

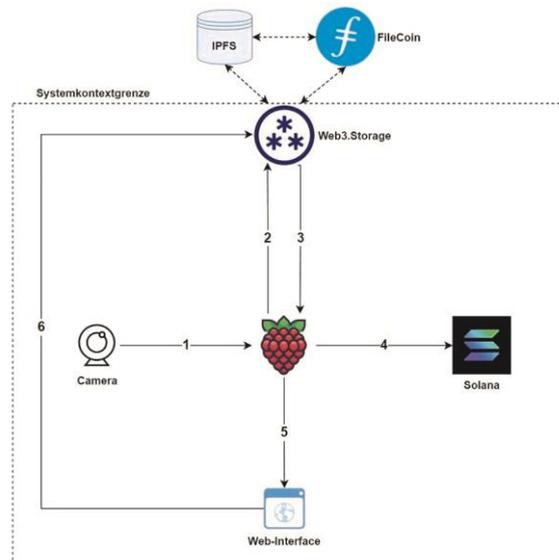
Fake-Proof Security Camera (Blockchain)

Zwei der Technologien, die in den letzten Jahren im Rampenlicht standen, sind Blockchains und Deep Fakes. Die Authentizität von digitalen Daten beweisen zu können, insbesondere von Bild- und Videomaterial, stellt sich nicht nur bei rechtlichen Disputen als Problem dar, sondern auch beim Diskurs in den Sozialen Medien und in vielen weiteren Bereichen. Unsere Arbeit untersucht, inwiefern Blockchain-Technologien verwendet werden können, um dieses Problem zu lösen. Dazu wird eine umfassende Umfeldanalyse der potenziell relevanten Technologien durchgeführt. Diese werden sowohl untereinander als auch im Bezug auf die Problemstellung verglichen. Auf Basis der gewonnenen Informationen entwerfen wir Lösungskonzepte für ein exemplarisches Anwendungsszenario: eine Überwachungskamera. Wir konzipieren ein auf einem Raspberry Pi basierendes System, welches die Daten der Überwachungskamera entgegennimmt und sowohl persistiert als auch den Nachweis derer Authentizität ermöglicht. Wir zeigen mehrere Variationen auf, um verschiedenen Anforderungen und Bedingungen gerecht zu werden. Anschliessend setzen wir eine der Variationen in einem lauffähigen System um. Das entwickelte System besteht die auf Basis der Anforderungen konzipierten Tests. Nicht abgedeckte Schwachpunkte werden erläutert und es werden Lösungen vorgeschlagen, um eine Weiterentwicklung des Konzepts zu unterstützen.



Diplomierende
Christian Filliger
Nikolay Kunev

Dozierende
Hans Wernher van de Venn
Zaniyar Jahany



Eine auf Web3.Storage und Solana basierende Variation des Lösungskonzepts, welche in einem konkreten, lauffähigen System umgesetzt wurde