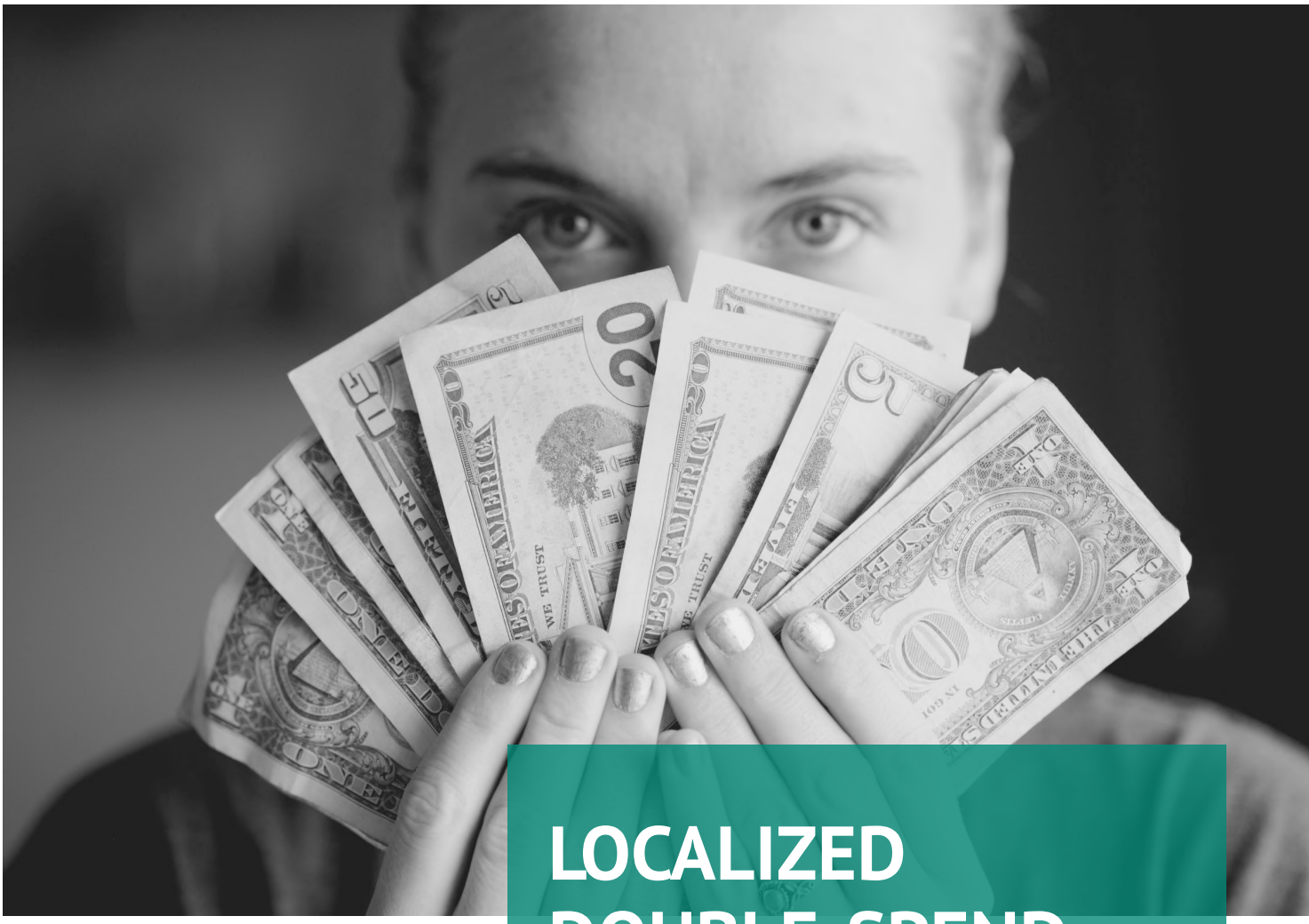
HALF EPSILON



LOCALIZED DOUBLE-SPEND PREVENTION AND DIGITAL BEARER ASSETS

A Technical Achievement by Half Epsilon

White Paper
Pralhad Deshpande, Ph.D.

July, 2020

Executive Summary

Paper has been an excellent medium for value transfer because it facilitates the transfer of value in a private and secure manner while including regulatory oversight on an as-needed basis. Present day digital value transfer systems often cannot achieve all these properties jointly.

Half Epsilon's technology enables Digital Bearer Assets. Like paper-based bearer assets, digital bearer assets have a single issuer, a single owner, and they can be securely transferred from one entity to another without any intermediaries. They retain the three key qualities of paper-based assets while substantially reducing the costs, delays and inconveniences associated with paper-based assets.

Digital Bearer Assets unlock several use cases including but not limited to wholesale CBDC, retail CBDC, one-click eCommerce, web-monetization, and trade related Digital Negotiable Instruments.

1. Introduction

How do you transfer something valuable to someone else? If it's a piece of gold, you can simply hand it over. If it's paper cash, you can also hand that over. But what if it is digital? You can't simply hand that over, can you? While we would like to maintain valuables, or their ownership rights, in digital forms, it is not straightforward to transfer them to someone else. This brings us to the double-spend prevention problem. How can we make sure that a digital asset is owned by only one entity? Preventing double-spend can unlock tremendous value. This is the central problem when it comes to building technologies for value transfer.

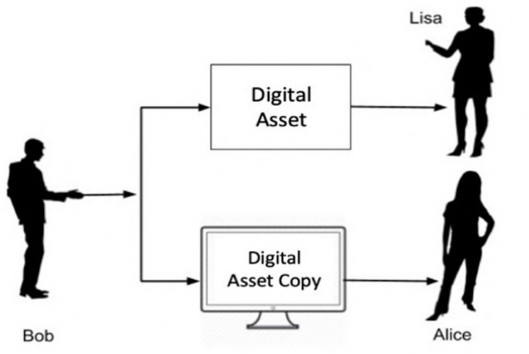


Figure 1: The double-spend prevention problem.

The above figure is an illustration of the double-spend prevention problem. Bob transfers a digital asset to Lisa. How can Lisa be sure that Bob has deleted the asset at his end and will not send a copy of it to Alice? Surely, solving this problem can unlock tremendous value.

Every time, the double-spend prevention problem has been solved, tremendous value has in fact been unlocked based on the specifics of the solution. When database technology became sufficiently mature and resilient to failures, and the web as we know it started to take shape, the digital banking revolution started. When Satoshi Nakamoto, a moniker for the inventor(s) of Bitcoin, came up with a new permission-less consensus algorithm, the crypto-economics revolution began. When trusted-hardware technology became secure enough and solutions to the replay attack were found, the one-tap payments revolution began. We now tap our phones and stored value cards against readers all the time to make payments.

In this white paper, we describe the various approaches to solve the double-spend prevention problem and the resulting impact. We also describe, at a high level, how Half Epsilon has gone about inventing a new solution to this problem

Our approach is localized, i.e., a Half Epsilon eWallet application does not have to pair with any intermediary to be able to change the ownership of a digital asset. This preserves transactional privacy. An eWallet also does not have to pair with the recipient's eWallet to perform the transfer. This allows for asynchronous transfers, i.e., a recipient need not be online to receive a digital asset transfer. The ownership can be changed locally and the digital asset can then be sent over to the recipient via any communication mechanism, even email or chat. We wrap up by describing the various value transfer scenarios that may get unlocked as a result of our technology.

2. Known Approaches to Prevent Double-Spend

If there is a digital system that helps in transferring value, you can be sure that it relies on a deep technical solution to the double-spend prevention problem.

2.1 Centralized Double-Spend Prevention

A simple way to solve the double-spend prevention problem is to use a database to store user identities and their assets. This simple but powerful approach unlocked the digital banking revolution. Something we all participate in our day-to-day lives. Of course, the web as we know it today also had to exist.

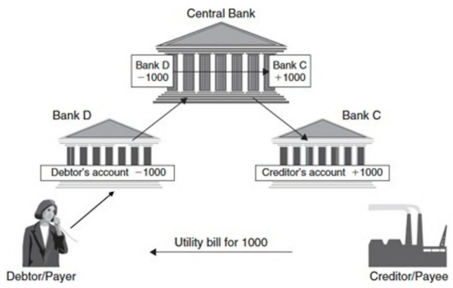


Figure 2: Resilient databases unlocked the digital banking revolution. Source: Payment Systems [1]

It has become exceedingly easier to pay someone within a single economy. Not only have banks gone digital, but today we also have various eWallet applications that facilitate convenient transactions.

From a technical standpoint, for a financial institution to maintain accounts in databases, the databases had to become extremely resilient. Consensus algorithms such as Paxos [2] went a long way to ensure that databases were tolerant to faults and crashes.

2.2 Decentralized Double-Spend Prevention

A second notable solution to the double-spend prevention problem is the one proposed by Satoshi Nakamoto [4]. The quest to create Internet money led Nakamoto to create a new consensus algorithm that allowed a changing set of 'miners' to jointly maintain a database. The term Blockchain was used to describe this database. Since a changing set of miners are responsible for securely maintaining the digital asset to owner mapping, this approach to double-spend prevention is considered decentralized.

The resulting crypto-economics revolution has taken off quite a bit. At its peak in 2017, the cumulative market capitalization of cryptocurrencies crossed $550 Billion

2.3 Preventing Replay Attacks using Trusted Hardware

One way to make sure that a digital asset is not spent twice is to ensure that it is not received twice by the recipient. This is true when a single database, whether centralized or decentralized, is not used to record the transfer of value.

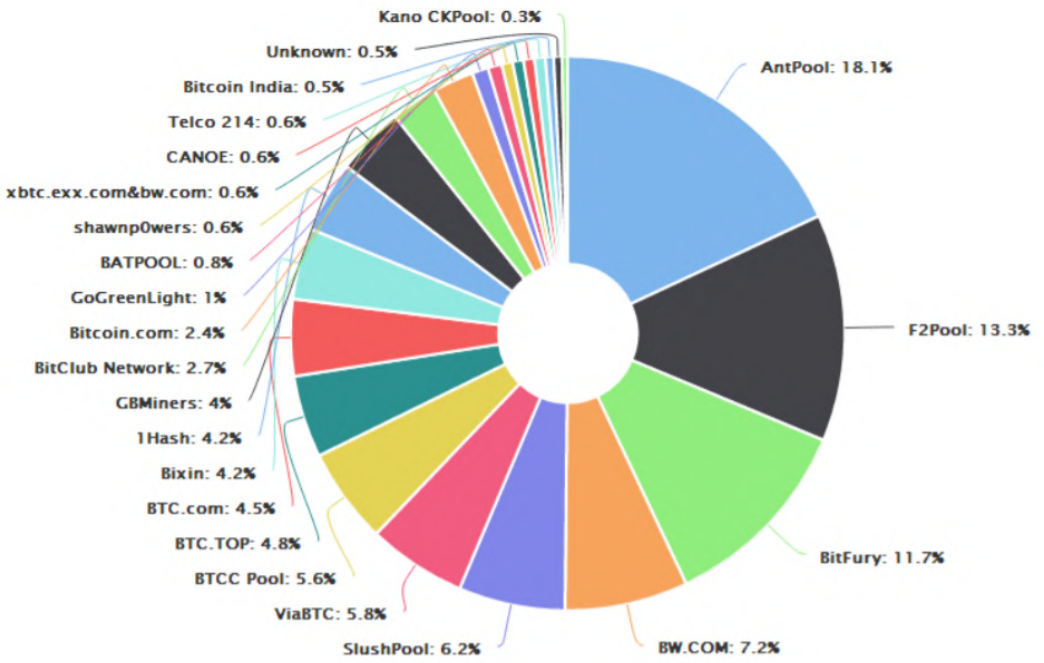


Figure 3: Bitcoin mining pools. Together, a changing set of miners and mining pools operate the Bitcoin network. The figure indicates the fraction of mining power contributed by each pool. Source: [3]

Consider loading eMoney into a stored value card at a kiosk. Value is deducted from a bank account and transferred into the stored value card. An adversary could record the communication between the reader and the card and replay it creating money out of thin air.

This problem is solved by leveraging trusted hardware and monotonic counters [5]. The trusted hardware is responsible for securely maintaining cryptographic keys, firmware, a small amount of secure memory, and monotonic counters. Monotonic counters only increase in value, their value can never be decreased. When a reader reads the value from a stored-value card, it also reads the value of the monotonic counter. When it generates a signed message to change the stored value, it increments the read counter value by one and supplies the new counter value as well as part of the signed message.

The trusted hardware accepts an incoming message as long as the counter value in it is one more than the value of the monotonic counter. This ensures freshness and prevents replay attacks. Upon changing the stored value in the card, the monotonic counter is incremented by one.

The one-tap payments revolution is currently underway for in-person payments.

3. Localized Double-Spend Prevention, a New Approach

Since our technology is patent-pending, we shall be, on purpose, non-transparent about it. We shall revise this section of the white paper after our patent [6] has been granted.

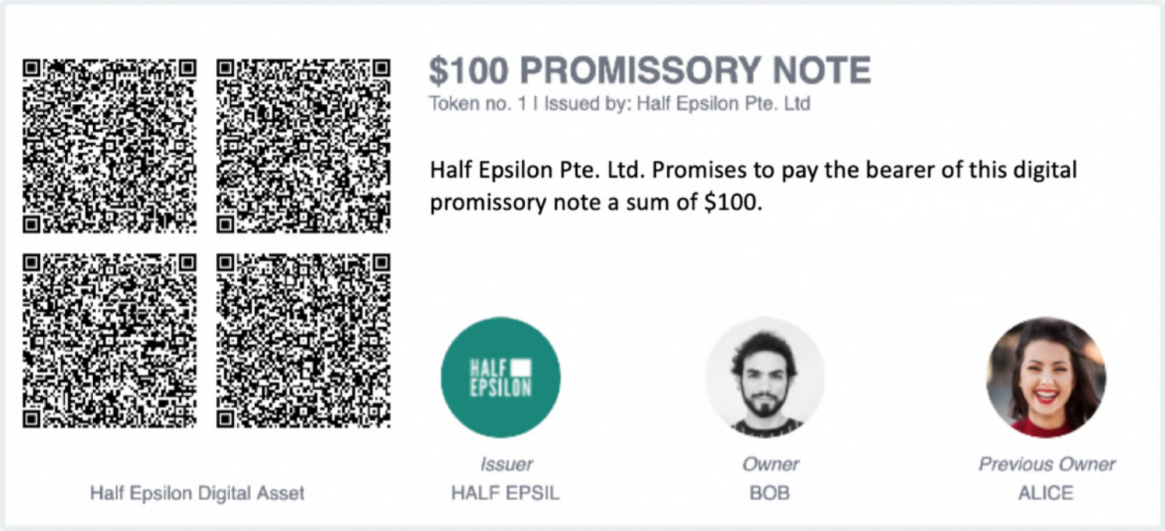


Figure 4: Digital Bearer Assets are very much like paper, except they are digital. Here, we show a promissory note issued by Half Epsilon and owned by Bob. The QR codes capture the cryptographic information representing issuance and ownership.

3.1 Solving the Deletion Problem – Forgetting by Remembering

> Transfer = Copy + Delete.

Transferring a digital asset is about sending a copy of it to someone else and then securely deleting the original digital asset. The two steps have to be done atomically. The first part is easy, however, deleting something securely is quite hard [7].

It turns out that the trick to forgetting something is in remembering what one has forgotten. If you have deleted something, you should remember that you have deleted it so that you won't transfer it again.

3.2 Digital Bearer Assets and the Trifecta of Value Transfer

There are three important aspects of any value transfer system:

- Transactional Privacy
- Security
- Regulatory oversight, on an as-needed basis

These form the trifecta of value transfer.

Paper has been an excellent medium for value transfer because it facilitates the transfer of value in a private and secure manner while including regulatory oversight on an as-needed basis.

Half Epsilon produces Digital Bearer Assets. Like paper-based bearer assets, digital bearer assets have a single issuer, a single owner, and they can be securely transferred from one entity to another without any intermediaries. They retain the three

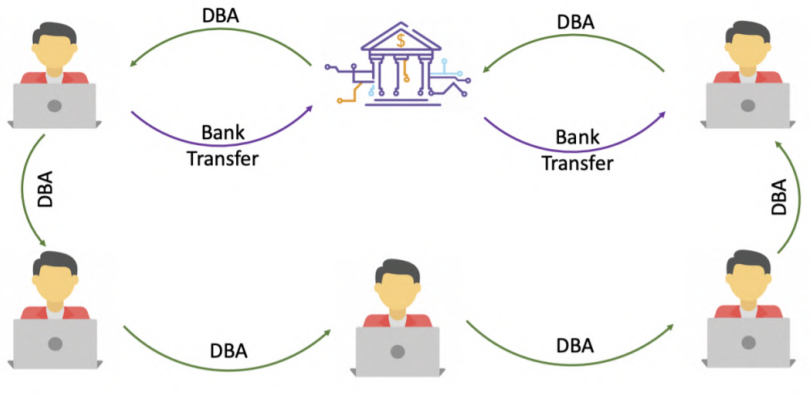


Figure 5: Digital Bearer Assets can be transferred without any centralized or decentralized intermediaries. They can be transferred over email or chat.

key qualities of paper-based assets while substantially reducing the costs, delays and inconveniences associated with paper-based assets.

4. New Use Cases Enabled by Digital Bearer Assets

Digital Bearer Assets unlock several use cases. Some use cases fall in the consumer segment and some are institutional in nature.

4.1 Wholesale CBDC

The business case for wholesale CBDC is quite powerful [8]. If there was a wholesale CBDC and it could be transferred with settlement finality, the same pot of liquidity could be pointed to various platforms and applications. Cash is often the worst type of asset and wholesale CBDC could reduce the amount of cash required to be maintained. For large financial institutions, the benefits could be significant.

At present, blockchain enthusiasts consider it to be useful for wholesale CBDC. This is a poor technological choice. Blockchains obtain their quantifiable security properties by large scale replication of data. However, replicating data, even encrypted data, accrues huge liabilities. This makes blockchains a poor choice in enterprise settings.

Digital Bearer Assets are the most suitable technology choice for wholesale CBDC. They can be transferred with security, privacy, and regulatory compliance.

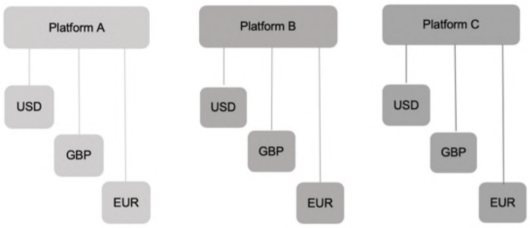


Figure 6: Financial Institutions lock up liquidity on various platforms. Wholesale CBDC can significantly reduce liquidity requirements.

4.2 Digital Bonds and Securities

Just like wholesale CBDC, digital bonds and securities can be created using Digital Bearer Assets. They can be transferred with security, privacy, and regulatory compliance. Some entities are trying to create blockchain-based solutions for this use case. For reasons cited above, blockchain is a poor technological choice.

4.3 Retail CBDC

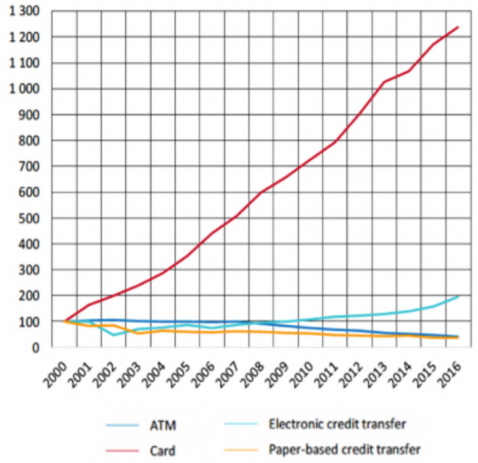


Figure 7: Trend for ATMs, cards, electronic credit transfers, and paper-based credit transfers.
Source: The RiksBank's e-Krona project [9].

The figure above is from the Riksbank, which is Sweden's central bank. It shows a clear move from paper-based payment services to electronic payment services. Between 2000 and 2016, card usage has increased 13 times while cash withdrawals at ATMs have nearly halved. This shows a clear consumer preference for convenience over other aspects of payment systems.

The Riksbank, like several other banks, is considering the development of a Central Bank Digital Currency (CBDC) for consumers. We paraphrase from their discussion paper below:

"In the not-too-distant future, Sweden may become a society in which cash is no longer generally accepted. This is a part of a greater trend towards digitalization in society and a movement towards a payment market that could be increasingly consolidated among a small number of commercial participants, payment services, and infrastructures. This development raises questions over the payment market's future security and efficiency, thereby giving reason for the Riksbank to look into a digital alternative to cash."

The Riksbank is expressing concern over the security and efficiency of the Swedish payment market in light of the heavy movement of consumers towards electronic payment systems provided by private players. What do they mean by the security and efficiency of the payment market? Essentially, they are talking about the emergency preparedness and continuity function that has long been fulfilled by paper cash. In the case of any emergency, even a hostile takeover of the electronic payment system, people should be able to continue transacting. This concern is shared by several central banks, all of whom are investigating retail CBDCs.

Digital Bearer Assets are a perfect building block for retail CBDC.

4.4 One-click eCommerce

Do you give away your credit card information to a new eCommerce website? One you encountered for the first time? What if you could make a payment without revealing your credit card information? Using Digital Bearer Assets, it is possible to create a payment system that allows you to pay with a single click without ever revealing your card or account information. Digital Bearer Assets can not only be transferred over chat or email, but they can also be transferred over HTTP headers. Ecommerce websites, new and old, could benefit from higher conversions.

4.5 A New Channel for Web-monetization

There are two models for web-monetization; the ad-supported model and the subscription model. Ad-supported web-monetization is privacy-invasive and is also very inefficient. A small fraction of the total ad-spend goes to the publishers and an even smaller fraction goes to the content generators. The rest is consumed by a whole host of middle-entities including supply-side platforms, demand-side platforms, and ad exchanges. As for the subscription model, publishers need well differentiated content to make this work. This is not an easy task for new entrants. Also, several consumers feel that they under-utilize their subscriptions. Enabling micro-payments can help introduce a third channel for web-monetization. Publishers can charge fractions of cents to view web-pages or small amounts for short term subscriptions or feature upgrades.

Digital Bearer Assets can enable one-click micropayments, even small fractions of cents.

4.6 Trade Related Digital Negotiable Instruments

Trade-related documents such as Bills of Lading are still paper-based. Several times they are title documents that represent the ownership of goods. Managing and transporting paper documents is a hassle. They often have to be couriered across the world.

Global trade bodies such as ITFA have often lobbied for trade document digitization. In recent times, blockchains are considered the technology of choice for trade document digitization [10]. For privacy-related reasons described earlier this is a poor technological choice. While centralized solutions exist, their uptake has been limited, also because of privacy concerns.

Digital Bearer Assets are an excellent choice for Digital Negotiable Instruments. Such documents can then be transferred with security, privacy, and transfers can go through regulatory approvals when necessary.

5. Conclusion

Half Epsilon has developed breakthrough technology that solves the double-spend prevention problem in a localized manner without requiring the involvement of any intermediaries. We produce Digital Bearer Assets which is the base technology for several use cases including but not limited to wholesale CBDC, retail CBDC, one-click eCommerce, web-monetization, and trade related Digital Negotiable Instruments.

Several entities are experimenting with blockchain technology to address these use cases. We argue that blockchains are a poor technological choice and urge the community to experience the security, privacy, and regulatory compliance benefits of Digital Bearer Assets.

6. References

[1] Rambure and Nacamuli, Payment Systems.

[2] Lamport L., The part-time parliament. ACM Transactions on Computer Systems 16, 2 (May 1998).

[3] https://en.bitcoinwiki.org

[4] Nakamoto S., Bitcoin: A peer-to-peer electronic cash system, 2008

[5] Schneier B., Security Engineering.

[6] 10202003785S, A System for Digital Asset Transfer in a Digital Transaction and a Method Thereof, filed by Half Epsilon Pte. Ltd.

[7] Gutmann P., Secure Deletion of Data from Magnetic and Solid-state memory.

[8] https://fnality.org

[9] Riksbank, Sveriges. "The Riksbank's e-krona project." Riksbank Studies, Report 2 (2018).

[10] ITFA Digital Negotiable Instruments (DNI) Initiative

ABOUT THE AUTHOR

Pralhad Deshpande, Ph.D. is an accomplished computer scientist, technologist and a serial inventor. As part of his doctoral work, he designed, implemented and experimented with wireless networking protocols for vehicular networks. After his doctorate, Pralhad joined IBM Research and was a Research Scientist there for 6 years. Pralhad also had a yearlong stint with a security focused company before venturing out on his own and founding Half Epsilon, a deep-tech company, where he is presently the CEO. Pralhad enjoys tackling real world socially impactful problems which are on the edge of computing.

HALF EPSILON

HALF EPSILON