



**MONITOR**  
—CHAIN—

Real-Time Security Alerts for Ethereum Tokens and Exchanges

# Cryptocurrency Hacks and Theft: A Multibillion Dollar Problem



**34,000 +**

Vulnerable Ethereum smart contracts



**14%**

Of major crypto currencies stolen



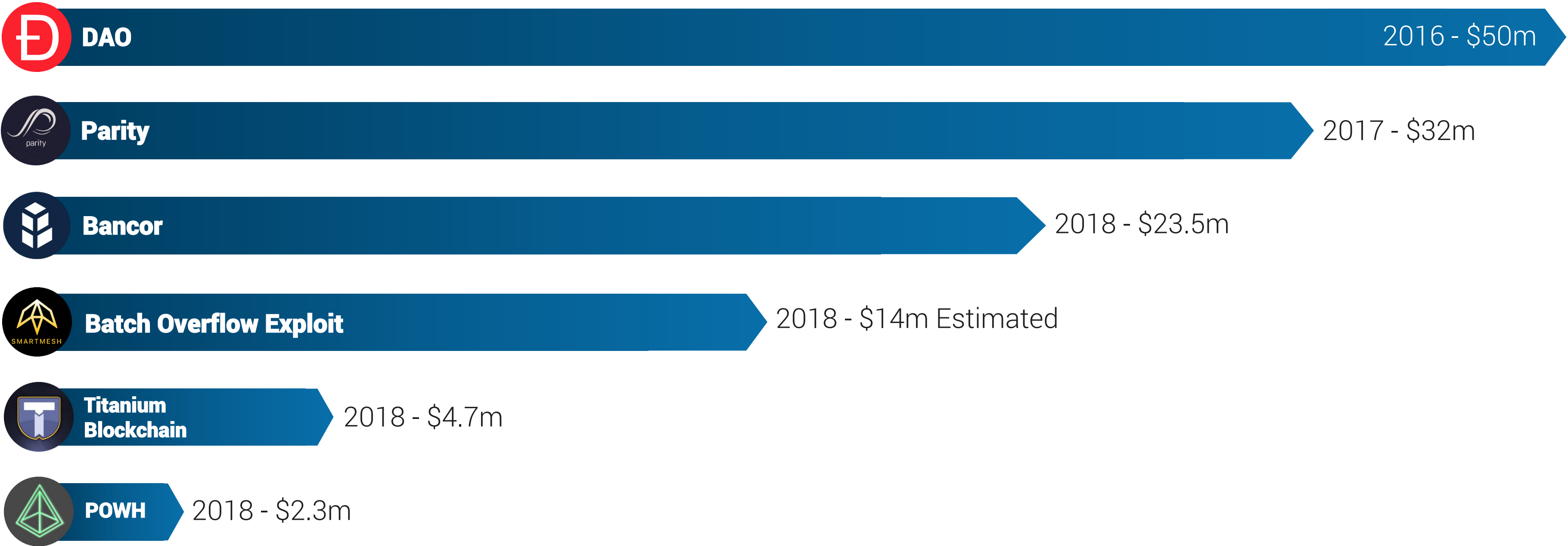
**1,100,000,000**

USD equivalent stolen so far in 2018

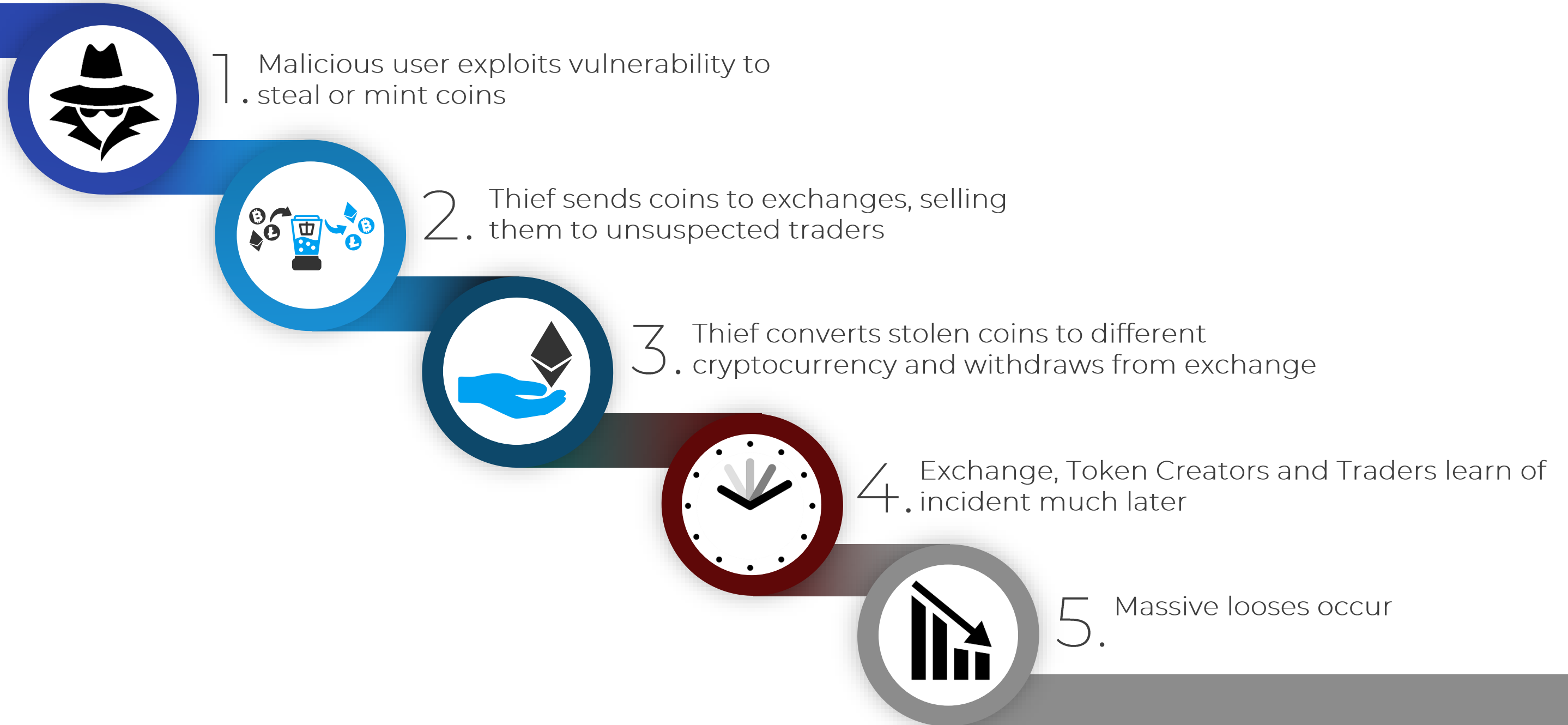
# Notable Hacks on Ethereum Blockchain

Numerous programmatic smart contract exploits that MonitorChain would have prevented

Crypto fraud is a multi-billion dollar industry.



# Anatomy of a Major Hack



# Meet the Victims of Crypto Fraud



## Traders and Investors

- *Traders unknowingly buy stolen / counterfeit tokens*
- *These tokens, formerly assets later become useless*
- *There is little to no recourse or asset recovery*



## Token Creators (ICOs)

- *There are over 550 tokens on Ethereum blockchain*
- *These tokens can be vulnerable to smart contract hacks*
- *Creators cannot suspend trading in case of an exploit or breach*




## Token Exchanges

- *There are hundreds of Token Exchanges operational World-Wide*
- *These exchanges are regularly targeted, hacked and exploited*
- *Hackers use these exchanges as Dumping Grounds for stolen tokens*

# Fraud of the Blockchain: batch / proxyOverflow Exploit

Transfers **Holders** Info Exchange ReadContract Write Contract <sup>Beta</sup> Comments (2)

 Token Holders Chart

Top 1000 Holders (From a total of 7387 Holderss)

[First](#) [Prev](#) [Page 1 of 20](#) [Next](#) [Last](#)

Rank	Address	Quantity	Percentage
1	<a href="#">0xdf31a499a5a8358b74564f1e2214b31bb34eb46f</a>	6.51330501959904E+58	2,073,249,379,858,110,000,000,000,000,000,000,000,000,000,000,000,000.0000%
2	<a href="#">0xd6a09bdb29e1eafa92a30373c44b09e2e2e0651e</a>	5.06590390413258E+58	1,612,527,295,445,190,000,000,000,000,000,000,000,000,000,000,000,000.0000%
3	<a href="#">0x5faf679d017438f481faf55e0f0cac3998ed1c88</a>	1.01E+20	3,214,929,851,059.8500%
4	<a href="#">0x80c0f1ba0e243f5c5c8cc45e0d6c95ce1cbff41b</a>	9.9999999999564E+19	3,183,098,862,434.1000%
5	<a href="#">0xe29526b6d7def7433823851c25f36a365567165f</a>	9.9999999999772E+18	318,309,886,243.4770%
6	<a href="#">0x38c1617864cbab17a5e4078ffd37a587ef0d4236</a>	1.0000000006561E+16	318,309,886.4524%
7	<a href="#">0xb4d30cac5124b46c2df0cf3e3e1be05f42119033</a>	100000000000000	3,183,098.8624%

- Hackers exploited math syntax error to create themselves unlimited tokens
- Newly minted tokens dumped on exchanges , crashing over books and costing millions

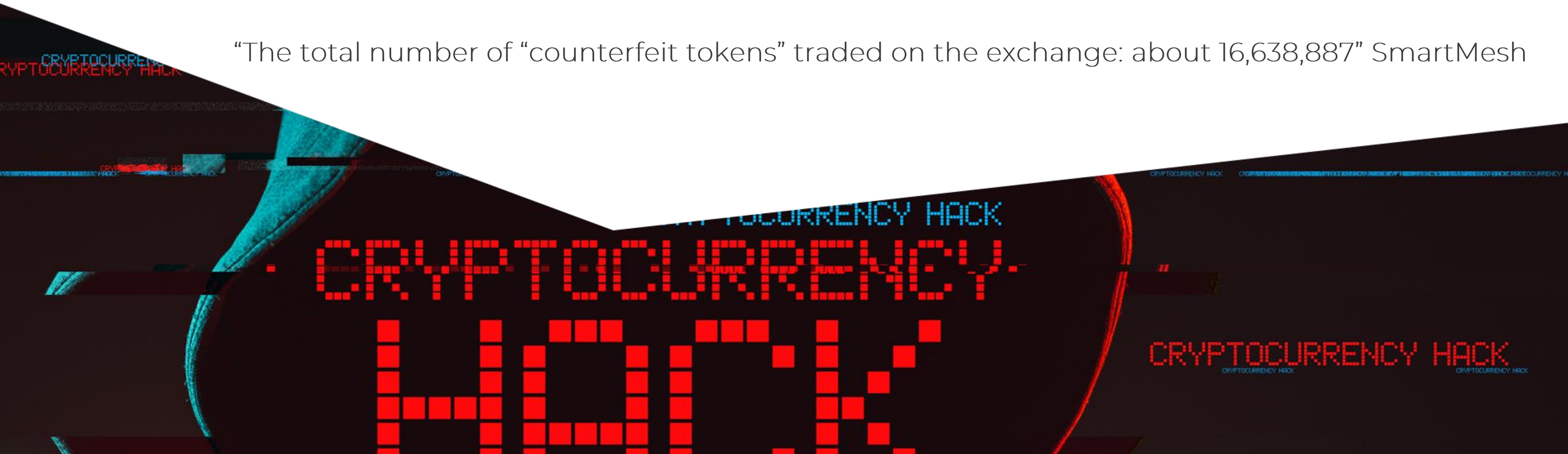


# Fraud of the Blockchain: batch / proxyOverflow Exploit

## Smart Contract Vulnerabilities

- 12 tokens effected over a period of 5 days
- Hacker minted tokens dumped on at least 3 top 10 exchanges
- SmartMesh (effected token) spent \$1.4m reimbursing victims
- Once discovered, mass panic caused many exchanges to suspend trading on hundreds of tokens for multiple days

“The total number of “counterfeit tokens” traded on the exchange: about 16,638,887” SmartMesh



# Fraud of the Blockchain: Monero Gold

## Inside Job

- \$4m USD ICO hid a backdoor in their code to complete exit scam
- Exploited their own burn function to create trillions of new coins
- Sent to CoinExchange.io and dumped on traders
- Vanished with Bitcoin and a farewell message on their website
- Exchange, ICO investors, and traders all suffer heavy losses

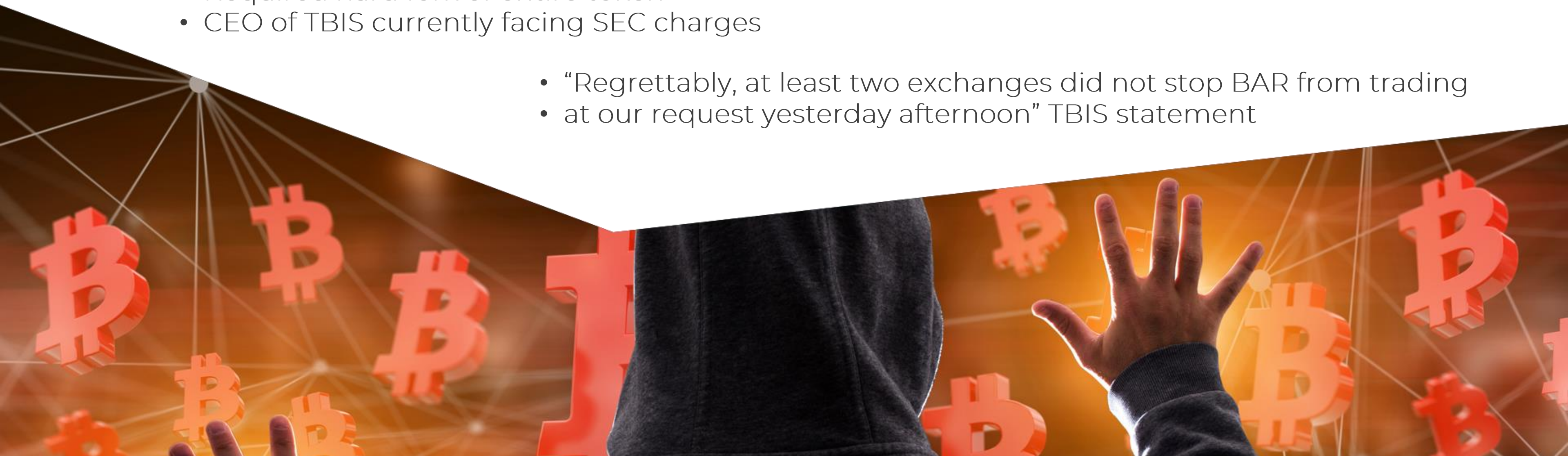




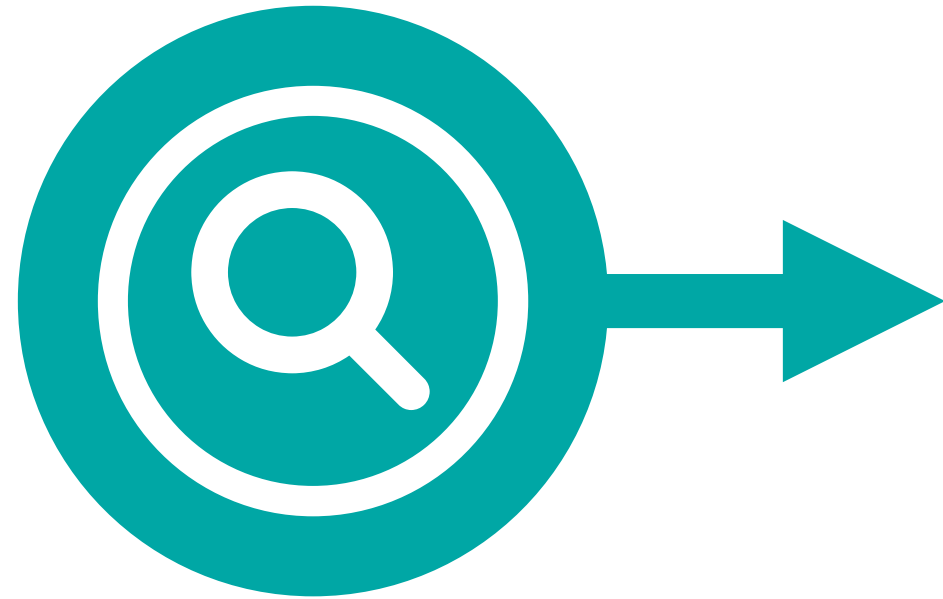
# Fraud of the Blockchain: Titanium Bars Infrastructure Service

## Organizational Security Weakness

- 16 million tokens stolen from team multisig wallet with time locked vesting
  - Theft occurred more than 24hrs before tokens dumped on exchange
  - Initial response dismissed a hack had occurred
  - Once team realized severity, asked exchanges to halt trading, which they did not in time
  - Required hard fork of entire token
  - CEO of TBIS currently facing SEC charges
- 
- “Regrettably, at least two exchanges did not stop BAR from trading
  - at our request yesterday afternoon” TBIS statement



# The Solution: MonitorChain



## MONITOR

*Live monitoring of token contract health  
for up to the block detection of potential exploits,  
hacking or theft patterns.*



## ALERT

*Immediate notification when a token  
may have been compromised  
delivered directly via the Ethereum  
Network*



## PROTECT

*Take preventative action by smart  
contract oracle and get notifications  
**before** stolen/counterfeit tokens are  
used.*



# How it Works...



## MONITOR

*Live monitoring of token contract health for up to the block detection of potential exploits, hacking or theft patterns.*

Oracle-ready proprietary alert feed on the Ethereum blockchain  
Compatible with 550+ Ethereum tokens  
Automated transaction surveillance






# Threat Ranking

Examples of events that may trigger subscriber alerts at each level of threat ranking.




**0**  
**Good**

- Nothing to alert.



**1**  
**Notice**

- Trading of more than 3% of total supply
- Minting of more than 1% of total supply



**2**  
**Warning**

- Sudden increase in transaction volume
- Suspicious transaction patterns



**3**  
**Severe**

- Transaction signatures indicate possible double spend
- Transfers in violation of coded terms in smart contract
- Substantial minting event



**4**  
**Emergency**

- Massive change of total supply in violation of minting rules
- Transfers more than 1005 of total supply
- Full balance of locked account holding > 10% supply transferred





## ALERT

*Immediate notification when a token  
may have been compromised  
delivered directly via the Ethereum  
Network*

Five tiers of alerts based on threat severity  
Securely broadcasted over Ethereum in contract readable form  
Notifications instantly upon start of a suspected heist

# Alert Notification Methods



## Smart Contract Oracle

Interface directly with Dapp and Token Contract admin functions for automated protection



## API

Connect to any existing platform via robust API interface



## Email

Instant alerts directly to the inboxes of those who need it most



## SMS

Alert to your phone.  
Coming Soon...





# PROTECT

Take preventative action by smart contract oracle and get notifications **before** stolen / counterfeit tokens are used.

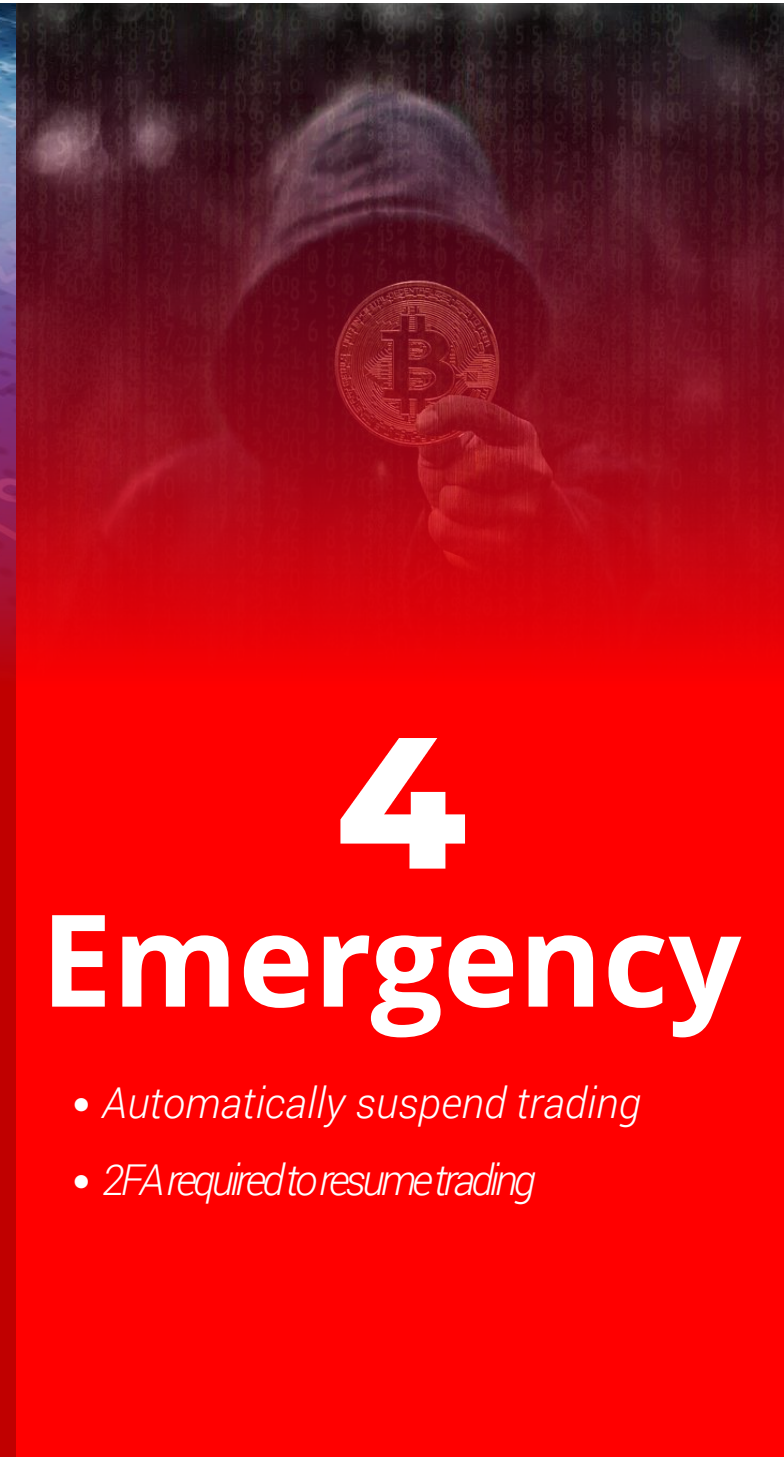
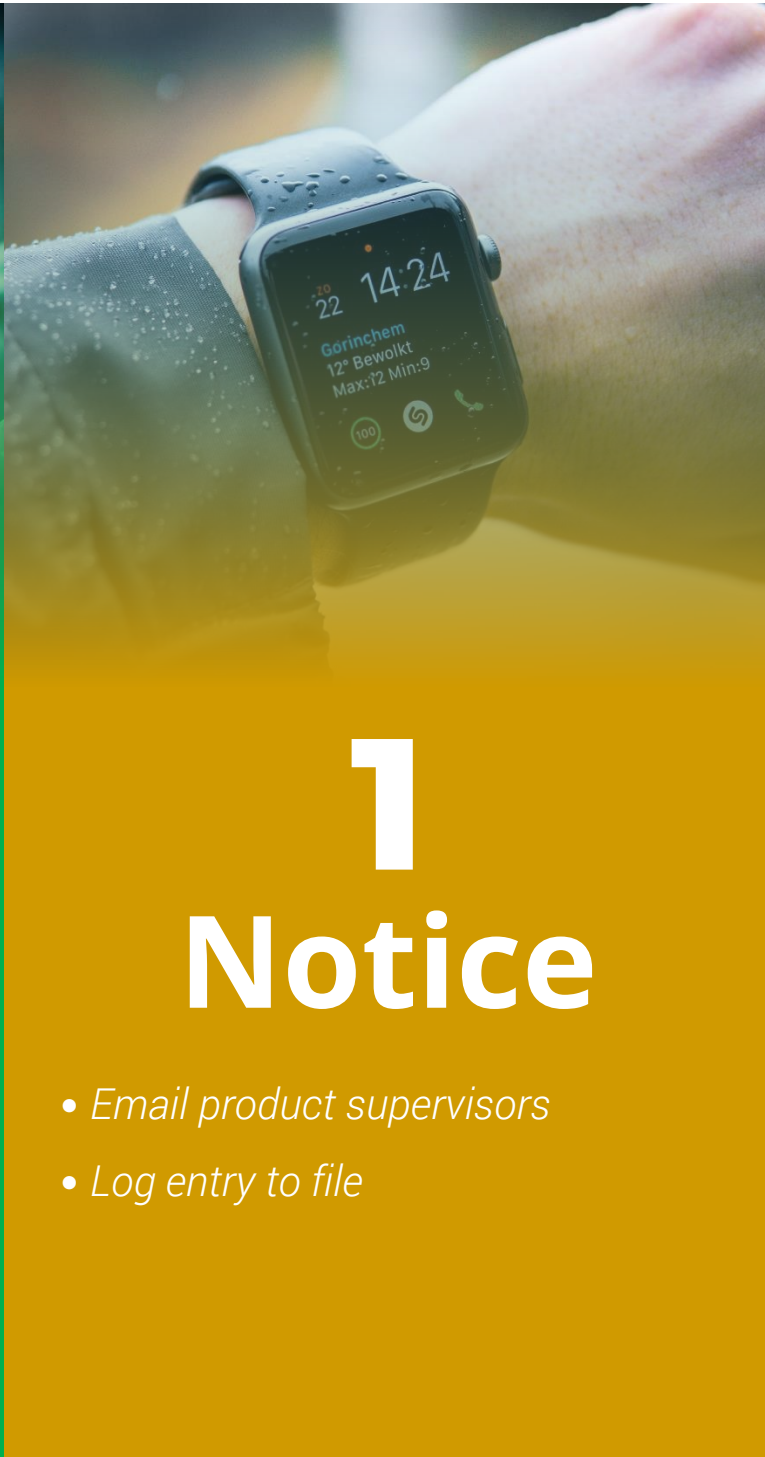
Automated actions based on threat rank  
Freeze trading **before** liquidation occurs  
Block the ability to trade stolen tokens





# Automated Actions

Examples of how subscribers can programmatically trigger events based on threat ranking.



# Features



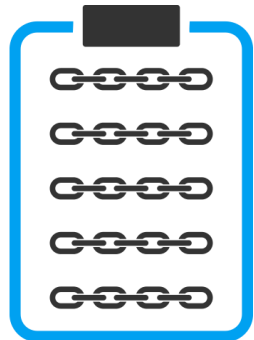
## Custom Monitoring

Set your own alert conditions. We work with you to set specific monitoring rules and alert thresholds based on your business needs. This allows complete customization as defined by you. *\*For Enterprise subscribers only*



## Bespoke Integration

For Enterprise clients, our dev team will work hands on to assist in full integration with your existing management systems and smart contracts, including the creation of new smart contracts to interact with your own and API customization. For all subscribers, we include a library of integration code samples to make using MonitorChain quick and easy.



## Blockchain Agnostic

MonitorChain can be modified and ported to any public or private blockchain as required.

**Dedicated  
Support**



**MONITOR  
—CHAIN—  
PROTECTED**





**MONITOR**  
—CHAIN—

**Your first-line defense against programmatic heists**

**Currently seeking partnership and investment. For more information, or to schedule a live demo of MonitorChain please email contact us.**

**[Seth@Zenchain.com](mailto:Seth@Zenchain.com)**

**<https://MonitorChain.com>**