ATROMG8
MESSENGER
WHITEPAPER

FEBRURAY 2020

IT WAS A VERY BAD DECISION TO ACCEPT FREE-OF-CHARGE SERVICES FROM PROVIDERS WHOSE BUSINESS MODELS REVOLVE AROUND SELLING OUR DATA WITHOUT OUR CONSENT TO THIRD-PARTY INSTITUTIONS. IN THE END, WE ARE PAYING A VERY EXPENSIVE PRICE FOR THESE SERVICES!

Vision

We want to create a secure environment, being conscientious of how our data is collected and used without undermining the progress of technology. The meaningful handling and utilization of personal data is a fundamental need for many people today. Our aim is to protect families and their members, aswell as making sure that the important information and communication from companies and researchers around the world is well-guarded.

ATROMG8 wishes to improve the current market offers in terms of the way we communicate and exchange value to a whole new level. We wish to work on creating a marketplace of the future in the digital world that meets the requirements of the online world. Thus contributing to raising people's awareness toward how financial markets operate and helping them connect more easily to such markets, unfolding and creating independent earning possibilities.

We want to encourage people all over the world to work with us and find their place in the ATROMG8 project. On the following pages you will find thoughts that move us and information about the technology we use. It is our endeavor not to create a scientific document, but an insight into our work and our goals. This whitepaper is not completely finished. Instead, it is constantly undergoing change given the ongoing evolutionary process of the regulatory environment and technical development in the industrie.

We the TEAM of ATROMG8 welcome you to the future.

Welcome to the ATROMG8 Project

The ATROMG8 messenger with payment gateway facility introduces a new and secure communication, payment, and real time ecosystem designed on a decentralized and privatized architecture.

ATROMG8 IS A NEW APPROACH TO MEET THE TECHNICAL REQUIREMENTS OF TODAY'S WORLD REGARDING COMMUNICATION AND THE WAY WE EXCHANGE VALUE.

ATROMG8 has not reinvented the wheel. Instead, we have cleverly combined the available technologies developed by thousands of developers over the past years. Leading experts from various fields of security, banking, and communication have supported and collaborated with us. Open source is the key for a sound society and ecosystem if we want to keep up with the rapid changes in the realm of technology.

Our primary goal is to participate in it with our own developments and in return get ideas from experts around the world to use and create a trustful and protected environment with collective contributions in today's digital world.

A mass adoption of this new way of lifestyle can only be achieved if we work and grow together. By doing so, we are building a sustainable solution with extraordinary user experience letting ATROMG8 achieve more for its participants and users as compared to what could have been possible with a single project team working on the ecosystem.

ATROMG8 envisions to function as a secure network in which people and companies across categories can communicate with each other, work, and exchange values. You decide who gets your data and how it may be used.

In order to offer a comprehensive set of services to its users, ATROMG8 partners with various service providers, including banks, trading platforms, and cryptocurrency exchanges. By doing so, ATROMG8 ensures that our certified service providers are all licensed and in compliance with the legal requirements.

Few years back, there were no industry-specific regulations. Today, the landscape has evolved rapidly and significantly with each country having its own set of regulations and legislations for this space. In an attempt to offer country-specific services that are in line with the laws and are supported by the regional authorities, ATROMG8 respects and complies with these regulations in each region. The secret is to embrace the differences in the regulatory frameworks, and hence, in the services offered.

Companies and other business participants from across the globe can create their own coin, or token, and products on the ATROMG8 open source multi blockchain-backed solution. Again, this happens in line with the country s regulations in a safe and protected environment. In addition to all this, the ecosystem's technology partners offer a diverse set of solutions to businesses ranging from complex integration designs to simpler RESTful APIs.

Together, the messenger, the payment gateways, and licensed service providers work hard and relentlessly to create ATROMG8's dynamic and secure real-time ecosystem. From truly private conversations to the most secure transactions currently available on the market. Users can enjoy it all on our application.

All the participants of this ecosystem operate with their digital IDs in a pseudo-anonymized fashion utilising the MixNetwork 5.0. Super Structure across all its offerings, whether it is the messenger, the payment gateway, or the open-source community.

MixNetwork 5.0. Super Structure is a combination of different Blockchains in our Projekt, which for a part act independent as well as interact so that no single Blockchain gets too big or heavy, thus loosing speed and security.

As a final note, ATROMG8's payment services do not hold any information about the transactions carried out on our app. Only the legally regulated licensed service provider, whose service the user wishes to utilize, can access this information all within the regulatory allowances.

All the messenger products and metadata are not visible to ATROMG8 or any other participant. It cannot be requested, recorded, or called at a later date as it is not stored anywhere and runs on a decentralized system of servers.

About Us

ATROM NETWORK SWITZERLAND AG WAS FOUNDED TO CREATE A FAIR AND PROTECTED COMMUNICATION ECOSYSTEM INTEGRATED WITH A ROBUST AND SECURE PAYMENT GATEWAY.

The company VISIONG8 (pronounced as Vision Gate) was dissolved and its functionings were united with that of the company ATRONOCOM DMCC (Dubai) under the name of ATROMG8 (pronounced as Atrom Gate), as part of ATROM Network Switzerland AG.

This ecosystem will be built with licensed service providers from each partner country. Further, the access rights to own the system and the blockchain will be granted via an access-right token and utility coin respectively.

Both the access tokens and coins serve as a means of exchange, a unit of account, and a store of value. In addition, they also offer access to the ATROMG8 Multi- blockchain as well as its infrastructure and technology, beyond its main use for peer-topeer transactions. Some of these infrastructure-access tokens and coins are Ether, Ether Classic, Cardano, Lisk, ICON, and EOS among others.

The team is comprised of over 150 passionately driven individuals spread across continents and countries, with many years of experience in development, and an open source community to welcome developers who want to be a part of this transformational journey.

The ultimate mission of this project is to design a real-time ecosystem powered by a globally active network with properties of security and privacy at its core.

The ATROMG8 application will soon be available on both Apple iOS and Android Google Play Store.

Introduction

You talk about ordering coffee with your friend and the next thing you see is an advertisement of a coffee brand while you are scrolling through your social media.

You watch a video on YouTube and the next morning you see more videos aligning perfectly with your new-found interest.

You frequently see prompts of purchasing gym equipment being the fitness enthusiast that you are, while your wife sees prompts of purchasing books being the avid reader that she is.

Sounds relatable?

Then you must read on to delve deeper and discover how this happens and why this could turn lives upside down.

This and a lot more can be accomplished with the help of the digital footprint that we all leave in the form of data and metadata. While most people know what data is, metadata is commonly ignored, misunderstood, and relatively unexplored.

It cannot be emphasized enough how important it is to understand what metadata is and what it can do while it appears to be seemingly harmless. The earliest example of metadata dates back to as early as 280 BC when the librarians at the Great Library of Alexandria attached a small tag to each scroll. Scrolls were the books back then. These tags had information about the scroll like its subject, title, and author. This served as a means to know what the scroll constituted without having to open it for returning it to its shelf.

Since then, metadata has evolved as a channel of assisting researchers, developers, and other professionals for discovering relevant documents and information. In the online world, it helps to provide digital identification, preservation of preferences, and archiving of data. It is actively and intensively used by businesses globally to find relevant leads and eventually convert them with the right targeting and retargeting.

Before getting into all that metadata consists of, it would help to see an example of more recent times. When you send a message, metadata is not the content of the message. It is a mix of data, which you might think cannot reveal a lot about you or your life, such as:

The time at which the message is sent

The sender and receiver of the message

The location from where it is sent

In case of an email, this would also include the subject.

As importantly and dangerously, it also includes the websites you visit.

As it is popularly known, metadata is data about data and can take several forms ranging from descriptive metadata to administrative metadata and statistical metadata.

IT HELPS TO SUMMARIZE BASIC INFORMATION ABOUT DATA AND IN TURN MAKES IT EASIER TO TRACK AND WORK WITH IT.

In case of a digital image, like when you upload your profile picture on a social media channel, this could include information about how big the picture is, its color depth, its resolution, the time of its creation, your location, and other similar details. A text document, like when you create a business proposal, could have metadata in the form of how long it is, its author, when was it first created, when was it last modified, the document outline, among other things. Web pages also have metadata defining them which can include a description of the content on that page, the keywords it targets, the time it was created, and a lot more.

One might question how can metadata, which is not even data itself but data about data, be as harmful as it has been portrayed till now? On the surface, it rather seems to be a helpful set of information used for tracking, archiving, storing, searching and other harmless purposes.

Unfortunately, this data can also be used for attacks driven by traffic analysis, mass surveillance, as well as catastrophic cybercrime. With only one week of metadata collected via innocent mobile apps, below are just a few things about your life that can be discovered:

Your age

Your full name

Your sex, race, address, contact number

What you do

Where you work/ study

How much time you spend working/ studying each day

For how long you travel everyday

Your to and from destinations on usual days

The names of your loved ones, like your partner, siblings, parents, and friends

How much you communicate with each of them

Your interests and hobbies

What you like to watch

What sort of shopping you do online

Whether or not you accept newsletters from various brands

How organized you are

How many email accounts you have and their purposes

What you sympathize with

Your financial transactions

Your Health data/history

Your political views

Device name, its ID, operating system, and software

Details of Your service provider

Your mood on most days

Go back, think about everything you did on your smartphone and laptop today. In just one day you could have revealed a lot with regards to the above details. Metadata of just one message might not be able to share much about you or your life.

However, when put together with all the hundreds of messages on that day, along with the calls that you made, the subject lines of the emails you sent, and the websites you visited, you and your life are close to being an open book, ready to be read.

Often, you might have seen reported in the news that thousands or millions of passwords got leaked. But how does anyone use these passwords or hints to passwords?

All these metadata points when combined with the requisite algorithm can help the hackers to connect the right password to the right account. All your accounts for emails, social media, online shopping, digital wallets, entertainment, and other are practically always at a risk of getting hacked. That is how easy it can be for cyber criminals and other malicious third parties to access such incredibly sensitive data with just little and seemingly harmless information.

 Furthermore, such acts do not require any extensive technical know-how and can be accomplished with readily available common software. This is when one gets their hands only on metadata and not on the actual data. If you ever hear "this is just metadata," you should know how flawed this statement is and what it could potentially translate into.

The problem of metadata is more grave that what you have understood till now. If you think about it, these millions of rows of metadata must be getting stored somewhere. The applications that you use on your mobile phone, the web pages that you visit, the social media scrolling that you do, the online quizzes that you take, the messages that you send.Every click, scroll, and visit submits a set of metadata to the respective entities. All this information gets stored in databases along with that of thousands of other users.

While these entities could possibly and hopefully mean no harm, these databases act as a single point of failure for everyone whose data is part of the database. It could scar people financially, materially, and emotionally. Not just one individual but all those who have their metadata stored in the database that gets hacked.

CYBER CRIMINALS ARE ACTIVELY SEEKING SUCH INFORMATION AND POINTS OF ENTRY WHICH ALLOW THEM TO ACCESS INFORMATION OF MANY TOGETHER

The problem is that all the data and metadata gets recorded on centralized databases. These may not be easy to hack, however, once a malevolent mind acquires the skills or the tools to accomplish the same it would put millions at risk of such ill intentions. As one can imagine, a hacker or cyber criminal would want to get hold of one single database with information of many individuals instead of going after all these individuals one by one.

In 2016 alone, losses driven by fraud and identity theft summed up to an all-time high of $16 billion.

A hacker or criminal can target important aspects of a users life such as insurance, credit card, and banking information, having devastating consequences. Such events in an individual's life not only impact them materially but also psychologically and emotionally. Identity fraud, filing fraudulent tax returns, loan applications, counterfeit cards, bill payments, money transfer, spamming/phishing attacks, blackmail, and hacktivism are some of the things that can happen with stolen or hacked data.

As strange as it might sound, there exists an underground market for the sale and purchase of such data, your data.

A research conducted by Trend Micro in 2015 revealed that personally identifiable information like names, birth dates, social security numbers, and addresses, was being sold at $1 per line. Similarly, complete credit reports with high credit scores could be purchased at $25 per report; bank login credentials for $200 to $500 per account; mature online accounts with years of transaction history for up to $300 each.

Unfortunately, from the time the internet has existed, users have blindly agreed to ambiguous terms and conditions or checked boxes that they did not know the purpose behind. Majority of the times when websites and applications collect or monitor data, there is a lack of notification for the user.

Even if there is a pop-up asking for certain permissions, it is not always fully descriptive or transparent. In such cases, technology applications like encryption are rendered ineffective because users end up giving the right to certain data and metadata themselves. This not only undermines their security but also damages drastically the integrity of communication ecosystems.
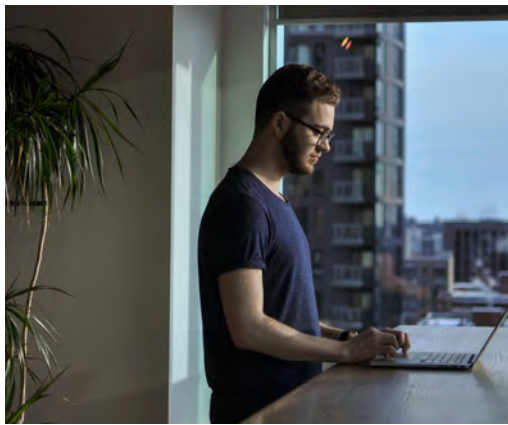
All those times when a new mobile application asks you for permissions such as your location, access to documents and photos, among other things, you could question why it requires such details given that the purpose of the application has nothing to do with any of these things. When you take those fascinating online quizzes, you end up sharing your public profile along with in-depth information describing your most personal traits. All these are examples of how users tend to fall prey to the existing data-sucking structures unknowingly.

Across countries, data and metadata is collected by authorities and government agencies for the protection and security of their citizens. As an example, the USA has deployed programs to get certain information about the lives of people living there as an attempt to prevent a massacre like the terrorist attack of 9/11. One of these programs is known by the name of PRISM and was launched in the year 2007. It was commenced with the objective of collecting stored internet communication data including videos, emails, video chats, text chats, photos, file transfers, and social media conversations among many other forms.

The servers of internet companies such as Apple, Microsoft, Facebook, YouTube, Google, and Yahoo! are supposed to provide this stored data on demand. While this is deemed critical for national security, the fundamental flaw is that all this data is stored on a centralized database and as previously mentioned, it offers a single point of entry as well as attack to cyber criminals.

Issues revolving around the collection of metadata have frequently been a part of earnest debates, where the parties who support it contend that metadata do not give any insight into private facts about individuals and it is not the same as content. In addition to this, they also argue that unless someone analyzes this data, nothing about an individual's life can be revealed.

However, several organizations and activists also argue that the collection of such data is against human rights. Instead of designing a new human rights framework, the existing one needs to be interpreted and executed more appropriately corresponding to the ever-evolving communication channels and patterns. As you have observed, metadata mapping does reveal personal and intimate information about individuals. All that is needed is genuine protection of human rights and privacy.

Of course, knowing the content of a call can be crucial to establishing a particular threat. However, metadata alone can provide an extremely detailed picture of a person's most intimate associations and interests. As a matter of fact, it is actually much easier as a technological matter to search huge amounts of metadata than to listen to millions of phone calls.

As NSA General Counsel Stewart Baker has said, metadata absolutely tells you everything about somebody's life. If you have enough metadata, you don t really need content.
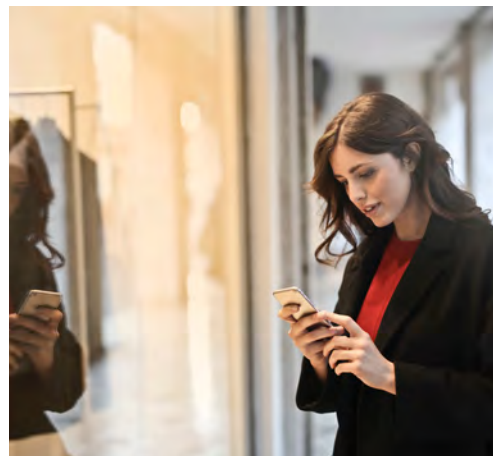
When ATROMG8 quoted Baker at a recent debate at Johns Hopkins University, its opponent - General Michael Hayden, former director of the NSA and the CIA - called Baker's comment "absolutely correct," and raised him one, further asserting that:
"we kill people based on metadata"

The Solution: ATROMG8

The world does not have a shortage of communication and messaging apps. In fact, today, there are also apps that allow end-to-end encryption. This would have been wonderful, if only it actually meant what the users believe it to mean.

Some of these apps need to be used in a particular mode (like a secret chat window or incognito) for the encryption to be enabled and it is not a default setting when you start using the platform - a condition that users are often unaware of.

Further, for apps that provide encryption irrespective of the mode, it is anything but end-toend. It is true that the content of communication, that is, the message itself will be encrypted before sending, but as you have read and understood, metadata is the game changer. None of the existing communication apps offer the encryption of metadata. Even the safest of apps take your permission to collect certain data for performance and service-related diagnostics, evaluations, and updates. This can include log files, activity reports, performance logs and reports. In addition to this, information about the operating system, browser - including the search history, IP addresses, and mobile network data is also collected and stored. All this as you slept peacefully at night, thinking your life belongs only to you.

Everything mentioned above exists over and above the quintessential threats of hacking and malware attacks on these platforms.

Many specialists and experts in the field also believe that having the platform designed and encrypted by a team of few individuals is always risky business. While one can control technological application, no one can control human intentions.

Despite the finest techniques, the ones who have access to the tools and databases need to be trusted for not ever turning malicious. If you think about it, there is an entire industry flourishing upon the raw materials that are the lives and data of people who are on the internet.
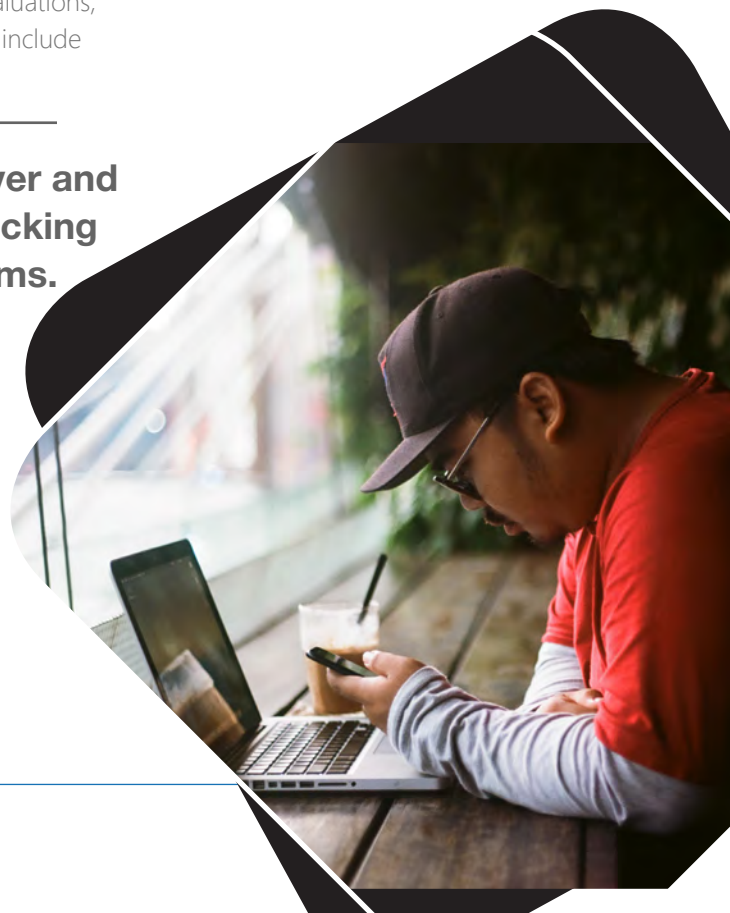
While this appears to be turning into a dead end, from where there is no road that takes you to accomplish safe and secure communication, there is immense scope that can still be leveraged. What people need is a trusted real-time ecosystem. This is where ATROMG8 enters and pledges to design a communication ecosystem which today is the most secure, encrypted, and private in all respects.

The ATROMG8 application and Ecosystem consists of three primary elements:

01

A secure messenger

02

Integration of payment gateways

03

Country-specific offerings and licensed service providers for the real-time ecosystem

Dear Friends and Community Members, we are working on the latest iteration of the Technology part of the ATROMG8 project. We are momentarily implementing the learnings of the last test phase and will in short time update the whitepaper with the latest technology part!