

Money? Or Not?

The use of bitcoin and other forms of cryptocurrency brings up questions in several financial sectors, including insurance.

What is money? Up until recently, insurance and cyber activity created conventional questions, generally revolving around the acronym of ACAI.

- **Act:** Was there hacking or some other covered act?
- **Causation:** Did the act “directly cause” the damages?
- **Authorization:** Was the actor authorized?
- **Intent:** Did the policyholder act intentionally?

These questions were new, but they fit within analytical categories that are old (act, cause, damages, etc.).

Two recent cases in the cyber arena raise an entirely new question: the meaning of money. These cases were decided just this past fall, *Kimmelman v. Wayne Insurance Group* and *Posco Daewoo America Corp. v. Allnex USA*. Both cases are from trial courts. In fact, *Posco* is explicitly not for publication (it can't be used as a precedent). But, these are the first cases on the issue, and for that reason they should be noted.

In *Kimmelman*, the policyholder sought coverage for approximately \$16,000 of stolen bitcoin.

Under the policy, the insurer's obligation depended on the status of bitcoin. If bitcoin was viewed as money, the insurer would apply a sublimit, and the policyholder's recovery would be only \$200. If bitcoin was viewed as property, the insurer would be required to pay more.

To argue that bitcoin is money, the insurer cited various media articles referring to it as such. The insurer also noted the widely used term “virtual currency.”

On the other hand, the policyholder noted that the IRS has stated that “for federal tax purposes,



By
Alan Rutkin

Policyholders, insurers and courts will need to wrestle with the meaning and consequences of both cryptocurrency and other related issues.

virtual currency is to be treated as property.”

Based on the IRS, the court allowed the policyholder's action to proceed as a claim for property.

In *Posco*, a thief hacked into the policyholder's computer system. The thief emailed one of the policyholder's customers. The customer, after receiving the thief's notice, sent its payment to the thief, rather than the policyholder.

The policyholder sued its customer. The customer argued that its payment to the thief satisfied its obligation to the policyholder. That is, the customer argued that the policyholder should bear the cost of the theft. The policyholder argued that its insurer should bear the loss.

The policyholder had coverage for “computer crime.” That is, the insurer agreed to “pay the Insured for the Insured's direct loss of, or direct loss from damage to, Money, Securities, and Other Property directly caused by Computer Fraud.”

But was the customer's payment to the thief a loss of the policyholder's money?

The court viewed the issue as: Who “owned” the mispaid money?

Ultimately, the court concluded that the policyholder had not sufficiently pleaded that it owned the money. Therefore the court dismissed the case against the insurer.

These cases really identify more questions than answers.

The cases are too few to suggest a trend. They're too new to appreciate appellate consequences. And they're too split to declare anyone a winner (insurers and policyholder can each arguably point to one victory).

These cases do, however, point to a new concern. Policyholders, insurers and courts will need to wrestle with the meaning and consequences of both cryptocurrency and other related issues.

BR

Best's Review columnist **Alan Rutkin** is a partner at Rivkin Radler in Uniondale, N.Y. He can be reached at alan.rutkin@rivkin.com.