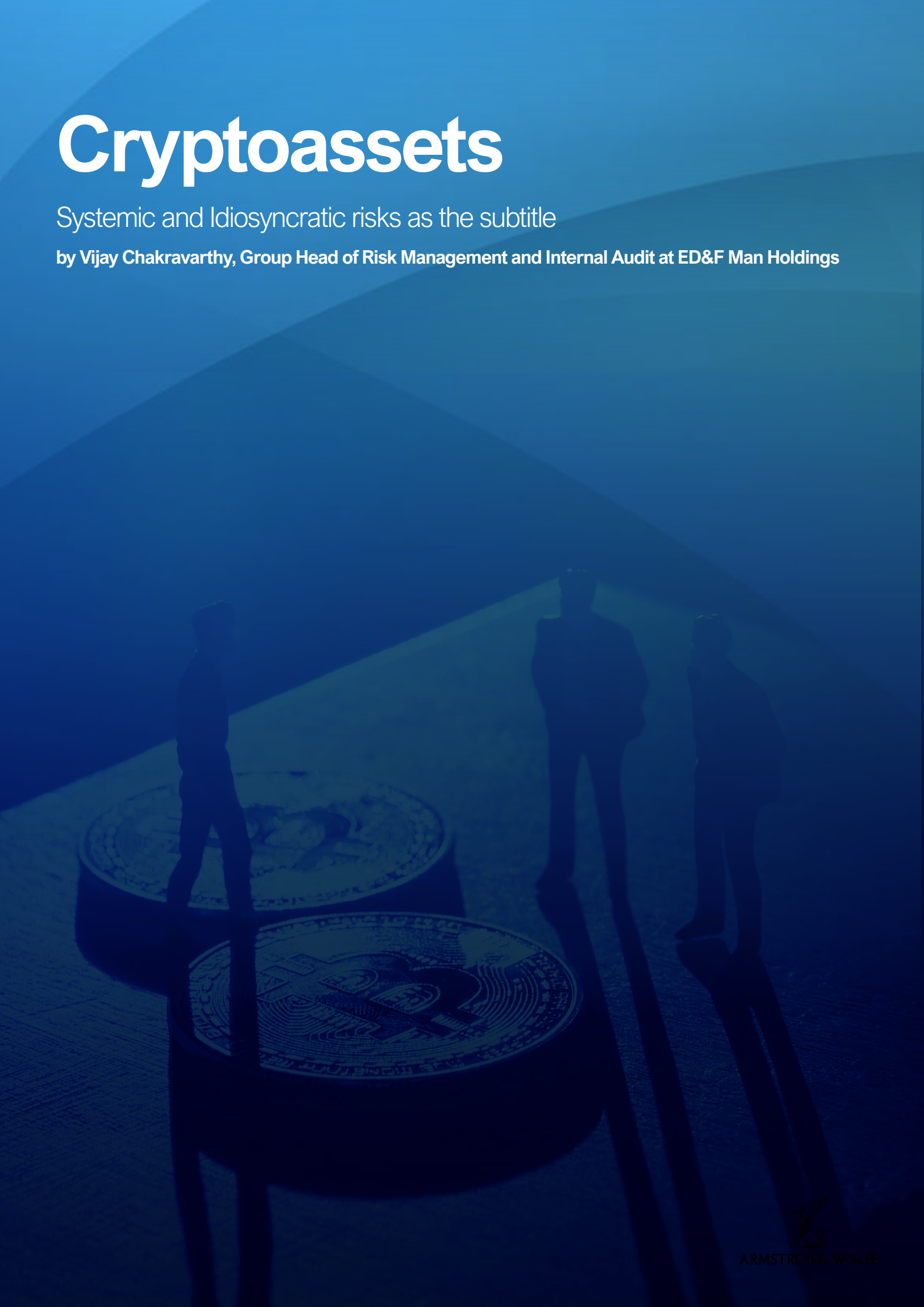
Cryptoassets

Systemic and Idiosyncratic risks as the subtitle

by Vijay Chakravarthy, Group Head of Risk Management and Internal Audit at ED&F Man Holdings



ARMSTRONG WOLFE

Systemic and idiosyncratic risks of crypto-assets and ecosystems

As I put the finishing touches to this article, China has banned all cryptocurrencies including trading and related investment and financial services. The PBOC has vowed a harsh crackdown on token issuance and derivative platforms and most crypto assets are down about 6% for the day.

Right at the outset, I will try and compress all key crypto asset innovation into a small paragraph so noone is left out when they read what follows:

Blockchains are immutable and time stamped append only ledgers that can be permissioned and closed to membership (centralised) or permissionless and open (decentralised) . Crypto asset ecosystems are various applications built on blockchain ledgers maintained without a central authority across the member community most importantly to effect currency issuance and title transfer, contingent settlement, transactions and exchange anything that can be safely encrypted and transferred electronically without duplication on the internet. Layers of cryptography are used for identity verification / identity concealment , transaction data versioning and secure data transfer and to maintain the integrity of the electronic assets. The final immutable ledger version is decided not by a central authority but by the majority through computing power or ownership stake.

Although the above architecture and market structure was proposed by Satoshi Nakomoto in his Bitcoin whitepaper in October 2008 (the timing is no surprise ; trust in the global financial system was at an alltime low then), several improved versions of it have been released since then with new tokens accompanying the launch of the ecosystems. The real life applications of the above incentive system and security architecture extend far beyond crypto assets and decentralised finance . This article will also look at how to manage the common internal and external risks of the crypto asset ecosystems.

Why am I writing this article now?

I am neither a crypto skeptic nor a maximalist. I respect Adam Bach, Satoshi Nakomoto , Vitalik Buterin, Nick Szabo as much as I admire Nouriel Roubini , Joseph Stiglitz and Paul Krugman. I love Gary Gensler for his unstinting efforts first as an educator and now as an empathetic regulator . I will put them in the innovators , incumbents and the guard compartments of this speeding train. I am the bystander on the platform , a risk officer who has been beaten into shape to sit still and pay attention to facts while waves of persuasion and distraction hit from every angle. I am also trained to look deep into the merits of both sides of an argument and broker a negotiated settlement before the curtains come down for the trading day. My approach to risk management developed over several thousand trading proposals is much like a zealous sportsman who is often seen gently remonstrating with the referee knowing well that this decision will not go in his favour but also working to gain one more cultural inch for a truly momentous occasion. As a graduate engineer , I understand the importance of thoughtful design and standards to ensure the utility and to protect the consumer from the product's Frankenstein potential .I have gone from

a comfortably oblivious crypto skeptic to a binocular wielding birdwatcher deeply fascinated by the many facets, utility and disruptive power of the new technology and the financial ecosystem.

I have witnessed and studied the many historical failings of the traditional financial systems with the contagion leading to large scale crisis. At its heart a build up to a financial crisis is illuminated with dizzying pace of change and the attendant thrills, rewards and promise as more and more converts join to marvel, contribute and benefit from the gravity and logic defying progress of the carnival.

The aftermath of a crisis leaves very deep scars and the repair job to restitch lives and livelihoods and to restore the fabric of trust and harmony sometimes takes decades. The policy response to fix the destruction in itself sows the seeds for future disasters by entrenching financial inequity and entitlement that could span generations. Most often the crises were due to failure of oversight and governance, market structure that misaligned incentives and the age old human qualities of fear and greed. The voices of reason whilst these crises were brewing have been muffled most often and on occasion derided and defenestrated to make room for energy and optimism in the direction of travel. The most recent and devastating systemic event was the global financial crisis of 2008 where the key drivers were,

- Predatory lending practices and almost infinite implicit guarantee of a secondary market recourse to federally backed institutions in the United States regardless of underwriting standards

- Failure of regulatory bodies in the US and Europe to establish limits on leverage and isolate concentration risk for mortgage backed securities for financial institutions and push for regulatory capital to cover for mark to market and counterparty risks

- Failure of financial institutions to understand the stressed market liquidity needs of the derivative instruments from the above key risks on their balance sheet and

- Failure of policy makers to appreciate the interconnectedness of the investment and global banking ecosystem

There is a reason why I am repeating this really boring history lesson already piped ad nauseum from preaching pulpits all over the world. I'm sure many folks who understood the enormity of the crisis knew how close we came to a total apocalypse for a few weeks just over a decade ago . We have come a long way and thank God the next Netflix drop is the main worry in most households and not the paycheck or even worse length of the soup kitchen line. Mark Twain once said history does not repeat itself but it does rhyme. It is not a surprising observation ; for all his success as a writer, Mark Twain had many an investment setback in his time. My risk career went from programming to operations to management and then to leadership . At every point I have seen how failure is gently embedded as assumptions in code, in minds and motives, in market structure , policies, practices and regulation and is finally unleashed when an event wave makes a splash slightly further from the shore.

To emphasise again, a financial market failure is a systemic event that tears up the aspirations of large sections of the society and takes years to remedy and rebuild . We have to be meticulous in seeking its avoidance by embedding a variety of defence mechanisms in financial systems that are vulnerable to failure.

What does this article try to accomplish?

This article identifies the various flashpoints for systemic and idiosyncratic events in the evolving crypto asset world where investor protection could be compromised at scale and financial market stability

could be endangered. Financial innovation from combining blockchain , security and computational power tested cryptography and a decentralised governance model have gone a long way in disrupting traditional banking and finance with potential use cases extending from inland and crossborder payments to complex bilateral and derivative transactions. A fast growing and a faster changing $2 trillion asset class has the potential to transform the financial system as we have known it since the collapse of the Bretton Woods model in 1973.

When the technological innovation is hurtling forward at multiple times the speed of legal framework, governance structure, standards and a public policy response it makes it very easy to conclude that mini disasters would be commonplace in this financial ecosystem. The internet went through a similar growth phase and is still a platform for abuse of personal data, journalistic and broadcasting standards , facts and copyrights at scale. But it has also delivered avenues for enormous collective advancement whilst ensuring mind boggling levels of inclusion for the majority. The new decentralised ecosystem has the potential to ensure financial inclusion for a huge section of the unbanked and financially and legally underserved population in emerging economies ; By delivering services such as remittances, loans , savings ,investments and transaction and title security at the touch of a phone screen , the ecosystems can make up for inadequate governments and poor governance. Hence the need for careful thought to avoid systemic events from such a promising set of technologies and architectures.

For the benefit of brevity and focus, this feature will only consider in scope the scenarios and probabilities of event risks from sponsored and anonymous initial coin and token offerings of crypto assets , permissionless blockchains and decentralised finance . The article will explore the design features and the incentive structures that underpin the ecosystems. You may notice the constant pivot back to mature technologies and standards for enabling payments and delivering all aspects of the transaction , trade and finance from connectivity to a central venue all the way to execution, transfer of title, settlement, dispute resolution and eventually custodianship. A study of decentralised finance and blockchain ecosystem is never complete without drawing parallels with the standards and governance structures built in the systems they have set out to disrupt. Choose between “isolation, integration and regulation” of crypto assets said Mark Carney former governor of Bank of England . Whilst the revenue office and the law enforcement are reacting to large real-world interactions of the crypto asset ecosystem, most governments and the markets regulators have been ambiguous in their approach. For them a comprehensive public policy response and regulation in itself confers legitimacy to an asset class that is gnawing at the foundations of monetary sovereignty and control . This working paper aims to bring various market participants on board to test the scenarios outlined below and to help develop effective mitigation. I will continue to publish improved versions of this document based on your feedback and further research.

Regulatory risk:

There is a distinct possibility of time called abruptly on the currency use cases of crypto assets by the regulator/central banks . China has done just that but other governments could follow very soon.

The biggest economic design strength and flaw in the system of crypto assets are the crypto assets themselves. Most often their issuance is controlled (a paradoxical situation for a decentralised peer to peer network). The purest by design is the Bitcoin where a collective action or an enormous hashing power by a single entity is needed to alter the issuance and inflation. The promoters of the crypto asset ecosystem have so far used the tokens to fund the design and development as an initial pretext but concentration of investment money has been an undeniable benefit. ICOs will soon clash with securities regulation and be seen as IPOs ie capital raising for an investment contract where disclosure requirements will make the currency issuance almost an untenable activity. SEC

charges against Boon. tech, RE coin or Diamond reserve club coin are cases in point . Stable coins whose values are pegged to fiat currencies will be seen as no different to ETFs as strict collateral requirements will make issuance of a digital currency simply seem like an expensive exercise in proxy. Coordinated regulatory action by securities regulators is expected to come in tidal waves potentially taking with it generations of crypto assets and pushing them away from financial market legitimacy. In short natively digital crypto assets could either get strongly tethered to fiat currencies or suddenly feel homeless and their mining and issuance could begin the relay flight to jurisdictions where the law and regulation are friendlier.

The potential impact:

Besides sudden and steep mark to market losses to investors , risk of a systemic event from the above regulatory intervention seems rather minimal . Whilst mining will be caught up in this net, trading/broking/ lending or custodianship of existing securities may retain status quo. Financial firms with counterparty risk that involves concentration of exposure to the mark to market of crypto asset (either through direct ownerships or clearing) could address them with high multiples of exchange margins as collateral placed only in highly liquid securities. Participants in the crypto currency ecosystem ie lending , exchange trading , custodianship will be impacted by the higher resulting volatility but they will be able to contractually isolate the securities for illiquidity risk and prepare for this risk event with simple risk management techniques.

Mitigation:

The markets could quickly solve Vitalik Buterin's Scalability, Security, Decentralisation trilemma by going permissioned and dumping the native token in their quest for efficiency and lower transaction costs. The blockchain based solutions for the FICC repo market in the US is a classic example. This also solves the mining problem and the accompanying environmental concerns for proof -of-work based algorithms.

Central bank digital currencies could be a part of the solution if high velocity of the token and prompt settlement is a desired feature. It is not hard to imagine a highly scalable solution with multiple transactions where payment entries are made directly between the individual and central bank ledgers bypassing payment gateways and merchant banks. The government could also use this channel if they wanted to provide financial relief and cut out intermediaries for a cross section of the unbanked population.

Risk of obsolescence – generations of crypto assets, "its raining copy cats and crypto dogs"

Currencies are recognisable, portable , durable and scarce and crypto assets fail many of these basic tests. They are mainly held for capital appreciation or as a store of value so we continue to regard them as commodity or investment contracts. The progressively shrinking inflation of bitcoin has become a moot point as more than 6000 crypto currencies are trading at this time of writing and inter-operability with features like Atomic swaps make for limitless supply of crypto assets with little or no friction. As any simple crypto price screen will tell you how correlated the coins' price moves are,so a bonfire of crypto assets precipitated by pure fratricide is not hard to imagine . The top two crypto asset underlying have had an 80-90 percent correlation of price returns for most of the past two years so there is nothing unique about them at least as a store of value.

Potential impact :

Crypto issuance inflation will cause financial loss for token holders , loss of volumes and liquidity in market venues like exchanges and clearing houses ; however this is the scenario that is least capable of causing wider damage to the financial markets as this will offer the crypto assets a soft landing over many weeks , months or even years.

Mitigation :

The aftermath of crypto currency hyperinflation will probably seem like status quo for most financial market participants. The settlements triggered on crypto based ecosystems will also be just fine .All remote and cold wallet owners will be able to access their private keys for orderly liquidation in this scenario . Secondary aggregator networks will also have minimal impact as they will get orderly settlement for their matching trades at frequent intervals.

Design & Architecture risk - interoperability / security risk

The cryptographic layers that deliver the security are identical to the ones that deliver encryption for emails, web based transactions , phone calls and chat sessions over the internet. The public key/ private key and the hash function cryptography are good enough for protecting content in its intended original form. The SHA hash functions developed by the United States National Security Agency have been adapted to deliver effective encryption (Bitcoin uses SHA-256 hash functions) for transaction information. As long as there is very high collision resistance (two different inputs almost never leading to the same hash output), the cryptography underlying the crypto asset ecosystem is fit for purpose. At least it is as secure as most transactions on the internet.

The architecture however has been adapted to widen the interoperability and this has the potential to compromise security in a big way. Smart contracts that are programs issued by one user but called at many points across distributed networks maximise the attack surface area and are open to major security breaches. From the earliest smart contracts in Ethereum where an attack happened within the network to the most recent Poly network attack across different crypto ecosystems , smart contracts on or across permissionless blockchains are a security risk with recourse almost non-existent. It was not surprising to witness the humiliating act of Poly network owners literally begging the hacker for mercy.

Mitigation :

The only solution to the web-based attack risk is a simplified architecture like bitcoin that allows very little programming and is not Turing complete (programmable loops) or adopt common standards in blockchain smart contract and security protocols. With several pieces of code called into smart contracts accessing different protocols of blockchain . a security breach will be very hard to prevent or prove in court.

Collective action event risk - crisis day hard fork

This is a dystopian scenario but our real lives are most often competing with contemporary science fiction these days. The catalyst could be fear or greed, ego or conflict but multiple hard forks could come about as the cult like order of public decorum evaporates in the face of personal ambition. A 51% attack could be coordinated successfully, and the coin issuance logic could be tampered with and the network could lose its fabric of trust. The founders could also cash their stake all in one go making the problem worse. The larger crypto networks have a natural moat against this collective action risk , however crypto asset blockchains have been subjected to attacks from security breaches to collective action breaches and they have hard forked or versioned themselves to safety each time.

Mitigation:

Sudden liquidation by the founders is more likely but collective action could mercifully be deployed to take this threat down. Further the likelihood of simultaneous collective action events across a variety of crypto asset ecosystems is very low. Smart contracts could embed 51% attack or phishing clause to ensure switch back to fiat currency settlement or an off-chain settlement. Clearing houses and broker firms could also embed this feature in their contracts with clients and counterparts to ensure smooth settlement when price discovery is made opaque by collective action on the underlying crypto asset.

State actor assertive action risk – piercing the censorship resistance by well funded multi-channel attack

A scenario in which a state actor attempts to subvert the consensus protocol for the top 3 or 5 crypto asset ecosystems purely with the objective of promptly retiring them is a very plausible one.

After all these systems threaten their monetary sovereignty, regulatory and capital controls and before long could be seen as a widespread threat to the state's command and control infrastructure . States take a wide faced hammer to such systems and the regulatory clampdown would mean sudden drying up of legitimacy to the legacy platforms and crypto assets. The state would view this as a few billion dollars of investment in ASICS/GPUs and electricity to wrest totality of control back for the benefit of the inland revenue, the central bank and the markets regulator. The most recent ban by China and the corresponding crackdown by PBOC and several enforcement agencies will be watched by other governments for a template to the reaction to the proliferation of crypto assets.

The impact and mitigation:

Potential for systemic crisis from this event is minimal as the state can ensure targeted action to ensure no undesired outcome outside of the crypto ecosystem. However price discovery for the securities and derivative contracts will become increasingly difficult without a functioning network.

The crypto asset exchanges trading and lending will be most impacted as the collateral cover could be inadequate . Clearing houses have to limit the notional value of the derivative contracts traded on their venue or have very high initial margin requirements to protect from this event becoming a systemic one. They also have to contractually protect themselves for poor price discovery caused by state action with a force majeure clause. Smart contracts have to embed an off- chain trigger and dispute resolution mechanism to deal with such an event. "Isolate crypto" is a very important strategy for clearing houses and brokerage firms and market makers dealing with crypto derivatives. As for primary exchanges ,they unfortunately do not have a defence if the main crypto assets come under a state sponsored attack and they cannot maintain liquidity and price discovery.

Litigation risk

Very early days but the laws around ownership, title transfer , custody and dispute resolution are not well developed for crypto assets. In fact the "very early days" phrase in itself is symptomatic of complacency and inaction. Smart contracts have trigger events embedded in the code making it even more difficult for lawyers to opine on the legality of the cases. Instead of making it efficient , smart contracts could make life difficult and legal recourse almost impossible. The entire legal framework around trigger events, evidence and settlement mechanism and dispute resolution could be encoded in legal language with common law jurisdiction contractually agreed in effect dumbing down and standardising smart contracts to design them for an effective legal recourse. Lawyers and courts use precedence in judging the merits of the case , so the lack of precedents should be clearly understood by financial market participants entering into smart contracts. To avoid systemic events, financial institutions may avoid entering into smart contracts involving large notional values until standards are established and their legal recourse is made clear. They are best served by testing them out on permissioned blockchains with trusted market participants. The evolution of insurance tech and chain link will provide many useful templates trigger event based bilateral and multilateral smart contracts

Compliance risk – the killer of killer apps

"Who are your clients or counterparts?

Where is their money coming from and what are they doing on your platform ?"

Crypto exchanges and trading venues struggle to answer these basic KYC questions leave alone KYCC/AML, audit trails and enhanced customer due diligence. Decentralised crypto asset ecosystems have a huge problem in the identity area where the bearer of the private key is the unopposed owner of the security and need not have an identity or proof of title. By design they are meant to conceal the identity of the beneficial owner and this will be a huge problem at every touch point with the law and the regulation. Binance, the crypto trading venue attracted regulatory fire from a string of regulators and some accusations went as far as saying the exchange was not compliant with anti-terrorism law. Most crypto asset enthusiasts think this area is quite not what should concern them or believe that a technology solution is very easy to retrofit once scale is achieved on their platform. This has the potential to shut down trading venues and exchanges and result in seizure of crypto assets by the authorities but might not precipitate a systemic event . Negligence in this aspect alone could attract regulatory crackdown that is disproportionate to the size of the offence.

Mitigation:

Most crypto platforms confuse privacy with identity . The entire architecture needs an overhaul to ensure privacy but strongly embed verification of identity . This is the only way to ensure compliance and future proof the crypto asset architecture . As for smart contracts they have to embed the entire KYC /AML standards and enhanced due diligence used by the established financial institutions for counterparty verification of individual and entity else they will be deemed not very smart.

Conclusion:

The development of crypto asset ecosystems is a brilliant and welcome challenge to the established financial order. The blockchain based applications have the ability to transform banking and finance and improve financial inclusion for billions of unbanked and underserved on this planet. However, the crypto assets issuance and their proliferation is a complete distraction to the promise of the underlying technologies. The tokens lack classic properties of currencies and will not upend the sovereign monetary framework developed over centuries.

The blockchain and smart contract applications might eventually separate themselves from their digital tokens but the journey to that state could be disorderly. Meanwhile , the financial institutions could do well to pay attention to the potential for systemic events, isolate crypto assets and choose simplified, compliant, regulated and secure architectures to avoid losses for themselves and their clients.

Vijay Chakravarthy 24/09/2021

PS The views expressed here are my own and expressed completely in a personal capacity.