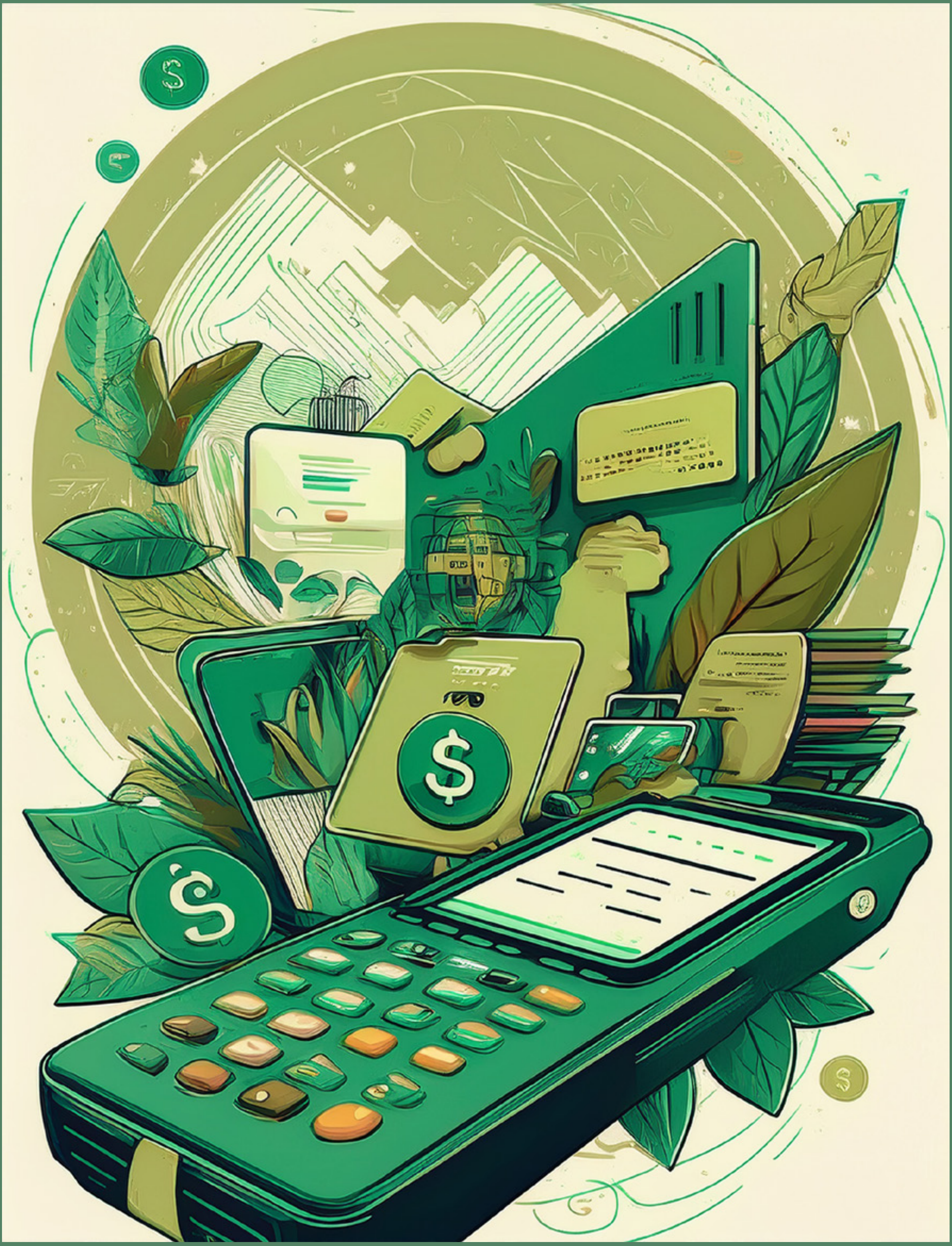
crunchfish



RETHINKING OFFLINE PAYMENTS

A GROUNDBREAKING ECOSYSTEM APPROACH

2025-05-27

Rethinking Offline Payments

A Groundbreaking Ecosystem Approach

A Whitepaper for the Digital Currency Conference, Bangkok, May 28-29, 2025

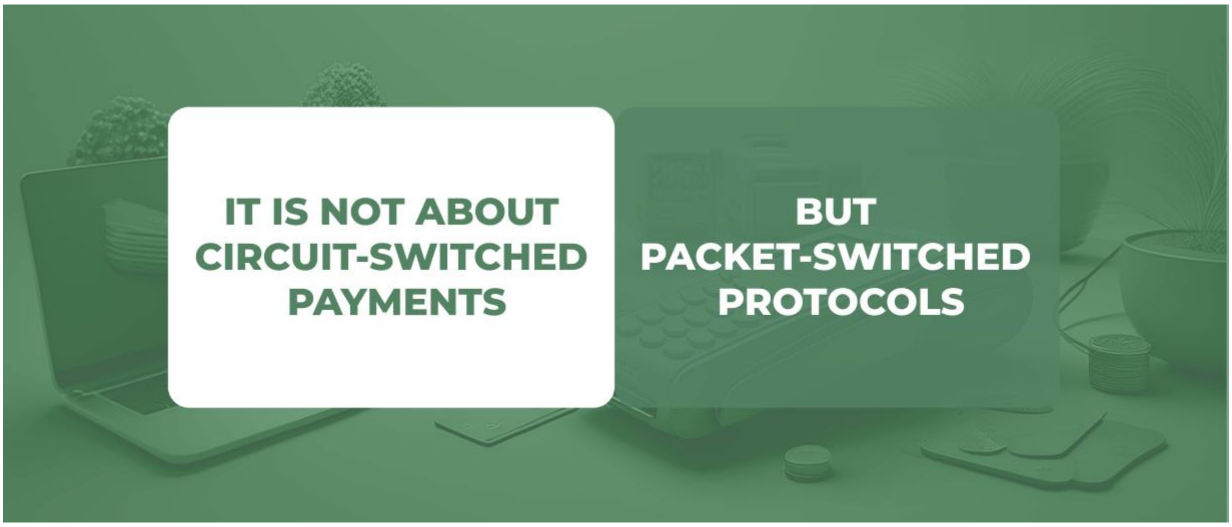
By: Joachim Samuelsson, Crunchfish CEO

In today's rapidly evolving financial landscape, the need for resilient payment solutions has never been more critical. Traditional digital payment systems assume network connectivity, which exposes vulnerabilities during network disruptions, but can also fail due to temporary server outages in the backend. This conference white paper addresses the challenges of implementing offline payments to solve fundamental issues within digital payments, including the reliance on the "happy flow" model, which do not provide payments applications with survivability in the face of failure. By rethinking offline payments and generalizing several foundational pillars of digital payments, Crunchfish aims to revolutionize not only offline payments, but also digital payments, with its groundbreaking technology.

IT IS NOT ABOUT THE HAPPY FLOW
BUT SURVIVABILITY IN THE FACE OF FAILURE

Introduction

Addressing offline payments is essential for solving the fundamental problems within digital payment systems. Traditional payment infrastructures are designed primarily for smooth operations, often resulting in a heavy reliance on ideal conditions, or the "happy flow." When failures occur, such as backend server outages or network connectivity issues, transaction processes come to a halt, leading to user dissatisfaction and translates into lost revenues for merchants. The focus should be on ensuring service availability, rather than merely enhancing network connectivity.



In the 1990s, circuit-switched communication was rendered obsolete by the introduction of the packet-switched protocols. This shift allowed for more resilient and efficient data transmission across networks, paving the way for the internet as we know it today. Similarly, the digital payments landscape is overdue for a similar transformative upgrade towards a more adaptable and resilient architecture.

A public good such as digital payments should have more built-in resilience than only working when everything works. It is the duty of financial regulators or central banks to demand better resilience. The technology that delivers it is already available. Crunchfish's Trusted Application Protocol (TAP) generalizes the communication protocols of the internet by enabling any application to function anytime and interact using both remote and short-range protocol in proximity. This is not just about rethinking offline payments; it's about fundamentally rethinking digital payments.

The focus of the remainder of this conference white paper is to explore how to design offline payments to arrive at an architecture that is secure and deployable at scale, either domestically or internationally. It is structured into three sections:

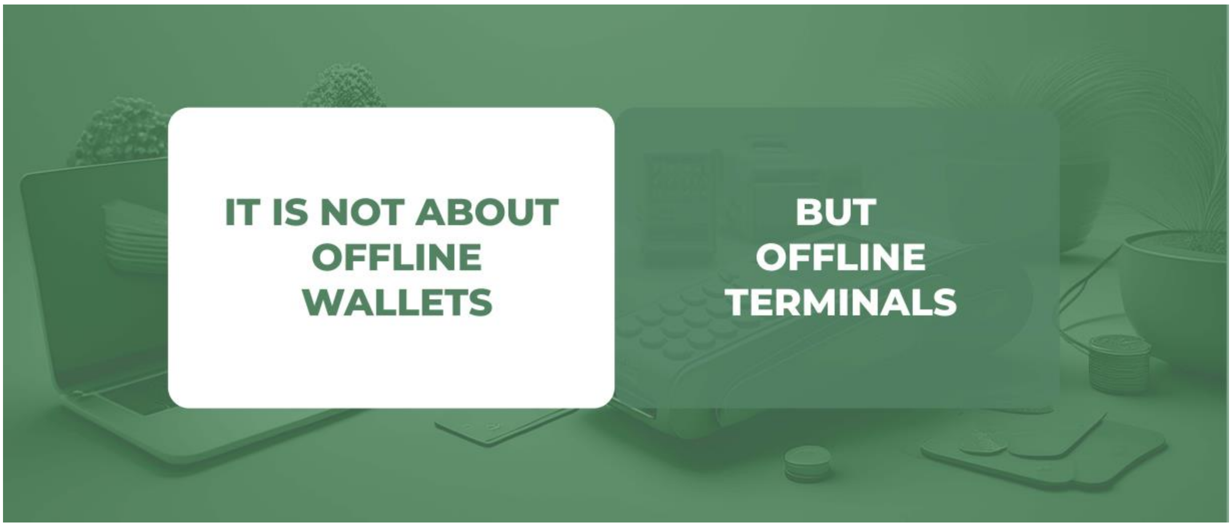
1. *Payment system roles,*
2. *Contrasting Digital IOU checks with Digital Banknotes, and*
3. *Generalizing foundational pillars of payments.*

The need for a complete rethink of offline payments is evident, as the industry has taken wrong turns on so many dimensions that hinders the deployment of wide-scale offline payment solutions. Previous approaches have had myopic security thinking and prioritized short-sighted gains over holistic, robust, scalable implementations, maintaining a fragile and fragmented payment landscape with compromised service availability. By addressing the critical challenges correctly by redesigning the fundamental framework for offline payments, it is possible to pave the way for a more resilient digital payments ecosystem, that operates seamlessly, even in environments with inconsistent network connectivity or temporary server outrages.

Payment Ecosystems Roles

IT IS NOT ABOUT OFFLINE PAYMENTS
BUT PAYMENT NETWORKS AND SERVICE PROVIDERS

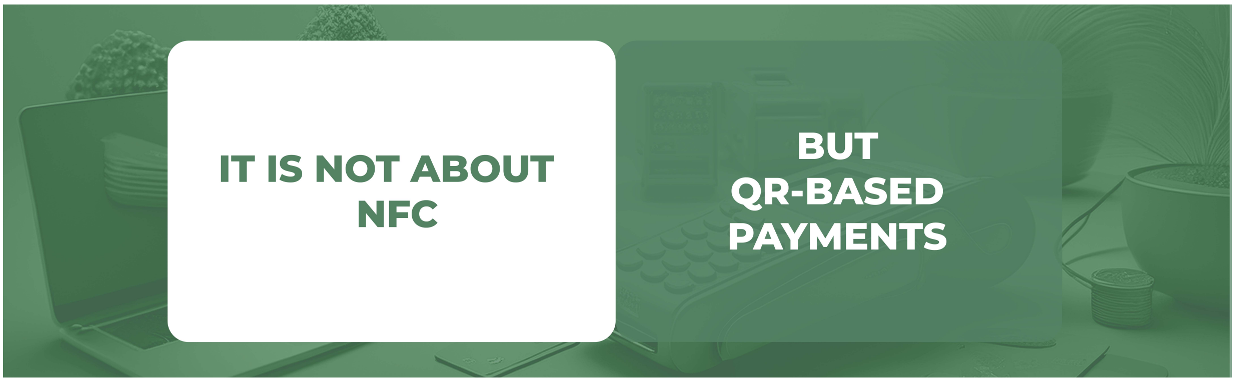
In the evolving landscape of offline payments, it is crucial to delineate and understand the roles played by two key stakeholders, namely payment networks and payment service providers. By allowing them to assume their natural roles also for offline payments, it ensures that digital as well as offline payments are delivered efficiently and effectively, contributing to ecosystem robustness, overall payment service availability, and at the same time fostering market innovation and competition.



A successful deployment of offline payment solutions requires a clear understanding of the distinct responsibilities of payment network providers and payment service providers. Payment network providers should focus on creating the necessary infrastructure to support terminals that facilitate the reception of offline payments for all participants. In contrast, payment service providers are tasked with deploying offline wallets, empowering end users to make payments without relying on online connections. This clear delineation of roles fosters a dynamic and interoperable market that drives innovation in offline payments.

To set up an offline payment ecosystem, the initial focus should be on establishing the ability to receive offline payments as widely as possible in the market. This task belongs to the payment network provider. The software-based offline terminals can be deployed as part of the payment rail's common library deployed in all payment service providers' payment applications, which immediately enables all end-users on various payment applications to receive offline payments. The offline terminal software may also be integrated in various business apps for merchants and existing POS terminals for wider reach. With the acquiring side in place, it is now possible to interest payment service providers to integrate offline wallets into their applications.

It is important to note that there is a security asymmetry between offline terminals and offline wallets as compared to the peer-to-peer payments between offline wallets. Whereas it is imperative to ensure an isolated runtime execution environment for offline wallets to avoid multiple attack vectors leading to double spending, the security requirements for offline terminals are not as strict. The role of the offline terminal, like the role of a card terminal, is to issue a payment request in proximity to an offline wallet, validate the incoming offline payment, store the offline payment, and then forward it for settlement when online connectivity is available. Hence, the offline terminal is only a relay station for offline payments that can validate, store, and forward a cryptographically signed offline payment from an offline wallet. The offline payment cannot be altered in any way, without making the offline payment invalid.

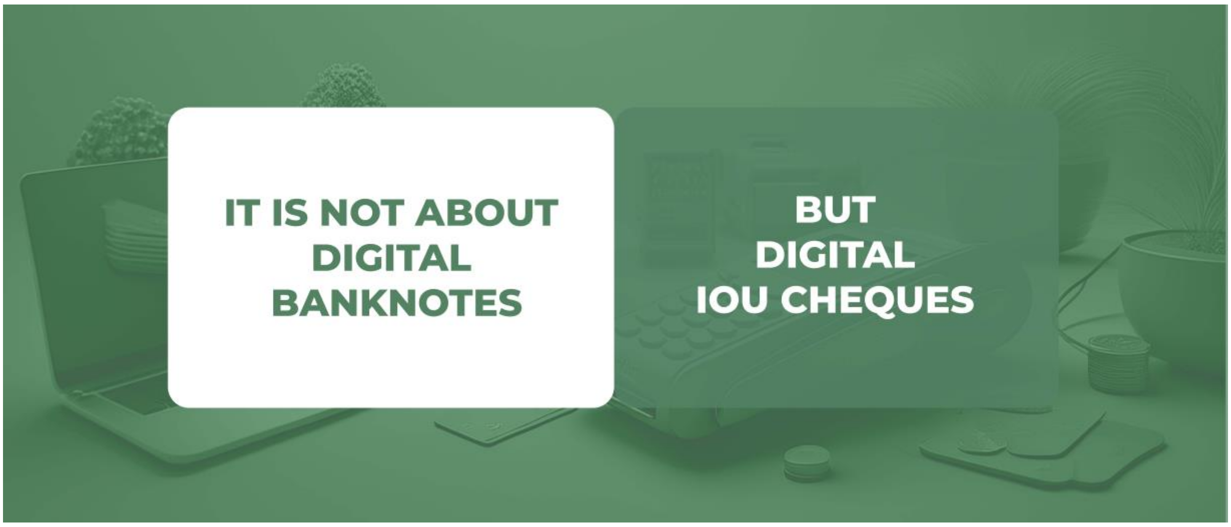


IT IS NOT ABOUT NFC BUT QR-BASED PAYMENTS

In terms of offline payments in proximity NFC (Near Field Communication) has been a popular choice. However, it has significant limitations, particularly in low-end smartphones that often do not support this interaction technology. Additionally, using NFC can complicate interactions between devices because users must align their devices precisely to initiate a transaction. As such, a more flexible approach to proximity interactions is necessary. Crunchfish is adopting an agnostic proximity interaction framework and can leverage various other proximity interaction methods as well — such as QR codes, Bluetooth, and ultrasonic signals — ensuring reliable and user-friendly payment experiences across a broader range of devices. This flexibility enhances accessibility and supports a wider demographic, enabling seamless transactions in any environment.

To summarize, the payment network should focus on deploying offline terminals as widely as possible in the market to enable to ability to receive offline payments and it is the role of the payment service provider to integrate offline wallets, with high security requirements, into their payment's applications for end users. It is important to enable payments between offline wallets and offline terminals as well as peer to peer payments between offline wallets. After the payment network have established the ability to receive offline payments, it is possible to onboard payments service providers and as well as end users for offline payments incrementally. In terms of proximity interaction method between wallets or wallets to terminals it should be agnostic to enable as many payment interactions as possible.

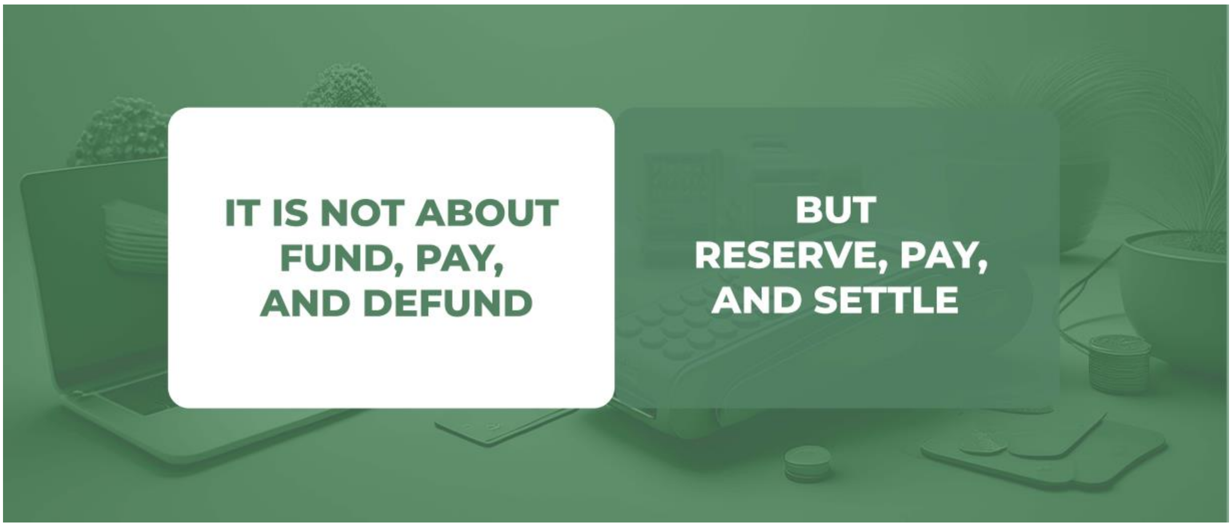
Contrasting Digital IOU Cheques with Digital Banknotes



IT IS NOT ABOUT DIGITAL BANKNOTES

BUT DIGITAL IOU CHEQUES

In the context of offline payments, it is essential to differentiate between digital banknotes and digital IOUs. The widespread card payment model operates on the principle of digital IOUs, albeit without any stored value in the offline wallet of the payer. It is beneficial to model offline payments as digital IOU cheques as well, benefiting from many years of experience from payments on the legacy card rails, facilitating a more fluid and flexible transaction process compared to unproven digital banknotes.



IT IS NOT ABOUT FUND, PAY, AND DEFUND

BUT RESERVE, PAY, AND SETTLE

The successful card payment model relies on online settlement of transactions between the user and the card terminal. This should also be the norm for offline payments with the main difference that the user has stored values on their devices to avoid any credit risks. The correct offline payment paradigm is a Reserve, Pay, and Settle approach, where offline payments are digital IOU cheques.

The Reserve, Pay, and Settle approach is superior to the Fund, Pay, and Defund approach which is common in many CBDC implementations. Whereas Fund, Pay, and Defund is working fine for online wallets as it mimics Pre-Paid Instruments, it introduces significant double spending risks in an offline mode. The fundamental problem of having a payee having a claim on the payment network, e.g. a central bank, after having received value from potentially many consecutive offline payments, is that there is no way of detecting from a payment network perspective if there has been any fraudulent offline wallets involved in the chain of transactions leading up to this claim.

Transferring digital banknotes offline with instant finality, without any subsequent online settlement, has no benefits whatsoever from security and efficiency perspectives, compared to implementing an approach with offline payment with online settlement. Offline payment with instant finality requires an extreme focus on device security with hardware-based secure elements, which leads to scalability challenges as no ecosystems exist to deploy and upgrade offline wallets on hardware-based secure elements.

Traditional hardware-based security solutions impose significant challenges in scalability and deployment, particularly considering the fragmented landscape of mobile devices.

IT IS NOT ABOUT SECURE ELEMENTS

BUT ISOLATED RUNTIME EXECUTION

Instead, a much better approach is to deploy offline wallets on app-integrated virtual secure elements as they do provide the isolated runtime execution environments necessary from a security perspective, without the scalability and upgradability issues as well as costly downsides of hardware-based deployments.

IT IS NOT ABOUT MAXIMUM SECURITY OFFLINE

BUT FRAUD DETECTION ONLINE

Having offline payments without settlement provides no chance for the payment network in discovering fraudulent offline wallets, unless centralized reconciliation systems are put in place. But these brings no value compared to leveraging the security readily available in the distributed core banking systems.

It is crucial to focus on privacy for both online as well as offline payments, rather than just having full anonymity for low-value, and therefore less-important, offline payments. The goal should be to ensure that payment details are kept confidential for the whole payment ecosystem; save for the user's trusted bank that may have exclusive access to the payer's transactional information. This approach to privacy goes hand in hand with having offline payments with online settlement and ensures that online as well as offline payments maintain equally high privacy standards.

To summarize, there are significant differences between the superior Reserve, Pay, and Settle and the cumbersome Fund, Pay, and Defund approach for offline payments. The latter emphasizes maximum device security but introduces complexities and risks associated with hardware dependence. Relying on centralized surveillance for payment security is increasingly viewed as inefficient and it comes with unwanted privacy issues with the payment network. In contrast, leveraging distributed core banking systems allows for enhanced security checks, efficiency, and privacy, creating a more resilient system that protects user data and promotes user trust in both online and offline payment processes.

Generalizing Foundational Pillars of Payments

IT IS NOT ABOUT TRADITIONAL ONLINE PAYMENTS
BUT NEXT-GENERATION OFFLINE PAYMENTS

Crunchfish's deep fintech advancements offer an opportunity to generalize four foundational pillars of digital payments all at once:

- *The Internet TCP/IP protocols,*
- *Real-Time Payment e-Wallets,*
- *Card Payments, and*
- *Conditional Payments.*

That Crunchfish deep fintech is so versatile provides an incredible flexibility as it provides enhanced interoperability, higher security and more resilience for any type of digital payment. Below is a brief overview of how Crunchfish's patented, and patent-pending technology generalizes four foundational pillars of digital payments.

The Internet's TCP/IP protocols

As stated in the introduction to this conference whitepaper Crunchfish enables applications to operate across various communications protocols using its patent-pending Trusted Application Protocol (TAP). This provides the survivability in the face of failure required of digital payments as a public good, instead of relying on a happy-flow approach, where digital payments only work when everything works. Client / Server applications can be trusted offline and transport its messages via any communication protocol in proximity and remotely, not just TCP/IP, using Crunchfish's patent-pending Trusted Application Protocol (TAP).

The TAP protocol is transport-layer agnostic and relies on secure client / server communications from secure endpoints. With an isolated runtime executing environment, implemented preferably within a virtual secure element, having a private key generated and operating from within the virtual operating system, it is possible to enable secure end to end communications between clients or between a client and the server without any trust gaps, on long-distance or short-distance channels, by means of PKI and cryptographic signatures. This enables not only secure offline payments communications but also improved client authentication security for online payments.

In the paper "The design philosophy of the DARPA Internet Protocols" published in 1988 by David D. Clark from Massachusetts Institute of Technology outlines that the internet fundamentally is "a packet switched communication facility in which a number of distinguishable networks are connected together using packet communications processors called gateways which implement a store and forwarding algorithm".

Crunchfish's offline solution is inspired by the design philosophies that was developed by the Defense Advanced Research Projects Agency (DARPA) in the 1970s and became the internet as we know it today. It is an incredible robust protocol based on packet switching. This is how Crunchfish Digital Cash works for payments. Clark outlines seven secondary design goals for TCP/IP, for which Crunchfish Digital Cash has an equivalent and patent-pending Trusted Application Protocol (TAP).

Crunchfish Digital Cash is based on the same design principles and may deliver for digital payments what the internet has done for digital communications.
Any public good in the society like the internet, electricity or telecom must be carefully designed to continue working despite temporary outages of the service. It is hard to understand why digital payments, certainly also a public good, is not as robust as other public goods. Digital payments service must be as robust, inclusive and private as cash payment.

Real-Time Payment e-Wallets
The generalization of offline wallets with the operational capabilities of standard Real-Time Payment e-Wallets presents a transformative approach to initiating payments. By leveraging the e-Wallets convenience, and accessibility, offline wallets can provide essential functionalities for users, mirroring the reliability of online payment methods.

Crunchfish technology enable client applications to be trusted offline as well as implementing or improving authentication security for online payments using Crunchfish's patented offline payment solution with online settlement and patent-pending Trusted Application Protocol (TAP). In a world where connectivity is not always guaranteed, offline wallets stand to bridge the gap, enabling users to engage in digital transactions smoothly, irrespective of their location or connectivity status. This evolution not only broadens the reach of digital payments but also fortifies financial inclusion on a global scale.

IT IS NOT ABOUT STAND-ALONE CARD NETWORKS
BUT INTEROPERABLE PAYMENT NETWORKS

Card Payments

Crunchfish's deep fintech provides several generalizations of the successful legacy card payment model. Payment applications can be trusted offline and transact offline without credit risk, as there is a stored value in the offline wallet. Transactions are not limited to a single card network, such as MasterCard or VISA, as it possible to pay offline and be interoperable on any payment scheme, i.e. Real-Time Payments, CBDCs, Stablecoins, Mobile Money, Cryptocurrencies, etc, and even EMVCo Card Payments. Like EMVCo systems, the modular design separates terminals and wallets, ensuring interoperability and standardization.

- *EMV Terminal Infrastructure:* In EMVCo systems, acquiring terminals ensure that payments can be received universally across the ecosystem. Similarly, the Offline Terminal Infrastructure serves as the foundational component for receiving payments, validating payer-side interactions securely and reliably.

- *Card Issuance Model:* EMVCo chips or cards from financial providers function as standardized payment origination tools. Similarly, Offline Wallets are the tools for initiating offline payments, provided as secure, standardized solutions aligned to payment network specifications.

- *Standardization and Interoperability:* EMVCo's specification enables issuers, acquirers, and merchants to operate on common standards. Similarly, this modular offline system ensures that terminals and wallets stay interoperable regardless of provider or user preference.

The benefits of a clear modular separation between receiving and paying components reduces implementation complexity and standardized specifications (e.g., for offline terminals and offline wallets) that foster competition and innovation within the ecosystem.

IT IS NOT ABOUT CONDITIONAL PAYMENTS
BUT CONDITIONAL OFFLINE PAYMENTS

Conditional Payments

The proposed Reserve, Pay, and Settle approach for offline payments aligns closely with conditional payments, or programmable payments or smart contracts as they often is referred to. Conditional payments are a generalization of standard online payments as they impose conditions on the settlement. Crunchfish deep fintech generalizes in turn conditional payments as it allows conditions to be defined offline and executed offline. Below are some comparisons with Etherium's smart contracts.

- *Programmable Constraints for Settlement:* In Ethereum's smart contracts, payments or transactions are executed based on pre-defined conditions programmed within the contract. Similarly, Reserve, Pay, and Settle (RPS) introduces settlement constraints for offline payments, ensuring funds are reserved before they are paid and reconciled securely once connectivity is restored. This parallels the way smart contracts enforce trust between parties without requiring a central intermediary for real-time validation. Offline payments achieve this trust by securely signing transactions in the wallet using cryptographic methods (such as PKI).

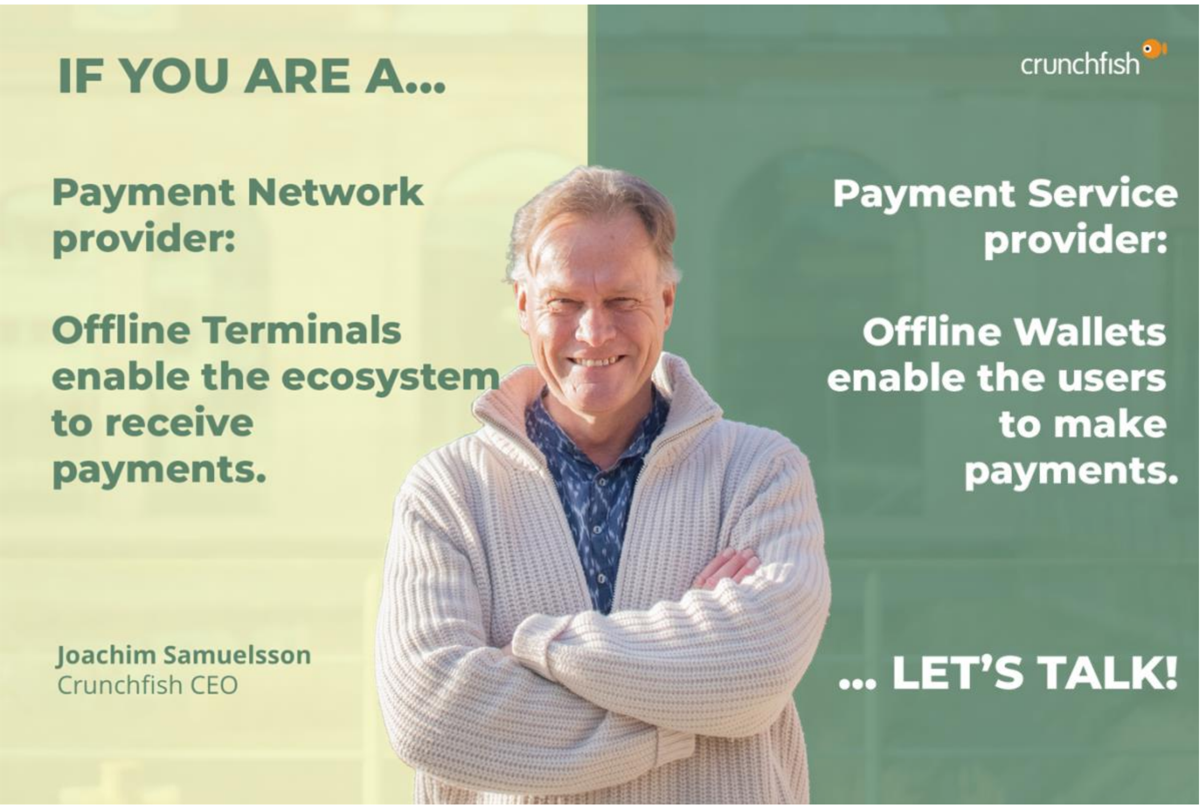
- *Deterministic Execution in Isolated Environments:* Ethereum's smart contracts execute within the Ethereum Virtual Machine (EVM), providing a tamper-proof environment for deterministic processing. Similarly, offline wallets in secure elements, whether virtual software-based or hardware-based, provide isolated runtimes to ensure the integrity of transaction signing and execution. For both approaches, isolated execution environments prevent external tampering and ensure transactions are initiated securely.

- *Automation and Reconciliation:* Smart contracts on Ethereum automate the settlement of transactions once predefined conditions are met, such as event triggers or external approvals. Similarly, the Reserve, Pay, and Settle approach automates the reconciliation process, validating offline transactions during online settlement and ensuring any conditions related to the payments — such as constraints on spending limits or usage validation —are enforced securely.

The benefits of this Reserve, Pay, and Settle approach is a trusted framework where offline payments rely on cryptographic trust mechanisms, just like Ethereum's smart contracts, to ensure integrity during execution, mitigating risks such as double spending. The Ethereum smart contracts operate universally on the blockchain via standardized protocols. Both approaches prioritize transaction security, leveraging isolated execution environments and cryptographic validation to maintain transactional integrity. Conditional offline payments introduce advanced use cases, such as escrow, pay-per-use models, or government-disbursed subsidies with strict conditional rules for usage.

Conclusion

In conclusion, the challenges associated with implementing offline payments have arisen from several missteps within the industry. It has taken wrong turns in so many dimensions, often focusing on narrow metrics. This era is about to change, as Crunchfish is collaborating with leading payment networks to bring its next-generation payment architecture to life for payment service providers. There is a need for holistic approach focused on service availability, emphasizing resilience in payment processing. By embracing an approach that prioritizes service availability over mere network connectivity, we can provide solutions that ensure resilient transactions regardless of disruption. Together, we can reshape the landscape of offline payments and create an inclusive and robust payments ecosystem for the future meets the evolving demands of consumers and businesses alike.


IF YOU ARE A...
crunchfish
Payment Network provider:
Offline Terminals enable the ecosystem to receive payments.
Payment Service provider:
Offline Wallets enable the users to make payments.
Joachim Samuelsson
Crunchfish CEO
... LET'S TALK!

About the author

Joachim Samuelsson is the CEO and main owner of NASDAQ First North-listed Crunchfish, a pioneering fintech company based in Malmö, Sweden. As a deep tech innovator and serial entrepreneur, Joachim has consistently driven groundbreaking solutions at the intersection of technology and business. Joachim is a recognized leader in innovation with over 20 granted patents in digital payments and communication technologies, Joachim holds a significant intellectual footprint in the industry. He is widely regarded as a pioneer in offline payment innovation, blending his expertise in robust communication systems with the growing demand for inclusive and resilient payment ecosystems.

Joachim is no stranger to success. He has held leadership positions in seven business exits, including four in which his automatic frequency planning innovation transformed mobile telecom networks. His ability to identify and implement transformative solutions makes him a key figure in the payment and technology industries. Joachim has received numerous awards for his entrepreneurship and vision and continues to lead from the front as Crunchfish shapes the future of offline payments globally.

About Crunchfish

Crunchfish redefines the roles in the payment ecosystem with banks and TPAPs responsible of sourcing in the offline wallets for their end users, while central banks or commercial payment network providers, responsible for the payment rail, offer an interoperable offline terminal infrastructure. This separation creates flexibility, scalability, and healthy competition within the ecosystem. Based on a Reserve, Pay, and Settlement approach it shares foundational similarities with conditional payments, a k a programmable payments or smart contracts. Please join to explore how this breakthrough architecture enables seamless offline payments in modular and future-ready CBDC and commercial payment systems.

crunchfish