

Ethereum's Cryptographic Future: What It Means for Tracing, Evidence and Control

Vitalik Buterin's vision of a cryptographic world computer points to an Ethereum that can establish computational correctness with increasing efficiency and certainty. But that does not necessarily make it easier to prove whose value moved, what proprietary object is in issue, or whether the movement was legally authorised.

The most important point in Vitalik Buterin's latest essay, "[The cryptographic world computer](#)", is not simply that Ethereum may become faster or more scalable. It is that the system is moving beyond the comparatively simple blockchain model inherited from Bitcoin.

Ethereum already combines proof of stake and general-purpose computation with L2s and on-chain applications using zero-knowledge proofs. In Buterin's vision of Ethereum in 2030, computation and data will be distributed more extensively across L2s and off-chain components; specialist provers will generate compact cryptographic proofs; nodes will sample whether data is available rather than each downloading all of it; and block construction itself will be divided among multiple participants.

Some of this architecture is already in use or development. Other elements, including more deeply proof-based L1 verification, automated formal verification, more advanced privacy machinery and post-quantum security, remain roadmap proposals or research topics. That distinction matters. But the direction is clear: Ethereum is becoming less a system in which every node independently re-executes and stores everything, and more a cryptographic verification and settlement layer.

For cryptoasset disputes, the central implication appears paradoxical. The network may become better at proving that a state transition was computationally correct, while the evidential narrative needed to establish provenance, ownership and authority becomes increasingly distributed, layered and, at times, less publicly visible.

What, then, does Ethereum's future architecture mean for lawyers and courts navigating digital asset disputes? I have identified five key issues.

1. Cryptographic validity proves neither provenance nor authority

A validity proof answers a protocol question: did the transition from one state to another comply with the system's programmed rules?

Tracing asks a different legal question: can the claimant's value be identified in a later asset or position despite mixing, substitution and changes in control?

A cryptographic proof may provide compelling evidence that the required computation occurred, but it does not determine who owned the value, whether the person who initiated the transaction was legally entitled to do so, or how competing proprietary claims should be resolved.

A transaction can be correctly signed and final according to the protocol rules and still result from stolen credentials, fraud, mistake or an agent acting outside authority.

The proof verifies the state transition. It is not itself the proprietary object, and it does not supply the applicable tracing rule.

2. Future Ethereum sharpens the distinction between BTC and ETH

The developing case law has not always paid sufficient attention to the fact that Bitcoin and Ethereum expose different kinds of evidence. The correct legal analysis in an individual case should begin with accurate identification of the underlying technical architecture, rather than the generic label “cryptoasset”.

Bitcoin’s UTXO model represents spendable value through discrete unspent transaction outputs. Each transaction consumes specifically referenced earlier outputs and creates new outputs, producing a graph of value movements.

That graph assists forensic tracing. It does not, without more, make BTC legally non-fungible or establish common-law following of persistent, individually identifiable coins. In my view, *Smithers v Persons Unknown* [2026] EWHC 1907 (Comm) wrongly treated the transaction graph between successive UTXOs as establishing that the “same” Bitcoin assets remained.

Ethereum is fundamentally different in its account-based model. Native ETH is reflected in account balances, while transactions and smart contract calls change Ethereum’s global state rather than consuming and creating discrete outputs. ETH is not divided into individually labelled units that persist through successive transfers. If misappropriated ETH enters an account containing other ETH, the protocol does not decide which part of a later outgoing payment represents the claimant’s value.

Buterin’s future architecture makes the distinction sharper. The relevant evidence may no longer be found solely in a L1 transaction history. It may be distributed across a L2 state, proof systems, bridge messages and off-chain execution or ordering records.

3. Tracing requires a layer-by-layer analysis of object and control

In a future Ethereum dispute, “ETH” may describe materially different positions: native ETH in an externally owned account; ETH controlled by contract code; ETH locked in an L1 bridge; a corresponding L2 balance; wrapped ETH issued by a token contract; ETH committed to staking; or a liquid-staking token issued in return.

These should not be treated as a single homogeneous object. At each stage, the legal and technical inquiry must identify:

- the proprietary object or position in issue;
- the system and layer in which it is instantiated;
- the rules under which its state can change;
- the person, code or combination of actors capable of transferring, withholding, freezing, upgrading or redeeming it; and
- whether the next position represents the same asset, a substitute, or a distinct contractual or tokenised claim.

Control may be individual, shared, custodial, contractual or programmatic. It may also be divided: one actor may hold a key, another may sequence transactions, another may administer a bridge, and another may hold upgrade or pause powers. That architecture matters to ownership, tracing, situs, jurisdiction and the identification of a respondent capable of complying with a court order.

4. Greater verification may coexist with reduced evidential visibility

A state commitment or proof may establish that a valid result was produced without placing every input, intermediate step or relevant actor before the court in a readily intelligible form.

Proof-based verification should not, however, be confused with privacy: not every cryptographic proof conceals the underlying transaction data. But in privacy-enabled or substantially off-chain systems, verification and disclosure may become increasingly separate.

Historical retrievability is also distinct from whether data was available when a state transition was accepted. Ethereum's roadmap materials explain that some transaction data used by rollups is held by network nodes only temporarily. The blockchain may retain a cryptographic commitment to that data without retaining the complete underlying information indefinitely. Later access may therefore depend on whether a rollup operator, user or archive service preserved it.

A later litigant may consequently have cryptographic evidence of an accepted result without ready access to all the evidence needed to reconstruct the surrounding events.

That changes the opening strategy in a dispute. Underlying L2 transaction data, proof inputs, state-change records, execution traces, sequencer and bridge records, and information held by wallets, custodians or other service providers may need to be identified and preserved immediately.

Urgent preservation and disclosure orders, including without-notice relief where justified, may therefore be required alongside proprietary or freezing relief. Evidence preservation cannot safely be left until ordinary disclosure.

5. Attribution and remedies become more fragmented

Buterin also envisages multi-party block construction. This displaces any simple assumption that a single block producer is responsible for every relevant aspect of a block.

Across the wider L1/L2 architecture, a sequencer may order transactions; a builder may assemble a block; a prover may generate a proof of computation; and the validator set may attest to blocks and finalise the chain. A bridge operator, custodian or governance body may hold the practical power relevant to recovery.

Technical participation does not, by itself, establish legal causation, responsibility or control. Equally, the actor holding the decisive evidence may not be the actor capable of freezing or returning the asset.

An actor-by-actor and function-by-function analysis will therefore be required when identifying viable claims and remedies. Disclosure, preservation and freezing orders must target the correct participant for the relevant purpose rather than treating "Ethereum" as though it were a single intermediary.

Conclusion

The cryptographic world computer may prove with extraordinary certainty what its code did. Cryptographic verification may provide powerful evidence, but it cannot itself supply the legal tracing rule.

Greater machine-level certainty may coexist with greater legal and evidential complexity. It cannot determine who owned the value, whether control was lawfully exercised, or whether the claimant's value remains traceable through mixing, substitution and movement between layers.

The programmability of code will therefore be tested against the law's capacity to apply established principles of proprietary characterisation, continuity and substitution, lawful authority and remedial control to an increasingly complex coded architecture.

The question for the next phase of English digital assets law is therefore not simply whether cryptoassets are property, nor even whether they can be followed or traced. It is more fundamental: what exactly has the computational system instantiated as the object of property, and what becomes of that object when the system changes state?

Only once that question has been answered should the law decide whether it is following the same thing or tracing its value into something new.

About the author:

Flavia Kenyon is a barrister at 33 Chambers with a specialist practice in digital assets disputes, blockchain technology, asset recovery, fraud, and the legal implications of emerging technologies.

This article is commentary only and does not constitute legal advice.

30 September 2026