



Toncoin and Its Use in Cybercrime: **KillNet Case Study**

By Anastasia Sentsova

Contents

Introduction	3
Key Findings	4
Toncoin: How it Started	5
TON's Come Back in 2021	6
September 2023: TON Finds its Way Back to Telegram	6
TONs of Features for Its Users	7
Fragment	7
Wallet	9
Crypto Bot	9
Donate	9
KillNet Case Study	10
Assessing the Risks	13
1. Shift of Illicit Activity from Tor to Telegram	13
2. Deep Integration of Toncoin Services with the Telegram Ecosystem & Presence of Russian Financial Institutions and Payment Services	14
Conclusion	15

Introduction

Investigating cybercrime is similar to putting together a puzzle – the entire picture is unclear until all the pieces are in place. The investigation itself is complex and involves multiple vital components to consider, with one of them being cryptocurrency. By integrating both on-chain and off-chain intelligence, the level of analysis is elevated. Cryptocurrency component is important as it is essentially a fuel that keeps cybercriminals running.

Blockchain and cryptocurrency are revolutionary technologies that offer multiple benefits to people and financial systems. However, they also became a lucrative tool for cybercriminals, leveraging advantages such as anonymity and privacy to support their malicious activity. The cryptocurrency market offers diverse options, and actors certainly develop their preferences. With Bitcoin (BTC) and Monero (XMR) known to be among the favored, actors also actively use less famous cryptocurrencies for various means; one of them is Toncoin.

This research explores the history, features, and native cryptocurrency of The Open Network (TON) blockchain. To demonstrate its current usage patterns by cybercriminals, this analysis provides a case study of Toncoin used by the pro-Russia hacktivist group KillNet. It aims to show the entire cycle from receiving funds to moving them to their last destination – the cash-out point. Furthermore, the article includes a risk assessment of factors that might contribute to an increased usage of Toncoin in illicit activity.

It is essential to remember that none of the cryptocurrencies are bad; people who misuse them are. It takes an effort to find a balance between fostering new technology and keeping it safe. Analyst1 aims to supply you with the knowledge to navigate this deep water.

Key Findings

- KillNet, a pro-Russia hacktivist group, was identified soliciting donations in Toncoin cryptocurrency. The group engages in DDoS attacks, primarily targeting NATO countries. While it is unclear if the group is government-controlled, their activity aligns closely with the Russian state's geopolitical agenda.
- Toncoin is a native cryptocurrency of the TON blockchain. Previously known as Telegram Open Network (which is now defunct), it was developed by Pavel Durov, founder of Telegram messenger. Long claimed to be fully independent from messenger, TON Foundation announced partnership with Telegram on September 14, 2023, with the goal for Toncoin to become a means of payment within the platform.
- As a result of the investigation, Analyst1 identified three KillNet addresses that received nearly \$44,000 USD as of September 15, 2023. Further analysis was conducted to demonstrate at least one instance of a complete cycle of receiving Toncoin and tracing it to its last destination cash-out point, a centralized exchange.
- The Toncoin ecosystem's deep integration with Telegram is cause for concerns. Given the noticeable increase in illicit activity stemming from actors transitioning from TOR to Telegram, there's a heightened risk of Toncoin gaining popularity among cybercriminals.
- The involvement of Russian financial institutions, including banks and payment systems integrated with Telegram/Toncoin services, adds to these concerns. This ease of access might offer cybercriminals a more straightforward means of cashing out, especially for those with ties to financial institutions inside of their home jurisdiction.

Toncoin: How it Started

In 2018, two brothers, Pavel and Nikolai Durov, also known as founders of the messaging platform Telegram, launched the [TON](#) blockchain (The Open Network), previously known as Telegram Open Network. Gram, TON's first native cryptocurrency primary goal was to establish itself as a payment medium to dominate the realm of social media-based transactions within the Telegram ecosystem.

In the same year, 2018, Telegram conducted a private sale of Gram tokens to a limited number of accredited investors as a part of an Initial Coin Offering (ICO). Telegram raised significant money, reaching around \$1.7 billion USD from private sales alone.

In March 2020, the U.S. District Court for the Southern District of New York issued a preliminary [injunction](#), halting the issuance of Gram tokens due to the Securities and Exchange Commission (SEC) investigation that identified violations of the federal securities laws. The defendants [agreed](#) to return more than \$1.2 billion USD to investors and to pay \$18.5 million USD as a civil penalty.

In May 2020, Pavel Durov officially announced the closing of the TON project due to legal challenges they faced. Before leaving the project, Durov made the TON source code public, hoping the community would revive it one day.

Soon after, at least two community-driven [TON projects](#) emerged. First, TON Crystal in May 2020, led by TON Labs, a venture capital tech company that helped Telegram launch the TON test network early on. The second community-driven project was the TON Foundation (called Newton until May 2021). The project was named TON, with its native cryptocurrency, Toncoin, and listed on several exchanges.

TON's Come Back in 2021

In a message shared on Telegram on December 23, 2021, Pavel Durov openly supported the TON project and its new native cryptocurrency, Toncoin.

The revived TON blockchain is built on previous source code and has long claimed to be fully independent from Telegram, a community-driven project.

According to TON's technical lead [Anatoliy Makosov](#), he started developing an open-source community named "TON Foundation" in 2020.

Makosov's goal was to further the development of Telegram Open Network, which later evolved into "The Open Network" (TON).

TON developers have high hopes for their project and promise it to become the "sexiest blockchain" on the market. Based on Makosov's assessment, "TON is technologically ahead of all other existing blockchains, especially in terms of its ability to scale to a large number of users and transactions." According to its [official website](#), TON's current capacity is millions of transactions per second (TPS), and it intends to reach hundreds of millions of users eventually.

September 2023: TON Finds its Way Back to Telegram

On September 14, 2023, Pavel Durov announced a partnership between TON Foundation and Telegram. According to the message, starting November 2023, the Wallet bot (which functionality we will discuss below) will be integrated into Telegram as [mini app](#). This service will be available for all Telegram users except in "the US and some other countries".

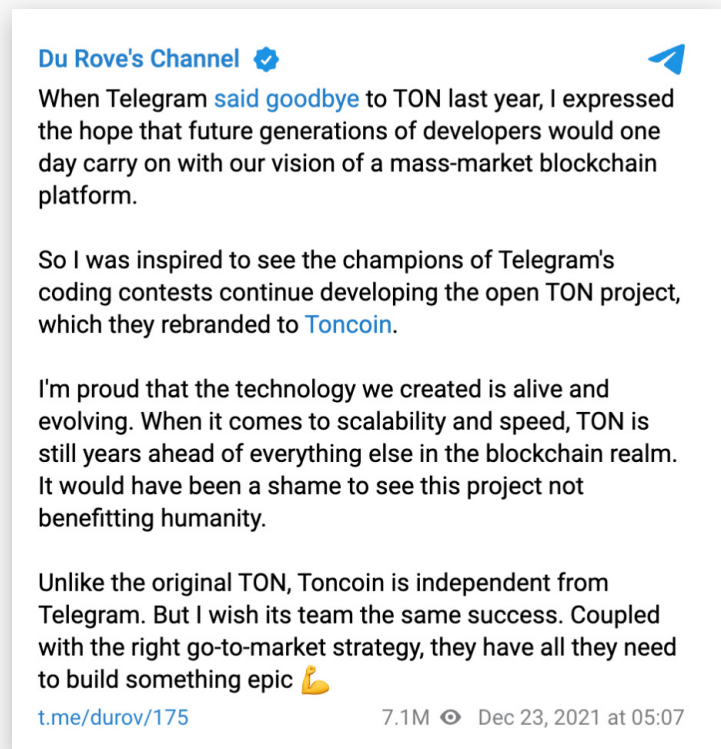


Figure 1: Message from Pavel Durov discussing his support of the TON project (Source: Telegram).

Du Rove's Channel 



Years ago, we built [TON](#) – a scalable and fast blockchain technology. TON was designed to serve hundreds of millions of social media users. Since 2020, the TON technology has been maintained and improved by the open source community.

Last year, we enabled our users to buy and sell Telegram usernames and IDs on [Fragment](#) – a TON-based auction platform. It was a phenomenal success. Telegram sold \$120M worth of digital assets in auctions, while early buyers of some Telegram-related digital assets – such as Telegram anonymous numbers – have seen a 27x (!) increase in value after only 9 months.

This success showed the potential of Web 3.0 on Telegram. For the first time in history, users were allowed to own their social media identities directly. Now we want to integrate blockchain technologies deeper into Telegram. To do that, we worked with the folks from the TON community to add their [TON Wallet](#) to Telegram as a [mini-app](#).

Starting this November, TON Wallet will be included in the settings and attachment menus for all our users outside the US and some other countries (if you added [@wallet](#) and have the latest version of Telegram, you can already see the wallet option in the menus). This step will allow developers to enable hundreds of new valuable features – similar to those pioneered on Fragment. TON Wallet, a third-party mini-app inside Telegram, will introduce a whole new dimension of Web 3.0 to hundreds of millions of Telegram users.

t.me/durov/225

284.5K  edited Sep 14 at 12:58

Figure 2: Pavel Durov's message announcing partnership between TON Foundation and Telegram (Source: Telegram).

Developers express a lot of optimism regarding the future of TON's native cryptocurrency, Toncoin. By introducing this feature, Telegram aims to onboard 30% (nearly 300 million people) active users to TON in the next 3 – 5 years.

TONs of Features for Its Users

With the original supply of 5 billion Toncoin, its circulating supply has reached \$3.43 billion USD and trading price at \$2.41 USD as of September 18, 2023, according to CoinGecko. Toncoin is listed on several centralized and decentralized exchanges.

In support of Toncoin's adoption, Telegram offers a variety of services to its users. An overview of these can be found below. Note that some of these services are used by KillNet as will be shown in the case study below.

Fragment

One of the services offered is the Fragment, NO-SIM signup feature designed to unlock a higher level of security and anonymity for its users. Previously, it required its potential user base to register with a phone number. Now, users can purchase an anonymous number in exchange for Toncoin through the Fragment platform. In addition, the Fragment platform offers usernames that can be resold later.



Figure 3: Front page of Fragment trading platform website (Source: fragment.com).

For these reasons, the Fragment service quickly became popular among Telegram users. According to Pavel Durov's Twitter post on November 30, 2022, Fragment sold \$50 million USD worth of usernames less than a month after its launch.



Figure 4: Message from Pavel Durov announcing successful launch of Fragment trading platform (Source: Twitter).

Other services worth mentioning are bots @wallet, @CryptoBot, and @donate. All three are directly integrated through Telegram and designed to provide crypto-related user experience without leaving the platform.

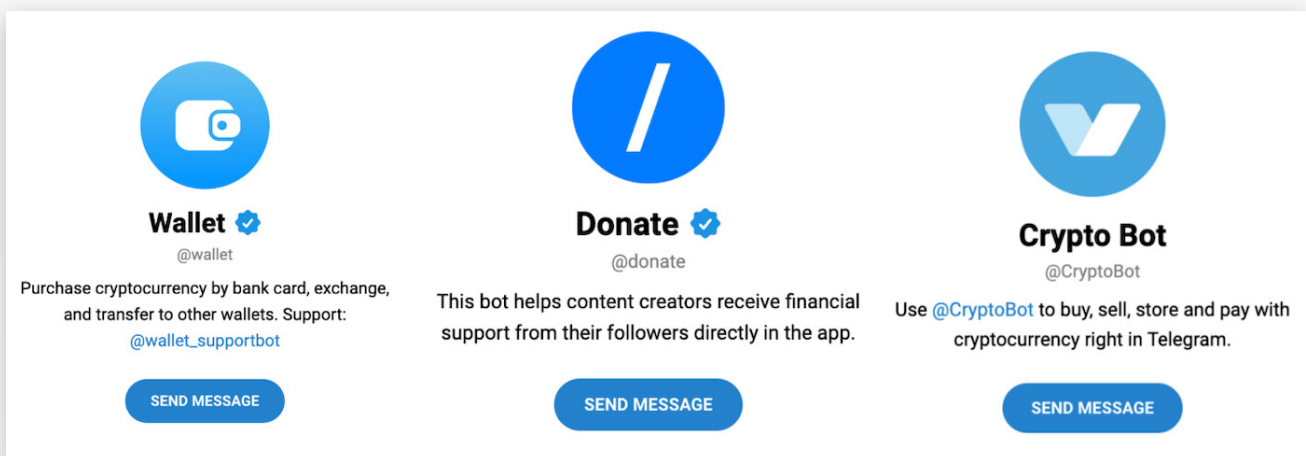


Figure 5: Telegram pages of crypto bots (Source: Telegram).

Wallet

Launched in April 2022, Wallet service added the first crypto functionality to Telegram. Some of the Wallet features are:

- P2P market to send TON, USDT and BTC to users' contacts,
- Multicurrency wallet to buy and store cryptocurrency directly on Telegram,
- SWAP feature to exchange TON into another cryptocurrency such as USDT.

Crypto Bot

Crypto Bot offers a variety of features allowing its users to make payments and exchange crypto. Some of them are:

- Multicurrency wallet to store, send, and receive TON, BTC, ETH, USDT (ERC20, TRC20, BEP20), BUSD, USDC, BNB;
- P2P (Peer-to-Peer) market that facilitates buying and selling coins for fiat currencies. Users have access to 10 payment methods, which encompass transfers to Russian bank cards (Sberbank, Tinkoff, Alfabank and others) and electronic wallets (JuMoney, WebMoney, QIWI);
- Invoices to request payments from other users.

Donate

Launched in 2021, the service is designed to provide Telegram users (content creators) the ability to accept donations. Donate features and rules include:

- Accept donations in cryptocurrency and fiat by content creators with more than 100 followers,
- Donations are available to make and accept through bank cards that work with all Russian banks and payment systems.

KillNet Case Study

KillNet, a pro-Russia hacktivist group operating since approximately late 2021 and engaging in DDoS attacks uses Toncoin as one of many cryptocurrencies to fund its operation. The group openly and fully supports the Russian state by attacking entities that the group considers opponents of the Russian geopolitical agenda. As of today, according to KillNet Telegram posts, the group launched numerous attacks mostly against NATO countries.

KillNet has a long history of online presence on Telegram, which it uses as the primary communication channel and a means for soliciting donations. In their messages, actors ask for financial support in fiat and various cryptocurrencies, including Toncoin.



Figure 6: KillNet actors asking for donations on their Telegram channel (Source: Telegram).

The successful outcome of blockchain investigation relies on the accuracy of attribution. This attribution is the intelligence collected as the result of analysis that allows linking a particular crypto address to an entity (ex. individual or cybercrime group). Based on our research, three Toncoin addresses were attributed to KillNet with a high degree of confidence. For the sake of clarity, we'll refer to them as KillNet Address #1, KillNet Address #2, and KillNet Address #3.

Supporters of KillNet have donated funds generously to the group. Notably, many of these donations are accompanied by patriotic comments cheering KillNet, such as “Glory to Russia”, “Keep work-ing, brothers”, etc. Furthermore, multiple transactions were made through Wallet and Crypto Bot services, which functionality we analyzed earlier.

20 Jun, 20:28	↓ Received TON	EQDspMob...K7DAQjny	Держи братан ,👊👊	+1 TON
20 Jun, 11:09	↓ Received TON	EQCl08Pz...6wg5kJgX	Спасибо!	+1 TON
19 Jun, 12:50	↓ Received TON	EQAZG1r9...AABB61Yu	-	+1.85 TON
19 Jun, 12:13	↓ Received TON	EQDzMfA0...T7emVd3L	Slava Rossii	+0.9 TON
19 Jun, 11:33	↓ Received TON	Wallet Bot	7a303eb6-d424-4230-b7e3-ebef0...	+0.05 TON
19 Jun, 11:10	↓ Received TON	EQC-_jWX...syJ8SHo-	-	+37 TON
19 Jun, 11:09	↓ Received TON	EQCtyF76...8ZXrFWcN	Работайте, братья	+5 TON
18 Jun, 15:15	↓ Received TON	EQCcZpU-...4WEUcJBH	👉👊	+10 TON
03 Jun, 05:33	↓ Received TON	EQASQ3XG...PBP6nvz2	-	+1.801 TON
02 Jun, 09:53	↓ Received TON	CryptoBot	-	+1 TON

Figure 7: Incoming transactions made to one of the KillNet addresses accompanied with comments from senders (Source: tonviewer.com).

In addition to Wallet and Crypto Bot services, the Fragment service used by KillNet was observed. Actors used the NO-SIM signup service to purchase a @killnet username linked to one of KillNet’s channels. It was sold on November 18, 2022, for 600 Toncoin.

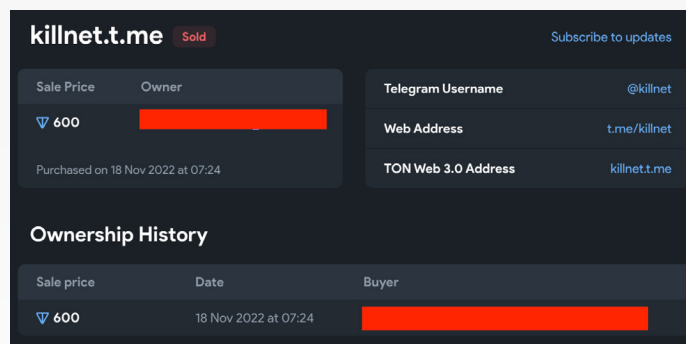


Figure 8: Image demonstrates purchase of @killnet username through Fragment trading platform (Source: fragment.com)

Based on the investigation, three addresses attributed to KillNet received nearly 16,800 Toncoin as of September 15, 2023, equivalent to nearly \$44,000 USD. (Disclaimer: numbers are based on public data from TON blockchain)

The graph below illustrates the movement of 2,783 Toncoin from KillNet Address #1 to KillNet Address #2, 2,000 Toncoin to KillNet Address #3 until actors transferred a portion of funds in the amount of 700 Toncoin to a centralized exchange.

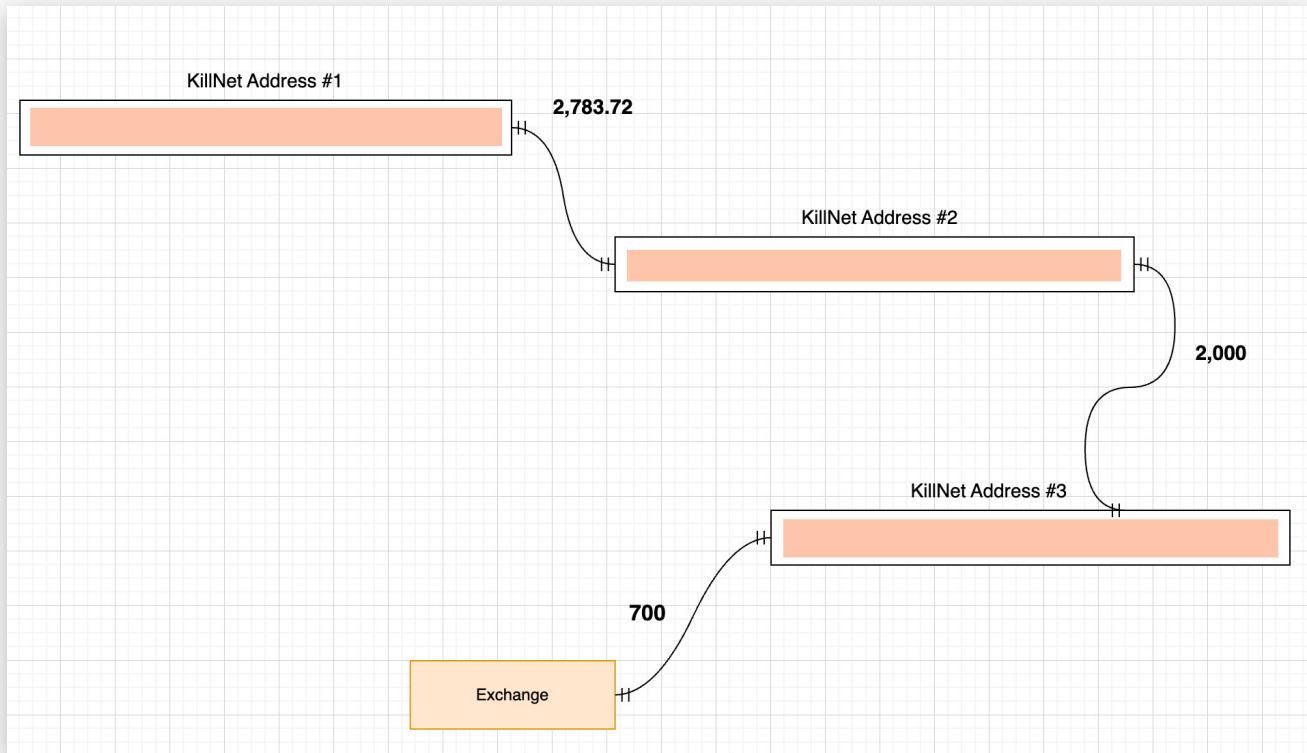


Figure 9: Graph shows movement of funds from KillNet addresses to the exchange (Source: Analyst1).

With this single instance, a complete cycle of receiving Toncoin and tracing it to its last destination cash-out point, a centralized exchange, is revealed. The nearly \$44,000 received by three addresses seems relatively high, especially compared to known BTC address used by actors for donations that received almost \$23,000 USD. To uncover the full spectrum of Toncoin used by KillNet requires further investigation.

Assessing the Risks

TON aims to onboard nearly 30% of active users, which is nearly 300 million people in the next three-five years. Such a sheer volume of users poses a challenge as it might potentially increase the likelihood of bad actors participating in the Toncoin ecosystem.

Cybercriminals frequently gravitate towards specific cryptocurrencies, often due to the features that enable their illegal activity more conveniently. There are two factors that might contribute to an increased adoption of Toncoin by malicious actors within the Telegram ecosystem.

1. Shift of Illicit Activity from Tor to Telegram

Over the past two years, the amount of illicit activity on Telegram has dramatically increased as more actors move from its natural habitat, TOR, to the messenger platform. We observe a variety of illicit services across Telegram including DDoS-for-Hire, money laundering services, Carding, Ransomware, initial access brokers, DarkNet Markets, hacktivist groups such as KillNet and many others.



Figure 10: Threat actors offer a variety of illicit goods and services on Telegram (Source: Telegram).

The dominant presence of Russian-speaking* users within the Telegram ecosystem is also worth considering. According to similarweb.com, Russia brings the majority of traffic at 30.73% to Telegram.

Considering the significant involvement of Russian-speaking actors from the Eastern Region in illicit activity, many of them might naturally gravitate toward using Toncoin.

**By referring to Russian-speaking actors, we point to Russia and multiple regions, as numerous people from former Soviet Union countries historically speak Russian.*



Figure 11: Distribution of traffic to Telegram shows Russia leading among other countries
(Source: similarweb.com)

2. Deep Integration of Toncoin Services with the Telegram Ecosystem & Presence of Russian Financial Institutions and Payment Services

Toncoin's deep integration within the Telegram platform and availability of various services such as (Wallet, Crypto Bot, Donate, and Fragment) pose a risk of being exploited by malicious actors. Buying and sending cryptocurrency without leaving a platform provides a great deal of convenience, anonymity, and accessibility for its users, including illicit actors.

The presence of Russian financial institutions, including banks and payment systems integrated with Telegram services, introduces additional concerns. Such accessibility creates potential opportunities for cybercriminals to simplify cash-out efforts, considering the involvement of foreign jurisdictions. This activity might involve multiple scenarios, from cybercriminals directly exploiting these financial institutions themselves to the participation of money mules.

Conclusion


TON's technical capabilities have promising potential for impacting financial systems. However, for its positive aspects to thrive, it is crucial to ensure its secure legitimacy and mitigate the risks posed by cybercriminals. Implementing robust measures and establishing regulations that would effectively deter illicit activities within the Toncoin ecosystem is essential.

While Toncoin is not the only cryptocurrency observed in cybercrime, its deep integration with Telegram poses concerns. Given the large amount of illicit activity across the platform, it provides convenience for cybercriminals to utilize it to support their operations.

Ongoing monitoring of the use of cryptocurrency in cybercrime is vital. Analyst1 continues monitoring Telegram and Toncoin ecosystems to identify and mitigate emerging risks promptly.

ABOUT US:

Analyst1, engineered by cyber threat analysts, offers an enterprise-scale platform that operationalizes threat intelligence and enables security teams and analysts to focus on deeper analysis and response. With **Analyst1**, organizations gain visibility into advanced persistent threats attempting to infiltrate their networks.

 @Analyst1

 analyst1.com/blog

Any technical information that is made available by Analyst1 is the copyrighted work of Analyst1 and is owned by Analyst1.

NO WARRANTY . The technical information is being delivered to you as is and Analyst1 makes no warranty as to its accuracy or use. Any use of the technical documentation or the information contained herein is at the risk of the user. Documentation may include technical or other inaccuracies or typographical errors. Analyst1 reserves the right to make changes without prior notice.