SCION and cross-border payments: Enhancing security and compliance in distributed ledger networks

Grace Cimaszewski, Francesco Da Dalt, Thomas Moser, Adrian Perrig

SNB Working Papers
15/2025

SCHWEIZERISCHE NATIONALBANK
BANQUE NATIONALE SUISSE
BANCA NAZIONALE SVIZZERA
BANCA NAZIUNALA SVIZRA
SWISS NATIONAL BANK

DISCLAIMER

The views expressed in this paper are those of the author(s) and do not necessarily represent those of the Swiss National Bank. Working Papers describe research in progress. Their aim is to elicit comments and to further debate.

LIMITATION OF LIABILITY

The SNB accepts no responsibility for any information it provides. Under no circumstances will it accept any liability for losses or damage which may result from the use of such information. This limitation of liability applies, in particular, to the topicality, accuracy, validity and availability of the information.

ISSN 1660-7716 (printed version)
ISSN 1660-7724 (online version)

SCION and Cross-Border Payments: Enhancing Security and Compliance in Distributed Ledger Networks*

Grace Cimaszewski[†] Francesco Da Dalt[‡] Thomas Moser[§]
Adrian Perrig[¶]

September 2, 2025

Abstract

Cross-border payments remain expensive, slow, and opaque due to reliance on correspondent banking. Distributed ledger technology (DLT) offers a possible alternative, enabling peer-to-peer transactions at lower cost with greater speed, transparency, and resilience. However, DLT systems largely rely on the public Internet, which exposes them to network-based outages and attacks. SCION, a secure next-generation Internet architecture, can operate side-by-side with today's Internet to mitigate network-related risks. In addition to the security benefits, SCION also provides a novel approach to enforce regulatory compliance on a permissionless DLT with a governance model well-suited for multi-jurisdictional platforms. We present the first practical blueprint for deploying a DLT-based settlement system on SCION and demonstrate, through a simulation-based analysis of the real-world DLT system Sui, that SCION can mitigate more than half of routing-based network attacks, even when only partially adopted by DLT validators. Overall, SCION can provide a robust infrastructure foundation for DLT-based cross-border payment systems by enhancing their security, reliability, and regulatory compliance.

Keywords: DLT reliability, DLT availability, network attacks, routing attacks, DDoS
JEL Codes: E42, F33, G21

*Disclaimer.** The views, opinions, findings, and conclusions or recommendations expressed in this paper are strictly those of the authors. They do not necessarily reflect the views of the Swiss National Bank (SNB). The SNB takes no responsibility for any errors or omissions in, or for the correctness of, the information contained in this paper.

[†]Princeton University
[‡]ETH Zurich
[§]Swiss National Bank
[¶]ETH Zurich, Anapaya Systems, Mysten Labs

1 Introduction

Cross-border payments, i.e., financial transactions in which the payer and payee reside in different countries, are essential to global trade and finance. While the majority of these payments are large-value or wholesale transactions between financial institutions and large corporations, retail transactions, such as online purchases from foreign retailers or remittances sent by migrants to their families, continue to grow in volume.

Despite their importance, cross-border payments are expensive, slow, and non-transparent [10]. They are expensive and slow because they rely on correspondent banking, which involves multiple intermediaries——each adding fees and costs related to compliance checks and pre-financing. Processing times are further delayed by differences in operating hours across time zones. Additionally, direct exchange between the payer's and recipient's currencies is often not possible. Instead, the transaction must first be converted through a widely traded currency, such as the U.S. dollar, requiring additional banks outside both the payer's and recipient's countries. The lack of transparency stems from the difficulty in tracking the exact route and processing stages of a transaction, and costs vary depending on the payment's path and can often not be determined upfront.

These inefficiencies contrast with domestic payment systems, where technological innovations have driven significant improvements in recent years, facilitating near-instantaneous transactions in several countries. Recognizing the need for faster, cheaper, and more transparent cross-border payments, the G20 has made this a policy priority—encouraging international organizations, such as the Bank for International Settlements (BIS) and the International Monetary Fund (IMF), to explore how new technologies can enhance payment infrastructures [9].

One such alternative is distributed ledger technology (DLT) and the use of digital currencies. DLT eliminates the need for intermediaries, enabling peer-to-peer payments with near-instant settlement anytime at any day of the week. Additionally, it enhances transparency, traceability, and auditability in cross-border payments, as every transaction is recorded on a shared ledger with real-time visibility. Finally, its decentralized structure promises to offer greater resilience to local outages.

In theory, DLT solutions can operate on any network that supports peer-to-peer data exchange. In practice, however, both permissioned and permissionless DLT deployments typically rely on the public Internet. Within a DLT-based peer-to-peer network, nodes use the Internet to submit and propagate transactions, exchange consensus messages, deploy smart contracts, and integrate off-chain data through oracle feeds. In essence, the Internet serves as the infrastructure for proposing, validating, and recording ledger updates.

Since DLT systems rely on the public Internet, they inherit the vulnerabilities that affect Internet-based platforms. Infrastructure-level attacks, such as distributed denial-of-service (DDoS) attacks and Border Gateway Protocol (BGP) address hijacking, can delay or disrupt information flow, potentially causing network partitioning by isolating one or multiple participants. SCION (Scalability, Control, and Isolation on Next-generation Networks), a next-generation Internet architecture, offers enhanced security and reliability at the routing layer, preventing or mitigating these threats [7]. By leveraging both today's Internet and SCION, a DLT system can greatly enhance availability and resilience to attacks.

In addition to the security benefits, SCION also provides a novel approach to enforce regulatory compliance on a permissionless DLT with a governance model well-suited for multi-jurisdictional platforms. The tools it offers would be similar to SWIFT's control in traditional cross-border transactions but in a decentralized manner. Overall, SCION can provide a robust infrastructure foundation for DLT-based cross-border payment systems by enhancing their security, reliability, and regulatory compliance.

2 Background

2.1 Vulnerabilities of DLTs on the Internet

Today's Internet represents one of the most impressive accomplishments of mankind, globally connecting billions of devices and people across many Autonomous Systems (ASes). An AS represents a single network entity such as Colt, SNB, or ETH Zurich. The dominant protocol in use today to connect all the inter-connected ASes is the Border Gateway Protocol (BGP). Unfortunately, BGP was not designed with a focus on security and thus suffers from numerous vulnerabilities. In contrast, to achieve high availability even in the presence of active adversaries, SCION is designed with security as its main design principle, also addressing fundamental sovereignty issues of BGP routing.

DLT-based cross-border payments require, as the name suggests, an exchange of information between globally distributed ASes. To achieve information transmission over the Internet, data is placed in *network packets*, which are transmitted hop-by-hop by a network of nodes (e.g., routers and switches) until the packet reaches the destination (Figure 1). The sequence of visited network nodes is referred to as the packet's *path*. Deciding on which path a packet should traverse the Internet is known as *routing*. In today's Internet, each BGP router selects the next node for the packet based on the packet's destination and the local forwarding table. Thus, packet forwarding with BGP is similar to the physical letter mail service, where the sender writes the recipient's address on the envelope and entrusts the mailman with the delivery. The mailman then follows signposts and road-maps (i.e., the forwarding tables) to deliver the envelope to its destination. In the same way that reliable signposts help mail carriers to ensure that an envelope reaches its intended recipient, a secure inter-domain routing system must guarantee that packets are delivered only to their correct destination and follow trustworthy paths – something BGP by itself cannot provide. In summary, BGP provides the sender with neither a path choice nor transparency of which path will be used.

Efforts have been made to retrofit traditional security measures to BGP. The most widely deployed system is based on the Resource Public Key Infrastructure (RPKI), which hosts cryptographic attestations of IP prefixes and AS numbers which can be used to validate BGP announcements. Route Origin Authorizations (ROAs), RPKI's most widely used resource, prevent the most common types of BGP hijacks by attesting to the AS owner of IP prefixes; in our mail system analogy, it is like an official postal registry verifying the owners of P.O. boxes. Benefiting from RPKI is a two-party process: first, network owners themselves must create and register ROA objects for the IP addresses they own; secondly, other connecting networks must filter the BGP announcements they receive based on RPKI data, a process known as Route Origin Validation (ROV). RPKI-ROV prevents the most blatant form of BGP hijacks where a malicious network falsely claims to own an IP address range. However, this secures only the origin of the BGP announcement, not the entire path. Attackers can still evade this defense by crafting announcements with more advanced path manipulations, such as a route with a truthful origin but other parts of the AS path are manipulated (similar to a corrupt postal worker

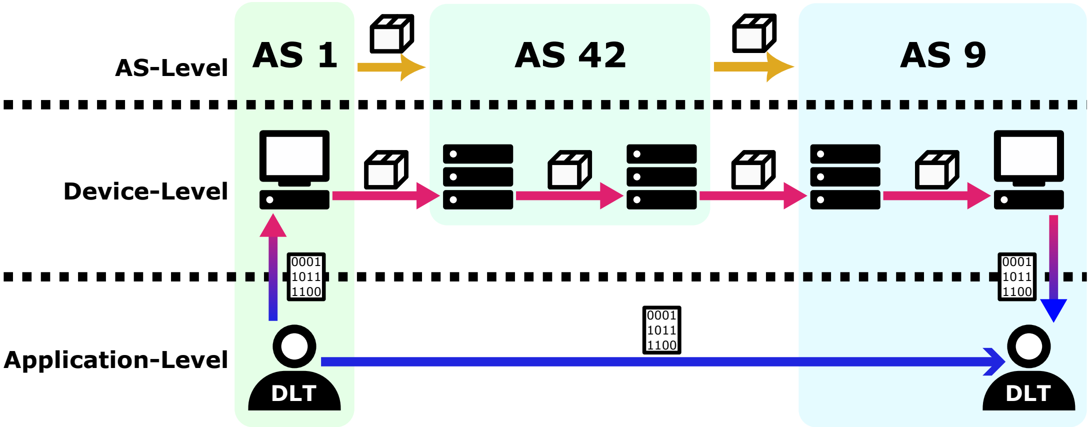


Figure 1: Messages travel from source to destination (blue) by traveling as network packets from device to device (red). In this process, packets may cross multiple Autonomous Systems (ASes) as shown by the yellow arrows.

intercepting the mail during delivery). RPKI deployment is steadily growing: an analysis of RPKI data at the trust anchors in March 2025 shows that over 54% of IPv4 routes are covered by a ROA [18]. However, RPKI does not fundamentally secure BGP; it merely forces attackers to use stealthier hijacks.

BGP routes can be hijacked in a number of different ways. These hijacking techniques differ in the scope of their effectiveness (i.e., what proportion of Internet traffic they redirect), visibility (how suspicious the routing update may appear), and their ability to evade RPKI/ROV and security filtering practices. The success of a BGP hijack also depends on the identity of the attacker network itself. A well-connected attacker with hundreds of peering connections with other provider networks will hijack more traffic than a "stub" attacker with only an upstream provider link. Due to all these factors, analyzing a network's susceptibility to hijacks is not a simple task. By fundamentally eliminating this class of attacks, SCION provides by construction more secure and robust DLT operations.

These vulnerabilities expose DLTs to attacks on their hosting infrastructure, which ultimately may circumvent or undermine their cryptographic guarantees. The Web3 vision of a decentralized Internet overlooks the critical reality that DLT applications still depend on traditional Internet infrastructure (including BGP, DNS, CDNs, and Certificate Authorities) and do not address the fundamental security issues beneath. DLT applications are a particularly attractive target for network attackers, due to the potential for high financial gain. As one recent example, a 2022 attack on the KLAYswap cryptocurrency exchange platform involved a BGP hijack on an IP address which hosted a 3rd party JavaScript library dependency loaded in the application client-side, resulting in over $1.9M of digital assets being redirected to attacker-owned wallets [21]. Detecting such attacks from the application level is difficult, as attacks can target indirect dependencies or may be observable only in certain parts of the Internet. Designing DLTs on a secure network platform is crucial to ensuring overall safety of the system.

2.2 SCION: A Secure Internet Routing Protocol

The persistence of routing layer vulnerabilities despite years of patches and workarounds suggests the need for a clean-slate approach. SCION is designed with security as its main

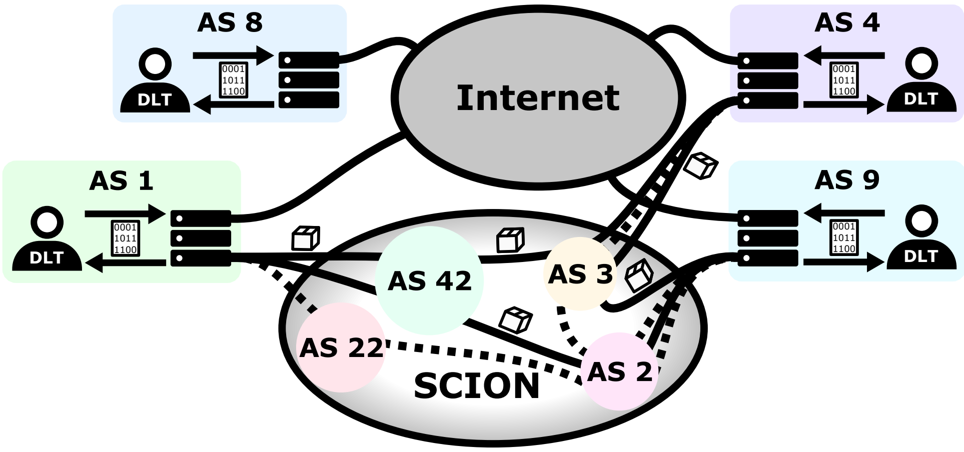


Figure 2: SCION and conventional Internet providing connectivity to DLT entities in parallel. Notice how the Internet is opaque and provides no information about what happens to data packets. SCION on the other hand provides greater transparency by enabling the sender to choose the explicit path the packets take, as well as providing multiple options for improved resilience and performance (dotted).

design principle, addressing fundamental sovereignty issues of BGP routing and achieving high availability even in the presence of active adversaries.

As a path-based network, SCION provides the sender with several concrete path options for a given destination. Such a path-aware network design offers fundamentally more secure packet forwarding by guaranteeing that a packet will follow the specific sequence of ASes along the sender-selected path. In the physical letter analogy, the sender attaches a sequence of locks, which can only be opened by trusted mailmen we gave the key to, to the envelope. For the letter to be delivered successfully, the envelope must therefore pass the trusted mailmen in-order. The recipient can verify this by checking the locks. In practice this is achieved by means of cryptographic authentication (Figure 2).

Today's Internet governance is dictated, making it difficult to adapt or evolve. SCION addresses this issue through the concept of ISolation Domains (ISDs). An ISD is a logical grouping of Autonomous Systems (ASes) that manage their own cryptographic keys and governance rules used to define and sign routing policies. Any group of ASes can establish an ISD, set governance policies, and connect with other SCION ISDs to achieve secure connectivity. The cryptographic root keys managed by a set of *core* ASes constitute the trust root of the ISD. It thereby enables sovereign self-government to the ISD. Additionally, ISDs provide *trust transparency*, making it explicitly clear which cryptographic keys and entities should be trusted for each operation.

SCION's embedded security mechanisms that cryptographically protect forwarding paths, along with the path-aware network approach enabling the sender to select the end-to-end path, offers several advantages to DLTs. We summarize some of the most significant advantages, ranging from availability to sovereignty, in the next paragraphs:

High Availability. DLTs require robust connectivity to ensure ledger distribution and prevent forking. The design and cryptographic protections of SCION defend against all known routing attacks, and the formal verification guards against new attacks. Moreover, SCION has built-in mechanisms to defend against DDoS attacks. Thus, by using both today's Internet alongside with SCION connectivity, the availability is dramatically improved—as long as either the Internet or the SCION network is operational, connectivity is ensured.

Rapid recovery from failure. Related to availability is the ability to rapidly recover from outages. Thanks to the multi-path operation of SCION, a link failure can be rapidly circumvented by selecting an alternate path. This feature has been successfully proven in the Secure Swiss Finance Network (SSFN) and can be an invaluable asset for ensuring minimal DLT downtime.

Efficiency. To ensure that DLT transactions can be processed at a high rate with low latency, ledgers need to be distributed rapidly over the network. Measurements on today's deployed networks show that when sending packets to destinations that are farther than 100ms (around 5'000km) SCION achieves 5–25% lower latency than the Internet thanks to its ability of finding and selecting low-latency paths [25].

Sovereignty and path transparency Through the ISD concept, SCION enables the definition of trust roots for public-key infrastructures, enabling sovereign operation and controlled governance if required. Moreover, path selection enables transparency of where information flows through the network.

3 A Blueprint for a SCION-protected High Availability DLT

Although the utilization of a new Internet architecture appears to require tremendous effort, we present a blueprint for a light-weight deployment that will result in significant advantages to a global DLT deployment. In particular, to avoid application-level software changes, we introduce the SCION-IP Gateway (SIG), which converts IP packets into SCION packets and vice-versa. The overarching goal is to increase availability: providing connectivity as long as either the Internet or the SCION network is operational. An adversary would need to successfully paralyze both networks to mount a successful attack. Even in a partial deployment setting where only some entities have a SCION connection, the availability will be enhanced, for instance a consensus operation can possibly proceed thanks to the SCION links that remain available while Internet links are under attack.

A natively integrated SCION support in the application reaps the most benefits from SCION, however, this approach requires a significant amount of additional implementation effort. A lighter weight approach is to make use of a SIG, which dynamically encapsulates IP packets into SCION packets. If the destination can be reached via SCION, the SIG selects the best path that adheres to the configured policy, and if the destination cannot be reached via SCION the packet is sent via the traditional Internet. Therefore, without any changes to the application software, the packet will reach the destination if either the Internet or the SCION network is operational.

Figure 3 depicts a setup with three entities: banks A, B, and C. Bank A operates within their own data center, without SCION connectivity. Bank B also operates in a data center but includes a SIG with SCION connectivity. Bank C operates in a cloud deployment, also with SIG and SCION connectivity. Entity A communicates with the other entities over the traditional Internet, while B and C can communicate over the Internet or over the SCION network. The setup is seamless and has been shown to

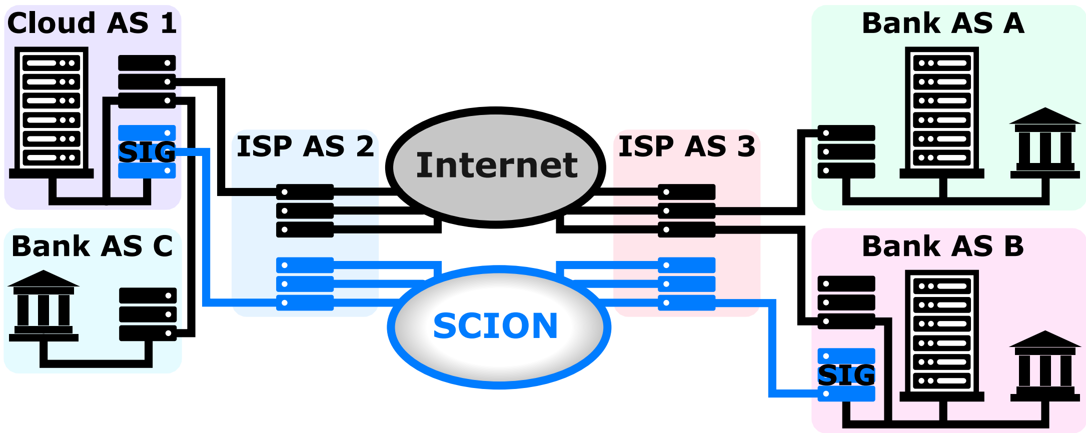


Figure 3: Deploying SCION for enhanced DLT operation. Banks are connected both over the public Internet, as well as over the SCION network. Black edges indicate conventional Internet connections, whole blue ones indicate SCION connections. The SCION-IP Gateway (SIG) acts as a translator between SCION and conventional Internet. Banks A and B run their own datacenter, while bank C uses a cloud service to host their operation. The Internet Service Providers (ISPs) manage the global connectivity of banks and cloud services.

work for the Sui blockchain [11, 17] in decentralized locations around the world. Specifically, testnet validators in New York, Tokyo and London are connected in this way, with efforts to extend the deployment to mainnet underway. SCION software is available as open-source [20] and as commercial product [1]. Several commercial providers offer SCION connectivity at global scale, including BICS, BSO, BT, Colt, Cyberlink, DLR, etc. The first large-scale real-world application of SCION, though not DLT-based, is the Secure Swiss Finance Network (SSFN), a SCION-based ISD launched in Switzerland for secure banking communications [22]. The SSFN's rollout demonstrated that participant onboarding can be achieved within a few months, highlighting SCION's practicality for real-world security-critical deployments.

While the SIG-based approach greatly simplifies the previously Herculean task of adopting an alternate Internet architecture, it still has its own challenges. Initial deployment does require investment in SCION infrastructure (SIG devices) and operational expertise, as demonstrated by the SSFN rollout which took several months [22]. In the partial deployment scenario where only a subset of DLT nodes adopt SCION connectivity, security benefits are limited to communication between SCION-enabled nodes, creating a bootstrapping challenge where early adopters bear costs before network effects materialize. Nevertheless, we argue that for high-value cross-border payment DLT systems these costs are justified by the substantial security and regulatory benefits SCION provides.

4 Network Vulnerability Analysis of a DLT Infrastructure

4.1 Introduction of Sui

We present the Sui blockchain as one such case study of how BGP hijacks that evade RPKI pose serious security issues to DLTs hosted on Web2 infrastructure [11]. Motivated by the demonstrated challenges of building secure DLTs on the legacy Internet, Sui is *the first DLT* to fundamentally mitigate these threats by leveraging SCION. We present an analysis of the vulnerabilities of Sui's legacy hosting to underline the usefulness of SCION adoption.

Sui is a next-generation, Proof-of-Stake-based Layer 1 blockchain designed for high-throughput transaction execution. Sui's $11.6B market cap (as of September 2025) rests on a network of 121 validators [8, 17], which work to propose transactions in blocks, confirm blocks proposed by other validators, and lastly finalize them via the quorum-based Mysticeti protocol [4]. Transactions achieve finality in Sui when validators representing at least two-thirds of the total network stake agree on the ordering of transactions. If a validator is disconnected from this supermajority quorum, it cannot participate in consensus or contribute to transaction finalization. Thus, reliable and secure connections between validators are critical for maintaining both safety and liveness in the protocol. Validator nodes in Sui are operated independently (often on cloud infrastructure) and communicate over the public Internet. Hence, they inherit many of the network-level vulnerabilities explained in Section 2.1.

4.2 Threat Model

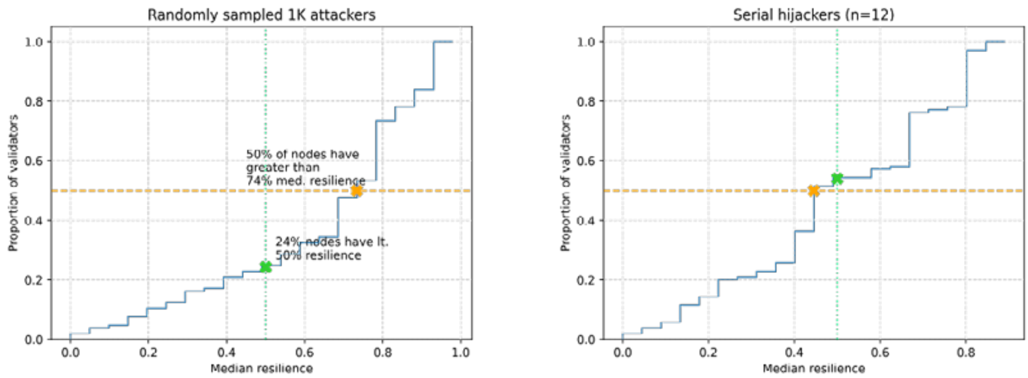
We consider an AS-level attacker capable of launching malicious BGP announcements. Specifically, the attacker can announce IP prefixes on which validator infrastructure is hosted, and can redirect or blackhole traffic without detection at the application layer. We assume that the DLT's underlying cryptographic protocols are secure and validators faithfully implement the protocol. Attacks that rely on compromised validator private keys, software vulnerabilities, unauthorized access to hosting infrastructure, or application-level vulnerabilities (e.g., smart contract exploits) fall outside the scope of our threat model.

The goal of the attacker is to impact validators' *liveness* (i.e., connectedness to at least two-thirds of the total stake) and thus prevent the DLT network from finalizing transactions by isolating a sufficient number of validators. This is achieved by disrupting routes (and by extension connectivity) between validators, rendering them unable to communicate and participate in consensus. If enough validators are made unreachable through hijacks, the network may fall below the threshold required for consensus, resulting in a global loss of liveness and transaction finality.

4.3 Evaluation

We present the outcome of simulated BGP hijacks launched by one thousand potential real attackers in the internet topology against Sui validators as of February 2025 in Figure 4. While 73% of Sui's stake is hosted on RPKI-protected prefixes, the overall network is still susceptible to adaptive BGP hijacks that evade RPKI. Validators' susceptibility to BGP attacks is measured by the *resilience* metric, which is the proportion of networks that retain the true route to the victim in the face of a BGP hijack. Routes to validators are easily disrupted by same-prefix BGP hijacks. 24% of validators scored less than 50% resilience, meaning that they can be successfully hijacked in the average case. Because Sui validators are concentrated in major cloud providers that tend to be popular hosting providers for DLT nodes, similar results can be expected for other DLTs.

BGP hijacks have grave implications for the resilience of not only individual validators, but also the network as a whole. Sui's consensus protocol relies on resilient network



(a) Randomly selected ASes ($n = 1000$). (b) ASes with history of BGP hijacking.

Figure 4: Sui validators' resilience to RPKI-evading simulated BGP hijacks.

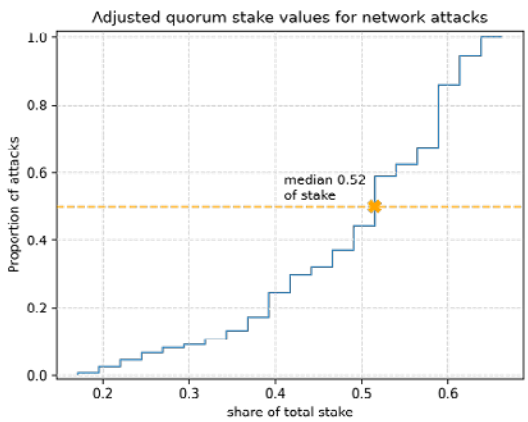


Figure 5: Change in proportion of live network stake in the face of BGP hijacks.

connections to a supermajority (i.e., at least 66%) stake-holding group of validators to validate transactions. While an attacker cannot spoof or modify validators' signed responses with BGP hijacks, the hijacks serve as a DoS attack whereby the stake held by hijacked validators is disconnected from the view of the network. If a sufficient number of validators are hijacked, the overall liveness of the network is threatened, as no transactions can be validated by a sufficient share of the stake. We apply the outcome of the BGP attacks presented in Figure 4 to a simplified recursive definition of validator liveness, where a validator must be connected to a supermajority of other validators to remain live (Fig. 5). The attack susceptibility of Internet-based blockchains is illustrated by the fact that over 83% of the simulated attacks succeed to take Sui's transaction confirmation offline. More than half of these attacks remove 48% or more of stake from the network. Migrating validator hosting to SCION can significantly mitigate the impact of these attacks, even under partial deployment. When modeling a scenario where validators controlling around 50% of the total stake are hosted on SCION, over half of the simulated attacks fail to partition or disable the network as the 66% stake threshold was reached in most cases despite the attacks.

When enabling SCION connectivity among a quorum of validators (holding over 66% of the stake), the Sui DLT achieves full resilience to these attacks.

5 SCION and Regulatory Compliance

As shown in the previous sections, an attractive feature of using SCION in a DLT-based cross-border payment system is its ability to significantly improve network security and reliability. Additionally, SCION can enforce regulatory compliance directly at the network level, offering a governance model well-suited for multi-jurisdictional platforms.

Regulated financial institutions generally prefer permissioned DLT applications because the pseudonymous nature of permissionless DLT creates compliance challenges. This is especially true in areas such as anti-money laundering (AML), countering the financing of terrorism (CFT), and sanctions enforcement. A specific concern often mentioned is that, in a permissionless DLT environment, financial institutions may unknowingly pay transaction fees to validator nodes controlled by sanctioned entities.

While permissioned DLT networks mitigate such risks by offering greater control, they come with trade-offs, such as limited network effects, reduced interoperability, and centralization risks. SCION can provide significant benefits within a permissioned DLT environment. However, by establishing a permissioned messaging layer on a permissionless DLT, SCION offers an alternative that blends compliance with decentralization. This approach allows institutions to leverage an existing DLT rather than building a custom compliance-focused blockchain from scratch. SCION's architecture is also well-suited for decentralized jurisdictional trust environments. By using SCION's ISDs as jurisdictional boundaries, regulators can enforce compliance rules within their respective regions without requiring modifications to the core DLT protocol.

For a cross-border payment system, each country or legal jurisdiction can establish a dedicated SCION ISD overseen by its financial regulator or central bank. The regulator, or a designated institution, would serve as the root Certificate Authority of its ISD, issuing SCION cryptographic certificates to financial institutions under its oversight. This ensures that possession of a valid certificate becomes a requirement for participation in the payment network, creating a strict access control mechanism at the network layer. This structure introduces a novel approach to identity verification: although the DLT remains permissionless at the consensus layer, each network node's affiliation is tied to a legal entity and a geographic region. Within an ISD, the regulator can set policies autonomously (e.g., which institutions obtain certificates, what network paths are permitted and thus which services are offered, such as CBDC, tokenized deposit DApps, etc.), achieving complete sovereignty over local network trust (Figure 6).

For cross-border transactions, national ISDs would need to interconnect. SCION natively supports secure inter-ISD communication through agreed trust anchors and peering links managed by ISD core nodes. Regulators can establish bilateral or multilateral agreements and embed these policies in their trust-root configurations to govern those peering links, ensuring that only messages that traverse authorized AS paths are forwarded. SCION's path-aware routing ensures that traffic complies with the respective ISD policies. For example, if a bank in Country A sends a tokenized deposit to a bank in Country B, both the sending and receiving bank can validate the authenticity and policy compliance of the entire network path. In particular, if transactions' network traffic is sent through a regulator's network device, the regulator can enforce additional control over transactions, allowing for swift enforcement of compliance measures such as certificate revocation or route blocking.

With regard to sanctions enforcement, SCION's architecture offers advantages over traditional centralized messaging networks like SWIFT. SCION gives jurisdictions their

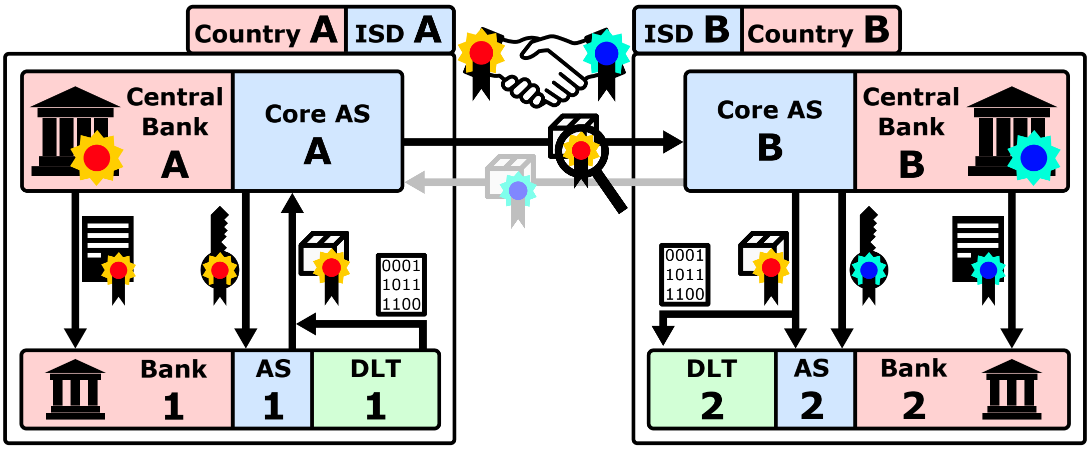


Figure 6: Regulated cross-border payments with a permissionless DLT over SCION. At a juridical level (red), central banks issue certificates to their financial institutes. At the network level (blue), the core-ASes of an ISD issue cryptographic keys to ASes in the ISD. At the DLT level (green), information (i.e. ledgers) are sent over the core ASes across ISDs. An agreement between core-ASes in different countries is needed to acknowledge each other's certificates, and allow cross-border payments. Core-ASes maintain sovereignty over their ISD by managing SCION's cryptographic root keys.

own ISDs, allowing each country to embed customized regulatory policies in its trust-root configuration. Because a sender can explicitly choose end-to-end network paths, messages can be constrained to travel only through authorised and compliant channels. If an institution later becomes sanctioned, the ISD can revoke that AS's certificate in its trust-root configuration, so endpoints that trust the updated trust-root configuration will no longer build paths that traverse the sanctioned node.

SCION can also enforce access controls for central bank digital currencies (CBDCs). For instance, Country A's central bank might mandate that only domestic institutions, or foreign institutions with established correspondents in Country A, may access its CBDC. SCION can enforce this by requiring transactions involving Country A's CBDC to pass through authorized SCION paths controlled by Country A's regulator. As a result, unauthorized institutions would be unable to obtain a valid network path to the CBDC's smart contract, ensuring compliance at the network level.

SCION also enhances regulatory compliance by improving network monitoring capabilities. Through the EPIC system [14], the receiver can obtain a cryptographic proof that the packets carrying the transaction traversed the correct set of intermediate ASes.[1] Unlike traditional networks, where IP addresses can be concealed using VPNs or TOR, SCION's EPIC extension provides verifiable network provenance and path verification, enhancing auditability and trust. Concretely, the sender can ensure path compliance given a transaction's requirements, and reject the transaction in case of a violation.

Overall, SCION's federated governance model is well-aligned with the structure of modern financial regulation. Each ISD operates independently under its national regulator's authority, while cross-border coordination is achieved through trusted peering agreements, which could be coordinated at the global level by a neutral, standard setting body. This model balances local control with global collaboration. No single country or entity would dominate the network because path control and trust are decentralized.

[1] Although the EPIC extension is currently not available in the SCION production network but only as a research prototype, it is expected that it will become available in case of user demand.

Specifically, each country or jurisdiction would remain in full control of its own domestic payment system. Moreover, SCION's governance structure separates network operations from governance decisions. Central banks and regulators can set policies without directly managing network infrastructure, relying instead on trusted technology providers to manage SCION routers within their ISDs.

Implementing compliance controls at the network level, as proposed here, represents a novel approach. One advantage of this network-layer strategy is that it does not require modifications to the DLT's core consensus rules. Instead, it adds an access or control layer to the existing protocol. This approach also avoids the introduction of on-chain overhead, which increases complexity and resource demands. In contrast, a base-layer (Layer 1) approach that manages identities and compliance on-chain burdens the protocol with additional data and logic. For example, every transaction might need to include proof of identity or reference to a credential, and every node might perform checks against revocation lists or whitelists. Similarly, enforcing compliance rules through smart contracts adds on-chain overhead.

Layer 2 solutions, such as sidechains, rollups, or state channels, address this issue by handling transactions off the main chain. However, their reliance on Layer 1 for final settlement introduces compliance risks, such as indirect fees flowing to sanctioned Layer 1 validators. Mitigating such risk requires sophisticated and complex bridging mechanisms.

The optimal compliance model is likely to combine various approaches, applying compliance logic at the most effective level for each requirement. Such a layered compliance approach can achieve the best balance of efficiency, scalability, and flexibility. The network level is best at handling broad and clearly defined compliance rules (e.g., licensing and sanctions), while higher layers can address more granular compliance requirements. Blocking sanctioned entities and jurisdictions at the network layer, before transactions reach protocols or smart contracts, can strengthen compliance while simplifying and reducing the burden on processes at the application layer.

6 Related Work

Network-layer attacks on DLTs. Network-based attacks that exploit the inherent lack of authenticity in Internet routing pose a well-studied threat to all DLTs hosted on the legacy Internet. Apostolaki et al. demonstrated that half of the Bitcoin network's mining power could be partitioned with a realistically scaled hijack of fewer than 100 IP prefixes [3]. A broader recent study found that other popular DLTs including Ripple and Ethereum are hosted in a similarly centralized way (and often colocated in a small number of shared ASes) as Bitcoin, making them equally susceptible to routing-based hijacks [19]. Beyond IP address hijacking, the Internet's lack of path verification enables well-positioned attackers to spoof IP origins and gradually monopolize a Bitcoin node's peering connections with attacker-owned IPs, thus disconnecting it from honest peer nodes [24]. Related work has also demonstrated that validator centralization in cloud providers increases their vulnerability to large-scale outages through DDoS attacks [12].

Mitigations. Mitigating routing-level attacks in the context of a pseudonymous, decentralized DLT is challenging. Third-party based proxies like SABRE require trusting externally hosted relay nodes (which themselves can become malicious), and hosting nodes on overlay networks such as Tor introduces even more severe vulnerabilities such as traffic manipulation and peer poisoning [2, 6]. These limitations reflect deep-rooted vulnerabilities in the Internet's architecture.

RPKI and its limitations. The Resource Public Key Infrastructure (RPKI) is the most widely deployed security mechanism for BGP today. RPKI-based defenses can secure the origin of BGP announcements, but do not protect against path manipulation. While deployment of RPKI both in terms of route filtering and route attestation registration is on the rise, RPKI provides limited benefit in a state of incomplete deployment [15]. RPKI can still be evaded by a range of more sophisticated BGP attacks, including forged-origin attacks, attacks that manipulate BGP communities [5], sub-prefix hijacks of misconfigured ROAs [13], BGP Vortex [23] and "hidden hijacks" [16] due to asymmetric filtering practices across ASes.

7 Conclusions

SCION addresses critical network-layer vulnerabilities in cross-border DLT-based payment systems by improving security, reliability, and regulatory adaptability. It could therefore provide an ideal network infrastructure for next generation DLT-based payment systems. Future research should explore real-world performance improvements in latency, resilience to attacks, and integration with payments.

In addition to these security and reliability benefits, SCION offers a novel approach to regulatory compliance directly at the network layer. By utilizing SCION's federated governance model, regulators can create jurisdictional boundaries (ISDs) and enforce compliance rules tailored to their region, including sanctions enforcement and CBDC access controls. Ideally, regulatory controls at the network layer would be combined with regulatory controls at the higher levels. Such a layered compliance model — ensuring broad compliance at the network level while allowing higher layers to address more specific requirements — could offer an optimal balance of efficiency, scalability and flexibility.

Acknowledgments

We gratefully acknowledge the feedback from William Boye, Denise Tischhauser, and Peter Thüring, which helped improve this article.

References

[1] Anapaya Systems AG. We're revolutionizing the internet with SCION. https://www.anapaya.net/, 2025. Accessed: March 31, 2025.

[2] Maria Apostolaki, Gian Marti, Jan Müller, and Laurent Vanbever. Sabre: Protecting bitcoin against routing attacks. In *Proceedings of the Annual Network and Distributed System Security Symposium*, page 02A1, Reston, VA, 2019. Internet Society. 26th Annual Network and Distributed System Security Symposium (NDSS 2019); Conference Location: San Diego, CA, USA; Conference Date: February 24-27, 2019.

[3] Maria Apostolaki, Aviv Zohar, and Laurent Vanbever. Hijacking bitcoin: Routing attacks on cryptocurrencies. In *IEEE Symposium on Security and Privacy (SP)*, 2017.

[4] Kushal Babel, Andrey Chursin, George Danezis, Anastasios Kichidis, Lefteris Kokoris-Kogias, Arun Koshy, Alberto Sonnino, and Mingwei Tian. Mysticeti: Reaching the latency limits with uncertified dags. In *Annual Network and Distributed System Security Symposium, NDSS*, 2025.

[5] Henry Birge-Lee, Liang Wang, Jennifer Rexford, and Prateek Mittal. Sico: Surgical interception attacks by manipulating bgp communities. In *Proceedings of the ACM SIGSAC Conference on Computer and Communications Security*, CCS, page 431–448. ACM, 2019.

[6] Alex Biryukov and Ivan Pustogarov. Bitcoin over tor isn't a good idea. In *IEEE Symposium on Security and Privacy*, 2015.

[7] Laurent Chuat, Markus Legner, David Basin, David Hausheer, Samuel Hitz, Peter Müller, and Adrian Perrig. *The Complete Guide to SCION*. Springer International Publishing, 2022.

[8] CoinGecko Research. Coingecko research reports and insights. `https://www.coingecko.com/research`, 2025. Accessed: March 20, 2025.

[9] CPMI, BIS, IMF, and World Bank. Joint report to the G20: Central bank digital currencies for cross-border payments, 2021. Accessed: March 6, 2025.

[10] Financial Stability Board (FSB). Targets for addressing the four challenges ofcross-border payments: Final report, 2021. Accessed: March 20, 2025.

[11] Sui Foundation. Sui advances network security and performance with SCION, 2025. Accessed: March 20, 2025.

[12] Adem Efe Gencer, Soumya Basu, Ittay Eyal, Robbert van Renesse, and Emin Gün Sirer. Decentralization in bitcoin and Ethereum networks. In *International Conference on Financial Cryptography and Data Security*, volume 10957 of *Lecture Notes in Computer Science*, pages 439–457, Nieuwpoort, Curaçao, 2018. Springer-Verlag.

[13] Yossi Gilad, Omar Sagga, and Sharon Goldberg. Maxlength considered harmful to the rpki. In *Proceedings of the ACM International Conference on Emerging Networking EXperiments and Technologies*, CoNEXT. ACM, 2017.

[14] Markus Legner, Tobias Klenze, Marc Wyss, Christoph Sprenger, and Adrian Perrig. EPIC: Every packet is checked in the data plane of a path-aware internet. In *Proceedings of USENIX Security Symposium (USENIX Security)*, August 2020.

[15] Robert Lychev, Sharon Goldberg, and Michael Schapira. Bgp security in partial deployment: is the juice worth the squeeze? In *Proceedings of the ACM SIGCOMM Conference*, SIGCOMM '13, page 171–182, New York, NY, USA, 2013. ACM.

[16] Reynaldo Morillo, Justin Furuness, Cameron Morris, James Breslin, Amir Herzberg, and Bing Wang. Rov++: Improved deployable defense against bgp hijacking. In *Annual Network and Distributed System Security Symposium, NDSS*, 2021.

[17] Mysten Labs. Sui coin: High-performance layer 1 blockchain. https://sui.io, 2025. As of March 21, 2025, Sui supports a real-world throughput of approximately 1,106 transactions per second (TPS) and has a market capitalization of approximately 7.16 billion USD.

[18] NLnet Labs. Routinator: Rpki relying party software. https://www.nlnetlabs.nl/projects/rpki/routinator/, 2024. Accessed March 2025.

[19] Muhammad Saad and David Mohaisen. Three birds with one stone: Efficient partitioning attacks on interdependent cryptocurrency networks. In *IEEE Symposium on Security and Privacy (SP)*, 2023.

[20] SCION Association. Revolutionizing internet technology. https://www.scion.org/, 2025. Accessed: March 31, 2025.

[21] Aftab Siddiqui. Klayswap – another bgp hijack targeting crypto wallets, 2022. Accessed: March 20, 2025.

[22] SIX. Secure swiss finance network (ssfn), 2023. Accessed: March 20, 2025.

[23] Felix Stöger, Henry Birge-Lee, Giacomo Giuliari, Jordi Subirà-Nieto, and Adrian Perrig. BGP vortex: Update message floods can create internet instabilities. In *Proceedings of the USENIX Security Symposium*, August 2025.

[24] Muoi Tran, Inho Choi, Gi Jun Moon, Anh V. Vu, and Min Suk Kang. A stealthier partitioning attack against bitcoin peer-to-peer network. In *IEEE Symposium on Security and Privacy (SP)*, 2020.

[25] François Wirz, Marten Gartner, Jelte van Bommel, Elham Ehsani Moghadam, Grace H. Cimaszewski, Anxiao He, Yizhe Zhang, Henry Birge-Lee, Flix Kottmann, Cyrill Krähenbühl, Jonghoon Kwon, Kyveli Mavromati, Liang Wang, Daniel Bertolo, Marco Canini, Buseung Cho, Ronaldo A. Ferreira, Simon. P. Green, David Hausheer, Junbeom Hur, Xiaohua Jia, Heejo Lee, Prateek Mittal, Omo Oaiya, Chanjin Park, Adrian Perrig, Jerry Sobieski, Yixin Sun, Cong Wang, and Klaas Wierenga. Scaling SCIERA: A Journey Through the Deployment of a Next-Generation Network. In *Proceedings of ACM SIGCOMM*, September 2025.

Recent SNB Working Papers

2025-15 Grace Cimaszewski, Francesco Da Dalt, Thomas Moser, Adrian Perrig:
SCION and cross-border payments: Enhancing security and compliance in distributed ledger networks

2025-14 Julius Mattern, Christoph Meyer:
Beyond interbank: Identifying critical participants in integrated RTGS systems using payment type and temporal dynamics

2025-13 Jonas Heim, Thomas Nitschka:
On the carbon premium in Swiss stock returns

2025-12 Marius Faber, Gabriel Züllig:
Kinky Europe: Evidence from the regional Phillips curve in the euro area

2025-11 Daniele Ballinari, Jessica Maly:
FX sentiment analysis with large language models

2025-10 Hubert János Kiss, Alfonso Rosa García, Lukas Voellmy:
Redemption fees and gates in the lab

2025-09 Laura Felber:
Exchange rates and cross-border consumer spending: Evidence from retail payments data

2025-08 Miriam Koomen, Laurence Wicht:
Granularity in the current account

2025-07 Elliot Beck, Michael Wolf:
Forecasting inflation with the hedged random forest

2025-06 Jessica Leutert, Rolf Scheufele, Selina Schön:
Wage-price pass-through in Switzerland

2025-05 Dirk Bezemer, Richard Senner:
Asset pricing and the Covid-19 deposit glut: an application of Liquidity Preference Theory

2025-04 Lukas Altermatt, Hugo van Buggenum, Lukas Voellmy:
Money creation in a neoclassical economy: equilibrium multiplicity and the liquidity trap

2025-03 Filippo Cavaleri, Angelo Ranaldo, Enzo Rossi:
The demand for safe assets

2025-02 Marius Faber, Kemal Kilic, Gleb Kozliakov, Dalia Marin:
Global value chains in a world of uncertainty and automation

2025-01 David Borner:
Central bank information and pure monetary policy surprises in Switzerland

2024-13 Aurel Ruben Mäder, Matthias Jüttner, Daniel Gatica-Perez:
You are how you pay: understanding and identifying the payment behavior of sociodemographic groups

2024-12 Francesco Audrino, Jessica Gentner, Simon Stalder:
Quantifying uncertainty: a new era of measurement through large language models

2024-11 Marc-Antoine Ramelet, Anna Zeitz:
Oil price shocks and household heterogeneity: the income side

2024-10 Jayson Danton, Terhi Jokipii:
A decade of low interest rates: impact on Swiss bank profitability

2024-09 Anders Brownworth, Jon Durfee, Michael Junho Lee, Antoine Martin:
Regulating decentralized systems: evidence from sanctions on Tornado Cash

2024-08 Valentin Grob, Gabriel Züllig:
Corporate leverage and the effects of monetary policy on investment: a reconciliation of micro and macro elasticities

2024-07 Thomas Nitschka:
Evidence on the international financial spillovers of the New York Bankers' Panic of 1907

SCHWEIZERISCHE NATIONALBANK
BANQUE NATIONALE SUISSE
BANCA NAZIONALE SVIZZERA
BANCA NAZIUNALA SVIZRA
SWISS NATIONAL BANK