REPLY NET

BLOCKCHAIN-BASED SECURITY
FOR SOFTWARE-DEFINED NETWORKS (SDN).

SECURECHAIN

Securechain is an innovation which delivers security, scalability and auditability to Software Defined Networks (SDN). Securechain leverages Blockchain technology, the same technology which powers the popular and highly disruptive cryptocurrency Bitcoin, but applied in a completely new and innovative way.

Using Reply's expertise in Blockchain and SDN, together with bespoke software development, Net Reply has created a brand new and powerful system to provide security, scalability and auditability to these future networks.

NET REPLY HAS DEVELOPED A WORKING PROOF-OF-CONCEPT TO SHOW THE POTENTIAL OF THIS SYSTEM, BASED ON THE ETHEREUM BLOCKCHAIN (THE SAME BLOCKCHAIN AS CHOSEN BY THE R3 FINANCIAL CONSORTIUM, MICROSOFT AND IBM/SAMSUNG), WHICH CAN NOT ONLY ALLOW VALID NETWORK ENTITIES SUCH AS SWITCHES TO ENTER THE NETWORK, BUT TO DETECT AND REJECT HACKING ATTEMPTS.

DRIVERS TOWARDS SDN

New trends in the global creation, transmission and use of information is creating stress and inefficiency on current traditional networks meaning that networks need to becoming far more dynamic.
Software Defined Networking deals with this with On-Demand provisioning of network elements much more effectively than traditional, fixed networks, and therefore migration to these SDN networks is occurring for these reasons, together with compelling commercial/RoI considerations too.

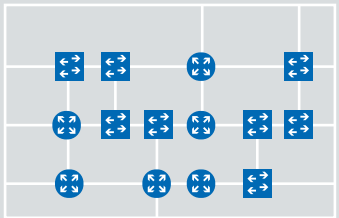
DRIVERS	• USERS EXPECTING ON-DEMAND SERVICES • HQ VIDEO/REALTIME SERVICES ON INCREASING NUMBER OF MOBILE DEVICES • COMMERCIALS/ROI CONSIDERATIONS
MEANING	• ON-DEMAND PROVISIONING OF MULTIPLE NETWORK ELEMENTS • UNPREDICTABLE AND LARGE TRAFFIC FLOWS REQUIRING FLEXIBLE NETWORK • NETWORK FUNCTION VIRTUALISATION WITH SDN MEANS MOVE TO GENERIC NON-PROPRIETARY SERVERS

Currently with SDN being in relatively early-stage development, and with all the focus on features, not security, there are no clear standards for defining security within it, and security measures tend to be done on an ad-hoc basis, varying from vendor to vendor and implementation to implementation.
Securechain seeks to fill this security void, agnostic of underlying SDN technology or vendor.

THREE KEY SDN CHALLENGES:

SECURITY, SCALABILITY AND AUDITABILITY
We recognise that the shift towards SDN networks opens up new attack vectors for hackers, as now the network itself can be addressed by APIs - not just the connected servers as per 'traditional' networking. The volume of entities which may connect to a SDN creates a further scalability challenge – one rogue element in a hundred valid ones needs to be detected in order to protect the network, and finally, hackers may seek to cover their tracks by changing the logs.
Securechain addresses all three of these challenges.

NEW ATTACK VECTORS ▶	SCALABILITY AND LOGGING ▶	SDN SECURITY CHALLENGES
SDN DEVELOPMENT IS FOCUSED ON FEATURES, NOT SECURITY, MEANING INCREASED RISK AND NUMBER OF ATTACK VECTORS	SHEER NUMBER OF SOFTWARE ELEMENTS WHICH CAN BE SPUN UP IN AN INSTANT RECORDS AND LOGS CAN BE FALSIFIED OR HACKED	NEW ATTACK VECTORS MEANING HACKERS CAN CORRUPT SDN MASSIVE NUMBERS OF SOFTWARE-DEFINED SWITCHES CAN NOW APPEAR IN AN INSTANT RECORDS AND LOGS CAN BE FALSIFIED TO COVER TRACKS



Securechain addresses this security challenges because the solution:

Protects the SDN

- The use of Securechain with defined Command Wallet addresses and codes within the messages means that only authorised, trusted entities can participate in the SDN;
- It ensures that rogue devices are detected and rejected, triggering an alarm for the admins.

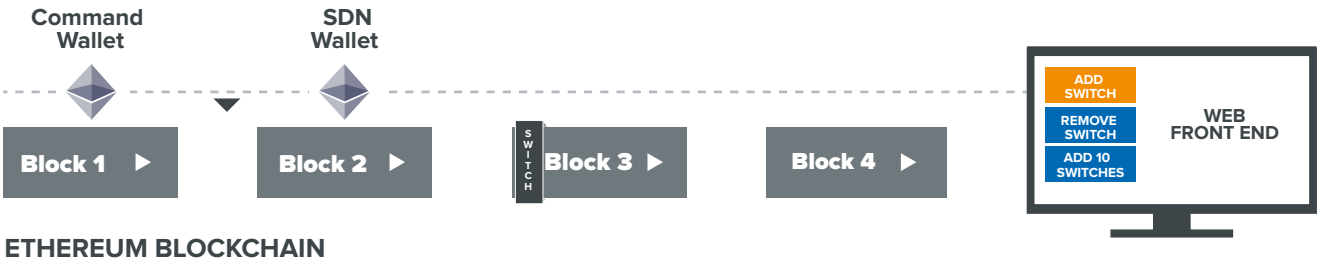
Creates forensic logs

- The use of Securechain ensures that any event – entity creation or deletion - valid instruction or hack attempt - is stored in the blockchain, free from any possibility of tamper due to the way the blockchain operates.

Two basic use-cases of Securechain are shown in the next section – adding a device to a network, and the rejection of an attempted network hack to add a 'rogue device' to the network.

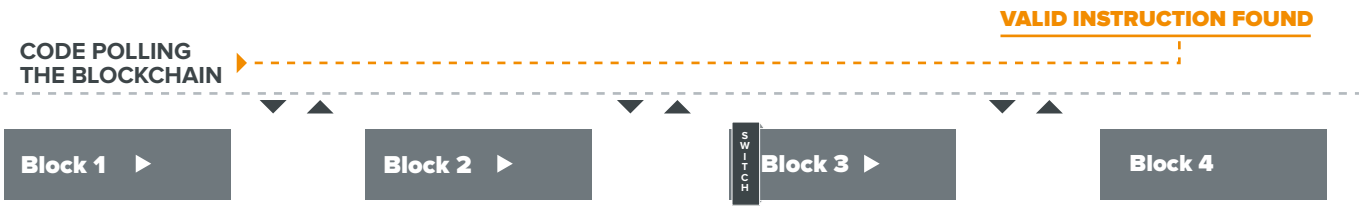
ADDING A DEVICE TO THE SDN

One basic use-case would be **adding a device to the Software Defined Network.** The first thing to happen would be the admin panel, or trusted entity, sends the transaction/request to the Blockchain from a whitelisted wallet.



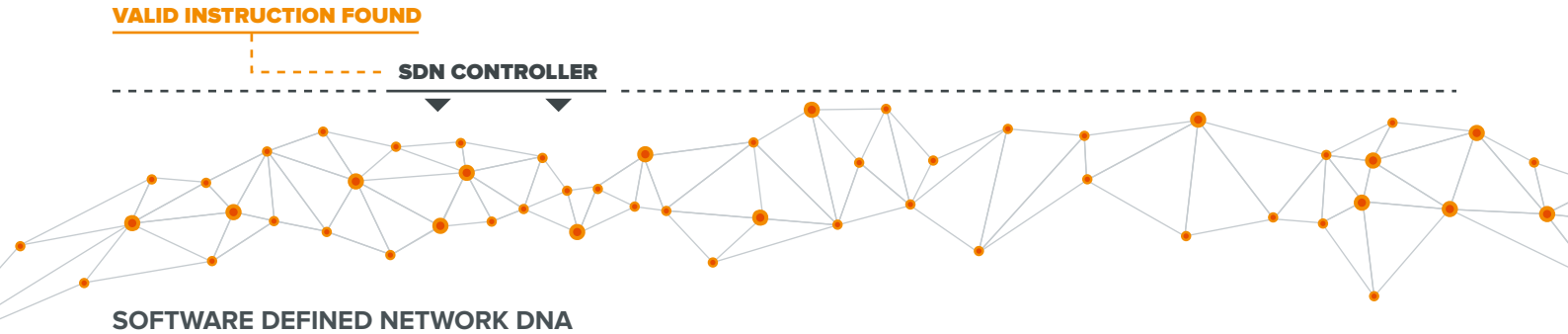
ETHEREUM BLOCKCHAIN

This request is then stored in the blockchain, which acts as a gateway into the SDN.



ETHEREUM BLOCKCHAIN

The SDN is polling the Blockchain for new requests and once it has seen a request it will deal with it. In this scenario the transaction/request has come from a whitelisted wallet, with a valid instruction, so the instruction can be implemented.

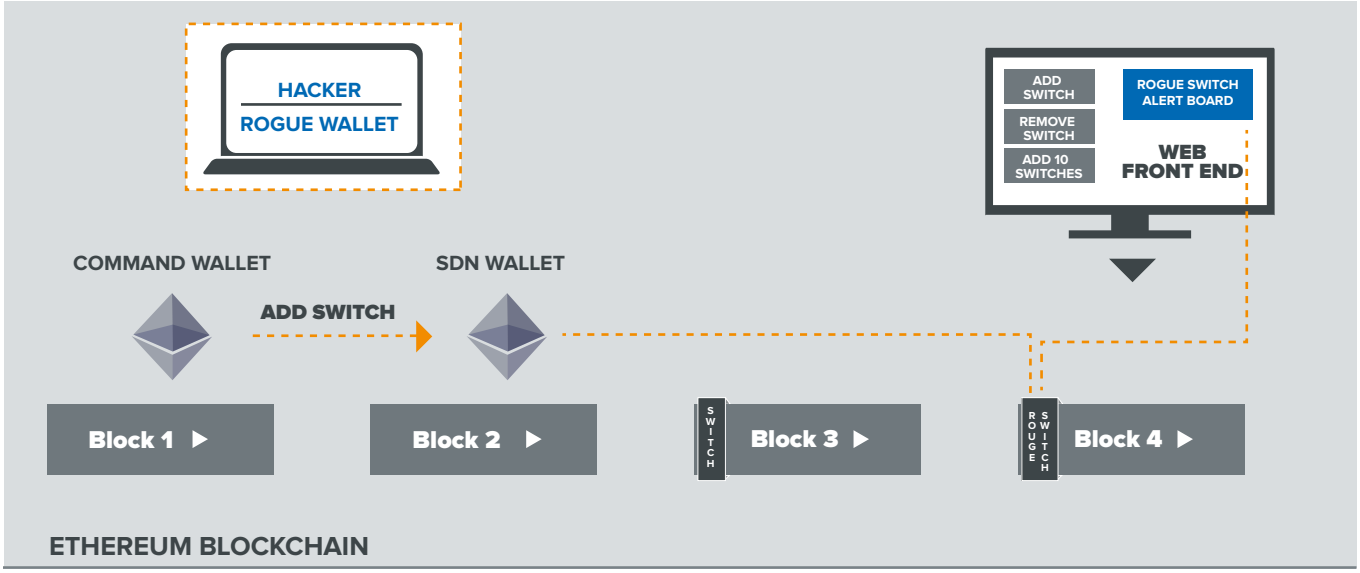


SOFTWARE DEFINED NETWORK DNA

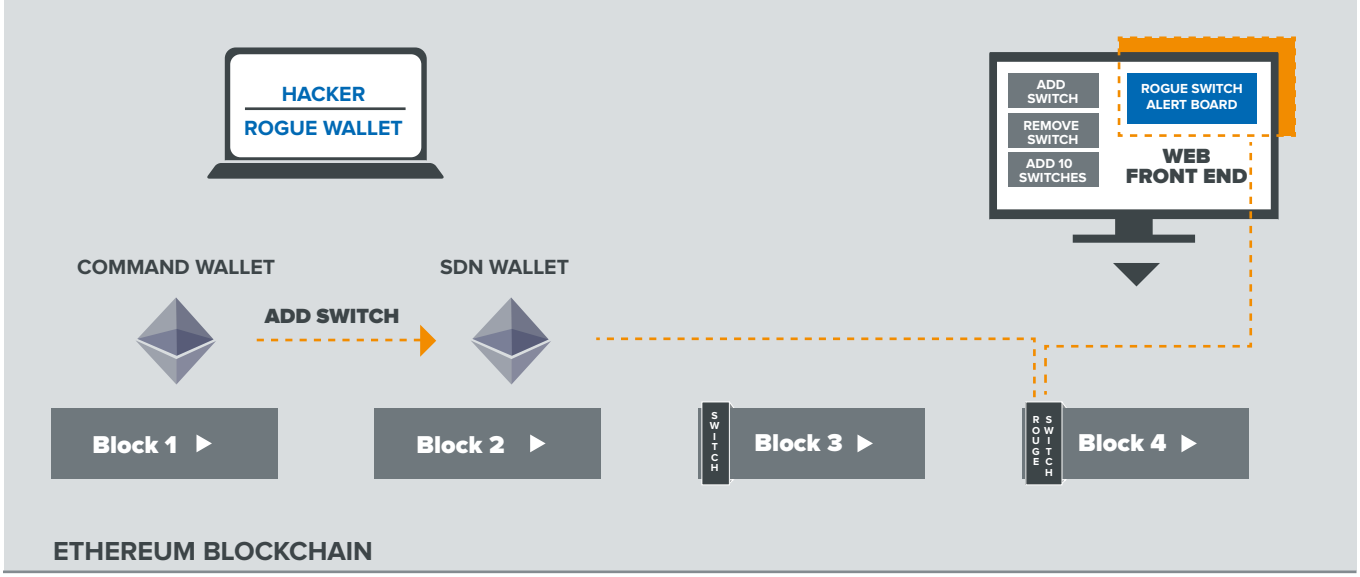
The network will inform the SDN controller to allow the device to start functioning and the element will then be able to be used as part of the SDN.

ROGUE DEVICE REJECTION

Another use case is the rejection of a rogue device. In this case a hacker with a valid instruction, but with a wallet address that is not whitelisted sending a message to the Blockchain to attempt to add a rogue device/element which could harm the SDN.



Because this instruction has originated from a hacker, the device is not added to the SDN, rather an alert is sent to the network admin to warn them of the hack, providing key details of the hack including wallet ID and timestamp.



The request is stored forever in the blockchain, which allows for a security audit at a later date free of the possibility of tamper. **In summary - Securechain delivers security, scalability and auditability to Software Defined Networks.**

REPLY
NET

Net Reply is the Reply Group company specialising in Network Transformation. In a world where Software and Networks are converging, Net Reply provides a proven combination of software development, agile delivery and network expertise to help organisations simplify, automate and integrate Network service delivery.
Using advanced Network analytics Net Reply can help resolve the operations and security challenges of migrating to cloud environments, optimising infrastructure investment and protecting critical infrastructure. Whether adopting new technologies or transforming the way you deliver Networking solutions, Net Reply can help you migrate, automate and secure your Network services.

www.reply.com