"Insurance claim processing involves multi-domain entities and multi-source data, along with a number of human agent interactions. Consequently, the processing is traditionally manually intensive and time-consuming. Blockchain technology-based solutions and intelligent automation can significantly improve the scale and response time of claim processing. However, there is a need to ensure security in such platforms in order to avoid fraud (e.g., duplicate claims) and compromise of data integrity through attacks such as Sybil. In this paper, we propose a novel “ClaimChain” consortium blockchain platform that increases shared intelligence amongst participating insurance agencies. To address security concerns, we perform threat modeling using attack tree methodology for various threats realizable and unique to ClaimChain. For significant threats identified, we apply security design principles to reduce the probability of their occurrence. Claimchain offers fraud detection using machine learning models for detecting prominent red flags in insurance claims by assigning risk scores based on risk severity. Additionally, we show the scalability of Claimchain with regard to both transaction volume and response time of claim processing. We evaluate our ClaimChain using both simulation studies as well as an experimental testbed setup in a public cloud environment. Our results show that ClaimChain is effective in protecting the intelligent automation of insurance claim processing as seen in reduction of 25% probability of loss of integrity before and after applying security design principles. Claimchain is also effective in detecting fraudulent activities with a detection accuracy of up to 98% for identified red flags."