Distributed Identity Whitepaper

Project Babbage
www.ProjectBabbage.com

Introduction:

Distributed identity is a concept that refers to the decentralization of identity data, giving individuals control over their personal information and enabling them to use it across different platforms and applications. This differs from traditional centralized identity systems, where personal data is stored and controlled by a single entity, often a large corporation.

In recent years, there has been a growing awareness of the need for greater control and privacy over personal data, as well as the benefits of decentralized systems. This has led to the development of distributed identity solutions that use blockchain technology to create secure and decentralized systems for identity verification and management.

Benefits of Distributed Identity:

1. **Improved Privacy:** In a centralized identity system, personal data is stored in a single location, making it vulnerable to data breaches and unauthorized access. In a distributed identity system, personal data is decentralized and stored directly on end-user devices, making it more secure and less likely to be compromised.

2. **Increased Security:** Distributed identity systems use cryptographic techniques to verify identities, making them more secure than traditional systems that rely on passwords and other easily-compromised forms of authentication.

3. **Greater Control:** With a distributed identity system, individuals have control over their own personal data and can choose which information to share and with whom. This allows for more control over personal privacy and the ability to selectively reveal only the necessary information.

4. **Interoperability:** Distributed identity systems are designed to be interoperable, meaning they can be used across different platforms and applications. This allows individuals to use the same identity across multiple platforms, rather than having to create separate identities for each platform.

5. **Increased Efficiency:** Centralized identity systems can be slow and cumbersome, requiring manual verification and authentication processes. Distributed identity systems use automated processes, making them faster and more efficient.

The next sections of this document explore each of these areas in detail:

Improved Privacy

Distributed identity systems like those provided by Project Babbage offer significant improvements in privacy compared to traditional centralized platforms. By putting users in control of their own encryption keys, data can be protected without revealing it to platform operators. Even if encrypted copies of user data are stored on servers in the cloud, the keys needed to decrypt and access personal information are only available to those whom the user has specifically granted authorization. This prevents servers from exceeding their authorized level of access to user data, thanks to client-side encryption.

One major challenge to privacy on traditional websites is ad-based targeting. In order to monetize their businesses, apps and service providers have turned to collecting information about users' preferences, interests, and spending patterns in order to target them with personalized ads and content recommendations. This targeting allows traditional apps and websites to make money from the time users spend on the platform, encouraging them to build addictive and unhealthy experiences that exploit users' personal preferences and manipulate their behavior without their knowledge.

By providing a micropayment-based monetization model, Project Babbage removes the need for platforms to exploit and manipulate their users. Rather than making money from funneling user attention and data to ad-based platforms like Facebook or Google, apps and services can make money directly from the people they serve. When combined with tools for easily protecting user privacy with strong encryption and informed consent, a new paradigm emerges in which users are put back at the center of every exchange.

While transactions on the Bitcoin SV blockchain used for micropayments are public, sensitive information such as messages and photos can be encrypted. Additionally, identity information can be firewalled from the rest of the system, as described in the original Bitcoin whitepaper. This trade-off between transparency and privacy is largely mitigated, ensuring that users can enjoy the benefits of a public blockchain without compromising their privacy.

Data breaches and data leaks often occur when large amounts of sensitive information are stored in a central location that can be compromised and used without authorization. By moving data out of silos and into the hands of individual users, Project Babbage's distributed identity systems mitigate the underlying problem that leads to these massive data leaks. With keys held across the world by individual users themselves, cyber-criminals are both less motivated and less able to steal sensitive information.

Finally, the MetaNet model exceeds the requirements of regulatory bodies such as the European Union's GDPR by enabling direct and peer-to-peer interaction between individuals and companies with informed consent. This furthers the goals of user privacy and puts users back in control of their personal data.

Increased Security

The Babbage Distributed Identity system, powered by Authrite, provides increased security compared to traditional authentication methods. One key factor in the security of any authentication system is the difficulty of masquerading as another user and forging their credentials. Humans are notoriously bad at creating and remembering random and secure passwords, resulting in low entropy keys. On the other hand, the Babbage Distributed Identity system utilizes machine-managed keys derived from authentication credentials stored directly on user devices, allowing for a full 256 bits of entropy. This level of security is made possible by distributing the keys across every user in the system, rather than concentrating them in a single vulnerable location.

In addition to the increased security provided by the use of machine-managed keys, the Babbage Distributed Identity system is also decentralized. This means that the compromise of a single identity certifier will not bring the entire system to a halt. This decentralized nature makes the Babbage Distributed Identity system immune to many classes of attack that have plagued centralized CA models.

The Babbage Distributed Identity system also excels in protecting trust relationships between parties. If an attacker tries to gain the trust of another party, they must do so by obtaining legitimate certificates trusted by their target. Once these trust certificates are obtained from well-recognized authorities, the attacker can either choose to conduct legitimate business or undermine the legitimacy of their own work by committing fraud. This reduces the risk that a user's counterparties will engage in fraud.

The Babbage Distributed Identity system's federated certificate system also reduces risk for both businesses and their customers by giving all parties the ability to choose which certifiers they trust and which ones they do not. By making context-aware decisions about whether to proceed with an exchange based on the information that has been revealed and certified by relevant authorities, businesses can implement smarter and more accurate risk management strategies while still protecting user privacy.

One example of the increased security provided by the Babbage Distributed Identity system is the successful deployment of an Authrite certifier by the MetaNet ICU. This certifier attests to club membership and rank, allowing anyone from the ICU to obtain a club certificate and anyone they interact with to request to see it with their permission. This enables apps and services to confidently verify legitimate members of the MetaNet ICU, turning away imposters.

Overall, the Babbage Distributed Identity system provides a higher level of security compared to traditional systems. Its ability to establish and secure mutual trust relationships, combined with its strong encryption and decentralized nature, make it a powerful tool for improving the security of online interactions.

No More Passwords

One of the most frustrating aspects of modern life is the proliferation of passwords. From social media accounts to banking apps and everything in between, it seems like we need a different password for every service we use. Not only are passwords hard to remember, but they are also vulnerable to being hacked and stolen. This is especially true when people reuse passwords across multiple accounts, or when they use weak passwords that are easy to guess.

Authrite solves this problem by enabling users to authenticate themselves with digital keys stored directly on their devices. These keys are much stronger and more secure than passwords, and they can't be stolen or guessed because they are generated using advanced encryption algorithms. This means that users no longer need to worry about remembering multiple passwords or using weak ones that can be easily hacked.

In addition to being more secure, Authrite's key-based authentication is also more convenient. Users no longer need to type in a long and complex password every time they want to log in to an app or service. Instead, they can simply use their device to authenticate themselves with a tap or a swipe. This is especially useful for users who access their accounts from multiple devices, as it eliminates the need to constantly enter and remember passwords.

Consider the story of Fred. Fred had always struggled with remembering too many passwords. He had a password for every website and app he used, and it seemed like he was constantly forgetting them or having to reset them. This was frustrating and time-consuming, and it made it hard for Fred to be productive.

One day, Fred heard about Authrite and how it could help him solve his password problems. He decided to give it a try and was amazed by how easy it was to use. Instead of remembering a different password for every website and app, Fred was able to use his Authrite identity certificate to log in everywhere. He simply needed to present his certificate to any website or app that requested it, and he was logged in automatically.

This was a game-changer for Fred. He no longer had to worry about forgetting passwords or having to reset them. He was able to log in to all of his favorite websites and apps with ease, and he was more productive as a result.

Fred was so happy with Authrite that he recommended it to all of his friends and family. They too were able to benefit from the convenience and security of using a distributed identity system like Authrite. Fred was glad that he had discovered a solution to his password problems, and he knew that he would never have to worry about them again.

Overall, Authrite's key-based authentication system offers a significant improvement over traditional password-based systems. By eliminating the need for passwords and offering stronger and more convenient authentication, Authrite makes it easier and more secure for users to access the apps and services they rely on every day.

Greater Control for Users:

With traditional web services, users have little control over how their data is used. Even when privacy policies are in place, they are often difficult to understand and are frequently violated by the companies that claim to uphold them. This lack of control creates a power imbalance between users and the apps and services they rely on, with users often feeling like they have no choice but to accept the terms of service or leave.

Babbage changes this dynamic by enabling users to grant access to their data on a selective basis, rather than having to reveal everything to every app and service they interact with. By using Authrite, users can choose which authorities to trust, and can selectively reveal data only when necessary. This puts the power back in the hands of users, who can decide for themselves whether to share their data and with whom.

Furthermore, Authrite's system of mutual authentication allows users to verify the identity of their counterparties, reducing the risk of fraud and other types of online scams. By using Authrite, users can transact with confidence, knowing that they are dealing with legitimate parties.

Overall, Babbage gives users greater control over their data, their privacy, and their security. By enabling users to make informed decisions about how their data is used, Babbage empowers them to take control of their online experience.

Interoperability

Interoperability is the ability for different systems to communicate and work together. This is especially important when it comes to distributed identity systems, as users should be able to easily move between different platforms without losing access to their personal identity information.

This is a key feature of the Babbage distributed identity system. With Authrite, users have control over their own identity information, rather than being locked into a single platform. This means that users can move between platforms with ease, taking their identity information with them. This gives users greater freedom and control over their online experience, and makes it easier for them to switch between different apps and services.

Authrite's federated certificate system is designed to be open and flexible, allowing for a wide range of certifiers to be used in the system. This means that users can choose which certifiers they trust, and which ones they don't, giving them greater control over their online identity. This is in contrast to traditional identity systems, which are often controlled by a single entity and can be difficult to switch away from.

Much in the same way that email users can switch between clients like Apple Mail, Outlook and Mozilla Thunderbird, different competing user interfaces that plug into interoperable backend systems enable more people to interact, even when they aren't using the same app. With

interoperability, users have greater control over their data and can choose the platforms and services that best meet their needs.

The interoperability of the Babbage distributed identity system also benefits app developers and service providers. By using Authrite, developers can build apps that are compatible with a wide range of identity systems, rather than being limited to a single platform. This makes it easier for developers to reach a wider audience, and gives users more choice in the apps and services they use.

Overall, the interoperability of the Babbage distributed identity system gives users greater freedom and control over their online experience, while also benefiting app developers and service providers. By adopting open standards and protocols for distributed identity, we can enable a more connected and decentralized internet where users are free to move between platforms with ease.

Increased Efficiency

The use of distributed identity systems can significantly increase efficiency for businesses and platforms that adopt them. By removing the need for manual authentication processes, businesses can streamline their operations and reduce overhead costs. Additionally, because distributed identity systems enable direct interactions between individuals and businesses, the need for intermediaries is reduced, further increasing efficiency.

For example, using Authrite, businesses can reduce the time and resources spent on verifying the identity of their customers and partners. This allows them to focus on their core business operations, rather than being bogged down by administrative tasks.

In addition, the use of distributed identity systems can also increase efficiency for users. By eliminating the need to remember multiple passwords, users can more easily access the services they need without the frustration of forgotten login credentials.

Overall, the adoption of distributed identity systems such as Authrite can significantly increase efficiency for businesses and platforms, as well as for the users that interact with them.

Conclusion:

Distributed identity systems offer a number of benefits over traditional centralized systems, including improved privacy, increased security, greater control, interoperability, and increased efficiency. As such, they have the potential to revolutionize the way we manage and verify identities online. Project Babbage is at the forefront of this movement, pioneering open protocols and federated hosting systems that aim to break down data silos and allow individuals to move freely among platforms. By adopting distributed identity solutions, businesses and individuals can take control of their personal data and enjoy the benefits of a more secure and efficient system for identity management.