

AUTOMATED VERIFICATION OF FAIRNESS IN SMART CONTRACTS**ABSTRACT**

5 A computer-implemented method of automatically verifying at least one fairness
property of a smart contract comprises: (i) performing symbolic execution on source
code of the smart contract to extract a mechanism model, wherein the mechanism
model comprises a representation of processing of inputs from a finite number of users
by the smart contract to produce an outcome; (ii) encoding the mechanism model and
10 the at least one fairness property as a satisfiability modulo theories (SMT) formula; and
(iii) automatically determining, from the SMT formula, whether the at least one fairness
property is satisfied for the finite number of users.

[Figure 1]

15