Investigating Vulnerabilities in Smart Homes: Access Control Through Ethereum Smart Contracts

Mateo Minato

UNIVERSITY OF OREGON

ABSTRACT

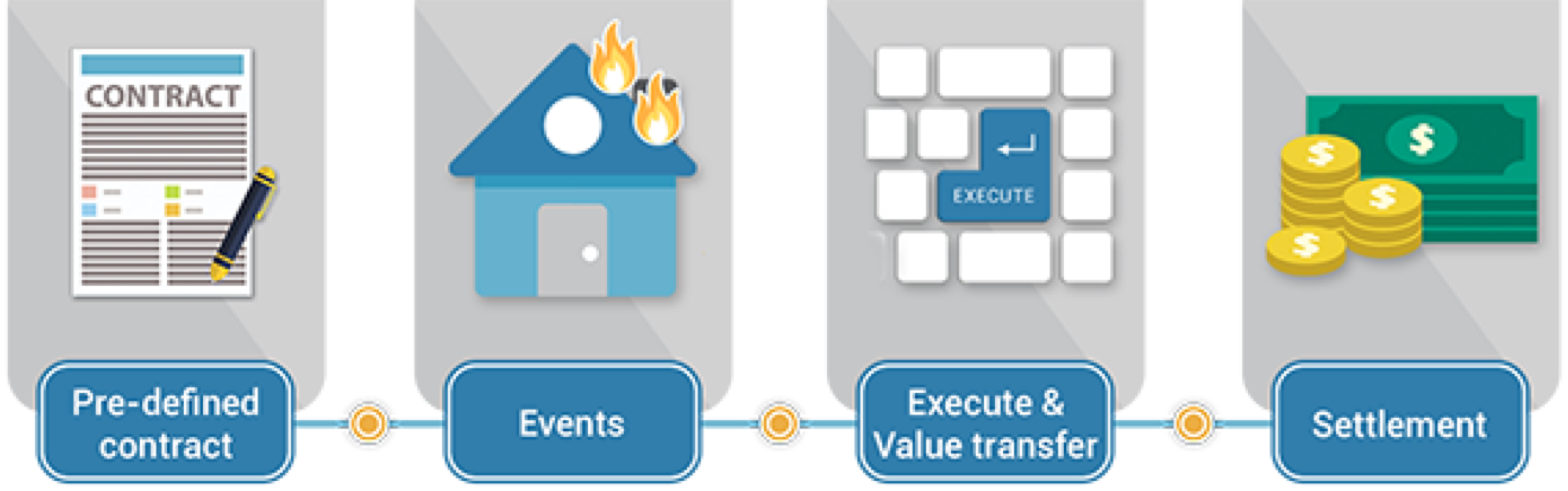
- As homes get more and more connected, researchers have found numerous vulnerabilities within these in-home networks that could compromise a users electronic privacy, or even physical space.
- Some researchers have proposed using blockchain as a form of more reliable access control, both in general and specifically for use with the Internet of Things.
- In light of this, my goals were as follows:
  1. Investigate known and unknown vulnerabilities in network enabled IoT devices and appliances.
  2. Investigate the efficacy of using a blockchain access control system to patch these vulnerabilities.

ETHEREUM SMART CONTRACTS

- Ethereum is the second largest blockchain platform.
- Smart contracts use an OOP language called Solidity.
- Smart contracts are self-executing code blocks that trigger based on events.
  - They operate as electronic “vending machines”.
- Smart contracts provide unique benefits over other blockchain platforms.
  1. They allow peer-to-ledge transactions to occur natively.
  2. There is a robust community and strong documentation.
- In the context of access control, they dramatically reduce complexity by allowing the definition of interactions between objects
  - For example, access requests between a user and a smart enabled device.

VULNERABILITIES

- **Lateral Privilege Escalation Attacks**:
  - Smart home devices require varying levels of security.
  - It can be trivial for hackers to gain access to ”low-level” devices.
  - Some hackers were able to use this access to modify data on or otherwise impact high-level devices.
- **Lack of System Defenses**:
  - Some smart homes do not employ transitive access control enforcement.
  - In these cases, hackers were able to trick smart homes into granting them higher access levels than desirable.
- **Lack of Bare Minimum Protections**:
  - In some cases, smart home devices were fixed with essentially no access control or protection at all.



Pre-defined contract

- Terms of the policy are agreed by all counterparties
- These are hard coded into the smart contract and cannot be changed without all parties knowing

Events

- Event triggers insurance policy execution

Execute & Value transfer

- The smart contract policy is automatically executed based on the pre-agreed terms

Settlement

- Payout / other settlement completed instantly and efficiently

ARCHITECTURE

- A central authority (i.e. hub) will manage authorization.
  - Upon initialization, the initializer will be remembered as the owner, or admin.
  - Additional users that are added will be given authorization through the central authority.
- Devices will sit on the other side of the central authority.
  - Requests authorized by the central authority will be passed to the device.
- A contract will exist for each user <--> authority relationship.
- A contract will exist for each authority <--> device relationship.
- This architecture allows for future expansion into limited access, such as partial or limited users.

CONCLUSION

- Blockchain based access control could be a viable alternative to conventional methods in smart homes.
  - Authentication comes free with use of Smart Contracts—only legitimate accounts are able to initiate transactions.
  - Authorization can be managed through the use of tokens, attribute authorities, or even limited to “owner only” systems.
- This solution directly addresses known vulnerabilities.
  - Unilaterally requiring blockchain based access control on all devices would eliminate the lateral privilege attack.
  - Provides transitive access control enforcement, providing substantive system defenses.
- However, more research is required
  - It’s difficult to test in a “production” setting, as few smart appliances are open source.