GFTN
Innovating Finance. For Everyone.

PROGRAMMABLE COMPLIANCE: OPPORTUNITIES, RISKS AND REAL-WORLD USE CASES

September 2026

ABOUT

The Global Finance & Technology Network (GFTN) is a Singapore-headquartered organisation that leverages technology and innovation to create more efficient, resilient, and inclusive financial systems through global collaboration. GFTN hosts a worldwide network of forums (including its flagship event, the Singapore FinTech Festival); advises governments and companies on policies and the development of digital ecosystems and innovation within the financial sector; offers digital infrastructure solutions; and plans to invest in financial technology startups through its upcoming venture fund, with a focus on inclusion and sustainability.

For more information, visit www.gftn.co

The Point Zero Forum is an annual gathering of 2,000 leading central bankers, regulators, policymakers, industry leaders, technologists, and investors from around the world. Over three days of dialogue and collaboration, we work to align policy, finance, and technological roadmaps to advance sustainability, inclusivity, innovation, and efficiency in the global financial ecosystems.

For more information, visit https://www.pointzeroforum.com/

FINMA is Switzerland's independent financial-markets regulator. Its mandate is to supervise banks, insurance companies, financial institutions, collective investment schemes, and their asset managers and fund management companies. It also regulates insurance intermediaries. It is charged with protecting creditors, investors and policyholders. FINMA is responsible for ensuring that Switzerland's financial markets function effectively.

For more information, visit https://www.finma.ch

University of St.Gallen IS the leading public university for executive education, with research and teaching excellence acknowledged across Europe. it develops responsible leaders who tackle the global challenges of a dynamic world and have a positive influence on people, organisations and society.

For more information, visit https://es.unisg.ch/en

© 2026 GFTN Limited, All Rights Reserved. Reproduction Prohibited.

CONTENTS

Executive Summary 04

1. Introduction 05

2. From retrospective checks to pre-validated proof 05

3. Real-world traction: from reporting to agentic commerce 06

4. Composability cuts both ways 06

5. Regulators still need to be in the room 07

6. The Legal Framework 07

7. Conclusion 08

References 09

Authors & Contributors 10

© 2026 GFTN Limited, All Rights Reserved. Reproduction Prohibited.

EXECUTIVE SUMMARY

This report summarises the results of the roundtable on programmable compliance held at the Point Zero Forum 2026 in Zurich. Speakers included representatives from the public and private sector, as well as from academia. The roundtable was chaired by Dr. Stefan Härtner, Senior Legal & Policy Specialist at the Swiss Financial Market Supervisory Authority FINMA. It was moderated by Prof. Nina Reiser, Associate Professor of Financial Market Law at the University of St. Gallen (HSG) and affiliated with the Centre for Financial Services Innovation (FSI-HSG). The discussion addressed how compliance can be encoded into digital financial infrastructure, the use cases and risks this creates, and how regulators should respond.

The first half of the roundtable addressed how compliance rules can be expressed as machine-readable policy, kept separate from the assets they govern so that they remain updatable, and paired with verifiable digital identity. Central-bank-lead projects already demonstrate that checks such as know-your-customer (KYC) and sanctions screening can be turned into portable cryptographic proofs able to travel with a transaction without exposing the underlying data. The second half turned to concrete fields of application of programmable compliance, from regulatory reporting to tokenised funds and agentic commerce. It also addressed the risks that come with automation at scale: governance failures, the consequences of composability, and the limits of what can meaningfully be encoded at all.

A principle-based legal framework and internationally aligned standards, were identified as important enabling factors for programmable compliance.

© 2026 GFTN Limited, All Rights Reserved. Reproduction Prohibited.

1. INTRODUCTION

On 25 June 2026, representatives from the public and private sector, as well as from academia shared their perspectives on programmable compliance at the Point Zero Forum 2026 in Zurich.

The session opened by a simple observation: cross-border payments are growing in volume and speed, tokenised assets are moving from pilots into production, and agentic systems are beginning to initiate financial transactions with limited human involvement. Compliance has not kept pace with this shift.

"Programmable compliance" describes the attempt to close this gap by encoding rules directly into the products, protocols and smart contracts that move money and assets. Instead of reviewing a transaction once it has already settled, an institution can validate it before execution, using a machine-readable version of the pertinent regulatory framework. Such solutions could have the potential to reduce friction and cost, speed up settlement, and create a shared, auditable language between institutions, payment networks and supervisors.

The discussion was held under Chatham House rules, and therefore its substance is reported without attributing statements to individual participants.

2. FROM RETROSPECTIVE CHECKS TO PRE-VALIDATED PROOF

Compliance today runs in silos and compliance checks, such as suspicious activity investigations, are performed separately, after a transaction has already been initiated, and rarely by more than one party at a time. This may cause delay, cost and uncertainty. None of these checks are linked to the moment money is settled, so parties cannot know in advance whether a transaction will clear.

The alternative explored at the roundtable is to check, prove and settle in a single, conditional step. The design principle is to separate the rule from its execution. A policy layer holds jurisdiction-specific requirements and can be updated without redeploying the underlying infrastructure. Off-chain checks, such as KYC checks or sanctions screenings, produce a cryptographic proof using a zero-knowledge proof protocol or a trusted execution environment. That proof, not the underlying data, is anchored on-chain as a condition for settlement. Thus, proof does not mean disclosure: the proof travels, the data does not.

A proof is only as useful as the identity behind it. Public blockchains today are fragmented into many separate ecosystems, each with its own way of identifying participants, because compliance and identity checks are rebuilt from scratch within every platform. This fragmentation, participants argued, is what prevents interoperable finance from being realised at scale. Liquidity stays locked inside individual platforms because no institution can be certain who it is transacting with beyond its own walls. There are solutions to uniquely distinguish entities globally and they are an important puzzle piece to make programmable compliance workable.

© 2026 GFTN Limited, All Rights Reserved. Reproduction Prohibited.

3. REAL-WORLD TRACTION: FROM REPORTING TO AGENTIC COMMERCE

Programmable compliance is no longer confined to pilots. While potential use cases are still being explored, three specific fields of application may be mentioned by way of example.

The first field is regulatory reporting. To the extent that compliance can be codified at the point a product is created, a transaction either complies or does not exist in the system at all. This removes the reconciliation work, the quarterly surprises and the supervisory follow-up that retrospective reporting still generates.

The second field is tokenised assets that carry their own rulebook. Encoding who may hold an asset, who may receive it and under what conditions it may move allows an issuer to embed compliance into the instrument itself.

The third field is agentic commerce. When an autonomous agent transacts on a principal's behalf, it needs machine-readable rules to act within and a clear delegation of authority to stay inside its mandate. Programmable compliance supplies the rails that let an agent execute at the point of need while remaining within its guard rails. Without them, participants warned, delegation to agents has no guard rails at all.

4. COMPOSABILITY CUTS BOTH WAYS

A blockchain transaction is closer to an instruction that triggers a chain of dependent contracts than to a single payment from A to B.

Composability and atomicity, while being key innovations of smart contract platforms, make governance failures dangerous. In October 2025, the issuer of a major stablecoin mistakenly minted 300 trillion tokens during an internal transfer. The tokens were burned within roughly 20 minutes and the issuer attributed the incident to an internal technical error (Butts, 2025). No customer funds were affected, but the episode illustrates the point participants of the roundtable drew from it. Where a retrospective compliance failure can be contained case by case, a fault encoded into a widely used contract fails everywhere at once, at the speed of the network.

Composability multiplies this exposure. A rule embedded at asset level interacts with every protocol that asset touches, so the question shifts from whether a transaction complies to whether every contract which calls it complies. The implication participants drew is not to avoid composability but to be mindful of where controls sit. Restricting a contract function to a small set of authorised callers, as token issuers routinely do, is as much a governance decision as a technical one. Who holds that authority, and under what oversight, matters more than the code itself.

© 2026 GFTN Limited, All Rights Reserved. Reproduction Prohibited.

5. REGULATORS STILL NEED TO BE IN THE ROOM

Encoding a duty does not discharge it. This was the roundtable's most repeated caution. A firm cannot point to a smart contract and say the failure was not its responsibility, any more than a bank today can blame a spreadsheet for failure to comply with AML regulation. Accountability remains with the regulated entity and, ultimately, with the people who decided how the system should behave.

Not everything can or should be coded. Legal provisions can be deliberately wide and legal interpretation is open to argument and changes over time. Participants warned against encoding the easy 80% of a rule while quietly assuming the ambiguous remainder does not matter. That gap does not disappear. It resurfaces later, and typically at the worst possible moment.

Several participants therefore argued that human and supervisory judgement becomes more important as compliance is automated, not less. Even where a system is described as fully automatic, someone must remain responsible for governance and for security updates. Where an AI agent acts, someone built and authorised it. Verifiable identity, discussed in section 3, is what makes this chain traceable in practice, linking an on-chain action back to the entity answerable for it.

6. THE LEGAL FRAMEWORK

In Switzerland, the Federal Department of Finance opened a consultation in October 2025 that would reserve the issuance of value-stable crypto-based means of payment, the new category of Swiss-regulated stablecoins, to licensed payment-instrument institutions. The draft goes further than licensing: the code of the token must enable the issuer at any time to block a transaction, to freeze the token held at a wallet address, and to withdraw it against the current holder's will, so that the issuer is technically able to execute an order from an authority, such as confiscation by a prosecuting authority, or to its own decisions, such as blocking under a blacklist (EFD, 2025, p. 44). Compliance capability must thus be written into the instrument. In the United Kingdom, the Financial Conduct Authority has made its Handbook available through an API, so that firms and their software can implement the rules directly in machine-readable form instead of parsing published documents (FCA, 2026). Participants described this as an early step towards "policy as code", while cautioning that machine-readable is not the same as machine-executable.

International standard-setters are moving in parallel, and the gaps they identify strengthen the case for compliance that travels with a transaction. The Financial Action Task Force's March 2026 report finds that peer-to-peer transfers through unhosted wallets remain a key vulnerability in the stablecoin ecosystem, one the global AML/CFT framework has yet to close (FATF, 2026, p. 3). Participants agreed that detailed, universally applicable standards will always demand compromises from individual jurisdictions, while principle-based standards are more flexible but leave more to interpretation. Both routes depend on a level of international collaboration that does not yet exist.

© 2026 GFTN Limited, All Rights Reserved. Reproduction Prohibited.

7. CONCLUSION

Programmable compliance looks promising, but it is not a universal solution. For some scalable, technology-driven business models, it may be close to a must-have. For activities that turn on legal ambiguity, discretion or case-by-case judgement, it may not work at all, at least not yet.

Principle-based regulatory frameworks already give supervisors meaningful flexibility to accept programmable compliance mechanisms. What remains is to demand each compliance mechanism to respond to the right question: who governs it, who is accountable when it fails, how it can be audited, and how it interoperates with heterogeneous technical infrastructure implemented by various jurisdictions. The building blocks need to answer those questions. Pre-validated proofs, portable verifiable identity and machine-readable rulebooks already exist and are being tested in live implementations. The task ahead is less about inventing new technology than about regulators, standard-setters and industry agreeing on how to implement it.

© 2026 GFTN Limited, All Rights Reserved. Reproduction Prohibited.

REFERENCES

1 Butts, D. (2025).

PayPal's crypto partner mints a whopping $300 trillion worth of stablecoins in 'technical error'.

https://www.cnbc.com/2025/10/16/paypals-crypto-partner-mints-300-trillion-stablecoins-in-technical-error.html

2 EFD (2025).

Änderung des Finanzinstitutsgesetzes (Zahlungsmittelinstitute und KryptoInstitute): Erläuternder Bericht zur Eröffnung des Vernehmlassungsverfahrens.

3 FATF (2026).

Targeted Report on Stablecoins and Unhosted Wallets.

4 FCA. (2026).

Making compliance simpler: opening up the FCA Handbook through our new API.

https://www.fca.org.uk/news/blogs/making-compliance-simpler-opening-fca-handbook-new-api

© 2026 GFTN Limited, All Rights Reserved. Reproduction Prohibited.

Authors

GFTN Research & Advisory

Prof. Dr. Nina Reiser
Attorney at law, LL.M., Associate Professor for
Financial Market Law at the University of St. Gallen (HSG),
Director at the Institute for Law and Economics (ILE-HSG),
affiliated with the Centre for Financial Services Innovation (FSI-HSG)
and Titular Professor at the University of Zurich.

Gian-Luca Wittwer
Research assistant at the chair of Nina Reiser,
Institute for Law and Economics, University of St. Gallen.

Production

Sachin Kharchane
Graphic Designer

© 2026 GFTN Limited, All Rights Reserved. Reproduction Prohibited.

GLOBAL FINANCE & TECHNOLOGY NETWORK (GFTN)

6 Battery Road, #28-01, Singapore 049909
gftn.co | hello@gftn.com

This document is published by Global Finance & Technology Network Limited (GFTN) as part of its FutureMatters insights platform. The findings, interpretations, and conclusions presented in GFTN Reports reflect the views of the author(s) and do not necessarily represent those of GFTN, its Board, management, stakeholders, or any individual participant and their respective organisations.

© 2026 Global Finance & Technology Network Limited, All Rights Reserved. Reproduction Prohibited.