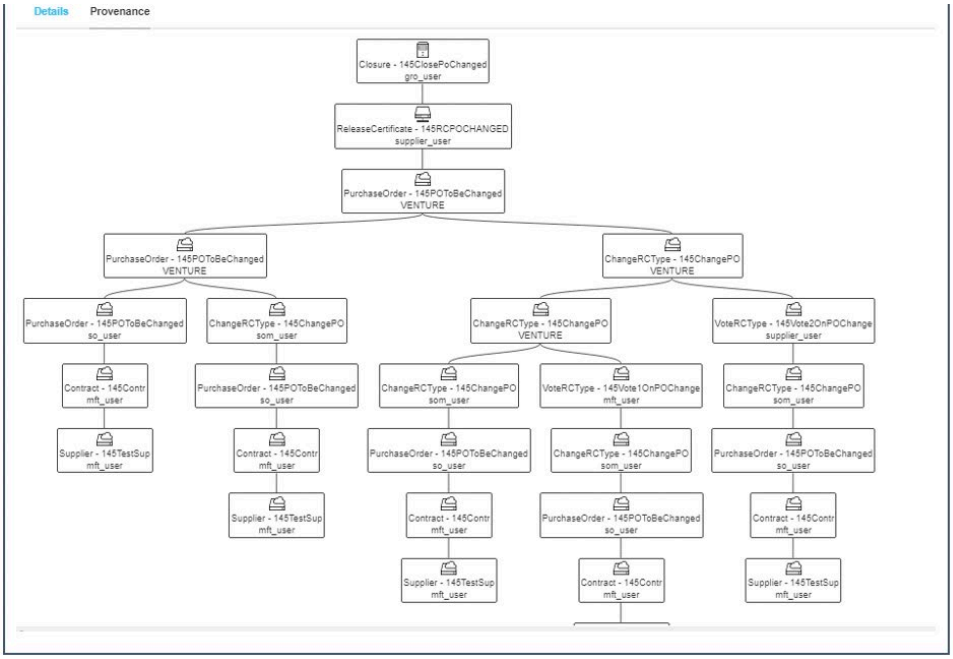
As insurance adapts to protect intangible assets it is the smart contract code that is not performing, rather than people, and parties participating in the development could be held liable to class actions if the outcome is not what is intended. This is known as basis risk where an action is triggered when it should not have been or vice versa. Smart contracts interact with independent data feeds known as “oracles” which trigger transactions on the blockchain. Data integrity and provenance of these feeds is paramount as they price assets and pay claims. These data feeds must have data availability, meaning the external data must always be accessible. They can be looked at as the application program interface (API) of blockchain often called the gatekeepers to the outside world.

Smart contracts are a crossroads between law, regulation and information technology and the standardisation still needs to mature with political understanding. Legal and regulatory objectives must be addressed so the smart contract becomes legally binding and enforceable.



The operation of smart contracts is a distinctive risk for insurers. Developers deploy open source code but have no liability when it fails. Investors put funds at risk without assessing the risk involved. How do insurers know who is liable when a smart contract fails? Data integrity and provenance must be applied to the triggers of the contract, creating a trust mechanism. Clients can opt to protect a protocol from this risk and receive a premium in return. There needs to be a complete data provenance on the code of the smart contract and on the external data feeds that trigger them. Insurers and auditors need to go to an independent repository so we can track, if necessary, to the first line of code written and checked by a developer. This is exacerbated when operating in multi cloud environments.

Data provenance is the history of data assets from the origin through the whole life cycle of the data showing who accessed it, how, when it was used and has it been tampered. When stored on a blockchain as a cryptographic event, it is possible to create a provenance graph to see who was liable as forensic evidence shown below. This increases data transparency and enforces data integrity. Privacy is preserved at all times as actual data is not stored on the blockchain only hash key identifiers to the real data stores. Every smart contract should have data provenance enforced and this should be a warranty for the insurance policy.



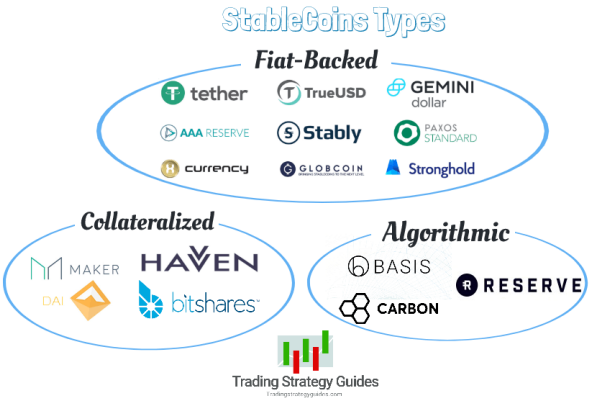
Smart contracts are composable and can be linked to each other via programmable interfaces. This means that an entire DeFi automated system is being built in the open domain by software developers which will bring legal challenges if an automated payment was incorrect, with no delay in place for human checkpoints and intervention, to withhold payment or verify the payment triggers. This could lead to litigation expenses, the very thing that parametric insurance is intended to reduce, so it may be conducive in the early days to build in pause conditions to the smart contract to mitigate basis risk before payment.

Data provenance and tamper proof techniques must ensure that data is protected from internal errors or external malicious attacks using real time alerts and tamper proof techniques. When an oracle provides external data to the blockchain, the integrity of the data should be guaranteed so that dApps can execute flawlessly in minimum response time. Malicious oracles tamper data or creates fraudulent activity on import of external data to the blockchain. This is a serious risk and should be mitigated by insurers before offering cover.

STABLECOINS and CBDCs

DeFi has created debate about trust in money, faith in machines over humans and moving away from central control. This centres around a triad of cryptocurrencies, Stablecoins and CBDCs all intertwining as the future of money. The differences are critical as regulation may deflect the course of the debate as some central banks may seek to counteract DeFi.

Cryptocurrencies are volatile and price fluctuation makes them, today, unsuitable for daily use, especially in insurance reserving and life insurance which need a digital asset that remains stable over time. As volatility market risk mitigators Stablecoin tokens are pegged to a less volatile asset such as gold or fiat currency (1:1) or baskets of unrelated currencies creating higher yield and low inflation. DeFi markets pair cryptocurrencies with Stablecoins to protect trader and investors during volatile markets. Traders can protect their positions by moving cryptocurrencies to a Stablecoin. Traders can also increase their crypto holdings by entering or exiting the market using Stablecoins without converting them to a fiat currency.



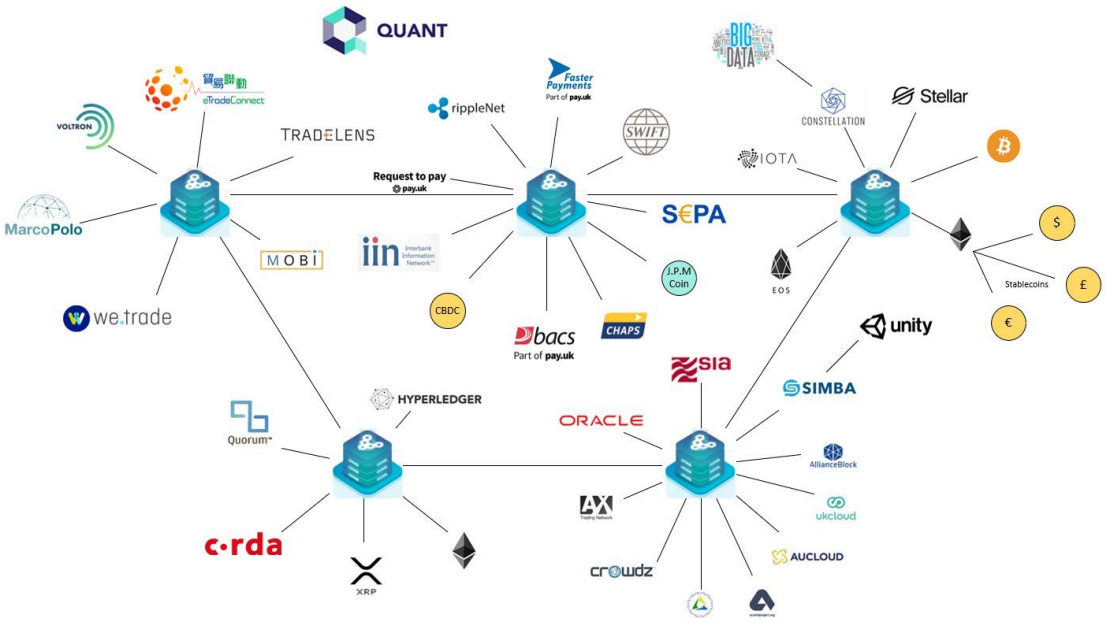
Stablecoins can be collateralized by fiat currencies, crypto currencies, commodities (gold) or no collateral at all. Regulation will determine the degree of decentralization allowed. The long-term purpose of these tokens goes beyond financial contracts to the evolution of payment systems and a new form of digital money controlled algorithmically instead of centrally, offering similar monetary benefits as fiat currencies. Conversely it can also be used for reserving in a CBDC. Stablecoins work with smart contracts and the software code automatically dictates the terms of the agreement and how and when money will be transferred. This makes Stablecoins the basis of stable collateralized programmable money. The transparent nature of blockchain based financial applications limits the downside of creating complex derivatives like CDO's (collateralized debt obligation). The risk profile of the DeFi lending app is far different than the reasons CDOs became a systemic risk during the 2008 global financial crisis when they were packaged with mortgage and credit risk.

CBDCs sees the central banks getting involved in digital money and motivations vary across jurisdictions where some governments are trusted and others not. Central banks that combine a scalable, provable, blockchain based platform as a value-based CBDC money scheme will achieve the best economics as it secures against both internal and external attacks on the system integrity and allows continuous mathematical verification of the total money supply. These deployments are designed to be resistant to potential attacks by cyber hackers and encryption failures because of lack of quantum immunity and compute.

However, CBDCs revolve around control of commercial digital payments with no investment value and are based on a private permissioned blockchain. Whereas DeFi are public, anonymous, permissionless blockchain networks and also act as digital assets and online currencies. This means that over regulation could threaten the very development of the digital asset returns widely anticipated, if it led to suppression or outright bans of DeFi, which is already in production and generating yield as investment platforms. Currently CBDCs are mostly in proof of concept or development mode but are progressing at an exponential pace on all continents. Sensibly, with proper interoperability standards, both can exist with the right level of regulation and most importantly DeFi is not seen to have been over regulated just because it is a potential competitor to CBDC. The two prime directives of blockchain are data integrity and interoperability and should be applied here free of geopolitics.

Hyperledger blockchain technologies are a significant player in driving CBDC projects into production for the automation of retail payments, cross border transactions, sharing digital currency amongst central banks, wholesale payments and at all times preserving privacy. This is a gaining traction on all continents and 2022 will be the launch pad for many of these innovations. As Hyperledger is open source technology and does not have crypto currencies or tokens it is a good choice for the central banks to build their permissioned blockchain platforms and can also interoperate with the Ethereum based protocols. The Bank for International Settlement [xiv] is central to the global development of CBDCs. They are involved in the launch of a cross-border central bank digital currency system as a proof of concept across multiple countries to make instant payments in a variety of currencies taking advantage of DeFi concepts. [xv]

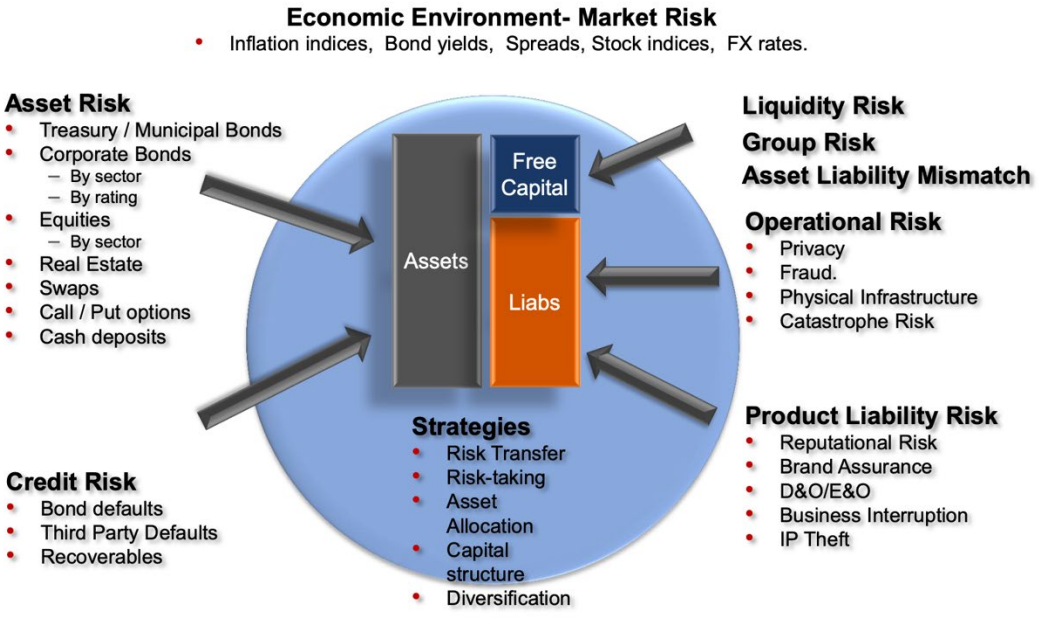
Asia, which leapfrogs in technology due to less legacy, may drive many of the CBDC proofs of concepts with government backed digital tokens using Stablecoins as reserving for stability. However, the impact in the short term is predominantly in the wholesale area and less so in retail areas which will take a longer period to evolve. Many initiatives are to assist with financial inclusion where there are unbanked communities and low insurance penetration. The following diagram show how the various parts can be connected for efficiency and this would be best practice.



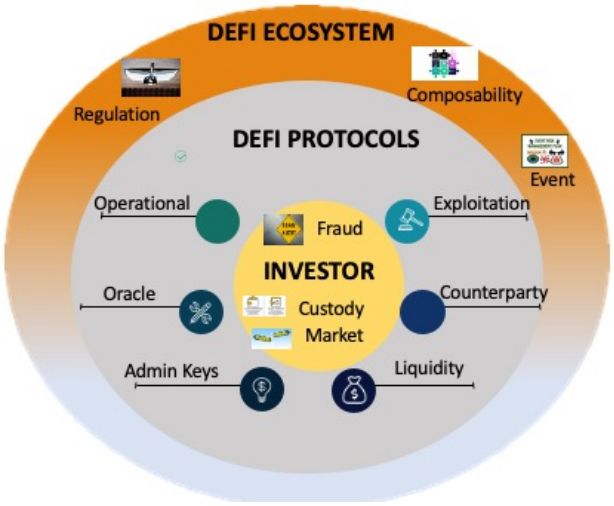
Source : https://twitter.com/cryptoseq/status/1237829840365068290

RISK MANAGEMENT

DeFi is a new line of business and by DeFinition a new risk sector with particular risks differing from the traditional financial sector and covering intangible risks. It will require modelling and correlation like other sectors but will have the advantage of real time granular data reducing the dependency of assumptions made in risk modelling. The following diagram shows the risk landscape as we perceive it traditionally pre DeFi evolution.



This is a centralized model where intermediaries and third parties perform risk analysis to match the assets with liabilities. Much of DeFi has similar categories, including puts and swaps, but the risk shifts to the technology as in the smart contracts and less to a human counterparty risk. The risk model moves to a decentralized ecosystem model as shown below. Like all risk assessment, frequency and severity of events drive the protection landscape and the parameters of the modelling.



The risk here is threefold - to the ecosystem, to the protocols and to the investor. Regulatory risk looms as regulators are starting to look at the sector with some exchanges under investigation or banned in some jurisdictions. There is a need to be compliant. As DeFi ecosystems need to interoperate, the composability technology (sidechains, parachains, bridges, crosschains) that links protocols, this presents a risk as these standards are still developing and each protocol has a different software code base. Jurisdictions need to be crossed and recent CBDC developments add to the risk. Event risk can occur on any financial market such as the Wall Street crash or Global Financial Crisis.

Technical or operational failures categorise most of the risk as DeFi is a digitized and automated investment sector based on software protocols. Smart contract and oracle failure needs to be mitigated by extensive audits, standards, testing and open source principles. Data integrity and provenance should be a warranty for the insurance but data accuracy is in the hands of the protocols and the investors, so the latter need to manage their personal risks. Updates and configurations to protocols needs to be applied on a regular basis to avoid any accidental forking of protocols [xvi] which can cause double spending or exploitation loopholes. That said, blockchain is known for trust and security, and technology is quick to fix. Custodial risk (security of keys) occurs where protocol developers hold “admin keys” that are used to push upgrades to the protocol and a risk exists from bad actors. Security of admin keys are operational security that can be compromised due to human error.

Regular audits should be carried out, some in real time and recorded incidents to date have been caused by smart contract bugs, oracle manipulation, whitelisting impostors, theft of digital assets, minting of unlimited tokens and hacks on flash loans, wallets, random number generators and voting. There are multiple attack surfaces and a good security posture is essential. Many attacks are carried out by white hat hackers who often become employed by the organizations they hacked. As DeFi uses economic incentives that are used for users to perform self-regulation and governance, failure of these tenets could lead to a bad outcome.

The investors that purchase insurance or risk tokens buy and take a percentage of risk in the protocol. They are rewarded with a higher rate of return on their principal purchase for taking the risk. Each insurance contract token has a short-term duration and a premium. They are deploying high-risk strategies to seek out yield involving lending, borrowing, liquidity mining or any other means. In the digital asset market with no intermediaries, investors take and shoulder risk. The market risk of having a negative result in investment based on asset or market price volatility is present in DeFi, just as in

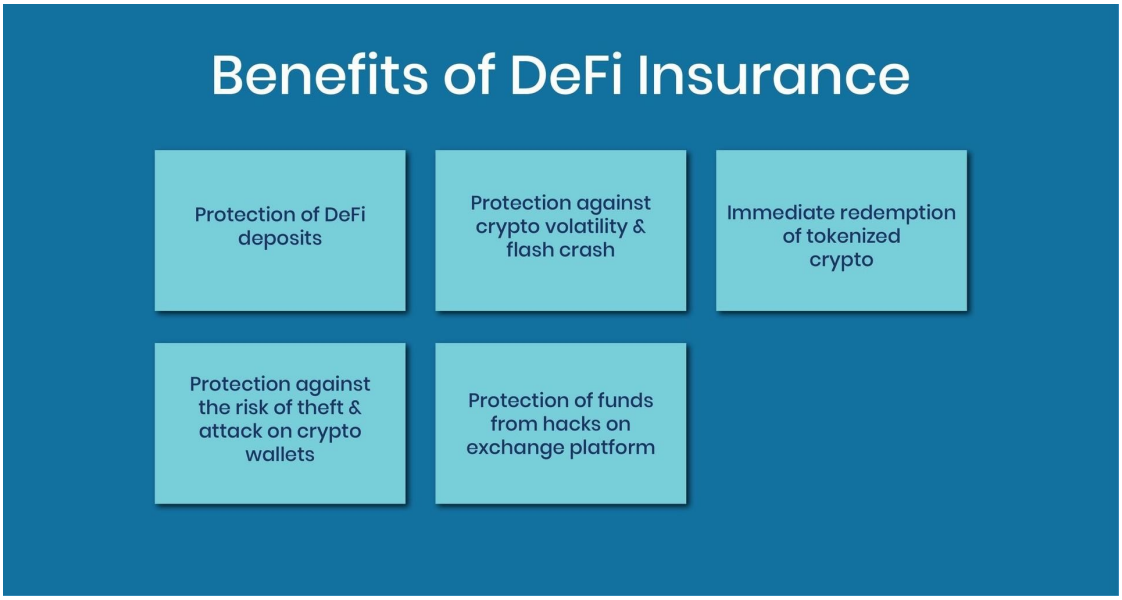
conventional markets, as crypto is universally known as a volatile asset class open to hacking, arbitrage and market manipulation.

Legal risks question the enforceability of smart contract liability, data privacy laws, intellectual property (IP) by ensuring that dApps being developed do not infringe others intellectual property rights (as managed by IPwe [xvii]), building arbitration and dispute resolution into smart contracts and consumer protection in general. Audit issues around tax are also pertinent as when data becomes a tangible asset it is liable for indirect tax.

There is a need to get risk adjusted premium income for insurers and liquidity providers which requires stochastic modelling in order to price the risk charge. However, this requires access to prediction markets as well as historical event data. The correlation between the risk run in investing and the performance of the investments is known as the risk-return trade off (higher the risk, higher the reward). Running predictive scenarios prior to smart contract development will assess the worst case scenario so we can mitigate in the crypto world that assets always exceed liabilities. DeFi should not be bucketed into general operational risk.

DEFI INSURANCE

Technology aside, today's finance sector is based on a centralized authority. Decentralized finance is the antithesis, meaning that a network can make its own decisions based on a consensus of participants. This moves the trust back to the community from insurers while maintaining the integrity of the contracts and mitigating any form of risk. This autonomous shift means that what a third party accomplishes now is done using mathematical techniques and tokens working for the mutual benefit of each community member participant with the help of specific incentives or cost reductions. It requires adaption and understanding.



Source:https://blockchainsimplified.com/blog/decentralized-insurance-an-emerging-sector-in-DeFi/

Decentralized insurance allows for public trades leading to issues around privacy and the autonomous nature leads to a perception that users cannot change their information or interact directly with their data. This has led to disputes and fraudulent cases in the industry as immutability is a crucial part of the blockchain technology. Data is not stored on the blockchain layer but on distributed ledgers and legacy data stores. If ownership of data allows, then access to data is permissible and the blockchain keeps an immutable audit trail of events by hash key. The "right to be forgotten" of privacy laws is not violated. With $2+ trillion of digital assets in circulation and $100 billion of DeFi intellectual property extant, the values at risk has greatly increased making access to (re)insurance capacity a critical need.

The traditional insurance market has been wary about underwriting risks relating to the DeFi space especially where the loss is denominated in crypto. Institutional investors are now entering the crypto world so as the emphasis shifts from early adopters to more risk savvy investors so insurance becomes the key barrier for entry of their involvement.

DeFi insurance and alternative risk coverage platforms therefore have the potential to fill the crypto-protection gap and to facilitate risk exposures faced by businesses operating in a decentralised economy. As smart contracts mimic parametric insurance structures already utilised in catastrophe management, it makes perfect sense for insurers to bootstrap these into decentralized systems using the same methodology. The insurance sector is also undergoing a major digital transformation with regulated digital insurers emerging and trading online.

There are 4 insurance models developing for digital asset risk:

- Self-insurance, beyond captives, handled by the ecosystem to protect protocols
- Protection of members via a digital mutual/cooperative approach
- Parametric insurance solutions
- Traditional insurers offering risk capacity in the intangible space

There are many intangible covers emerging but base cover is about smart contract protection that might result in loss of funds or identity from a technology failure. The income to the liquidity markets and the sum insured is the TVL amount created by yield farming investors. These protocol owners are cost sensitive about insurance and are searching for protection covers embedded in the ecosystems, essentially insurance tokens. This is a self-governance approach where participants take a percentage of the risk by staking more tokens for higher yield and they in effect take the risk on technology failure as they have access to the open-source audits of the protocols and likely feel comfortable with the mitigation. Conversely, on the risk adverse side investors can purchase claim tokens which reduces their yield in return for a level of cover. So, in effect investors who want to stay hedged against exploit risk buy claim tokens while others who believe the underlying protocol is secure buy premium tokens. When there is an event the claims process will be managed by the participants (token holders) on the network where they vote on a claim and the majority decides which claims are to be paid and the settlement amount. The losses are not directly aligned to the indemnity but to events aligning with a parametric approach. A reserving approach is taken when insurance tokens are purchased, the majority of the premium is returned to the pool to cover the risk and locked in. The participants themselves become the risk assessors and claims handlers.

Efficient on chain governance of claims processes are required to protect users and protocols to quantify smart contract risk to help determine claim pay outs. Oracles activate smart contracts enabling them to access real time data off chain that is related to real world events that trigger claims. The blockchain can be used to mitigate fraud and provide forensic evidence. Once a smart contract is triggered then the assets in the pool should be frozen to allow claims investigation and assessment. If the claim is successful it is paid and the funds in the pool released. This mechanism raises questions of claims reserving and will no doubt get regulator attention, but it is clear how this approach could be applied in an ecosystem.

An alternative is to utilise a regulated mutual company operating as a DAO where cover is purchased by opt in of members' whose contributions flow into a capital pool which improves the funding position of the mutual. The cover is priced to generate a long-term surplus which is then mutually shared between the membership base. This means the mutual grows as its capital resources steadily increase over time. A good example is Nexus Mutual [xviii]

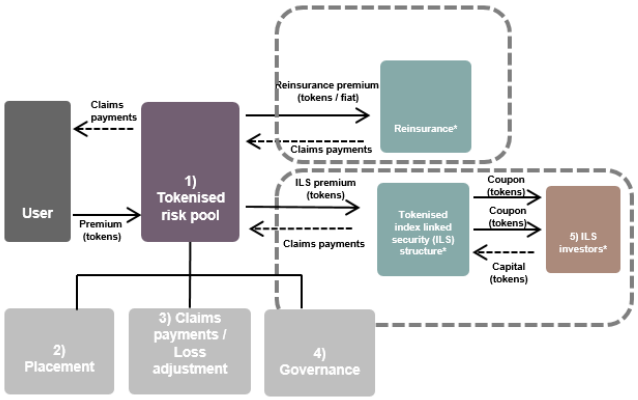
Custody cover will protect users who put funds into an organisation responsible for the safekeeping of cryptocurrency assets private keys on behalf of users. Users are covered if the custodian gets hacked and the user loses more than a certain percentage of their funds, or cannot withdrawal funds from the protocol for a certain number of days. In general, cold storage of cryptocurrencies (held offline) and hot storage (wallets online) are subject to insurance as long as the process to get from cold to hot storage and vice versa is secure.

REINSURANCE

Reinsurance will be a natural consequence of the insurance development in DeFi but will be done in a more automated fashion, flattening out hierarchies, and moving automatically to access the various layers in the reinsurance tower.

DeFi tokens can also be utilised to support a sale of an insurance-linked security (ILS) and any capital market participation will need to be on a regulated basis through well-documented SPV structures that offer investors transparency. It is unlikely that cryptocurrency and digital asset risk will become a significant peril within the ILS market in the short term, but will form a new marketplace for DeFi insurance contracts to raise money from capital markets. If the structures and mechanisms for risk transfer and ultimately securitization are in place, and in the right jurisdiction, then risk could still be transferred using ILS products to capital market investors for whom the returns from an insurance-related digital asset linked to cryptocurrency risk could be attractive.

An illustrative example of a DeFi insurance, or an alternative risk solution model, is as follows:
SOURCE NORTON ROSE



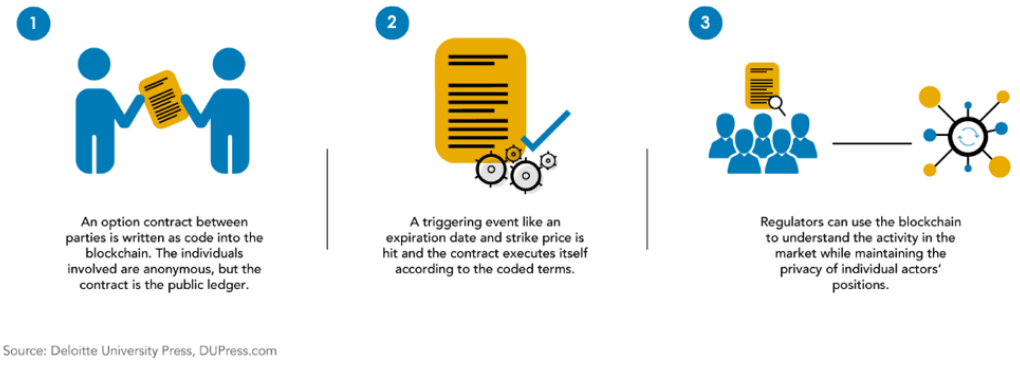
DeFi attracts funding into pools by giving incentives, similar to coupons, in return for staking crypto money for a period of time to cover the risk. These coupons are tokenised and consist of smart contracts containing tokens managed by the protocol. ILS investors earn interest on staked collateralized crypto assets locked within the smart contract without selling the crypto assets. This is very similar to a traditional sidecar based structure. This would be backed by parametric structures using a self-governance claims mechanism described earlier. The digitized insurance market is starting to develop alongside DeFi to provide capacity.

Collateral protection insurance brings together leading crypto-backed lenders to share risks and remove bottlenecks. CBDC developments will also be a catalyst to reinsurance once they become established as government backed issuances.

B3i RE [xix] is an ecosystem company of insurers and reinsurers. It is a blockchain based digital ledger reinsurance placement platform that is capable of structuring and placing reinsurance contracts which are transacted in the market. This gives the ability to automate the reinsurance process by layer using smart contracts. As there is always a single version of the truth, contract certainty is an inherent part of the reinsurance process and B3i ecosystem is available to interoperate with the DeFi networks as the need arises.

NYDIG [xx] are cryptocurrency asset managers and insurance professionals and are new entrants, capitalised with BTC and are an insurance industry world first.

Parametric Insurance is the way forward for digital asset risks.



Source: Deloitte University Press, DUPress.com

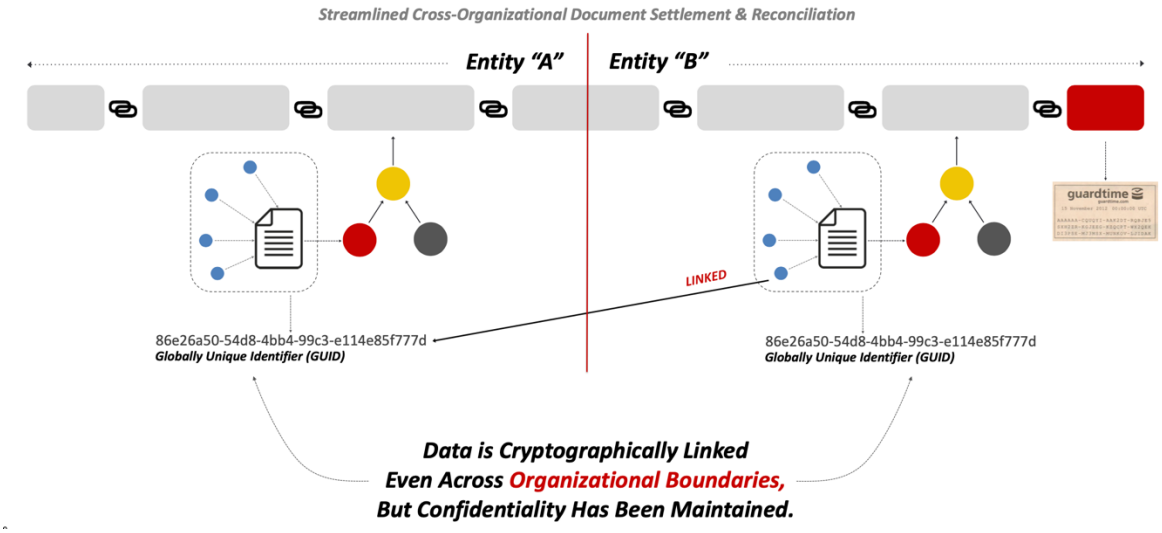
Insurers find it difficult to use traditional insurance covers to insure against potential DeFi and Crypto "Black Swan" events so parametric risk management products are feasible alternatives which would protect specific digital assets backed by Stablecoins using a combination of smart contracts and data feeds.

Smart contracts and protocols can be linked together to form insurance pools in a placement marketplace where underwriters and risk managers/buyers seamlessly interact. Market players decide on which insurance pool is to be used to hedge the crypto risk. A smart contract is mathematically measurable, has formal security and can be embedded in policy wordings. Parameterization in trigger design sets the range of values and conditions for which a policy needs to meet the pre agreed sum insured before the trigger is alerted and a quick payment is made, removing the need for lengthy claim investigations, subrogation, claim reserving and expenses. When DeFi is the line of business, claims investigations also include elimination of network "gas" fees based on time spent in gaining consensus. Parameterization can be complex to DeFine the events and result in nested smart contracts. Procedures would need to be put in place for a delay period if any human interaction was required to approve the triggers to pay the claim and address basis risk.

Since blockchains cannot make external calls due to built-in functionality to preserve security, the claims process requires an additional piece of secure middleware known as a blockchain oracle to bring data on-chain. Oracles retrieve external data on behalf of the smart contract, validate it via unique cryptographic signatures, and broadcast it on the blockchain to be ingested by the smart contract proving the origin of data supplied.

INTEROPERABILITY

DeFi ecosystems should not exist in silos otherwise there will be no scalability, interoperability or transmission of value across different blockchain networks (cross chain). This will afford blockchain networks an effective means of value transmission and settle cross-border transactions. The use of cryptographic hash on the meta data is key as the body of data stays in the country to obey privacy laws but the meta data can cross border and make sure identity is intact and data tamper free. This is especially true as the need to interconnect private, public and consortium blockchains is important. Cross chain, technology on its own has the potential to address scalability issues that have affected blockchain ecosystems since inception.



When a user transfers assets from one blockchain to another using a decentralized bridge, those assets are not moved anywhere. Instead, functionality is leveraged by first locking the assets on the blockchain where they reside using a smart contract. New tokens of an equal amount are created on the receiving blockchain. When the user wants to redeem the assets, the equivalent tokens are destroyed and then the original assets are unlocked. This process prevents the assets from being double spent in any way on both chains at the same time and data integrity and provenance gives cyber integrity.

The smart contract world is isolated from a much larger expanding non blockchain world known as IOT (internet of things) where devices and sensors interact across all industries each with their own interfaces. It would be unthinkable for progress if these two worlds would not be connected to drive IOV.

Oracles were mentioned earlier and they are the only link to the physical world for blockchains. For DeFi there is a need for market feeds to determine reconciliations, insurance parametric contracts need IOT data to trigger pay outs. These payments often need to be made in fiat currency triggered by conditions in the supply chain, connected car, smart transport and factories. For on-chain transactions to be complete, there has to be concensus but off-chain transaction agreements happen outside the blockchain. Therefore it is necessary for blockchain to have an oracle in the form of middleware to listen, collect and deal with trusted data from the outside. These middleware assets exist on the market but centralized oracle feeds can cause a single point of failure, so care has to be taken in the design to avoid cybersecurity issues.

EFFECT ON FINANCIAL INCLUSION

Trust, transparency and accountability have been the barriers to entry for financial services in developing countries and underserved populations in developed countries. Much of this is caused by top down driven strategies when a grass roots approach is required. If we look at the village level we can take a community and cooperative driven approach to finance, especially now as we have access to technology that allows democratization and consensus where every village could be a node on a blockchain even contributing to open source.

The evolution of social payments, wallets, mobile money, financial inclusion solutions designed from grass roots up combined with parametric insurance removing the trust DeFicit from claims paying, now brings promise of moving the informal sector closer to access to trusted financial services on their doorstep. Users can make and receive small payment transfers quickly without high transaction fees with better gaming and ecommerce experiences The ability to market and administer smart contract-enabled parametric insurance policies solely through internet-connected smartphones can aid in reaching underserved populations and increase the IOV through social payments and social reinsurance [xxi].

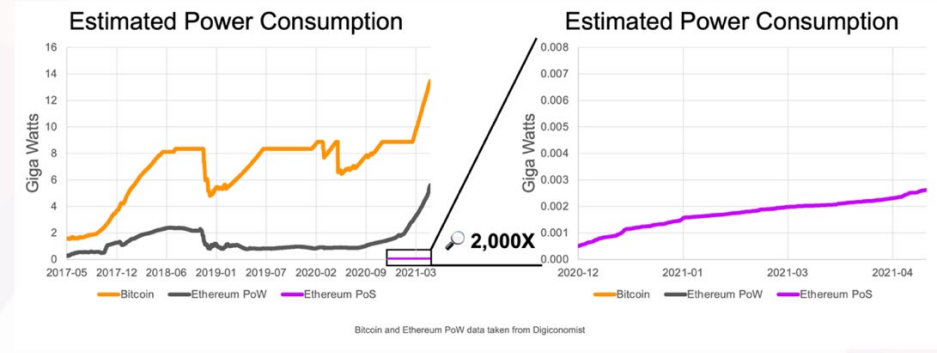
DeFi brings programmable money and wallets to the table and therefore the link to digital payments platforms is key to enhance the scalability and to the IOV by transfer of value. Anything of monetary or social value can be transferred between parties, including currency, assets, stocks, securities, intellectual property rights, scientific discoveries and more. Transferring value is already supported by legacy but the new digital protocols are now emerging especially around IOT where payments and exchange of value can occur at the device to device level. Moving money is currently expensive, especially when it comes to cross-border payments, cross-system transfers and settlement is slow. Remittance providers look at cryptocurrencies like Stablecoins as an efficient solution to settle international payments. Cross-border remittances done this way are faster, cheaper, and more efficient than traditional methods. This parallel shift is taking place in payments to get interoperability with legacy and open finance protocols that can be accepted at any point of sale at low cost. Digital identity infrastructure is vital for DeFi/CBDCs to work in the informal sector. Close alignment to the following relevant United Nations SDG (sustainable development goals) here is a good ethos.

CONCLUSIONS

Regulation, climate change friendly, confluence of intangible risks and protocol interoperability will decide the speed of DeFi adoption and increase the IOV.

1./ REGULATION - the elephant in the room for $2 trillion industry, currently too big to fail, but runs that risk unless balance is created. Both the finance industry and blockchain technology have trust as their directives. Regulators are used to overseeing intermediaries but now investors are interacting directly. DeFi is leading the drive for the insurance sector to use public blockchains in a permissioned fashion moving away from the closed private blockchains and consortiums with limited scope of interoperability but the CBDCs developments can challenge the whole DeFi market or choose to closely interact for mutual benefits. The development of REGTECH will be an important factor to automate compliance.

2./ ESG – public blockchains use electricity in providing consensus by mining for cryptocurrencies such as BTC in a mechanism known as Proof of Work. This puts the DeFi industry on a collision course with climate change programs and with the insurance industry net zero program. ETH has moved to another consensus mechanism called Proof of Stake (POS) which uses 99.5% less energy. Creation of the Crypto Climate Accord [xxii] and the Universal Protocol Alliance [xxiii] organizations are moving the crypto sector to a greener future. Other mining is now done using volcanic renewable energy.



3./ INTANGIBLES – they comprise 90% of the assets in the FORTUNE 1000 companies today and the insurance industry has flipped to intangible insurance covers with tangible riders. As digitization increases there is more emphasis on data, cyber, IP, IOT and crypto assets and the value of these intangibles is moving to corporate balance sheets. These intangible classes do not exist in isolation as data can be compromised, IP created in real time, devices communicating with each other with human involvement and ecosystems cross communicating. Confluence of intangibles gives more capital appreciation and broader consumer access to more complex financial instruments normally only available to wealthy investors and institutions such as Bondblox [xxiv] which allows fractional corporate bond trading to the wider audience. Data is the ultimate intangible to move to the balance sheet.

4./ MULTICHAIN – the landscape of DeFi is too vast for protocols to exist in isolation. To increase the IOV there must be interoperability with cryptographically secure connections across borders, ecosystems and jurisdictions with identity and privacy preserved.

The next generation INTERNET (Web 3.0) promising metaverses, sovereign identity and data ownership, secure from compromise, can become reality quickly. There is still work to do and the future is bright but will be down to political will to increase wealth, health, global GDP and better consumer experiences.

REFERENCES

The author acknowledges Julian Gordon, Vice President of Hyperledger Asia Pacific and Nathaniel Gordon a business student at Durham University, U.K. for their help in reviews of this paper.

[i] https://www.cnbc.com/2021/04/06/cryptocurrency-market-cap-tops-2-trillion-for-the-first-time.html
[ii] https://gatehub.net/blog/what-is-the-internet-of-value/
[iii] https://en.wikipedia.org/wiki/Fork_(blockchain)
[iv] https://ethereum.org/en/
[v] https://wifpr.wharton.upenn.edu/wp-content/uploads/2021/05/DeFi-Beyond-the-Hype.pdf
[vi] https://www.coindesk.com/markets/2021/04/29/defi-is-now-a-100b-sector/
[vii] https://defipulse.com/
[viii] https://defillama.com/home
[ix] https://en.wikipedia.org/wiki/Internet_of_things
[x] https://martin-thoma.com/cryptocurrency-types/
[xi] https://en.wikipedia.org/wiki/Network_effect
[xii] https://ilp.mit.edu/node/24497
[xiii] https://www.metaco.com/crypto-insights/silo-by-metaco-unified-hot-to-cold-storage/
[xiv] https://www.bis.org/
[xv] https://www.bis.org/about/bisih/topics/cbdc/wcbdc.htm
[xvi] https://cacm.acm.org/news/255277-ethereum-weathers-bug-that-underlines-possible-blockchain-risks/fulltext
[xvii] https://ipwe.com/
[xviii] https://nexusmutual.io/
[xix] https://b3i.tech/home.html
[xx] https://nydig.com/
[xxi] https://openknowledge.worldbank.org/handle/10986/15211
[xxii] https://cryptoclimate.org/ /
[xxiii] https://www.universalprotocol.io/
[xxiv] https://www.bondblox.com/?gclid=EAIaIQobChMI2f227pbY8gIVwmkqCh2zQA5CEAAYASAAEgIQI_D_BwE

9.2021

David Piesse
CEO, DP88

About the Author:

David Piesse is CEO of a family office, DP88, specialising in InsurTech initiatives in Asia - www,DP88.com.hk. David has held numerous positions in a 40 year career including Global Insurance Lead for SUN Microsystems, Asia Pacific Chairman for Unirisx, United Nations Risk Management Consultant, Canadian government roles and staring career in Lloyds of London and associated market. David is an Asia Pacific specialist having lived in Asia 30 years with educational background at the British Computer Society and the Chartered Insurance Institute.