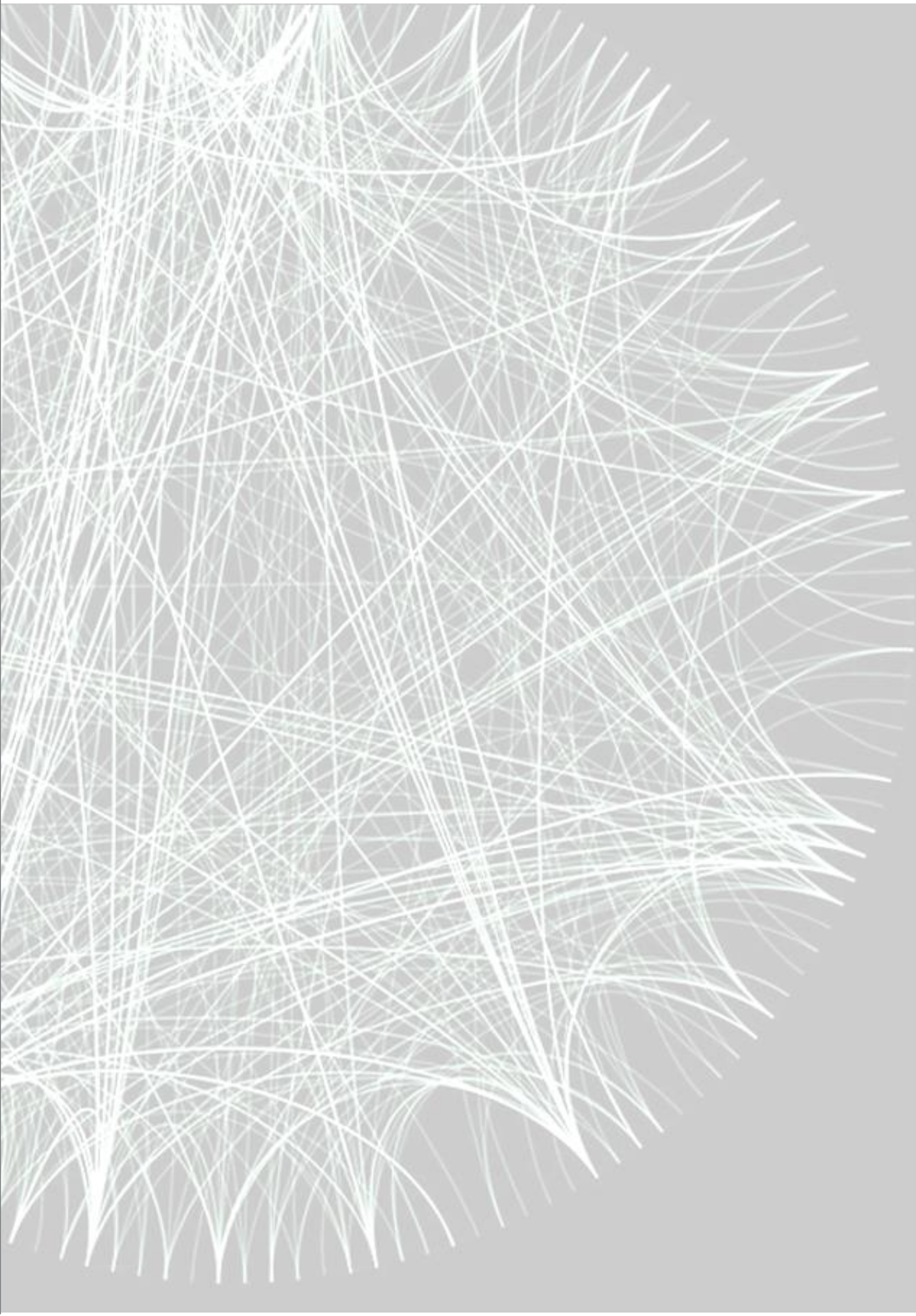


Overview of BitFinex Hack

The problem with redundant controls

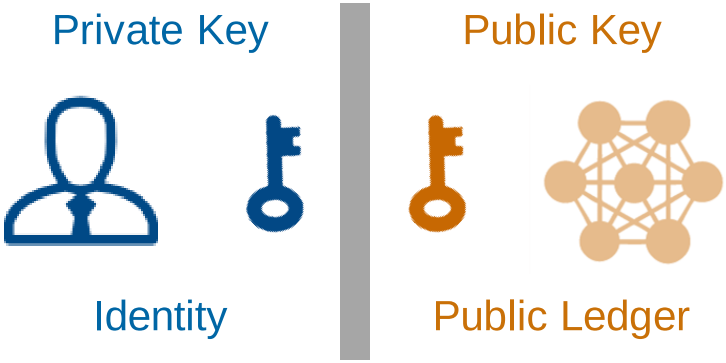
August 2016

Anonymity / Encryption

In order to maintain anonymity on the blockchain, all transactions are make between random strings of characters called “public keys”. Your identity is linked to a private key which is cryptographically linked to the public key. The counterparty can see your public key, but they will never know who owns the corresponding private key.

Encryption / Anonymity

Encryption



Private Key

Public Key

Identity

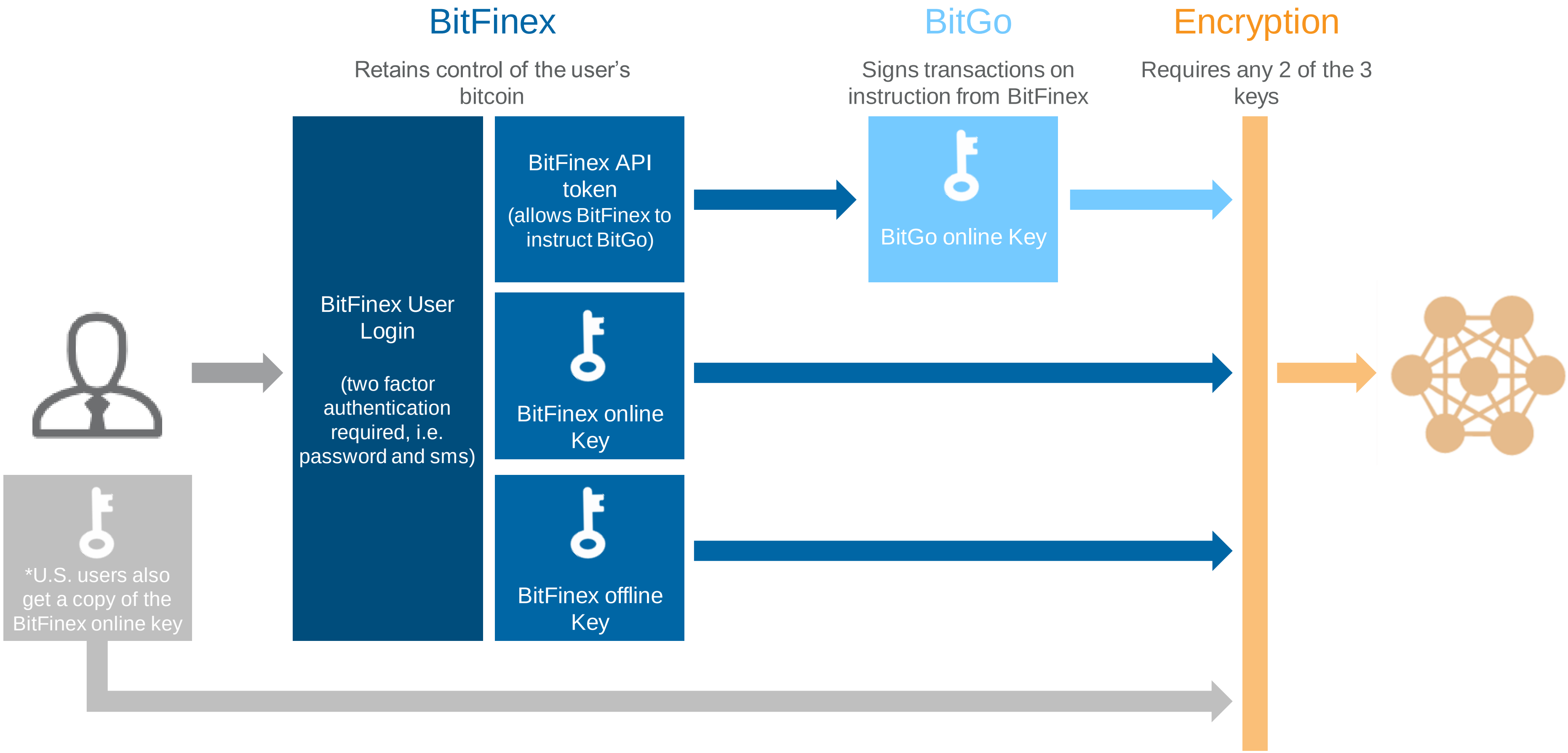
Public Ledger

You use your private key to authorise a transaction, and your public key to receive the transaction.

Risk: institutions will have to keep a very careful record of their public and private keys. If you lose a private key, you lose ownership of the assets that correspond to it.

How BitFinex Works

BitFinex is an online "exchange" that allows users to trade bitcoin and other crypto-currencies. In order to increase security, BitFinex generates three different private keys for each public key and requires at least two keys to sign every transaction. The three keys are stored in separate locations with one being held by a third party security firm.



BitFinex

Retains control of the user's bitcoin

BitGo

Signs transactions on instruction from BitFinex

Encryption

Requires any 2 of the 3 keys

BitFinex User Login

(two factor authentication required, i.e. password and sms)

BitFinex API token (allows BitFinex to instruct BitGo)

BitGo online Key

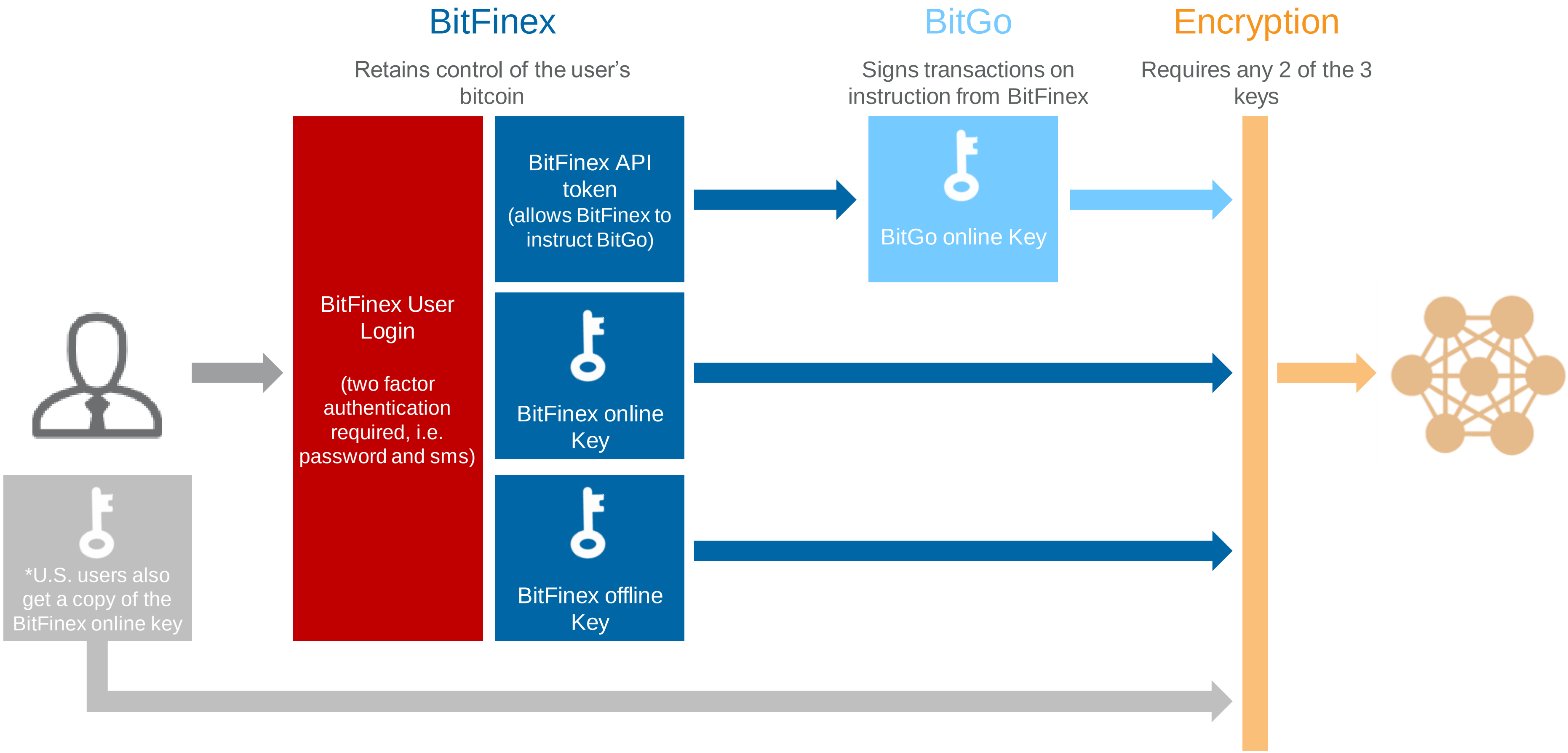
BitFinex online Key

BitFinex offline Key

*U.S. users also get a copy of the BitFinex online key

The problem with redundant controls

Under this model, an attacker can instruct payments if they: steal the user's login.



BitFinex

Retains control of the user's bitcoin

BitGo

Signs transactions on instruction from BitFinex

Encryption

Requires any 2 of the 3 keys

BitFinex User Login

(two factor authentication required, i.e. password and sms)

BitFinex API token (allows BitFinex to instruct BitGo)

BitGo online Key

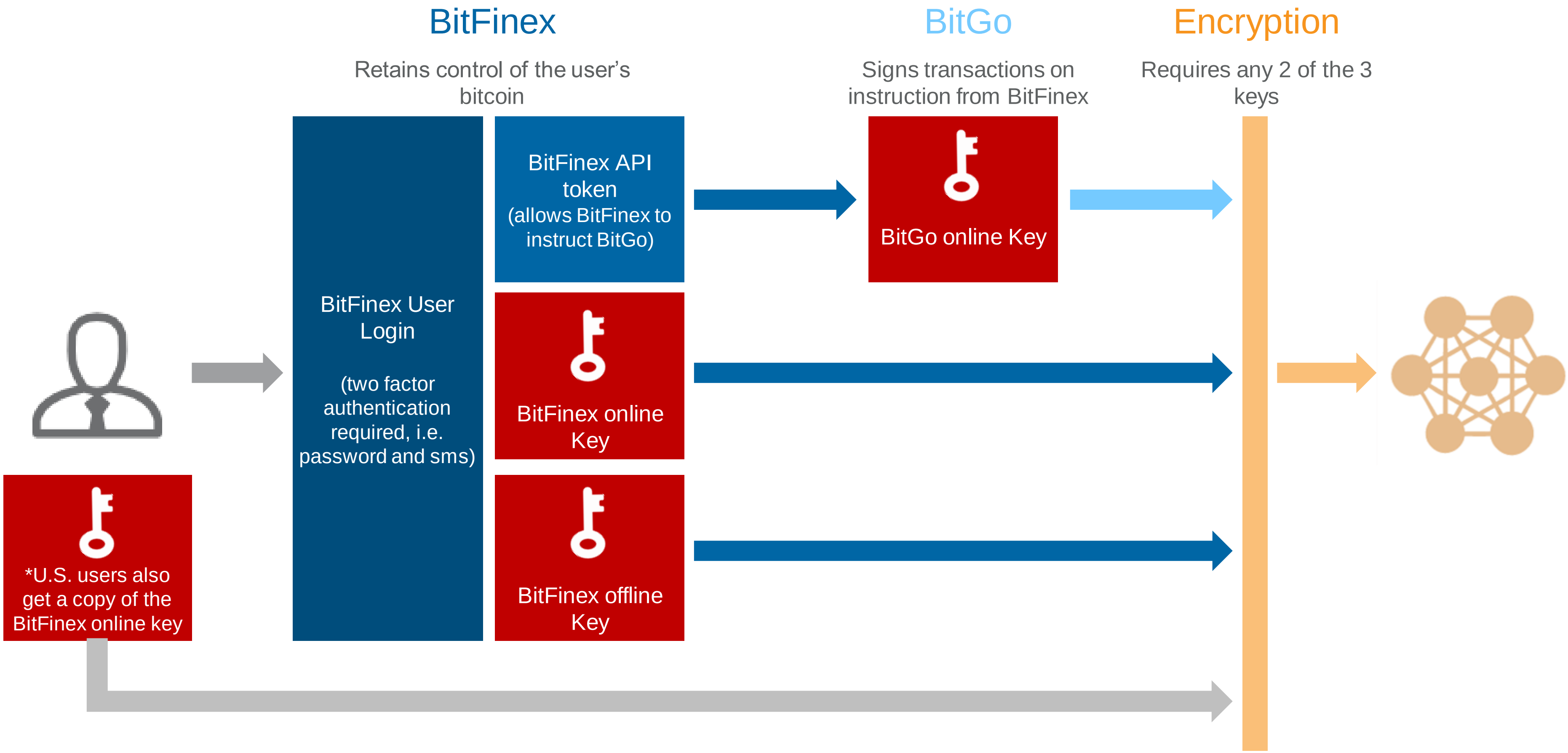
BitFinex online Key

BitFinex offline Key

*U.S. users also get a copy of the BitFinex online key

The problem with redundant controls

Under this model, an attacker can instruct payments if they: steal any two of the three keys (stored in 4 locations).



BitFinex

Retains control of the user's bitcoin

BitGo

Signs transactions on instruction from BitFinex

Encryption

Requires any 2 of the 3 keys

BitFinex User Login

(two factor authentication required, i.e. password and sms)

BitFinex API token (allows BitFinex to instruct BitGo)

BitGo online Key

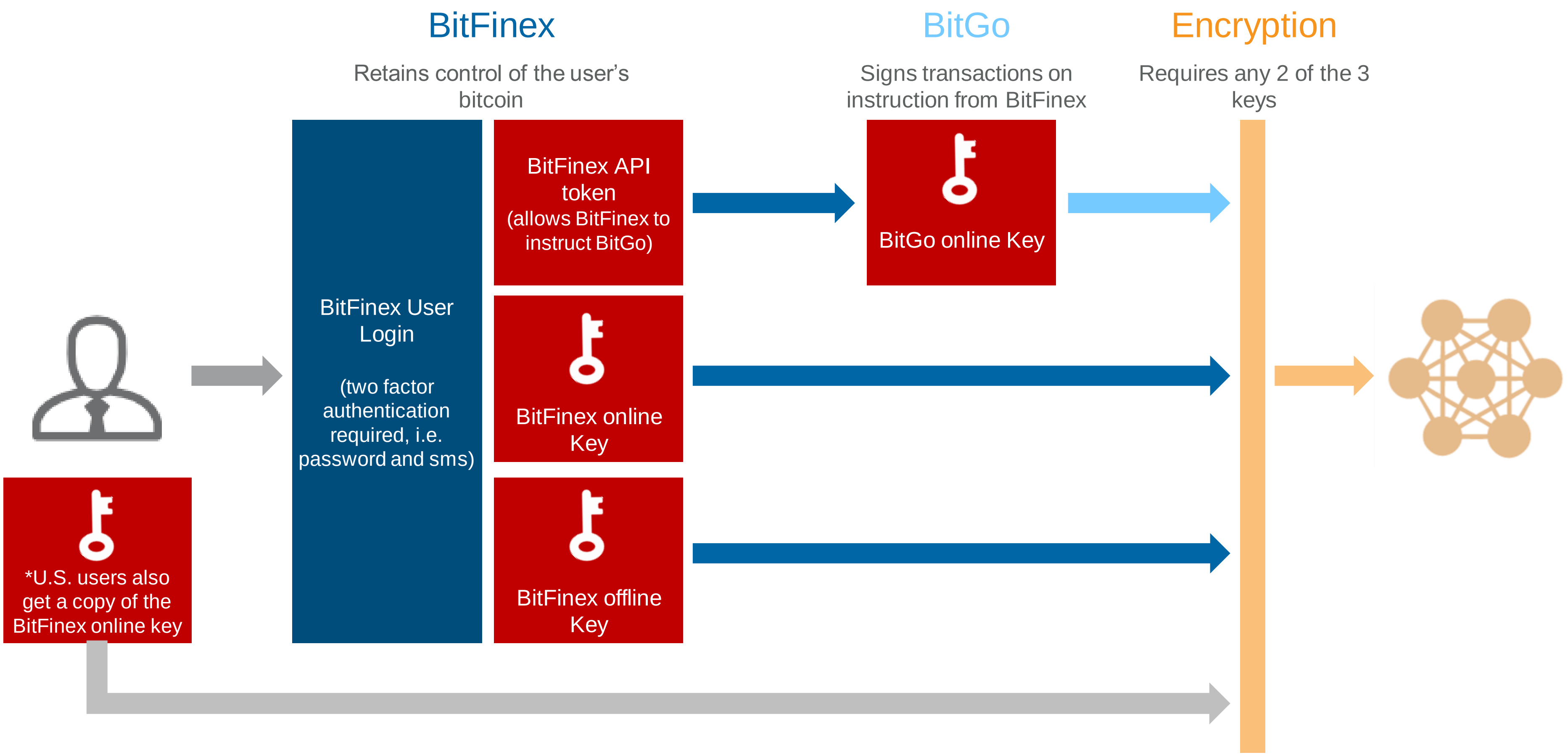
BitFinex online Key

BitFinex offline Key

*U.S. users also get a copy of the BitFinex online key

The problem with redundant controls

Under this model, an attacker can instruct payments if they: steal one key and the BitFinex API token.



BitFinex

Retains control of the user's bitcoin

BitGo

Signs transactions on instruction from BitFinex

Encryption

Requires any 2 of the 3 keys

BitFinex User Login

(two factor authentication required, i.e. password and sms)

BitFinex API token (allows BitFinex to instruct BitGo)

BitGo online Key

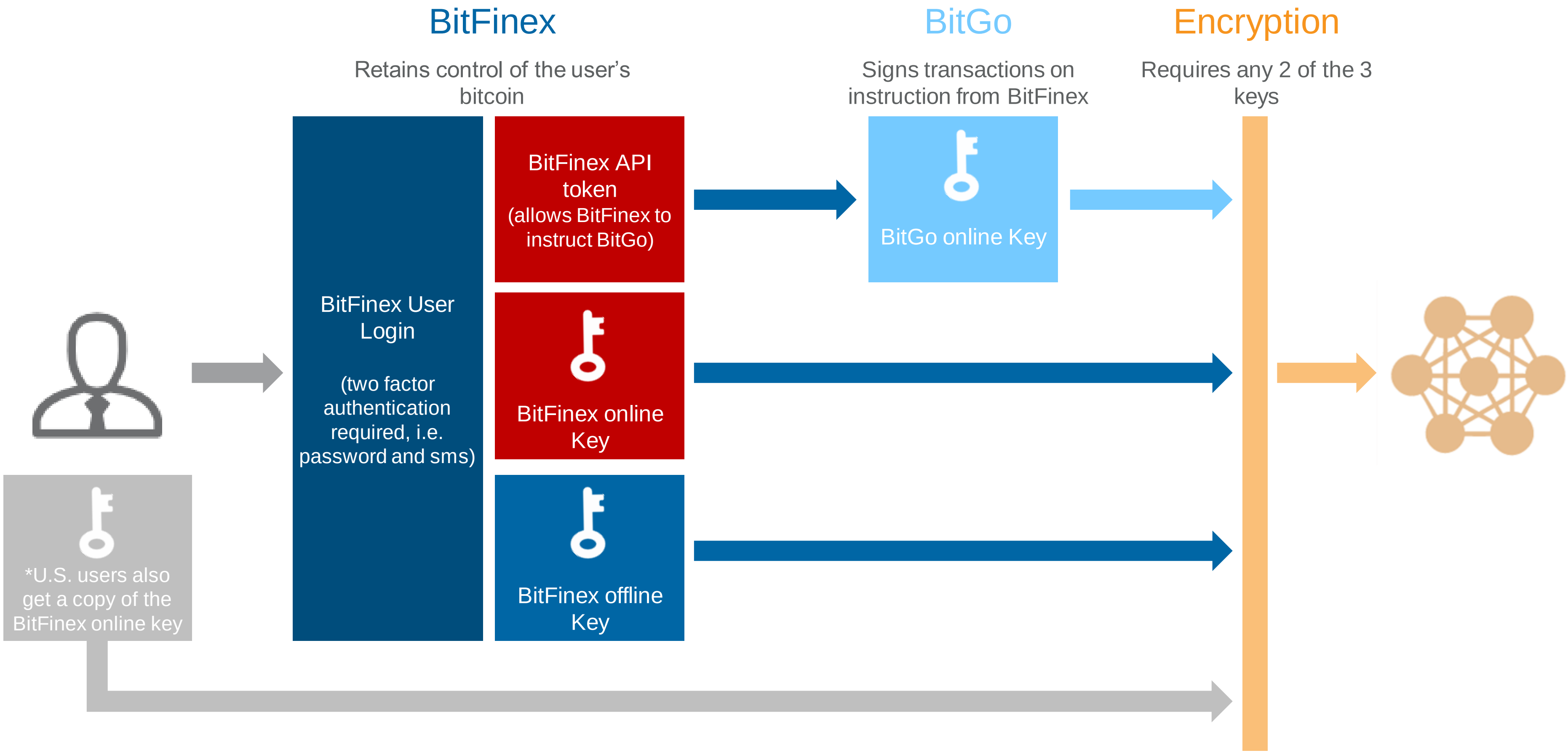
BitFinex online Key

BitFinex offline Key

*U.S. users also get a copy of the BitFinex online key

The problem with redundant controls

The prevailing theory at the moment is that the hacker obtained the private keys held online by Bitfinex, coupled with API access to BitGo to instruct BitGo to sign the withdrawals.[1]



BitFinex

Retains control of the user's bitcoin

BitGo

Signs transactions on instruction from BitFinex

Encryption

Requires any 2 of the 3 keys

BitFinex User Login

(two factor authentication required, i.e. password and sms)

BitFinex API token (allows BitFinex to instruct BitGo)

BitGo online Key

BitFinex online Key

BitFinex offline Key

*U.S. users also get a copy of the BitFinex online key

[1] http://hackingdistributed.com/2016/08/03/how-bitfinex-heist-could-have-been-avoided/

The problem with redundant controls

Rather than create additional layers of security, BitFinex created layer upon layer of redundancies, increasing the number of possible attack vectors.

BitGo’s key is redundant

- BitFinex claims that transactions are more secure because it uses “Multi-Signature Wallets” whereby each transaction needs to be signed by two keys, one held by BitFinex and usually one held by BitGo.
- In practice (if you have access to the BitFinex servers) only one key is needed to sign a transaction (one of the two keys controlled by BitFinex) because BitGo uses its “keys to sign transactions as directed by BitFinex”[1].
- The only control BitGo’s key seems to provide is a limit on the size of transactions. BitGo’s white paper claims “the service can refuse to sign large transactions”[2], but doesn’t list any other fraud prevention controls. This control could possibly be circumvented by submitting multiple small transactions.
- Therefore, in practice BitGo’s key seems to act as an automated ‘tick in the box’ for any “transaction that is first signed by BitFinex.”[1]

Keys can be stolen by common malware

- BitGo’s White Paper states: “One potential weakness with the 2-of-3 address is that it does have 2 of the 3 keys online in the user’s browser at the time of address creation. Malware that specifically targeted an application using 2-of-3 wallets could lie-in-wait of an address to be created, steal the keys, and then extract the funds later.”[2]

Why create redundant layers of security?

- The CFTC recently fined BitFinex $75,000 for breaching Dodd Frank requirements by not “actually deliver[ing] bitcoins to the traders who purchased them. Instead, Bitfinex held the bitcoins in deposit wallets that it owned and controlled”.
- This breaches the Dodd Frank requirement that “financed commodity transactions – including those in cryptocurrencies like bitcoin – must be conducted on an exchange, unless the entity offering the transactions can establish that actual delivery of the bitcoins results within 28 days. Where actual delivery requires a transfer of possession and control of the commodity.”
- According to BitGo “the Bitfinex configuration was unique”. One potential explanation for this could be that BitFinex was looking to address regulatory concerns rather than security in its set up, ensuring that:
  - —U.S. users could be provided with a key that would denote “possession and control” over the bitcoin. At the same time BitFinex would retain ultimate control by storing a copy of that key on its own servers and retaining the ability to instruct BitGo whether to co-sign a transaction.
  - —Non-U.S. users would still have no access to their keys.

[1] See BitFinex Terms of Service (accessed 09-Aug-2016)
[2] See the BitGo White Paper (accessed 09-Aug-2016)
[3] See the BitGo’s BitFinex Breach Update (accessed 09-Aug-2016)