Valoores Crypto Management System: Mitigating Risks and Building Security Foundations for Digital Assets

Everyone is talking about crypto, the colloquial term for digital assets. Love it or hate it, it seems to be on everyone's lips. The fact is that crypto is now mainstream and VCMS stands at the forefront of digital asset protection. With a commitment to safeguarding the integrity and confidentiality of your assets, this system offers a dynamic and adaptive solution that aligns with the rapidly changing nature of the crypto space, providing users with peace of mind in an inherently volatile environment.

By seamlessly integrating cutting-edge risk mitigation protocols and robust security measures, VCMS not only shields against emerging threats but also pioneers a new era in digital asset management.

Table of Contents

Introduction

In the ever-evolving landscape of finance, the emergence of cryptocurrencies has ushered in a new era, challenging traditional financial paradigms and fostering a paradigm shift in the global economic system.

Chapter 1 of this document delves into the multifaceted dimensions of this new financing regime, exploring the development of virtual currencies, scrutinizing the international legal framework surrounding them, and dissecting the specifications that define these digital assets. Additionally, it examines the remarkable growth in market share and the evolving landscape of Crypto Services Providers, while also shedding light on the alarming increase in crimes facilitated by cryptocurrencies. Ultimately, this chapter seeks to unravel the underlying needs that propel the quest for innovative solutions in this dynamic domain.

Transitioning to **Chapter 2**, the focus shifts towards regulatory compliance as an essential facet of ensuring the responsible integration of cryptocurrencies into the global financial ecosystem. The Financial Action Task Force's (FATF) Anti-Money Laundering (AML) and Countering the Financing of Terrorism (CFT) standards stand as pillars for establishing a robust framework. This chapter meticulously explores the scope of these standards, elucidates the implementation of Crypto Digital KYC Solutions, introduces the Wallet Name Matching System (WNMS), and highlights the efficacy of a Crypto Risk-Based Approach (CRBA). Furthermore, it examines the critical role played by Crypto Rules and Transaction Monitoring in maintaining compliance within the ever-dynamic crypto landscape.

Chapter 3 delves into the instrumental role played by VALOORES Crowd Intelligence System (VCIS) in the realm of crypto investigations. Unraveling the complexities associated with location intelligence, this section underscores the added values brought forth by VCIS and assesses their effectiveness in combating crimes involving cryptocurrencies. As we traverse through this comprehensive exploration, it becomes evident that understanding the intricacies of crypto investigations is pivotal for creating a secure and accountable financial environment.

Chapter 1: A new financing regime with the rise of cryptocurrencies

A. The development of virtual currencies and the international legal framework

Cryptocurrency appeared in 2008 with the emergence of bitcoin by anonymous users who used the pseudonym Satoshi Nakomoto and published a book titled "A Peer-to-Peer Electronic Cash System" on the website "CYPHERPUNK" to explain the protocol. They described this innovative currency as “a medium of exchange, an electronic payment system, and a revolution in financial technology.”

From the beginning of 2011, new cryptocurrencies began to appear. In 2012, Bitcoin was initially accepted as a payment method by some official websites, such as WordPress and Microsoft. In February 2014, the first Bitcoin ATM was opened, reaching almost 1,500 worldwide in October 2017, and in 2015, the US-based Coinbase wallet became the first crypto virtual currency exchange.

So these types of currencies continue to prosper and diversify, their value increases, and their infrastructure develops. The value of all existing cryptocurrency is around $1.05 trillion, with around $508 billion of that being attributed to Bitcoin (as of Aug. 28, 2023), according to CoinMarketCap.com.

The global payments revenue is expected to top $3 trillion by 2026, according to a McKinsey report.

Virtual cryptocurrencies are decentralized convertible virtual currencies that rely on cryptography to verify transactions and issue monetary units. They are a means of abolishing the role of regulators in terms of issuing, monitoring, and controlling cash, as well as the role of financial institutions in intermediating money transfers. They are a digital representation of value that is exchanged electronically in a specific or undefined virtual community.

Its principle of issue and circulation depends on cryptographic techniques and not on central banks. They do not constitute any obligation towards the parties who use them, not even towards their developer. It does not have the legal status of cash currencies but exercises a credit function similar to theirs as a means of exchange and unit

of account. Most cryptocurrency systems have been programmed to gradually reduce currency production and cap their total amount to simulate precious metals, compared to regular currencies held by financial institutions or that can be held with cash on hand. In light of the many characteristics that distinguish virtual cryptocurrencies, there has been a difference in classification by countries' legal systems:

Cryptocurrencies are described **as a currency** that acts as legal tender because it appears at first glance to be parallel to these and is used to buy and sell goods and services ranging from small transactions for the purchase of cars and real estate to the payment of debts. Additionally, they can also be converted and exchanged for legal and international currencies, such as the US dollar.

Cryptocurrencies are described **as an investment tool** based on the concept that many people buy in order to invest and profit from the difference between buying and selling prices. They have practically led to the rapid fluctuation of their value during a single investment period. In Norway, for example, the General Tax Administration classified cryptocurrencies as an investment, which opened the door to the imposition of new taxes on profits made from speculating in them.

Cryptocurrencies are described **as electronic assets**. The proponents of this point of view believe that cryptocurrencies are not currencies because they are not issued by a central authority in accordance with the laws of the monetary systems of the countries of the world and because their price is unstable, unlike legal currencies and outside the control of central banks, which play an essential role in the regulation of financial activities and their emissions and the insurance of their cover, which allows their circulation, use, and acceptance as currency in the issuing state and abroad. They call them similar commodities to gold because they share many similarities with this material: both are not supervised by a central authority; they are extracted by mining, which provides a limited number of quantities, but cryptocurrencies have no physical existence. They are digital assets held in a digital wallet. They are an asset with a finite number of tokens. They are driven purely by supply and demand.

In 2014, in the United States, the Internal Revenue Service adopted the classification of cryptocurrencies as a commodity by treating virtual currencies for tax purposes as intangible property that is subject to the same provisions applicable to traditional property and which is valid for barter of goods and services over the Internet and is subject to capital gains tax.

In short, the classification of cryptocurrencies is still a subject that raises a lot of controversy and cannot be resolved with certainty, especially in the absence of a global legal regulatory framework for all its aspects.

Many international organizations, such as the FATF and central banks, have defined virtual currencies as "a digital representation of value that is not issued by a central bank or public authority and without any regulatory authority that controls the issuance process."

B. The specifications of virtual cryptocurrencies

The cryptocurrency relies on three essential points: blockchain technology, dual-key encryption (public and private), and the mining process.

Blockchains

Blockchain technology constitutes a decentralized participatory digital record system that is used to record and store digital transactions, such as financial transactions, without the possibility of making changes to the information that has been stored and without the need for a central authority that controls the conduct of financial transactions, such as central banks.

This record is located on a common database distributed across a secure, global network of millions of nodes that use the same technology to manage the shared database. The blockchain is shared among all users who own a similar copy of the block chain, which includes all digital transfers. Each operation is automatically verified by all network subscribers before being recorded.

This system is impossible to hack because it needs to change data on all registers of all subscribers at the same time. This technology promotes the concept of publicity and transparency of data and ensures their issuance and circulation in complete security, protected from the risks of fraud, theft, or hacking.

Dual-key encryption, public and private
Each digital wallet user receives a pair of encryption keys: a public key and a private key. The message will be encrypted by the sender's private key and the recipient's public key. This makes it possible to prove and confirm the identity of the sender of the message as the owner of the transferred units and exclusively gives the recipient the power to decrypt and benefit from the transferred units. This encryption is an effective means capable of harming acts of hacking.

The mining process
Mining is the process by which transactions are verified on the blockchain. It is also the way new coins are entered into circulation. "Mining" is performed using hardware and software to generate a cryptographic number that matches the criteria. The first miner to find the solution to the problem receives the coin reward, and the process begins again.

The coin reward that miners receive is an incentive that motivates people to assist in the primary purpose of mining: to legitimize and monitor crypto transactions, ensuring their validity. The blockchains use different mechanisms, which would affect their block times, for example:

- On the Bitcoin blockchain, a block is verified by miners, who compete against each other to verify the transactions and solve the hash, which creates another block.
- On the Ethereum blockchain, a block is validated by randomly selected nodes, which must be faster because there is no competition.

C. The growth in market share

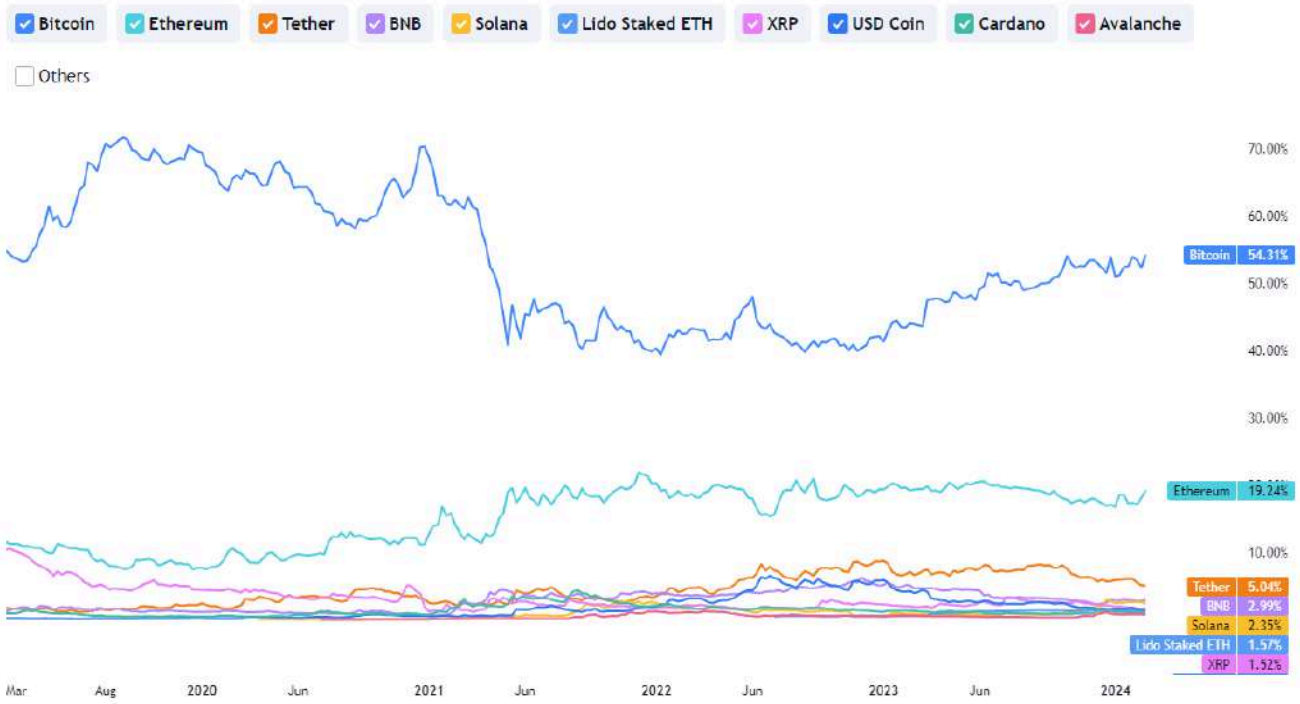
Currently, the cryptocurrency market has been experiencing a period of volatility, with fluctuations in the value of major cryptocurrencies such as Bitcoin, Ethereum, and Dogecoin. The market has also seen a rise in the number of altcoins, or alternative cryptocurrencies, with unique features and use cases. Several growth factors are driving the growth of the cryptocurrency market, including increasing acceptance and adoption of cryptocurrencies by individuals and institutions, growing interest in decentralized finance (DeFi) platforms, and the potential for cryptocurrencies to serve as a hedge

against inflation and political instability. Additionally, advancements in blockchain technology and the increasing use of cryptocurrencies for cross-border transactions are also contributing to market growth.
The cryptocurrency market is expected to continue growing in the coming years. The increasing adoption of cryptocurrencies by businesses and individuals, along with the ongoing development of DeFi and other blockchain-based platforms, is likely to fuel this growth. However, the market is also likely to experience volatility and corrections, as is typical with any emerging and rapidly evolving market.

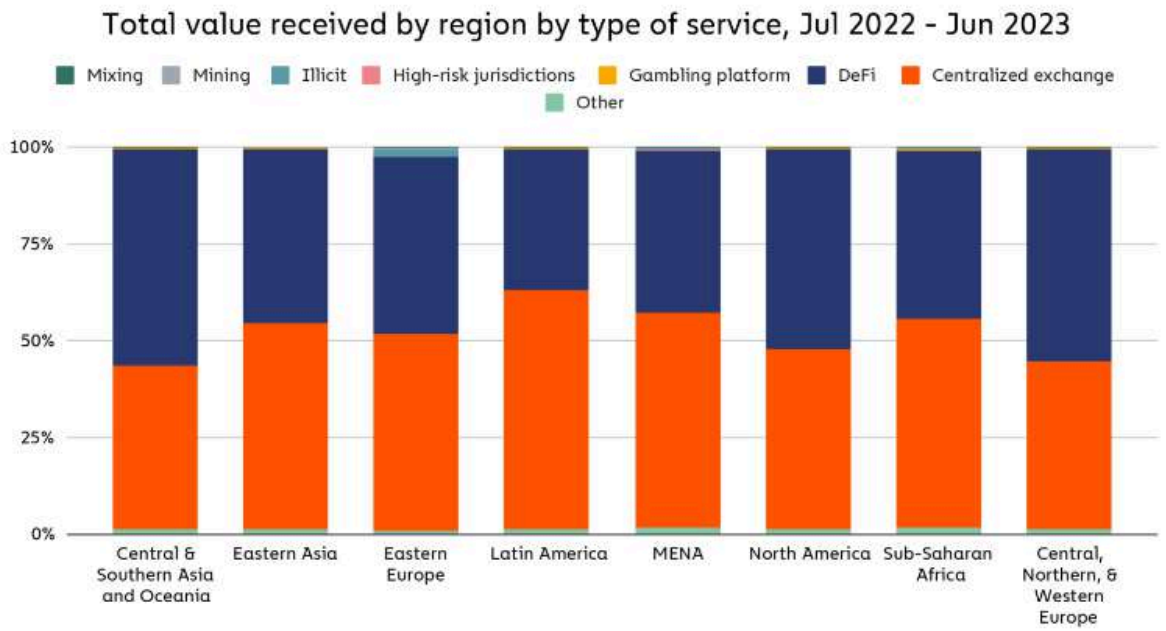
Worldwide

***Total Crypto market cap*,** calculated by TradingView, is the combined value of the top 125 cryptocurrencies. Market capitalization, in this context, is determined by multiplying the current price of each cryptocurrency by the total number of coins in circulation:

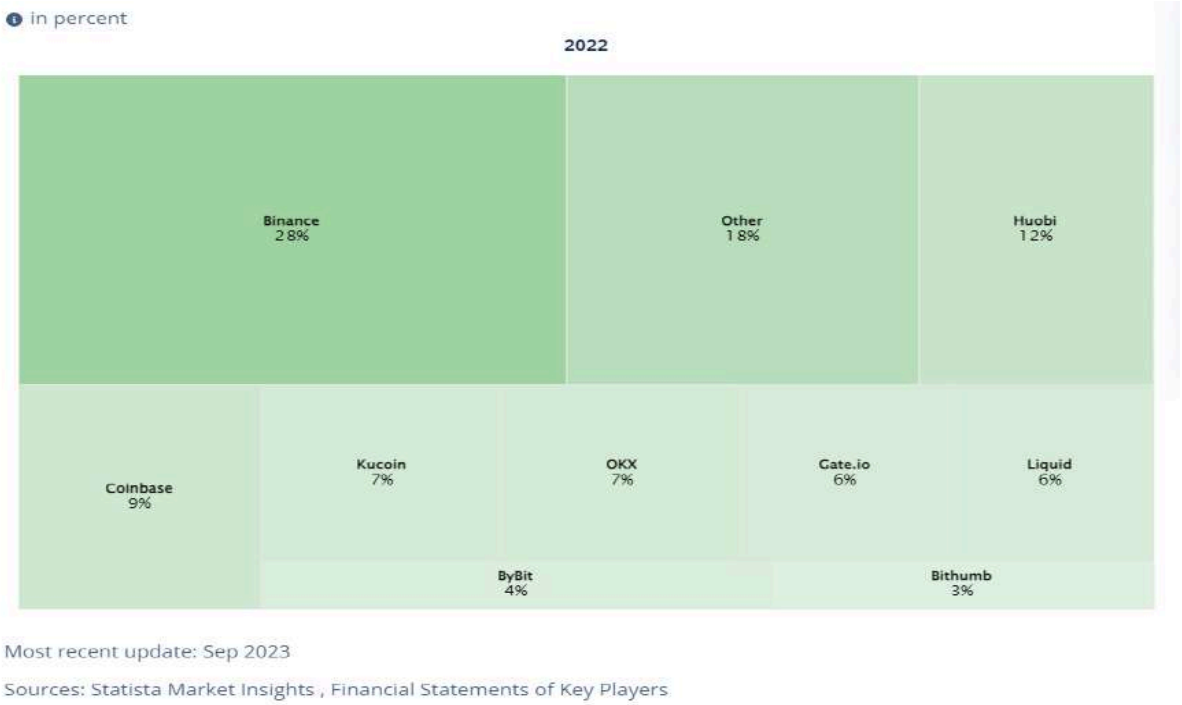
Dominance by Market cap, shows how much of the entire cryptocurrency market a specific coin represents.



Most used services: Cryptocurrency users predominantly utilize decentralized finance (DeFi) platforms for permissionless financial services and Centralized Exchanges.

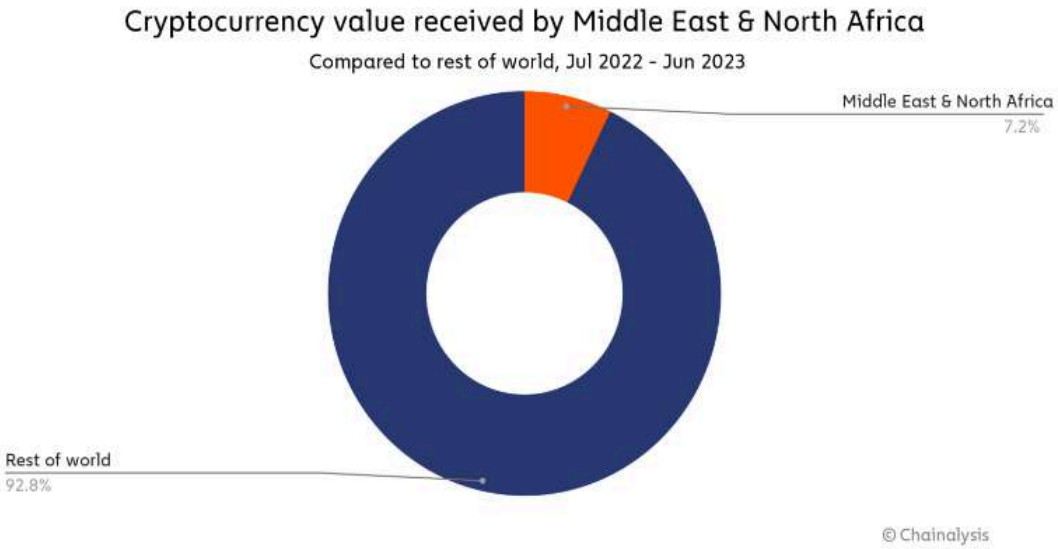


The graph below shows the distribution of centralized crypto services, highlighting dominant platforms such as Binance, Coinbase, and Kraken, showcasing their market share within the cryptocurrency ecosystem.

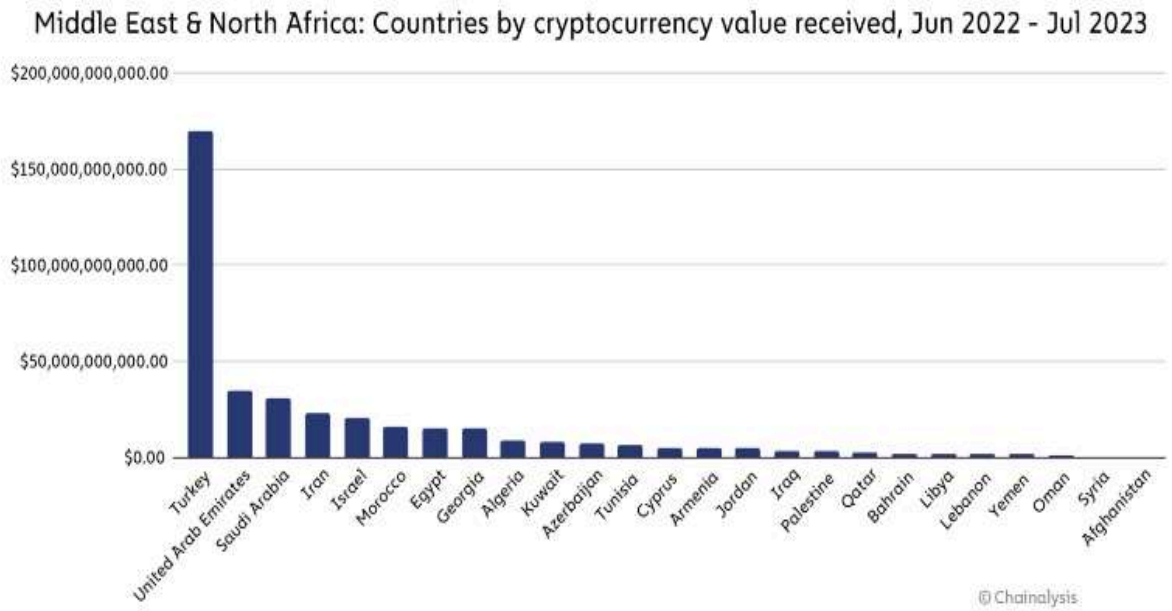


Middle East & North Africa

The Middle East & North Africa (MENA) has the sixth largest crypto economy of any region we study this year, with an estimated $389.8 billion in on-chain value received between July 2022 and June 2023. This represents nearly 7.2% of **global transaction volume** during the period studied.



MENA is also home to three of the top 30 countries in this year's index: Turkey (12), Morocco (20), and Iran (28). However, Turkey dominates in terms of raw transaction volume, as we see below.



Largest cryptocurrencies by market cap

Bitcoin gets all the headlines when people talk about cryptocurrencies, but there are literally thousands of other options when it comes to these digital currencies. In fact, cryptos that aren't Bitcoin are usually considered an "also ran" – what are called "altcoins," or alternatives to Bitcoin.

While Bitcoin may have been the first major cryptocurrency to hit the market – it debuted in 2009 – many others have become highly popular, even if not quite as large as the original.

Here are the largest cryptocurrencies by the total dollar value of the coins in existence, that is, the market capitalization, or market cap. *(Data is from CoinMarketCap.com, as of February 20, 2024.)*

Total Cryptocurrency Market Cap: $2,212,753,008,632

Rank	Name (Symbol)	Market Cap	Market Share	Price (USD)	24 Hr % Change
1	Bitcoin (BTC)	1,167,150,972,377	52.7466%	$59,427.1269639979	3.79974212
2	Ethereum (ETH)	398,512,347,011	18.0098%	$3,316.7627129304	1.21087169
3	Tether USDt (USDT)	98,437,401,878	4.4486%	$1.0004722437	-0.03219223
4	BNB (BNB)	60,954,737,215	2.7547%	$407.6076992017	1.83535437
5	Solana (SOL)	49,192,279,056	2.2231%	$111.1746259553	-0.27354209
6	XRP (XRP)	31,878,821,125	1.4407%	$0.5839227146	4.23433465
7	USDC (USDC)	28,561,785,225	1.2908%	$0.9998781336	-0.00841371
8	Cardano (ADA)	22,330,711,000	1.0092%	$0.6294566759	0.74158991
9	Avalanche (AVAX)	14,927,999,524	0.6746%	$39.5754483677	-0.47804888
10	Dogecoin (DOGE)	14,086,561,091	0.6366%	$0.098329165	3.48302816

The cryptocurrency market is a Wild West (although the U.S. government is taking a more active role in overseeing the crypto space), so those speculating in these digital assets should not put in more money than they can afford to lose. Crypto assets faced downward pressure for much of 2022, and trading remained volatile in 2023. It's also important to note that individual investors often trade against highly sophisticated players, making it a fraught experience for novices. In 2024, the SEC approved several spot Bitcoin ETFs for trading, giving investors a simple way to bet on Bitcoin's rise.

D. The Evolution of Crypto Services Providers

The definitions of VAs and VASPs provided in the FATF's updated guidance (FATF 2021, 109) are vital to understanding the impact of FATF recommendations on crypto businesses and services. Anti-money laundering and counter-terrorism financing (AML/CTF) frameworks apply to certain crypto assets and services across the globe, and these definitions inform which types of crypto assets and services AML/CFT frameworks should cover across the globe.

FATF defines VAs as the following:
A virtual asset is a digital representation of value that can be digitally traded or transferred and can be used for payment or investment purposes. Virtual assets do not include digital representations of fiat currencies, securities, or other financial assets that are already covered elsewhere in the FATF Recommendations. *(FATF, 2021b, p. 109)* such as Bitcoin, Ether, Solana, Tether, and Litecoin.

FATF defines VASPs as the following:
A virtual asset service provider (VASP) means any natural or legal person who is not covered elsewhere under the recommendations and, as a business, conducts one or more of the following activities or operations for or on behalf of another natural or legal person:

- the exchange between virtual assets and fiat currencies;
- the exchange between one or more forms of virtual assets;
- transfer of virtual assets;
- safekeeping and/or administration of virtual assets or instruments enabling control over virtual assets; and
- participation in and provision of financial services related to an issuer's offer and/or sale of a virtual asset. *(FATF. 2021b, p. 109)*

Several types of businesses fall under the definition of virtual asset service providers. These include cryptocurrency exchanges, ATMs, wallet custodians, and crypto hedge funds. They are now required to comply with the FATF's crypto **travel rule**.

- **Cryptocurrency Exchanges**

A cryptocurrency exchange is an obvious example of a VASP. Also known as digital currency exchanges, these organizations facilitate the trading of cryptocurrencies, both for other digital currencies and for fiat money.

- **ATMs**

ATMs aren't just for fiat currencies these days. Bitcoin ATMs allow customers to buy Bitcoin in exchange for cash, and

sometimes to sell it too. As such, they fall under the VASP definition.

- **Wallet Custodians**

As the VASP definition includes organizations that administer and store virtual assets, as well as exchange and transfer them, cryptocurrency wallet custodians are also considered to be VASPs.

- **Crypto Hedge Funds**

Some high-value investors use crypto hedge funds as their investment vehicles. Such funds fall under the VASP definition.

- **Mining pools**

A mining pool is a group of cryptocurrency miners who connect their mining machines over a network to boost their chances of earning the reward for opening a new block.

- **Brokerage services**

Facilitate the issuance and trading of VAs on behalf of a natural or legal person's customers; order-book exchange services, which bring together orders for buyers and sellers,typically by enabling users to find counterparties, discover prices, and trade, potentially through the use of a matching engine that matches the buy and sell orders from users; and advanced trading services that allow users to buy portfolios of VAs and access more sophisticated trading techniques, such as trading on margin or algorithm-based trading.

Although the underlying technology is not new—non-fungible tokens (NFTs) originated in 2013 with Colored Coins, a colorful representation of bitcoin coins—in 2021, the volume of NFT trading spiked, and news of NFT purchases repeatedly made it to mainstream headlines.

E. The Increasing Pattern of Crimes Using Cryptocurrencies

This mechanism of action of cryptocurrencies presents challenges on several levels, especially security and economics: decentralization which is not affiliated with a central authority, the absence of a regulatory authority, the speed of execution of transactions, the rapid fluctuation of its prices in close periods and sometimes within the same day, the irreversibility of all transactions associated with cryptographic technology even if an error has occurred in the party to which the currency was transferred or in the value transferred; the ease of being used in Internet-related criminal activities; the possibility of anonymity especially as transactions are recorded and the identity of users is only known through virtual digital addresses issued by cryptocurrency trading systems.

Virtual cryptocurrencies constitute a secondary corridor for money laundering and terrorism financing away from the gaze of censorship and control of financial flows through central banks and related authorities. Criminals are turning to cryptocurrencies as a new means of financing their actions and activities for several reasons, especially anonymity, ease, speed, and the non-monitoring of the authorities on these transfer channels. They allow criminals to receive large sums in a single transfer, hide and keep millions of dollars on a small cell phone, and transport them from one place to another to use them clandestinely, especially across borders, and finance terrorist acts with decentralization.

Several international organizations have declared the potential of these currencies to be used to finance terrorists and to hide their criminal harvests and money laundering, such as the FATF through their reports.

There are numerous precedents associated with the use of cryptocurrencies to finance terrorism, such as publishing an article in 2014 entitled “Bitcoin wa Sadaqat al-Jihad” in an online blog incites the facts about the financing of ISIL and the mujahideen via Bitcoin.

Likewise, after the Paris attacks in 2015, the media spoke of a detection by the organization “Anonymous” of a single wallet containing three million USD used by Daesh to carry out terrorist attacks.

In August 2020, US authorities announced the largest government seizure of digital currencies under the CFT after stopping al-Qaeda and ISIL and confiscating millions of dollars from more than 300 CMV accounts linked to the activities of these organizations.

In 2022 alone, Chainalysis tracked a total of $23.8 billion worth of crypto laundered by cybercriminals, but keep in mind that this figure only includes funds associated with addresses tied to forms of crime that are inherently related to cryptocurrency, like ransomware, exchange hacks, and crypto scams.

In 2023, illicit addresses sent $22.2 billion worth of cryptocurrency to services, which is a significant decrease from the $31.5 billion sent in 2022. Some of this drop may be attributed to an overall decrease in crypto transaction volume, both legitimate and illicit. However, the drop in money laundering activity was steeper, at 29.5%, compared to the 14.9% drop in total transaction volume.

Why do attackers demand ransom in digital currency?

There is a clear connection between ransomware incidents and cryptocurrencies, as attackers consistently demand payment in Bitcoin or other digital currencies. The inherent anonymity of cryptocurrencies provides

criminals with an effective means to acquire and conceal funds. Despite the cybersecurity community emphasizing cryptocurrencies as significant facilitators of ransomware, experts suggest that enforcing stricter regulations or banning blockchain-based currencies is unlikely to curb the surge in such attacks, as reported by Tech Monitor.

Attackers prefer receiving cryptocurrency as the ransom payment for the following reasons:

- **It is decentralized:** no middlemen are involved in transactions with cryptocurrency. As there is no central authority or third-party involvement, anyone (including the attacker and victim) can join or participate in the public blockchain network and perform transactions without the gateway of a bank.
- **It is lucrative:** Cryptocurrencies such as Wrapped Bitcoin and Bitcoin are valued at over $31,000 each. With the advent of the Ransomware as a Service model, even amateurs can carry out attacks successfully and easily rake in the profits from their ransomware Bitcoin payments.
- **High access and reach:** With cryptocurrency exchanges going public and new, affordable cryptocurrencies being launched every other day, their access and reach have increased exponentially.
- **Lack of standard legal jurisdiction across countries:** Essentially, cryptocurrency transactions are "borderless." This means that the attacker could be in one country and the victim in another, and it would have no impact on the transaction speed, efficiency, or limit. Moreover, since there is no central authority or global compliance standards for these transactions, and money moves between countries, attackers usually escape the brunt of legal repercussions.
- **Difficult to detect:** The irony of cryptocurrency transactions is that while the records are all publicly available on the cryptographic ledger of blockchain, the identities of the individuals involved are anonymous. This makes tracing the transactions difficult. But, difficult doesn't mean impossible.

This reflects the urgent need to regulate this sector, create a system that mitigates the risks of money laundering and terrorist financing, and create a mechanism that allows tracking the flow of illicit funds.

F. The needs behind our solution

Block chain technology represents a new era of FinTech; it is the future of digital transfer and trading, which promotes transparency. There is only a need to put cryptocurrencies under the control of a regulatory authority, to be covered by central banks, and to enable crypto-activities to be investigated by security and judicial authorities.

Perhaps the decentralized cryptocurrency system makes it extremely difficult to track the purchase and sale transactions made; however, cryptocurrencies are not anonymous. Rather, they adopt a transparent and public system that is not subject to modification or manipulation. Although the wallet addresses do not contain any personal information such as name, residential address, etc., this anonymity is only relative because every transaction made on the block chain is recorded where possible to know the user and balance of all wallets using analytical methods after registering a digital KYC. The principle of tracing money essential for FT or ML investigations can be applicable in the case of cryptocurrencies.

It can be said that tracking transfers of virtual cryptocurrencies is much easier than tracking physical money transfers. It is subject to the same principle as bank transfers, with the irony that bank accounts are all known while the identities of e-wallet owners can be inferred through user KYC, interactions, and activities.

In the ever-expanding universe of cryptocurrencies and virtual assets, the Valoores AML Crypto solution emerges as a beacon of integrity and security, reshaping the narrative around money laundering and financial crimes.

Considering it as more than just a sophisticated engine, it's the hero that the digital financial landscape needs. In a world where taxes and regulations often feel like distant concepts, this solution becomes the watchful guardian, ensuring that the promises of transparency and accountability are not just words but a lived reality.

Valoores AML Crypto solution represents the connective tissue that binds regulators, Virtual Asset Service Providers (VASPs), and tireless champions in law enforcement.

As cryptocurrencies become the preferred playground for financial crimes, the Valoores solution steps up to the challenge, creating an unbreakable link between those who set the rules, those who adhere to them, and those entrusted with enforcing them. It’s a new regime of compliance and an effective tool for investigations.

What makes this solution valuable is its ability to adapt and evolve alongside the ever-shifting landscape of the crypto world. It's not merely a technological upgrade; it's a dynamic force that anticipates and combats the ingenious ways in which financial criminals exploit technology to escape regulatory scrutiny. Real-time monitoring, instant response capabilities, and an unyielding commitment to upholding the principles of fairness and justice. The Valoores AML Crypto solution encapsulates all of these elements.

In this era, where the traditional boundaries of finance are being redrawn, the Valoores solution stands as a testament to the fact that innovation and regulation can coexist harmoniously. It is not just about securing transactions; it's about safeguarding the essence of financial systems, monitoring suspicious activities, and banning criminals from exploiting these channels of transfer.

As users, investors, and enthusiasts navigate the complexities of the crypto world, the Valoores AML Crypto solution is their steadfast ally, ensuring that the promises of a transparent and secure financial future are not just aspirations but tangible realities. It is not just a technology; it is a commitment to a brighter, more secure digital financial tomorrow.

The Valoores AML Crypto Solution is a protector of financial integrity in the age of digital currencies.

Chapter 2: Cryptocurrency compliance system with the FATF's AML & CFT standards

A. The scope of the FATF standards

In October 2018, the Financial Action Task Force (FATF) adopted changes to its recommendations to explicitly clarify that they apply to financial activities involving virtual assets. FATF also added two new definitions to the glossary: "virtual asset" (VA) and "virtual asset service provider" (VASP).

"Virtual asset" is a digital representation of value that can be digitally traded or transferred and can be used for payment or investment purposes. Virtual assets do not include digital representations of fiat currencies, securities, and other financial assets that are already covered elsewhere in the FATF Recommendations.

"Virtual asset service provider" means any natural or legal person who is not covered elsewhere under the recommendations and, as a business, conducts one or more of the following activities or operations for or on behalf of another natural or legal person:

1. Exchange between virtual assets and fiat currencies;
2. Exchange between one or more forms of virtual assets;
3. Transfer of virtual assets; and
4. Safekeeping and/or administration of virtual assets or instruments enabling control over virtual assets;
5. participation in and provision of financial services related to an issuer's offer and/or sale of a virtual asset.

In June 2019, the FATF adopted an Interpretive Note to Recommendation 15 to further clarify how the FATF requirements should apply in relation to VAs and VASPs, in particular with regard to the application of the risk-based approach to VA activities or operations and VASPs; supervision or monitoring of VASPs for AML/CFT purposes; licensing or registration; preventive measures, such as customer due diligence, recordkeeping, and suspicious transaction reporting, among others; sanctions and other enforcement measures; and international cooperation.

The objectives of those changes were to further clarify the application of the FATF Standards to VA activities and VASPs in

order to ensure a level regulatory playing field for VASPs globally and to assist jurisdictions in mitigating the ML/TF risks associated with VA activities and in protecting the integrity of the global financial system. The FATF also clarified that the standards apply to both virtual-to-virtual and virtual-to-fiat transactions and interactions involving VAs.

In March 2020, the FATF released its Guidance on Digital ID to assist in identifying customers in the digital context.

In June 2020, the FATF completed its 12-Month Review of the Revised FATF Standards on VAs and VASPs, which identified areas where greater FATF guidance was necessary to clarify the application of the revised FATF Standards

In September 2020, the FATF also released a report on VA Red Flag Indicators of ML/TF for use by the public and private sectors
In March 2021, the FATF released its Guidance on a Risk-Based Approach to AML/CFT Supervision.
In July 2021, the FATF released its Second 12-Month Review of the Revised FATF Standards on VAs and VASPs.

Under the RBA and in accordance with paragraph 2 of INR. 15, countries should identify, assess, and understand the ML/TF risks emerging from this space and ensure that measures to prevent or mitigate ML/TF are commensurate with the risks identified. Similarly, countries should require VASPs (as well as other obligated entities that engage in VA financial activities or operations or provide VA products or services) to identify, assess, and take effective action to mitigate their ML/TF risks.

A VASP's risk assessment should take into account all of the risk factors that the VASP as well as its competent authorities consider relevant, including the types of services, products, or transactions involved; customer risk; geographical factors; and the type(s) of VA exchanged, among other factors.

B. Crypto Digital KYC Solution implementation

Crypto digital KYC is a process utilized by government agencies, financial institutions, and regulators within the cryptocurrency compliance system. It aims to verify the identity of individuals involved in cryptocurrency transactions and assess any potential criminal risks associated with them. This process entails collecting, verifying, and maintaining identifying information about individuals, including their name, address, date of birth, other relevant **personal details**, and **digital information** such as wallet addresses, IP addresses, device IDs, device IMEIs, and other relevant technical information.

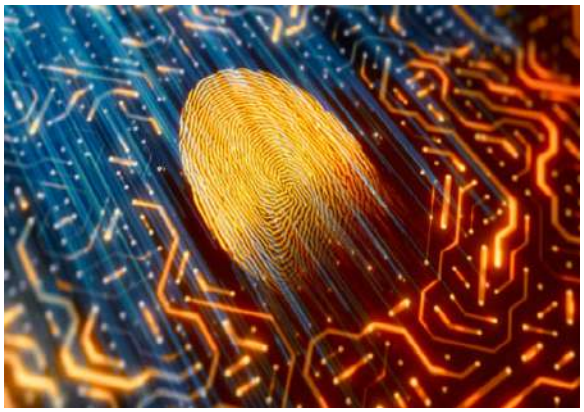
An application is designed to verify the users through an advanced biometrics technology and to authenticate all personal data, while also extracting information from provided IDs. Authentication and verification of individuals and their submitted documents serve as the initial gateway in our solution, which aims to identify the wallet owner and track all transactions associated with it, while also detecting relation to money laundering or other financial crimes. Our advanced biometrics technology includes:

Face ID identification

Facial recognition technology analyzes an individual's facial features, such as the distance between the eyes, nose, lips, ears, chin, and eyebrows, to identify them. It is highly accurate and provides results in just a split second. Our face recognition system utilizes a unified embedding to identify individuals. When given a picture of a face, the system extracts high-quality features and predicts a feature vector representing these features, known as a face embedding. The system directly learns a mapping from face images to a compact Euclidean space where distances correspond to face similarity.

Fingerprint

Accurate identification via fingerprints has become one of the most popular and important ways of maintaining security systems in today's world.



OTP

The OTP (One-Time Password) feature is a security measure that helps prevent identity theft by ensuring that a captured username/password pair cannot be used more than once. With OTP, the user's login name remains the same, but a unique password is generated for each login session or transaction.

Multiple user identification

A multiple user identification is an entity used to identify users on a website, software, system, or within a generic IT environment. Multi-Factor Authentication (MFA) was used to identify multiple users.

Session timeout

Session timeout represents the event when a user does not perform any action on a web site during an interval of

time. We implemented session timeout using the time-out function. A liveness check could be requested from users in order to proceed after or during the session timeout so that the user wouldn't lose the session and perform the work accordingly.

Voice recognition

Voice recognition technology is a software program or hardware device that has the ability to decode the human voice. Vector quantization (VQ) was used as an algorithm. It is a classical quantization technique from signal processing that allows the modeling of probability density functions by the distribution of prototype vectors.

Address Verification of Customer

The address verification prevailing solution utilizes identity documents submitted by the user to extract relevant information.

But what if the declared address is fake or has been changed later? VCMS offers document authenticity checks that utilize advanced technology, powered by a geo-smart location approach, to verify the user's complete address against specific parameters.

Our dynamic business rule engine can categorize and group addresses into residential groups, generating accurate reports that meet KYC/AML standards and regulations.

Why is digital KYC important for cryptocurrency compliance?

Crypto digital KYC is a critical process to comply with anti-crime and anti-terrorism laws and regulations and the FATF's AML & CFT standards. It involves collecting, verifying, and maintaining identifying information about individuals, corporations, or associations engaged in cryptocurrency transactions. This comprehensive approach helps assess potential criminal or terrorist risks associated with them, allowing government agencies to identify and mitigate these risks to safeguard the nation's safety and security. The process aids in detecting and preventing cryptocurrency-related criminal activities, which can have significant financial and security implications. The classifications and elements of Crypto digital KYC are integral to effective crime prevention.

Crypto digital KYC is crucial in preventing financial crimes such as money laundering and terrorist financing within the cryptocurrency space, ensuring compliance with regulatory requirements specific to the realm of digital assets.

C. Wallet Name Matching System (WNMS)

Our matching system is engineered to simultaneously match names and wallets, constituting a multitask

matching system that operates on intricate and advanced criteria. This capability enables our solution to adopt a defensive approach to money laundering by utilizing lists that can be implemented within the system to detect matching names or wallets, while also adhering to all international standards regarding crypto compliance. For example UN 1267 list which refers to the United Nations Security Council (UNSC) Consolidated List, This list is maintained by the United Nations Security and it aims to impose sanctions, such as asset freezes and travel bans, on those deemed to be involved in terrorist activities.

Another example would be the national list 1373. It established a framework for combating terrorism and called upon all UN member states to take various measures to prevent and suppress terrorist activities.

Any list or sources of data can be integrated into the solution to enhance the ability to identify all Crypto users who are considered suspicious.

D. Crypto Risk Based Approach (CRBA)

Incorporating cryptocurrency into the Basic Risk Matrix and Case Relative Risk adds an extra layer of complexity and sophistication to the RBA risk-based approach in KYC.

Cryptocurrency Transaction Analysis in the Risk Matrix:

- In the detailed Risk Matrix, one can integrate the analysis of cryptocurrency transactions associated with an individual or entity. Cryptocurrency transactions often present unique challenges and opportunities for risk assessment. Unusual patterns, high-frequency transactions, or connections to known illicit activities in the crypto space can significantly impact the calculated risk.
- Admin users might have the capability to override the risk based on specific cryptocurrency-related findings. For instance, if an individual is involved in multiple transactions flagged for potential money laundering or fraud, the admin user could adjust the risk level accordingly.
- Clicking on the risk lookup could reveal not only traditional risk factors but also detailed insights into cryptocurrency-related risks. This might include involvement in dark web transactions, association with flagged wallet addresses, or engagement in activities linked to cryptocurrency-based scams.

Cryptocurrency Tracking in Case Relative Risk:

- The VCMS Tool can extend its capabilities by incorporating cryptocurrency-related information to identify potential risks. Individuals who might seem harmless based on conventional indicators could be flagged if their cryptocurrency transactions align with suspicious patterns.
- The VCMS could raise a relative risk alert if someone is found to have engaged in cryptocurrency transactions linked to known criminal activities or has received funds from a wallet associated with illicit practices. This approach allows for a more nuanced and targeted identification of risks, especially when dealing with cases involving cryptocurrency-related crimes.

By integrating cryptocurrency analysis into the risk matrices, KYC processes become more comprehensive and adaptive to the evolving landscape of financial transactions, providing a more effective means of identifying and mitigating potential risks associated with individuals or entities.

E. Crypto Rules and Transaction Monitoring

Our solution operates on a framework of dynamic rules specifically customized for cryptocurrency transactions. These rules are meticulously implemented across one or more blockchain ledger databases, forming the backbone of our system's capability to identify suspicious activity. When triggered, these rules generate alerts that are meticulously analyzed, taking into account transaction specifics and the historical data associated with the relevant wallet. This meticulous analysis ensures that any potential risks or illicit behavior are thoroughly investigated, allowing for swift and effective response measures to be taken.

Implementing the Travel rule based on FATF rec. 15

In the context of cryptocurrencies, the Travel Rule requires VASPs to exchange specific customer information (such as name, address, and account number) for transactions exceeding a certain threshold. This information is transmitted securely between the originating VASP (the sender's provider) and the beneficiary VASP (the recipient's provider) to facilitate compliance with AML/CFT regulations.

Based on Recommendation 15,the Travel Rule aims to enhance transparency and traceability in cryptocurrency

transactions, thereby mitigating the risk of illicit activities such as money laundering and terrorist financing within the virtual asset space.

Transaction Monitoring Location Based

Many financial institutions continue to rely on IP addresses to verify a user's location, even though this method is vulnerable to spoofing and is not very effective. However, by implementing VCMS and VCIS, which include a real-time and historical risk engine and patterns of behavior in correlation with geospatial data, suspicious activities and high risk acts can be detected by identifying the country of residence, country of work, nationality, other nationality, secondary resident country, country of registration, country of incorporation, parent registration company and others.

Same Transaction Amount Monitoring

Sometimes, suspicious or illegal activities can go unnoticed when a certain amount of money is transferred periodically, appearing as a normal pattern. However, with VCMS, such transaction processes can be compared against several parameters, such as the income and social class of the sender based on our solution's classification, as well as the recipient's identity and location, in order to identify potential fraudulent or illegal activity.

Exchange Locations & Amounts Records

The increasing use of faster payment methods and digital acceleration has created an environment that fraudsters and cybercriminals can exploit. For instance, they may attempt to make multiple transactions from a single account located in different, distant locations within a short period of time. However, VCMS utilizes the ledger database to identify patterns and track changes in customer behavior by examining the scope of generated alerts over a specific period. This solution can also help locate the accurate site of the account owner and stop any suspicious activity as soon as it is detected.

Chapter 3: VCIS role in Crypto investigations

A. Location Intelligence

In today's world, billions of devices are connected to the Internet of Things, granting executives and decision-makers unparalleled access to business data, including a plethora of geospatial information. Geo-Smart Location enables the visualization and analysis of vast volumes of data in a location-specific context, empowering holistic planning, prediction, and problem-solving. By viewing all pertinent data in the context of location, whether on a smart map, app, or dashboard, unique insights can be gleaned.

Geospatial data combines location information (usually coordinates on the earth), and often also temporal information, the time or life span at which the location and attributes exist. There are many benefits to using geospatial data for cyber security. With geospatial data, cyber threat data can be captured, including, for example, the location of attacks, the number of attacks, the proportion, dates, types, and various other factors. Encapsulated into a visual representation, the information can be better interpreted and processed. With geospatial data, information can be organized better and ideas can be communicated more effectively. This helps enhance comprehension, interpretation, and processing. It also increases the ability to find patterns and relationships. For example, when attacks are plotted on a map, frequent attacks on more urbanized locations can be identified, or a pattern of a certain attack can be identified in specific locations that are susceptible to a vulnerability. The literature about using GIS in cyber security is limited. A strong foundation is required to enable the use of geospatial data for cyber security. To assist with this, the researchers provide a multi-dimensional framework that can be used as a starting point for integrating geospatial data for cyber security. Future work includes applying the framework to various use-cases.

Why VCIS?

VCIS is a revolution in Geospatial Technology through an Innovative Crowd Intelligence System that creates behavioral analytics models that enable us to analyze the digital footprints of

anonymous devices based on their movements and behaviors. These models reveal incredibly intelligent patterns.

Investigate: Geospatial data provides a contextual understanding of crime scenes, crime reconstruction, suspects identification and evidence gathering.

Monitor: Track Suspects and Assets: Monitoring of mobile devices, tracking suspects, revealing networks, identification of the assets, enhancing recovery measures.

Protect: Protecting Soft Targets: Assess vulnerabilities, identify potential targets, enabling proactive protective security measures.

Prevent: Predicting Crime Hotspots enabling targeted preventative measures and resource allocation; forecasting Future Attack Trends; anticipating monitoring of potential hotspots & analyzing behavior patterns, disrupt potential attacks.

B. VCIS Added Value

Visibility

VCIS provides unparalleled "Global Visibility" by offering data insights beyond borders. The software manages a vast amount of data, processing up to 100,000 applications feeding mobility data daily, integrating 50 billion records seamlessly. With coverage spanning almost all countries, VCIS eliminates the need for traditional cooperation with local service providers, ensuring law enforcement and investigative agencies can access critical information globally, enabling a more effective response to transnational crime.

Data Correlation with Multiple Data Sources

VCIS excels in "Data Correlation with Multiple Data Sources," integrating telecom data (CDR & SDR), GIS, KYC, CCTV, NMS/IMS, tracking device data and other consolidation sources. This comprehensive approach allows investigators to establish connections and patterns across diverse datasets, facilitating a holistic understanding of criminal activities. By consolidating information from various sources, VCIS enhances the accuracy and depth of crime analysis, empowering investigators with a comprehensive toolkit.

Offline System

VCIS ensures security and accessibility with its "Offline System," operating as a standalone server without the need for an internet connection. This feature is crucial for sensitive investigations, allowing law enforcement to maintain control over access to critical crime and geospatial data. The offline capability ensures that investigators can conduct

covert operations without the risk of data compromise, providing a secure environment for strategic and confidential activities.

Friendly Graphical User Interface

VCIS prioritizes user experience with a "Friendly Graphical User Interface" that synchronizes different platforms among agencies. The software offers different data modules in one suite, eliminating the need for technical skills. This user-friendly design promotes efficient collaboration and information sharing among investigators, ensuring that agencies can seamlessly work together to analyze geospatial data and combat various crime types.

Giving the Investigator the Ability to Achieve Technical Tasks

VCIS empowers investigators by eliminating the need for sophisticated queries. The investigator can accomplish a wide range of tasks, limited only by their imagination. The software reduces the circle of confidentiality, enabling investigators to explore and analyze data without unnecessary barriers. This approach fosters a more dynamic and responsive investigative process, allowing for swift and effective action against criminal activities.

Technology, Big Data, and AI

VCIS integrates cutting-edge "technology, big data, and AI" handling both structured and unstructured data. The software efficiently ingests large amounts of data in measurable time, executing queries and scenarios in seconds. It performs complex predefined scenarios in the background, flagging suspicious devices or entities. VCIS provides alerts and daily threat analysis reports, leveraging AI to enhance predictive capabilities and ensure law enforcement stays ahead of evolving criminal tactics.

Navigating in Time

VCIS introduces the innovative feature of "Navigating in Time," facilitating backward and forward investigation. Investigators can understand the past, analyze the present, and predict the future. This temporal navigation enhances the software's capabilities to provide a dynamic and comprehensive view of criminal activities over time, empowering investigators to make informed decisions based on historical context and future trends.

C. The role of VCIS in combating Crimes Using Cryptocurrencies

Tracking the digital wallets' devices with geospatial technology

VCIS introduces a formidable capability in the realm of combating cryptocurrency-related crimes by providing an advanced means to track the devices associated with crypto wallets. This functionality relies on the utilization of device IDs, meticulously recorded in the Digital Know Your Customer (DKYC) within our VCMS solution. The DKYC serves as a robust repository, encompassing a comprehensive database that not only contains information about crypto wallet owners but also details various personal and technical aspects related to them. The fundamental strength of VCIS lies in its ability to empower law enforcement agencies in tracking the activities of these crypto wallet devices. By tapping into the data stored within the DKYC, VCIS facilitates the real-time monitoring of device actions, enabling authorities to delve into the intricate details of user interactions within the cryptocurrency ecosystem. This includes the dynamic capability to uncover links with individuals flagged as suspicious or associated with criminal networks. Moreover, VCIS extends its utility to investigators by providing a powerful tool for comparative analysis. The system enables investigators to cross-reference the tracked activities of these devices with transactions conducted by suspected individuals, all of which are meticulously recorded in the ledger database. This holistic approach enables law enforcement to gain a profound understanding of the behavioral patterns of criminals within the cryptocurrency landscape. By scrutinizing and correlating these activities, VCIS assists investigators in identifying not only the primary suspects but also discerning the users of other digital wallets linked to these individuals.

Tracking the flow of crypto transactions through a dynamic knowledge graph

VCIS presents a highly effective approach to monitoring and understanding the movement of cryptocurrency transactions through the implementation of a dynamic knowledge graph. This innovative tool proves invaluable in the tracking of illicit financial activities, offering law enforcement agencies an advanced solution for navigating the complex landscape of cryptocurrency transactions.

VCIS operates by concurrently tracking cryptocurrency transactions across various blockchain ledgers. This simultaneous monitoring allows for the creation of a dynamic knowledge graph,

a visual representation that captures the intricate relationships and flows of cryptocurrencies. By presenting these transactions on a common graph, VCIS facilitates the detection of the movement of funds from one wallet to another within the same blockchain. Additionally, it enables the identification of the exchange or swap of cryptocurrencies between different blockchains.

Beyond transaction tracking, VCIS further enhances its capabilities by establishing connections between wallet addresses and real persons or legal entities. This is achieved through a correlation process that involves cross-referencing data from the Digital Know Your Customer (DKYC) database with blockchain ledger databases. This integration empowers law enforcement to not only understand the financial transactions but also to link the identified wallet addresses to specific individuals or legal entities. If the individual is registered directly with the VCIS DKYC, their identity can be directly ascertained. In cases where direct registration is absent, the system employs sophisticated analysis techniques based on the extensive archive within the DKYC to indirectly identify the owner of a suspicious wallet address.

Identification of the digital wallets' owners by correlation between geospatial data and crypto transactions

The AI engine within VCIS is instrumental in discerning the owners of wallet addresses within specific geographical areas. To achieve this, the system dynamically tracks the activities of virtual asset service providers operating in those regions. This strategic approach allows VCIS to correlate geospatial data with the information stored in the online ledger database, thereby establishing connections between the physical location and the associated digital wallet addresses.

One notable outcome of this correlation is the automatic linking of device IDs to wallet addresses. VCIS efficiently captures and saves this amalgamated information within the Know Your Customer (KYC) database, creating a comprehensive repository that intertwines geospatial context with individual wallet identities. This process not only enhances the accuracy of identification but also contributes to a more detailed understanding of the users' geographical affiliations.

Moreover, the AI engine embedded in VCIS extends its capabilities beyond mere identification. It possesses the prowess to analyze the behavioral patterns of individuals associated with these wallet addresses. This includes an

examination of their activities, addresses, and network connections within the cryptocurrency ecosystem. By delving into these intricacies, VCIS equips law enforcement with the means to track and monitor potential illegal activities, shedding light on the misuse of cryptocurrencies in criminal endeavors.

Financial Criminal Links and POI circles

Each transaction is inherently linked to a specific location, and comprehending the spatial relationship between risks and portfolios is crucial for proactively minimizing fraud.

VCIS employs a sophisticated approach by leveraging machine learning and Geo-Smart location analytics to establish a comprehensive network of individuals and their associations within the financial realm. This innovative solution goes beyond merely processing transactions; it creates a dynamic representation of the spatial relationships between financial activities, individuals, and their respective points of interest. This contextual analysis provides a swift understanding of the environment surrounding a suspicious customer or transaction.

The system's ability to form connections and draw correlations in real-time allows VCIS to generate a complete view of the context within seconds. By creating a network of relationships, the solution identifies potential points of interest, whether they are geographical locations or specific financial entities. This capability facilitates the rapid follow-up of leads, enabling law enforcement and financial institutions to dynamically filter data and detect new relationships as they emerge. The emphasis here is on proactive and timely decision-making, ensuring that stakeholders possess a clear understanding of the larger picture surrounding financial transactions and potential risks.

Location-based Authentication

The implementation of geospatial technology in Location-based Authentication involves verifying the geographical origin of a transaction request. This is achieved by analyzing the physical location or geographical coordinates associated with the initiation of the transaction. Authorized locations are predetermined and considered legitimate, aligning with the expected areas where the account or user is likely to conduct transactions.

If a transaction request deviates from the anticipated or authorized geographical location, the system responds by triggering additional security measures or generating alerts. This dynamic response mechanism is crucial in promptly identifying and mitigating potential security threats. The

deviation from the expected location may signify unauthorized access, a compromised account, or an attempt at fraudulent activity, prompting the system to take preventive actions.
The benefits of Location-based Authentication extend beyond simply verifying the authenticity of transactions; it also acts as a proactive defense against unauthorized access and potential security breaches. By incorporating real-time geospatial data into the authentication process, the system adds an extra layer of scrutiny, making it more challenging for malicious actors to manipulate or exploit cryptocurrency transactions.

Risk Analysis and Anomaly Detection

Geospatial data can be integrated into security algorithms to analyze patterns and detect anomalies in transaction locations. Unusual or unexpected changes in geographic transaction patterns may indicate fraudulent activities, triggering further investigation or security measures.

Geospatial data, encompassing information related to the physical locations of transaction activities, becomes an integral part of the risk analysis process. By marrying this geographical context with advanced security algorithms, the system gains the ability to discern regular transaction patterns from irregular or anomalous ones. Unusual shifts in transaction locations or sudden deviations from established norms can serve as red flags, signaling potential fraudulent behavior.

In the event that the system detects anomalies in geographic transaction patterns, it triggers a series of responses. These responses can include initiating further investigation into the flagged transactions or implementing additional security measures to safeguard the financial system. The goal is to promptly address and mitigate any potential threats posed by fraudulent activities.
The strength of Risk Analysis and Anomaly Detection lies in its ability to proactively identify potential risks and deviations. By leveraging geospatial data, the system gains a nuanced understanding of transaction behaviors in different geographical regions. This understanding allows for the establishment of baseline patterns against which anomalies can be detected. In turn, this proactive stance enables financial institutions and security systems to respond swiftly and effectively to emerging threats, minimizing potential damages.

Conclusion

In conclusion, this document has navigated through the intricate corridors of cryptocurrency financing, regulatory compliance, and investigation methodologies. The rise of cryptocurrencies has not only transformed financial landscapes but has also brought forth a host of challenges that demand innovative solutions. By comprehensively examining the development, specifications, market dynamics, and the dark underbelly of cryptocurrency use, this document strives to uncover the needs that underscore the quest for viable solutions.

The exploration of regulatory compliance through the lens of FATF standards and the implementation of cutting-edge solutions like Crypto Digital KYC, WNMS, CRBA, and transaction monitoring underscores the commitment to a responsible and secure integration of cryptocurrencies within the global financial system. Finally, the in-depth analysis of VCIS and its pivotal role in crypto investigations highlights the importance of sophisticated tools and approaches in combating financial crimes facilitated by digital assets.

As we embrace the opportunities and challenges posed by the rise of cryptocurrencies, it becomes imperative to foster an environment that balances innovation with accountability, ensuring a resilient financial ecosystem for the future.