MERKLE SCIENCE
RegWatch

MAS Whitepaper: Next Generation Transaction Monitoring For Cryptocurrency Services Compliance

Abstract

The licensing and regulation of payment service providers in the e-money space, especially where cryptocurrency is involved, is a complex problem in today's world. Cryptocurrency transactions are tracked via the blockchain, analogous to a linked-list in a high-level sense, wherein the only data that is available over and beyond the transaction value is the transaction ID, the destination wallet address, and the source address.

In order to prevent criminal activities involving the use of cryptocurrency, payment providers need to source enriched data that adds in threat levels for a particular transaction proposal. This becomes paramount as the blockchain increases in complexity and size, since it becomes non-trivial to understand where the money eventually lands. While this is a problem that is fairly mature in the conventional currency space, this is very new in the cryptocurrency space.

Assessing threat levels in an accessible way, and providing APIs and tools to evaluate threat levels, will speed up the acceptance of cryptocurrency as legal tender in countries around the world as this will help payment providers comply with laws such as the Payment Services Act 2019 [1]. This paper goes into Merkle Science's implementation of a solution that hopes to alleviate the concerns of payment providers in this space and to improve the speed at which a given transaction can be assessed for a palatable level of threat in order to both prevent fraud and to comply with guidelines set by a local authority.

Introduction

As cryptocurrency becomes mainstream and larger players are assessing the legal tender status of the various coin-based platforms, it is necessary to carry over the rules that have successfully shepherded the payments platform space in the past to accommodate these coins. Doing so, however, is not a simple task, since the blockchain contains no identity associated with any transactions [2]. All that payment companies have access to are the transaction metadata that comes from the blockchain. By the nature of cryptocurrency, the receiver and senders' identities are obfuscated, thus rendering the implementation of any sort of payment regulation harder than traditional payment methods.

Through enriched metadata that we put atop of the blockchain data, Merkle Science has been able to monitor transaction risks, thereby identifying the taint level in a transaction. This facilitates payment providers, banks, regulators, and law enforcement agencies with the power to ascertain the risk in a cryptocurrency transaction. This level of intelligence is required to comply with regulations such as the aforementioned Payment Services Act 2019 [1], the PSN02 Notice [3] and the FATF Red Flag Indicators [4].

This paper discusses how we have built this system, which is a behavior-based rule engine, to enable crypto-businesses, financial institutions, and law enforcement agencies to manage direct and indirect cryptocurrency risk exposure. This engine is already empowering businesses from Singapore and the rest of the world to comply with regulatory acts.

Problem Statement

Cryptocurrencies are known to be used for criminal activity around the world. Various forms of cryptocurrency have been used to fund terrorism or to launder funds. Regulatory bodies interested in dictating compliance with their guidelines and acts require new tools and platforms to both police cryptocurrency usage and to encourage it. These regulatory bodies also need to meet the pressure that is bearing down upon them by global agencies that are interested in using cryptocurrencies for legitimate transactions.

Existing transaction monitoring tools, more interestingly those monitoring cryptocurrencies, focus on detecting criminal activity based on a database of cryptocurrency addresses that are associated with, or identified as being directly controlled by, criminal entities. Although these methods are sufficient for tracing the movement of funds from sanction addresses and known criminal bodies, they fail to assess the risk associated with transactions involving the more privacy focused cryptocurrencies such as ZCash [5], Dash [6] or Monero, or anonymity features such as the Lightning Network [7] and zk SNARKs [8].

This paper discusses Merkle Science's behaviour-based rule engine which goes beyond the capability of prevailing solutions and helps regulators, financial institutions, and crypto businesses detect not only direct risk but also indirect risk exposure, including the scenarios when the criminal is using advanced methods to bypass FATF guidelines [9][10] for AML/CFT [11].

Our Implementation

We seek to address this dual-problem faced by existing cryptocurrency companies, fintechs, and next-generation financial-institutions by:

1. Accurately detecting and preventing financial crime across cryptocurrencies on public blockchains.
2. Identifying suspicious transactions conducted using privacy-focused cryptocurrencies or features.

This solution involves a two-pronged approach:

1. A behavior-driven rule engine for classifying the risk level of potential transactions based on transactional history.
2. Building a broad cryptocurrency coverage for ingestion and analytics.

According to the book “Smart (enough) Systems” by James Taylor and Neil Raden, a business rule engine [12] is a system that helps encapsulate one or more workflows that are associated with a "transaction" in the general sense of the term. These rules are oftentimes related to regulatory directives, or internal logic that is esoteric to the operation of a business. Such a system is primed for utilization in a system that can be used to translate regulatory systems into code without baking in the logic into the system in and of itself.

We built our rule engine to translate customer and regulatory rules into actionable code. This grants users the ability to create finely-tuned rules, custom-designed to identify high-risk behavior using cryptocurrencies and allow companies to not only comply with one country's compliance rules but to tune their rules to meet the regulatory requirements of others as well.

And when it comes to building broad cryptocurrency coverage, aggregating additional cryptocurrencies into our system provides a wider landscape for payment companies to harvest on-chain data, thus furthering the adoption of bleeding-edge cryptocurrency formats.

Rule Engine

Using the methodology described above, we then utilize GSQL [13] queries to build multi-hop analytics to identify the taint on a node address. Not only do these help identify transactions congruous to the FATF Red Flag Indicators [14], but this also gives us the ability to quantify the risk associated with transacting with an address. When an address interacts with a crypto exchange, their taint for exchange-type addresses increases, which is good for their credibility. However, when the user interacts with a malicious party, either directly or indirectly, it tarnishes their credibility with a negative taint, associated with malignant players in the cryptocurrency space.

Every customer is allowed to set their preferred rules in the system, and the rule engine thereby classifies the addresses for them based on these rules. The UI offers intuitive selections for these, which are then translated to SQL and GSQL filtered queries.

The rules that our platform supports currently can be broadly classified into the following variants:

1. Address Rules
2. Transaction Rules
3. Behavioral Rules

Address rules are solely considered with the nodal type taints associated with a node. These can be used to perform validation depending upon whether a node is a malicious node or if it is trustworthy.

Transactional rules involve all parties in a transaction. This analyses not only the incoming funds but also the outgoing funds.

The above two rules can be categorized as Source of Fund Rules, while the behavioral rules can take historical data into account. This enables customers to set rules based on transactional history associated with a node.

The system builds views using these rules in dedicated views, so as to help access the results when needed. However, not all rules can be thus cached. At the moment, the graph queries are not precached, and are executed on demand. While this works for the current bandwidth, we are cognizant of the scaling issues and hope to set up pipelines to pre-cache all queries in the future. This is a major feature for our work in the future. Figures 1 and 2 below showcase the user interface for the rule engine feature of our platform.

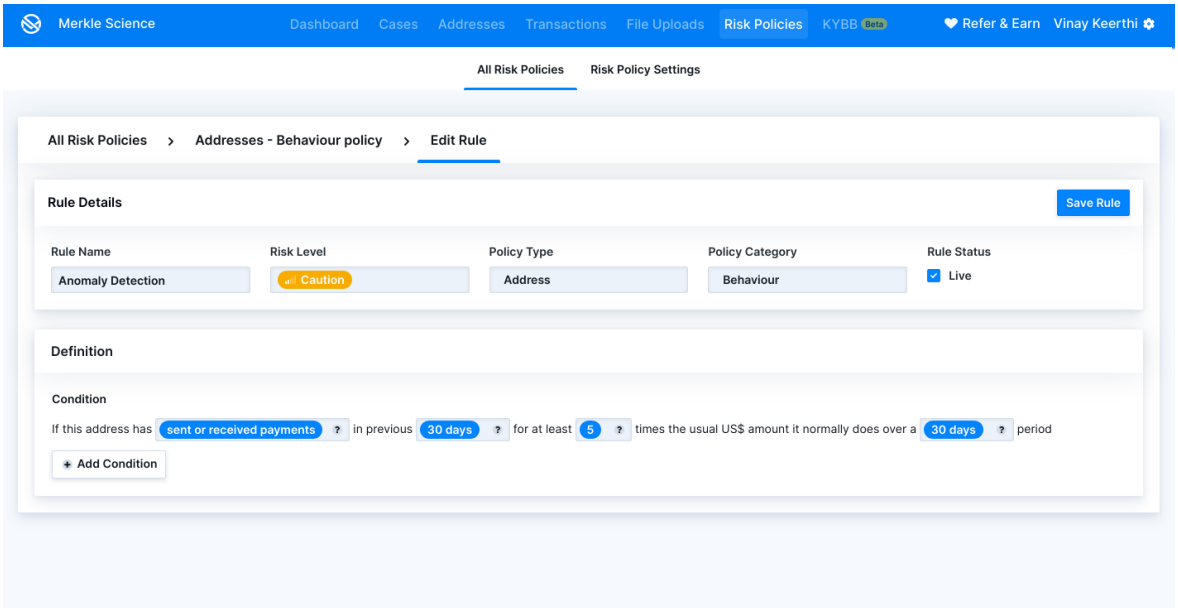

Fig 1. User Interface for anomaly-detection with address-based rules.

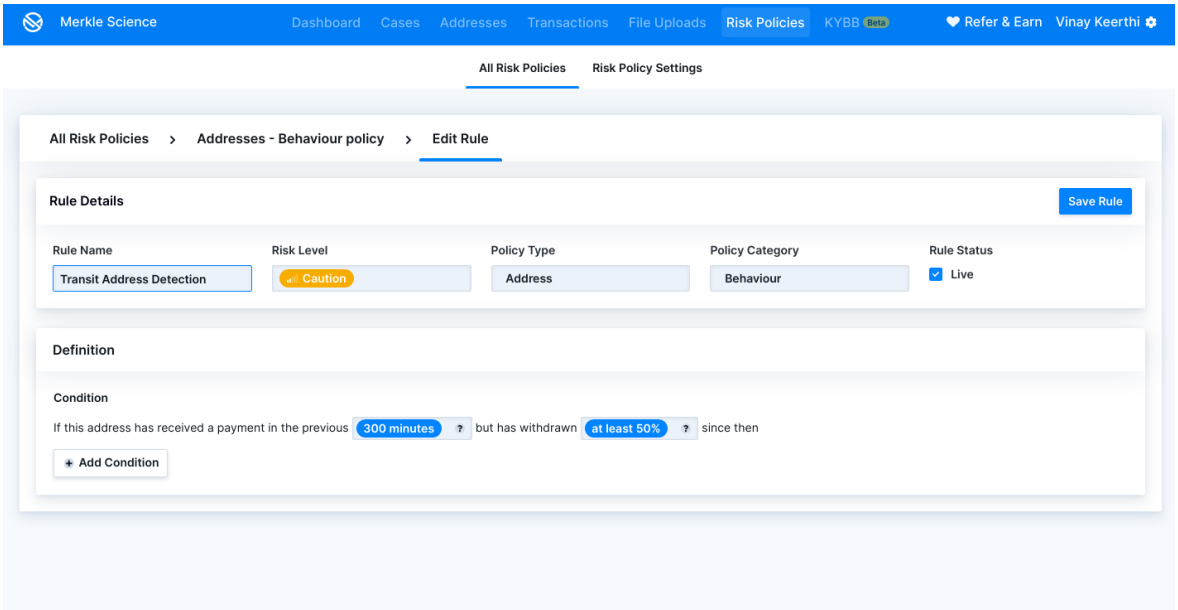

Fig 2. User interface to define a rule.

Related Work

While several efforts to improve the analytics around cryptocurrencies exist [15][16][17], some of them promising claims around cross-chain analytics [18], our approach has been to go beyond the blacklist. Blacklisting a series of addresses solves only a small subset of the problem described above. It is our belief that our multi-hop analysis, bolstered with machine learning and artificial intelligence-driven metrics, can further improve the compliance of cryptocurrency transactions with regulatory guidelines that have been applied to conventional digital currency transactions.

Conclusion

The risk assessment platform that we offer has integrated well with several existing coin formats, including, but not limited to:

1. Bitcoin
2. Ethereum
3. Litecoin
4. Bitcoin Cash
5. Ripple
6. Bitcoin SV
7. Dogecoin

In addition, we perform risk assessments on the following ERC-20 Tokens, but not limited to: Pundi X (NPXS), Tether (USDT), Paxos Standard (PAX), TrueUSD (TUSD), USD Coin (USDC), Basic Attention Token (BAT), XSGD (XSGD), Digix Gold Token (DGX), Function X (FX), Aave (AAVE), Ampleforth (AMPL), Bancor (BNT), Band Protocol (BAND), Binance USD (BUSD), Binance Coin (BNB), Celer Network (CELR), Celsius (CEL), Chainlink (LINK), Civic (CVC), Compound (COMP), Crypto.com Coin (CRO), Curve DAO Token (CRV), Dai (DAI), Enjin Coin (ENJ), Finxflo (FXF), The Graph (GRT), Kyber Network Crystal (KNC), Maker (MKR), Decentraland (MANA), Polygon (MATIC), OMG Network (OMG), SushiSwap (SUSHI), Swipe (SXP), Synthetix (SNX), TRON (TRX), Uniswap (UNI), Wrapped Bitcoin (WBTC), yearn.finance (YFI), SKALE Network (SKL), Zilliqa (ZIL), Gemini Dollar (GUSD), DFI.Money (YFII), 1inch (1INCH), Balancer (BAL), 0x (ZRX), IDEX (IDEX), Injective Protocol (INJ), Loopring (LRC), AirSwap (AST), MyNeighborAlice (ALICE), Alpha Finance Lab (ALPHA), AMP (AMP), Aragon (ANT), Bytom (BTM), BitTorrent (BTT), CRYPTO20 (C20), Compound Dai (cDAI), Compound Ether (cETH), Cartesi (CTSI), Compound USD Coin (cUSDC), Dent (DENT), DODO (DODO), aelf (ELF), Fei Protocol (FEI), Fetch.ai (FET), Ampleforth Governance Token (FORTH), FUNToken (FUN), Golem (GLM), GateToken (GT), HEX (HEX), Holo (HOT), Huobi Token (HT), HUSD (HUSD), IOST (IOST), IoTeX (IOTX), KuCoin Token (KCS), UNUS SED LEO (LEO), Metal (MTL), Nexo (NEXO), NKN (NKN), Numeraire (NMR), Ocean Protocol (OCEAN), OKB (OKB), Harmony (ONE), Orchid (OXT), PAX Gold (PAXG), Pundi X (PUNDIX), QuarkChain (QKC), Quant (QNT), QuickSwap (QUICK), REEF (REEF), Revain (REV), iExec RLC (RLC), Reserve Rights (RSR), The Sandbox (SAND), SHIBA INU (SHIB), Status (SNT), Storj (STORJ), sUSD (sUSD), Telcoin (TEL), OriginTrail (TRAC), UMA (UMA), Uquid Coin (UQC), Neutrino USD (USDN), TerraUSD (UST), Utrust (UTK), VeChain (VEN), Wrapped Filecoin (WFIL), Wrapped NXM (wNXM), Wootrade (WOO), SwissBorg (CHSB), Chiliz (CHZ), LockTrip (LOC), Livepeer (LPT), Origin Protocol (OGN), XinFin XDCE (XDCE), Orbs (ORBS), Prometeus (PROM), Ren(REN), Rocket Pool (RPL), THETA (THETA), Unibright (UBT), Voyager Token (VGX).

References

1. *Republic of Singapore Government Gazette Acts Supplement - Payment Services Act 2019 (https://sso.agc.gov.sg/Acts-Supp/2-2019/Published/20190220?DocDate=20190220)*
2. *Nakamoto, Satoshi - Bitcoin: A Peer to Peer Electronic Cash System (https://bitcoin.org/bitcoin.pdf)*
3. *Monetary Authority of Singapore - Notice PSN02 Prevention of Money Laundering and Countering the Financing of Terrorism - Digital Payment Token Service (https://sso.agc.gov.sg/Acts-Supp/2-2019/Published/20190220?DocDate=20190220)*
4. *FATF - Virtual Assets Red Flag Indicators of Money Laundering and Terrorist Financing (https://www.fatf-gafi.org/media/fatf/documents/recommendations/Handout-Red-Flags-VA-Public-Sector.pdf)*
5. *z.cash - How It Works (https://z.cash/technology/)*
6. *Dash - Documentation (https://docs.dash.org/en/stable/)*
7. *Lightning Network - How It Works (http://lightning.network/how-it-works/)*
8. *z.cash - What are zk-SNARKs (https://z.cash/technology/zksnarks/)*
9. *FATF - 40 Recommendations (https://www.fatf-gafi.org/publications/fatfrecommendations/documents/the40recommendationspublishedoctober2004.html)*
10. *FATF - IX Special Recommendations (https://www.fatf-gafi.org/publications/fatfrecommendations/documents/ixspecialrecommendations.html)*
11. *imf.org - Anti-Money Laundering/Combating the Financing of Terrorism (https://www.imf.org/external/np/leg/amlcft/eng/)*
12. *Prentice Hall - Taylor, James; Raden, Neil - Smart (Enough) Systems - ISBN - 0-13-234796-2*
13. *TigerGraph - GSQL Query Language - (https://www.tigergraph.com/gsql/)*
14. *FATF Recommendations - Virtual Assets Red Flag Indicators of Money Laundering and Terrorist Financing (https://www.fatf-gafi.org/publications/fatfrecommendations/documents/virtual-assets-red-flag-indicators.html)*
15. *CypherTrace Armada - Cryptocurrency Intelligence to Boost Your KYA-AML Program (https://www.niceactimize.com/anti-money-laundering/cryptocurrency-intelligence/)*

16. Sift One Pager - Digital Trust & Safety Vendor Evaluation Checklist: Machine Learning vs Rules (https://resources.sift.com/onepager/digital-trust-safety-vendor-evaluation-checklist-machine-learning-vs-rules/)

17. TRM Labs - Why We are different (https://www.trmlabs.com/)

18. Chainalysis Data Network - Documentation (https://docs.chainalysis.com/api/cdn/#introduction)