MERKLE SCIENCE

[DRAFT]

MERKLE SCIENCE CORPORATE NARRATIVE

GUIDELINES – HOW TO USE THE NARRATIVE

This is the full articulation of the strategy as an overall story, which builds out the logical flow of the argument, and identifies where proof points and evidence should be included.

The narrative structure has gone through a rigorous credibility test through the stress-testing process, ensuring we have the right credentials and evidence to substantiate any claims.

This should be used as the reference material for all communications.

KEY AUDIENCES

1. **Government entities (regulators, law enforcement agencies, tax authorities)**
2. Crypto businesses (C-suite, compliance officers)
3. Traditional financial services companies (Compliance officers)
4. Partners (Tech integration partners, referral partners)
5. Policymakers, leading industry analysts, influencers and media

STRATEGIC POSITIONING

1. This is the single phrase articulation of the winning territory
2. It is not a strapline that should be used in any external materials or communications, but a short summary of the argument that the narrative articulates
3. This will ensure there’s internal alignment on all communications activities

Narrative	"Narrative Spine"	Longform Narrative	Proof Points
Fundamentals / Context	Digital assets will inevitably become a key pillar of the $22 trillion financial ecosystem, but continues to face skepticism and resistance	**Cryptocurrencies and digital assets are a once in a lifetime opportunity to improve financial access and reimagine the way the world transacts value.** The products and infrastructure built today will have long-lasting impacts on the future of business and finance. However, the use of cryptocurrencies has been met with skepticism and resistance so far — threatening the healthy growth of the sector. To this day, the digital asset sector continues to be plagued by negative reputation, stemming back from Mt Gox hack in 2014. **Despite proving its role as a hedge against inflation and its ability to retain value, cryptocurrencies still stoke negative reactions and doubts from many key figures in traditional finance.** While the last year has seen significant institutional adoption of crypto, the sector still has many hurdles to overcome in order to become a key pillar of the financial ecosystem and realize its full potential. Arguably, one of the biggest hurdles toward digital assets' full legitimization is abusive and illicit behavior — both real and perceived — within the industry that governmental bodies are struggling to navigate and manage.	**Global crypto market cap** - 2020: $758 billion USD - April 2021: $2 trillion USD **Mainstream crypto adoption** - Venmo: users can buy, hold, sell crypto (Apr 2021) - Tesla holds Bitcoin - Deustche Telecom stakes CELO (April 2021) - Companies working on crypto capabilities: Visa, Square, Tesla, PayPal, Goldman Sachs (CNBC) - Possible frictions: taxable events, ESG, BTC volatility **Crypto can help overcome financial exclusion:** - Hundreds of millions of people globally have no checking or savings account (Global Finance) - COVID has increased reliance on digital payments - matter of life or death. - Financial exclusion leaves people vulnerable to predatory lenders and with limited safeguards for job loss - FE in major markets: India (20%), China (20%), Israel (7%), USA (7%), S Korea (5%), HK (5%), UK (4$)
	As blockchain technology advances and the digital asset ecosystem expands, illicit activity continues to grow in volume and complexity. Across the board, industry players are struggling to keep up with the pace of change.	The cumulative market cap of cryptocurrencies grew 300% in 2020, reaching $758 billion USD. As of April 2021, global crypto market cap is over $2 trillion USD. With the expansion of the digital asset ecosystem, crypto crime is happening at greater volumes and criminals are becoming more sophisticated in their use of crypto in illicit activity. In 2020 alone, blockchain hackers stole over $3.7 billion USD. The recent surge in popularity for technologies such as DeFi lending platforms, NFTs, and P2P payment providers have caught the attention of the FATF and regulators everywhere, and for good reason. The DeFi rush meant that products were brought to market without proper verification tools and compliance in place. Criminals are exploiting those weaknesses. As a result, DeFi became a haven for money launders and DeFi hacks accounted for 20% of losses in 2020. There is a knowledge gap for government agencies when it comes to digital assets — making digital asset regulation and enforcement seemingly unattainable. And as blockchain technology advances, the gap widens even more. Government agencies need greater support with more training and better tools to keep up with the progressively complex criminal behavior.	**Chainalysis** (Jan 2021) - Ransomware increased by 311% year over year. - Dark net markets were the second-largest crime category, accounting for $1.7B worth of cryptocurrency activity — a roughly 30% increase from a year earlier. **DeFi Hacks** - Crypto crime slows in 2020 but DeFi hacks rise: Ciphertrace (Reuters) - Losses grew to $468M, up 30% from 2019 - about 20% (98M) ame from DeFi - **Surge in DeFi was what ultimately attracted criminal hackers - Blockchain hackers stole nearly $3.78B in 122 attacks throughout 2020

		Crypto businesses and financial institutions — who may be directly or indirectly exposed to digital asset risks — also need to keep abreast of developments in criminal behavior involving crypto so that they may fulfill their regulatory obligations. In the case of fraud, companies typically have to bear the loss of the theft and reimburse the user, ultimately damaging companies' reputations and hurting their bottom lines.There is strong incentive for industry players to build robust systems that can detect abusive behaviors or recover lost funds. As transaction risks become increasingly complex, greater resources are required to manage these risks — ultimately detracting from the companies' core competencies.	**NFTs** - No data around NFTs currently, but none of the major NFT trading venues (OpenSea, Rarible) have KYC or AML/CFT screening for users (Cryptonews) - Recent explosion from the number of celebrities that are looking to tokenize their offerings have regulators concerned; more areas of exploitation **Bank account closures** - Singapore (2017 BT article) (2017 startups deal with acct closures) - Irish Crypto Firms Squeezed by Bank Account Closures - Nigeria (Personal Account Closures)
	Regulatory ambiguity is hindering both innovators and legacy players from fully realizing crypto industry's full potential	Over the last two years, countries — such as Singapore, Hong Kong, Japan, the UK, Switzerland, Canada, and the U.S. — have made efforts to prioritize digital asset regulations and implement the FATF's guidance on virtual assets and VASPs. However, implementation in the majority of these countries have been delayed — making it difficult for businesses to operate. Issues abound for regulators as they cannot keep up with the pace of new technology, hindering their ability to provide regulatory guidance. Certain niches of digital assets, such as DeFi, don't have clear regulatory guidelines. And for areas that have clear regulatory requirements, such as the Travel Rule, there are no clear methods or technology mature enough to help businesses comply. The confusion surrounding global regulations comes at a cost and may sometimes be catastrophic for startups. Often strapped for resources, these startups may also have a difficult time securing funding as established corporations and entities do not want to put their businesses at risk. With reputations and licenses on the line, institutions would rather wait for clear guidance from regulators before they make large investments into the sector.	UK: FCA registration regime — over 200 businesses still awaiting licensing Japan: Licensing as money transmitter very slow Singapore: still awaiting licensing under the PSA U.S.: New York BitLicense - stagnant. Most recent was May 2020 - Eris Clearing (subsidiary of ErisX)
	As global rollouts of digital asset regulation pick up speed, AML compliance will be unavoidable. Those who are proactive in setting compliance frameworks will be at a clear advantage.	Even though digital asset regulations have been delayed or stalled, government agencies have been diligent in applying punitive fines for companies failing to meet regulatory requirements under the traditional finance framework. Regulatory arbitrage, which was rampant during the early days of the digital asset industry, is being curtailed by the FATF's measures. Non-compliance is no longer an option for crypto businesses. Regardless of jurisdiction, crypto businesses need to take the FATF measures seriously and need to operate as though there are already regulations in place. The crypto businesses that proactively apply best practices and establish compliance frameworks will be able to mitigate regulatory risks.	Countries that do not implement the FATF recommendations face severe consequences. Countries are blacklisted and effectively frozen out of the world economy — increasing the pressure for countries to comply. E.g. U.S. DOJ, CFTC and SEC expected to exercise increasing oversight and enforcement (see BitMEX) **BitMEX, Binance** Volume of fines, detailed examples of fines such as Bitmex and Binance cases

	Current AML/CFT tools in the market are insufficiently effective in helping businesses manage their full range of transaction risks	Legacy tools are overly dependent on blacklists and historical data. It is a reactionary approach to monitoring and risk detection, making companies susceptible to large blind spots. Legacy tools also take one-size-fits-all approaches to classifying risks, which does not make sense, given the range of risk factors that differ from entity to entity — such as geography, business vertical, company size and types of blockchains. When transactions are flagged, the transaction needs to be further classified and deciphered in order to determine where it fits within their own internal policies — creating more work for the companies. This method of blockchain tracking is antiquated, and will only become more archaic as new blockchain technologies continue to emerge. The digital asset industry deserves a better approach that will look beyond the blacklists and keep up with innovation.	Customer feedback: false positives with legacy tools as they are not customizable for certain geographies. - Something that is criminal activity in Singapore may not be considered criminal activity in the U.S. Blacklists cannot track privacy coins such as Monero — 45% of darknets use Monero (2nd most popular for criminals after Bitcoin) - Other popular privacy tokens: Zcash, DASH, Verge, Horizon, Beam Zksnarks, bitcoin taproot
Strategy / Evidence	Merkle Science is making cryptocurrency conventional — legitimizing the asset class and bringing it within regulatory scope without stifling innovation.	In the last year, we have seen institutional adoption and acceptance of crypto pick up speed — making headlines nearly every week. In our opinion, the convergence of cryptocurrencies and traditional finance is inevitable. But large scale adoption of crypto by governments and financial institutions can only happen if there are advanced tools in place to limit risks that arise from cryptocurrencies. To enable this transition, Merkle Science provides a predictive cryptocurrency risk and intelligence platform to detect and prevent illegal activities that involve cryptocurrencies. By allowing industry participants to see and understand cryptocurrency risks, we can help the industry grow in a safe and healthy manner and become a key pillar of the financial ecosystem.	
	Merkle Science's predictive risk and intelligence platform helps crypto companies, financial institutions, and government entities keep pace with the industry's increasingly complex illicit activities.	Unlike other blockchain monitoring and investigative tools on the market, Merkle Science's platform takes a risk and behavior-based approach to transaction risk management, resulting in more adaptive and effective crime monitoring and investigations. ***For Crypto Companies and Financial Institutions*** ● Merkle Science's **Monitoring Tool** allows crypto businesses and financial institutions to detect illicit activity from their incoming and outgoing cryptocurrency activity and helps them meet their local AML and KYC regulatory compliance obligations. ● Through the use of **Behavioral Rule Engine**, businesses can go beyond the blacklists and identify suspicious transactions and criminal wallets. This enables financial institutions to detect undetected AML risks that legacy providers might miss. ● In the case of suspected criminal activity, **Merkle Science's Tracker** helps businesses forensically investigate crypto-financial crime. The tool allows users to visualize and track stolen crypto funds —and identify exit nodes and crypto criminals — so that teams may take expert, evidence-based action accordingly. ● **Radar** helps businesses fully understand the retail and corporate crypto exposure of current and potential partners. Merkle Science's **Know Your Blockchain Business (KYBB)** report identifies and performs due diligence on crypto businesses and customers while the **Enhanced Due Diligence (EDD)** report flags risky transactions and generates a 360-degree report on the business.	Merkle Science's platform helps clients keep track of the risk rules and provides users with data to improve upon their compliance process. - The engine can provide insights on which rules worked, and which didn't. - Our vision is to build a machine learning model on top of the rule engine that proactively refines the rules and proposes new ones. **How customers use Monitoring Tool** ***Example 1: Simple*** - For certain jurisdictions, transactions over a certain amount (e.g. $1000) requires enhanced due diligence. Criminals would want to make sure their daily transactions don't hit this limit - Behavior Based Rules look at customer's txn behavior and see that he's always transacting close to the limit but never going over

		For Law Enforcement Agencies and Regulators ● The Monitoring Tool goes beyond blacklists, which inherently looks at past behavior, to help regulators understand the risks across all the different crypto businesses — and stay on top of emerging technologies such as DeFi platforms — in order to deter illicit activity. ● Law Enforcement - Tracker (Geist) ● Regulators - Monitoring & Radar - help regs get a risk profile of crypto companies and financial institutions that they're looking to license And as criminal activity evolves, Merkle Science's intelligence platform evolves with it. Merkle Science's platform can observe transactional activity and identify addresses that are likely to be linked to previously-undetected criminal activity.	- CREATE RULE: looking at range-bound transactions, whether address has sent or received txm amounts between a certain range - Compliance may monitor this customer over the span of a week and the rule has been flagged 6 or 7 times - Up to business whether to stop working with the client and report (also dependent on reporting thresholds) ***Example 2: Potential Scam Activity - Ransomware*** - Scammer may send out 100K emails, and 100 people fall for it - CREATE RULE: if an address is receiving payment of similar amounts from many different counterparts (already eliminates client from being a normal retail client) - Combine with other rules, such as range bound transactions (e.g. between $900 to $1100) Or after wallet collects funds, will try to move into new wallets that the individual creates - The more conditions you put into a rule, the harder it is to satisfy all the conditions. Should someone satisfy all the conditions, changes of him engaged in criminal activity is very high. ***Example 3: What can we do, but not quite there yet*** - Rather than wait for an exchange to screen an address, we can run analysis over the entire Bitcoin blockchain - Look at the behaviors on the wallets and identify which ones fits the definition of a potential criminal - Can use this data to predict that certain addresses could potentially be used by scammers
	Merkle Science's proprietary predictive risk and intelligence platform is highly customizable and easy-to-use — allowing	While businesses want to identify as much criminal behavior as possible, they recognize that resources are limited. Merkle Science built a highly-customizable and easy-to-user platform that is jurisdiction and business agnostic. Users can adapt the rules and conditions in the Behavioral Rule Engine based on their compliance policies in order to find the right balance when it comes to flagging illicit behavior. And when maximized, the rule engine saves crypto-related businesses time and resources so that they may effectively operate with leaner compliance teams.	**Regulators and law enforcement agencies will already recognize this risk-based approach** — it is common practice for tracking criminal activity in cash and a standard that regulators would expect from a compliance transaction monitoring system.

	crypto businesses to stay ahead of developing regulation and focus on their business.	Four key factors help determine compliance policies and rules for any organization exposed with crypto-related risks: 1. ***Geography*** — Differing compliance obligations mean that compliance policies need to be fine-tuned by jurisdiction. 2. ***Business vertical*** — Differing verticals, such as crypto exchanges or custodians, will be exposed to different levels of transactional risks. 3. ***Size of company*** — Companies of different sizes will have different levels of susceptibility to attacks. 4. ***Types of blockchains and tokens involved*** — Illicit behavior and transactional risks differ based on the blockchain and token. The flexibility and granularity of the Behavioral Rule Engine allows businesses to tailor their rules and policies according to their risk matrices. It provides clarity and insight so that businesses can effectively manage their risks and improve their bottom lines. Ultimately, the platform allows businesses to focus on their core competencies and continue to build a healthy digital asset ecosystem. In addition, the Behavioral Rule Engine's granularity makes it easier for crypto businesses to scale across multiple geographies and business lines — simplifying compliance and turning compliance from a cost to a competitive advantage.	
Vision	Merkle Science is building a predictive cryptocurrency risk and intelligence platform, setting the standard for the next generation of financial safeguards and criminal detection. We are creating the infrastructure necessary to ensure the safe and healthy growth of the industry, supporting the transition as cryptocurrencies consolidate with the $22 trillion financial services market. Merkle Science envisions a world powered by crypto. We are the catalysts enabling crypto companies — trailblazers and disruptors who are pushing the boundaries of innovation — to scale and mature so that a full range of individuals, entities, and services may transact with crypto safely.		