BLOCKLÁNC ALAPÚ RENDSZEREK INFORMÁCIÓBIZTONSÁGI KIHÍVÁSAI

Csabai Csaba, blogger, blockchain evangelista

2018.1.15.

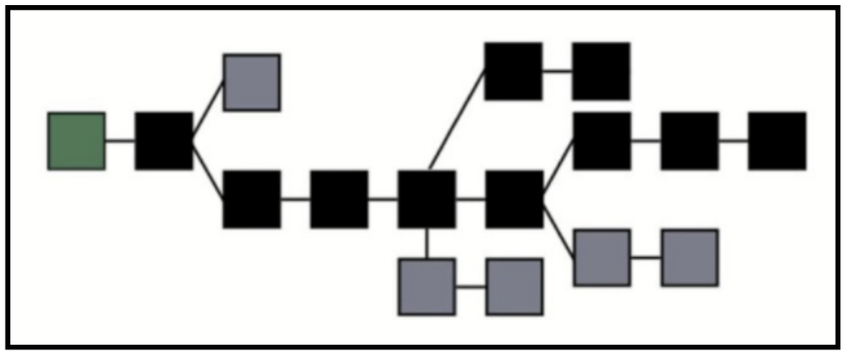
VARIANCE
www.variance.hu

TÉMÁK

Az előadás célja, hogy bemutassa a Bitcoin és a blocklánc technológia adta lehetőségek mellett azok információbiztonsági kihívásait is:

- kulcsok és wallet védelme,
- HD wallet (BIP32),
- decentralizált blocklánc (longest chain elv),
- peer-to-peer tranzakció (UTXO),
- közvetítő fél nélküli jogi ügyletek (okosszerződések),
- trustless layer-2 payment routing és atomic-swap,
- csalások és visszaélések (scam ICO-k, harforkok, airdroppok).
- Unconfirmed és Low-Confirmed (<6) visszaélések (pl. RbF tranzakció visszavonás)

A BITCOINTÓL A BLOCKCHAINIG



"A blockchain technológia elsődleges célja a manipulálás elleni védelem" (Vitalik Buterin - Ethereum)

3rd party eliminálása - "Trusted strangers are secuity holes" (Nick Szabó)

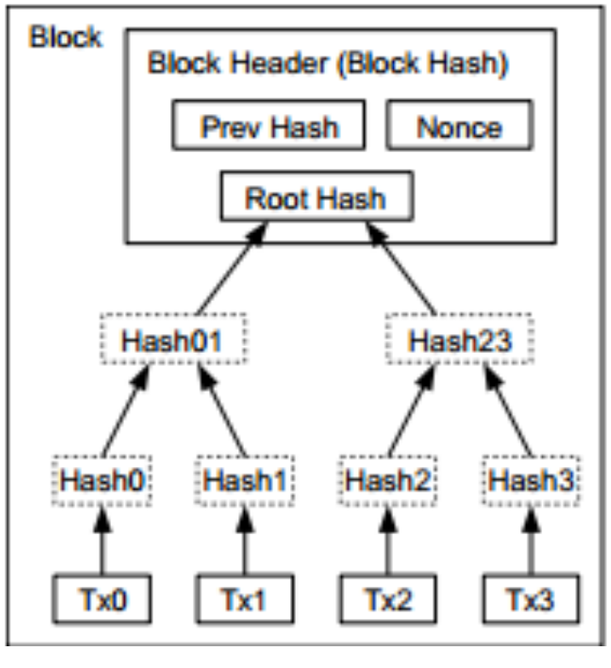
Kötött formátum, keretek(!) - A blocklánc technológia bármire jó, de egy konkrét blocklánc implementáció jellemzően egy dologra.

Satoshi Nakamoto: „peer-to-peer electronic cash system” (2008. október 31.)

- Nick Szabó: bit gold (2005), smart contract (2002)
- Hal Finney: RPoW (2004)
- Adam Back: hashcash (2002)

Minden igazán új dolog sikeréhez kell egy kis misztérium: pszeudonim publikáció 2011-ig.

A genezis blokk: "Chancellor on brink of second bailout for banks." (2009.01.03)



MI AZ A BITCOIN?

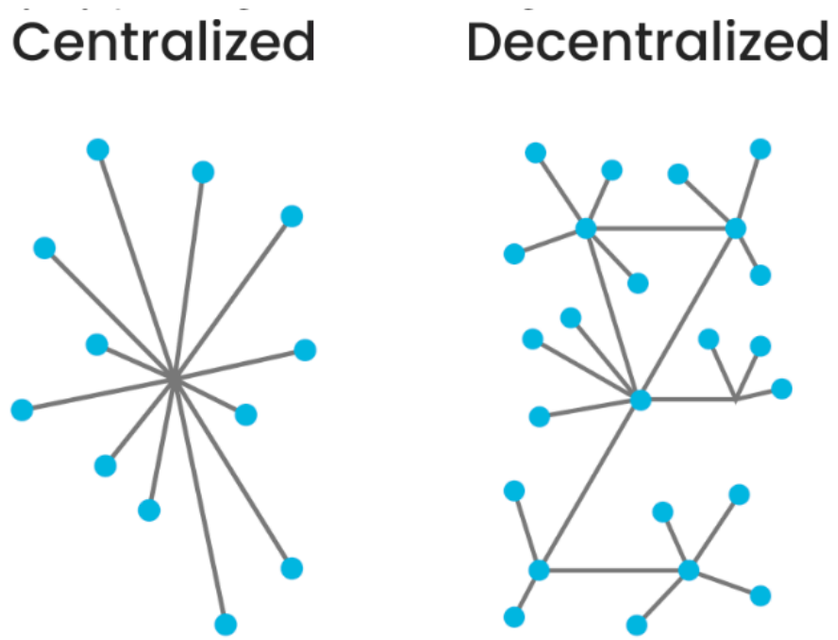
Mi is az a Bitcoin? (pénzügyi szempontok alapján)

- Inflációs modell: 21 millió coin, 10 perces blokk idő, 4 évente reward felezés
  - Éves kummulált infláció jelenleg 2,2%, ami folyamatosan csökken a reward felezéseknél
  - 2020-től követően a kumulált infláció már 1% alá kerül, 2040-től pedig 0,1% alá kerül
- Potenciális hedging terméke a fiat alapú termékeknek.
- Elosztott főkönyv a tranzakciók tárolására
- Pszudonim privacy - "The internet of money"
- Commodity termék

btc: 3Dnw5G6V6SrQPhXMYhbERtsdXGfahxxM9w
ltc: LgRLZq9Su77C4hQSE8PMQXpdPgN3a1rJaX
eth: 0xc4d18e736c8890df6878f6fd61059768ff580f05
zec: t1ZbCn5TpFwuwPBr2SHcSeBv7NevRwTWKsN

Decentralizáció:

- Centralizált vs Decentralizált rendszer szemlélet: költség, kockázat, rendelkezésre állás és kritikussági aspektusok
- Legjobb decentralizált rendszer példája: az internet
- peer-to-peer információ megosztás
- Ha megbízol a technológiában,akkor nincs szükség közvetítőfelekre.
- Szabályzás hiánya?

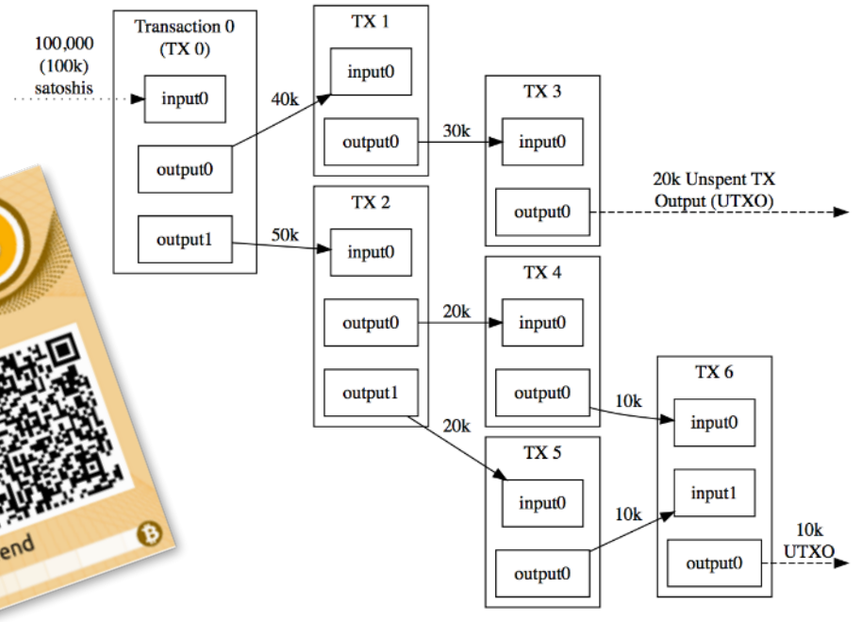


HOL ÉS HOGYAN TÁROLHATÓK A KRIPTOVALUTÁK

A valóságban a cryptovaluták a blockláncon tárolódnak, azokhoz semmilyen módon nem lehet onnan kihozni. Amit a "walletekben" tárolunk, azok a hozzánk rendelt "coinok", "tokenek" kezeléséhez szükséges privát kulcsok.

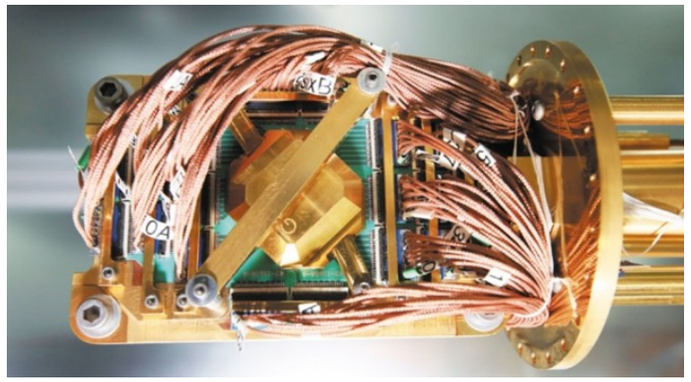
Alapelvek és lehetőségek:

- Centralizáció hiányában nincs olyan, hogy "elvesztett jelszó" gomb... Ha valaki elveszti a privát kulcsát, akkor elveszti a coinjai feletti kontrollt is. Erre alternatíva a multi-signature wallet.
- coinokat nem tárolunk tartósan exchangeken: szabályozás hiánya, hacker támadások, belső visszaélések(?)
- Nem szükséges full node-ot üzemeltetni. Akár egy paper wallet is elég!
- Fizikai tárolók (TREZOR, Ledger Nano S)
- Mobil pénztárcák



Triple-Entry Bookkeeping (Transaction-To-Transaction Payments) As Used By Bitcoin

HOGYAN GARANTÁLJA A BÁNYÁSZAT A DECENTRALIZÁLT BLOCKCHAIN BIZTONSÁGÁT?



Bitcoin: ECDSA (256) priv-pubkey encryption, double SHA-256 hashing.

PKI: Public Key Infrastructure

Elliptic Curve Digital Signature Algorithm

Quantum számítógép (shor módszertan, szuperpozíció) védelem?

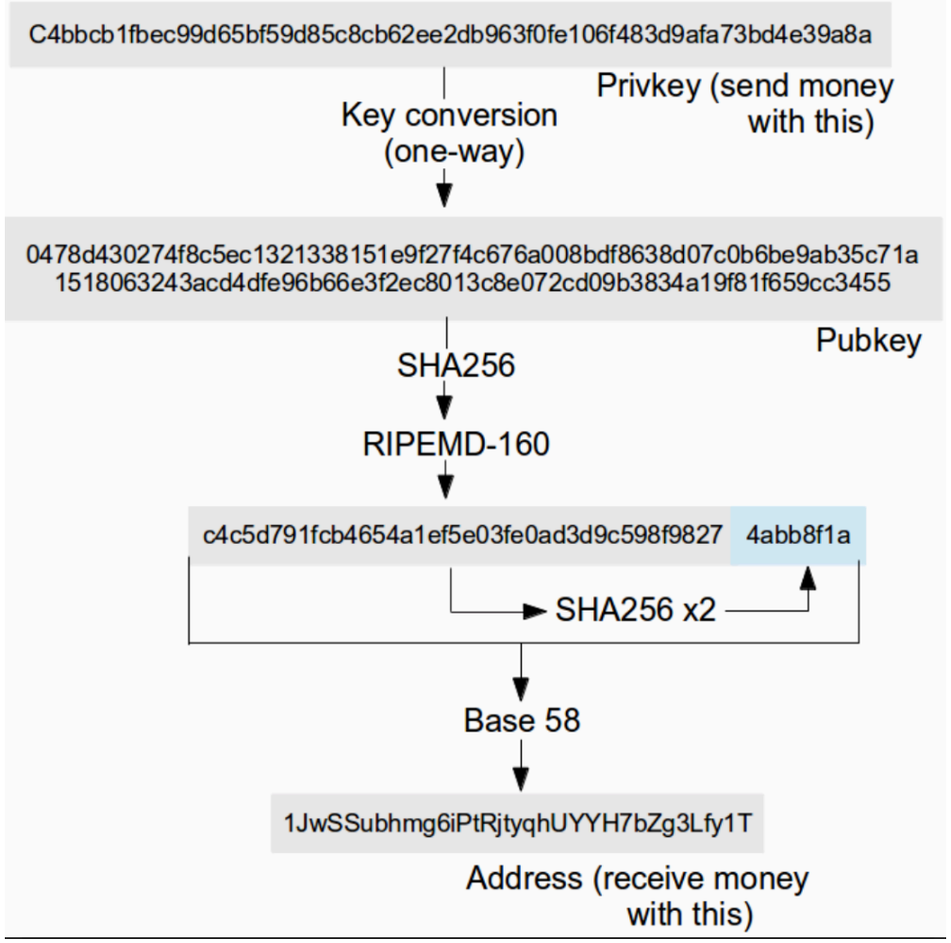
Csak a stabil qubitek száma védi a rendszert?

Gyakorlati garanciák:

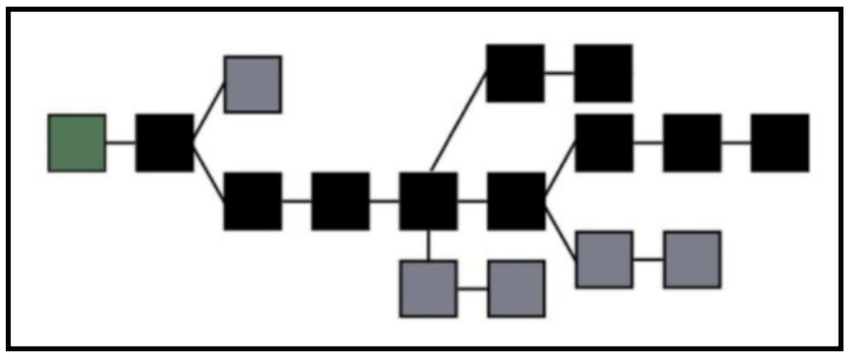
Publikus kulcs =/= Address: három szintű védelem (ECDSA 256 + Double SHA256 + RIPEMD-160)

Egyszer használatos addressek! Alapszabály:

> *"minden address-t csak egyszer használjon, ha utalnia kell onnan, akkor egyrészt új address-re utalja a "visszajárót", másrészt pedig gondoskodik arról, hogy ne lehessen módosítani a tx-et (nSequence=UNIT_MAX)"*



HOGYAN GARANTÁLJA A BÁNYÁSZAT A DECENTRALIZÁLT BLOCKCHAIN BIZTONSÁGÁT?



Mi is az a bányászat?

Hogyan keletkeznek a blokkok? Verseny a megfelelő hash-ért

Unconfirmed transaction (mempool)

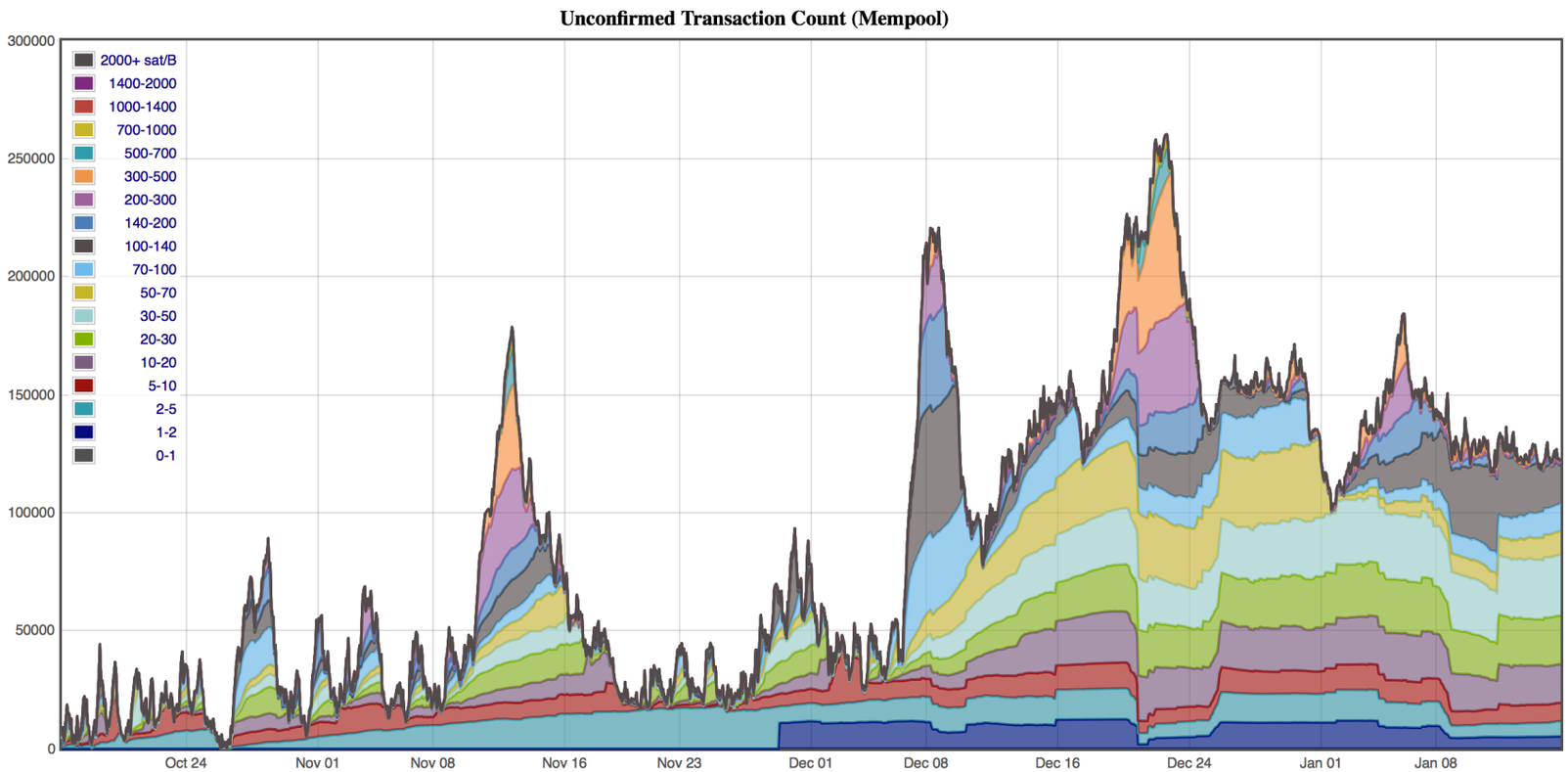
1st confirmed ls 6th confirmed státusz fontossága

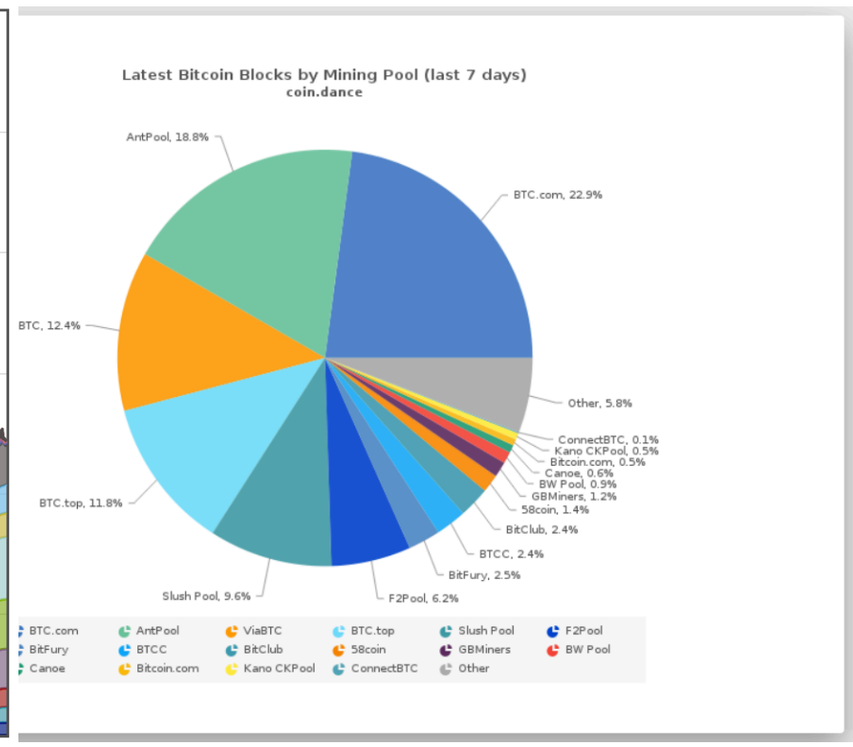
"Longest Chain" elv (nincs abszolút igaz blokklánc)

Mitől keletkeznek leágazások: Egy kis játékelméleti matek!

Orphan/Uncle blokkok

RbF (Replace by Fee)





CSALÁSOK ÉS VISSZAÉLÉSEK (SCAM ICO-K, HARFORKOK, AIRDROPPOK)

ICO (Initial Coin Offer – az IPO torz ikertestvére):

Közösségi cryptovaluta alapú finanszírozás egy új innovatív kezdeményezésre.

Web 3.0? Solidity alapokon fejlesztett dAppok.

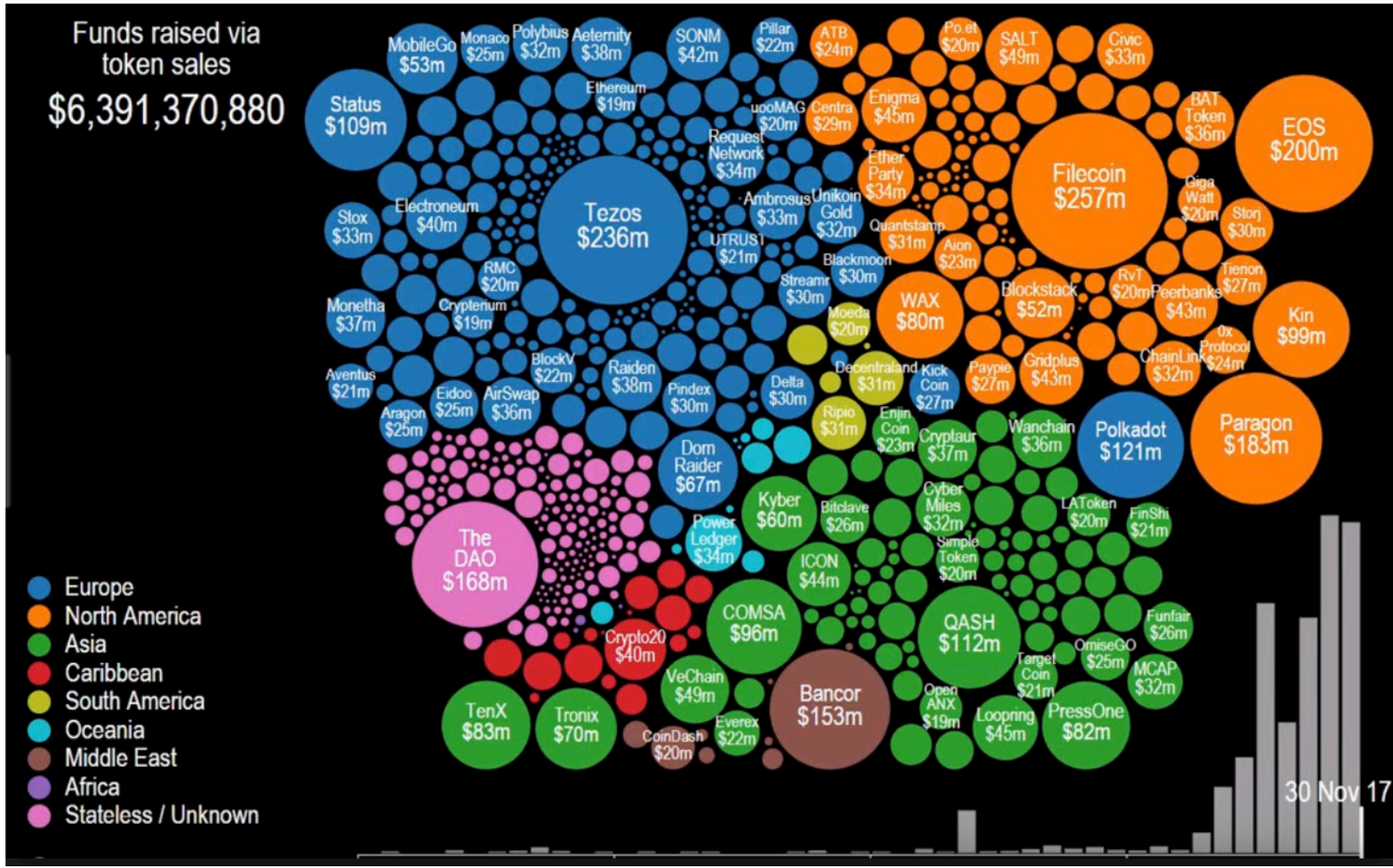
Tokenizált erőforrások: az innováció fűtőanyaga.

ICO vs Startup finanszírozás megközelítésének veszélyi

Vitalik Buterin: „Az ICOk 90%-a bukásra van ítélve”

Airdrop: A mézesmadzag amik általában csalásokhoz vezetnek...

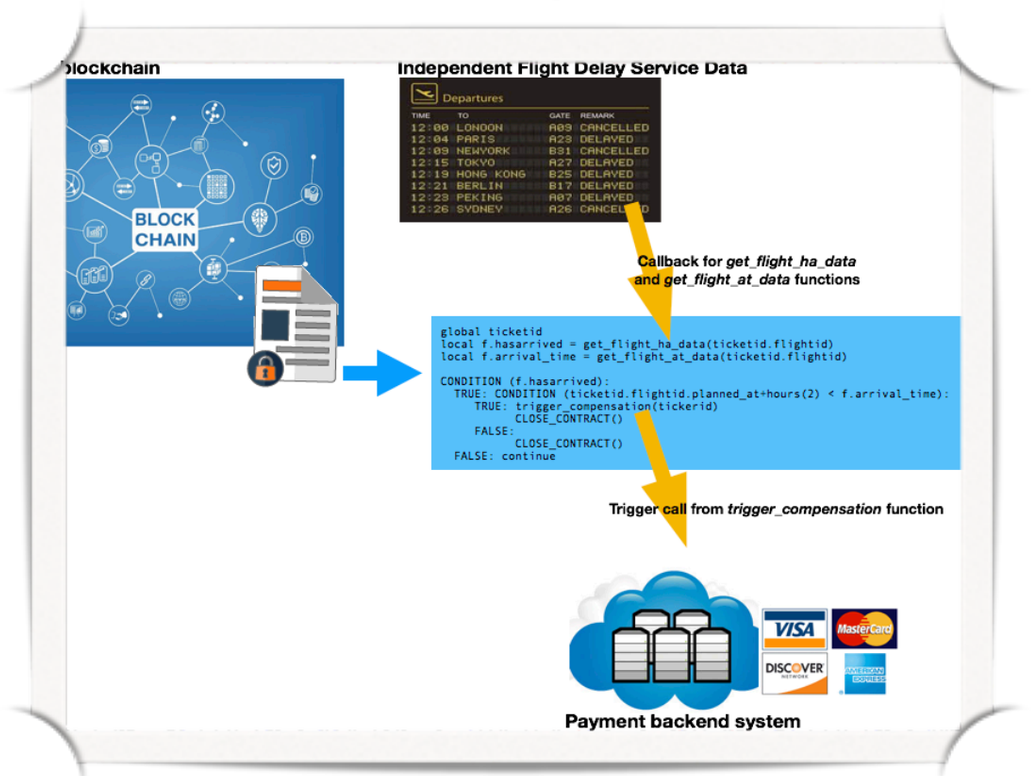
Hardfork: A leleményes lemaradók eszközei



MITŐL IS LESZ "OKOS" A SZERZŐDÉS?

*Okosszerződések = A jogrendszer következő **evolúciós** lépése?*
*Az okosszerződések kimenetelét a jogrendszer **automatikusan** elfogadja?*

- Semi-Smart Contracts:
  - A kiértékelési logika és a kapcsolódó érték is független rendszerekből származik. A blockchain csak triggerként funkcionál
  - Csak részlegesen fut a blockláncon
  - A kontraktus nem hordozza magával annak értékét, nem teljesül a "store of value" elv és vita esetén mediációra lehet szükség.



- Valós okosszerződések:
  - A blockláncon tárolódik
  - A szerződés minden érintettje azt aláírja
  - A megkötéskor tárolódik a fedezet!
  - A teljes kiértékelési logika on-chain a blockláncon megtalálható adatokból építkezik
  - Konszenzus hiányában a fedezet befagyasztásra kerül, csak mediáció útján szabadítható fel
  - A kontraktus nem csak triggereli a paymentet, de végre is hajtja azt!

MI AZ OKOSSZERZŐDÉSEK ELŐNYE, HÁTRÁNYAI?

"Hagyományos" SZERZŐDÉS

```
<CONTRACT>
 <BENEFITS> // előnyök
  Konzisztens //minden fél ugyanazt érti
  Világos // minden fél részéről
  Előre ellenőrizhető
  Szimulálható
  Hatékony, automatizálható
  Eseményvezérelt
  Privacy biztosítható
  Megmásíthatatlan
  Költséghatékony
  Független
  Végérvényesen végrehajtódik
 </BENEFITS>
 .
 .
 <DRAWBACKS> //hátrányok
  "Titokzatos!"
  "Furán újszerű" a jognak
  Bonyolult, körülményes
  Minden eshetőség kezelendő
  Függőségek biztosítása
 </DRAWBACKS>
 .
 .
</CONTRACT>
```

AZ EGYSZERŰ SCRIPTEKTŐL A BONYOLULT KONTRAKTUSOKIG

"Okosszerződések" a Bitcoin hálózaton

Smart contract = Bitcoin p2SH script (buta contract…)

- Stack-alapú lineárisan végrehajtódó műveletek
- OP kódokkal vezérelhető futás és feltételek
- Nehézkes (assemblyhez hasonló) szintaxis. Nagyon kötött
- A kontraktus csak az UTXO részleges vagy teljes elutalásával hívható meg.
- A kontraktus költsége maga a script „súlya” (mérete) adja meg. Tx fee = mining fee, mely befolyásolja a tx prioritását
- Főbb felhasználási területei: multi-signature wallet, időzített műveletek (HTLC), payment channels, „végrendelet” contract.

```
OP_If
    <Alice's pubkey> OP_CheckSig
OP_Else
     "3 months timestamp" OP_CSV OP_Drop
     2 <Bob's pubkey> <Charlie's pubkey> 2 OP_CheckMultiSig
OP_EndIf
```

Okosszerződések az Ethereum hálózaton

Smart contract = dApp, Ethereum = World Computer

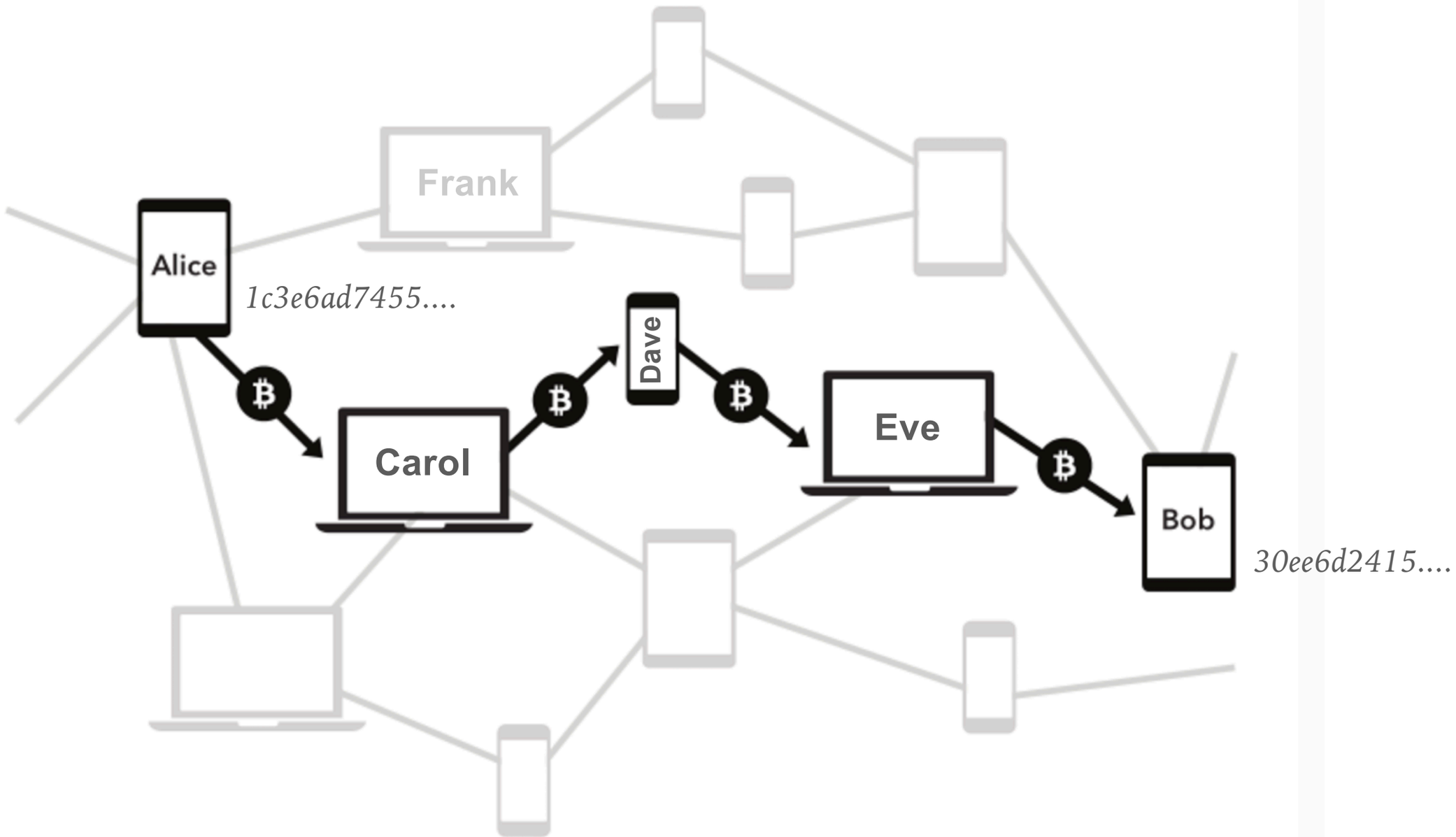
- Solidity: contract-alapú high level programnyelv, JavaScripthez hasonló szintaxis, ami EVM-en fut (Ethereum Virtual Machine)
- Támogatja a statikus típusokat, öröklődést, könyvtárakat (libs) és a komplex felhasználó által definiált adatszerkezeteket is.
- Leggyakoribb felhasználási területei: szavazás, közösségi finanszírozás, vak aukció, multi-signature wallets, stb.
- Minden contract a blockchainben jön létre és ott is fut le. Minden műveletnek költsége van (yellow book, gas price)

```
pragma solidity ^0.4.0;
contract SimpleStorage {
  uint storedData;

  function set(uint x) {
    storedData = x;
  }

  function get() constant returns (uint) {
    return storedData;
  }
}
```

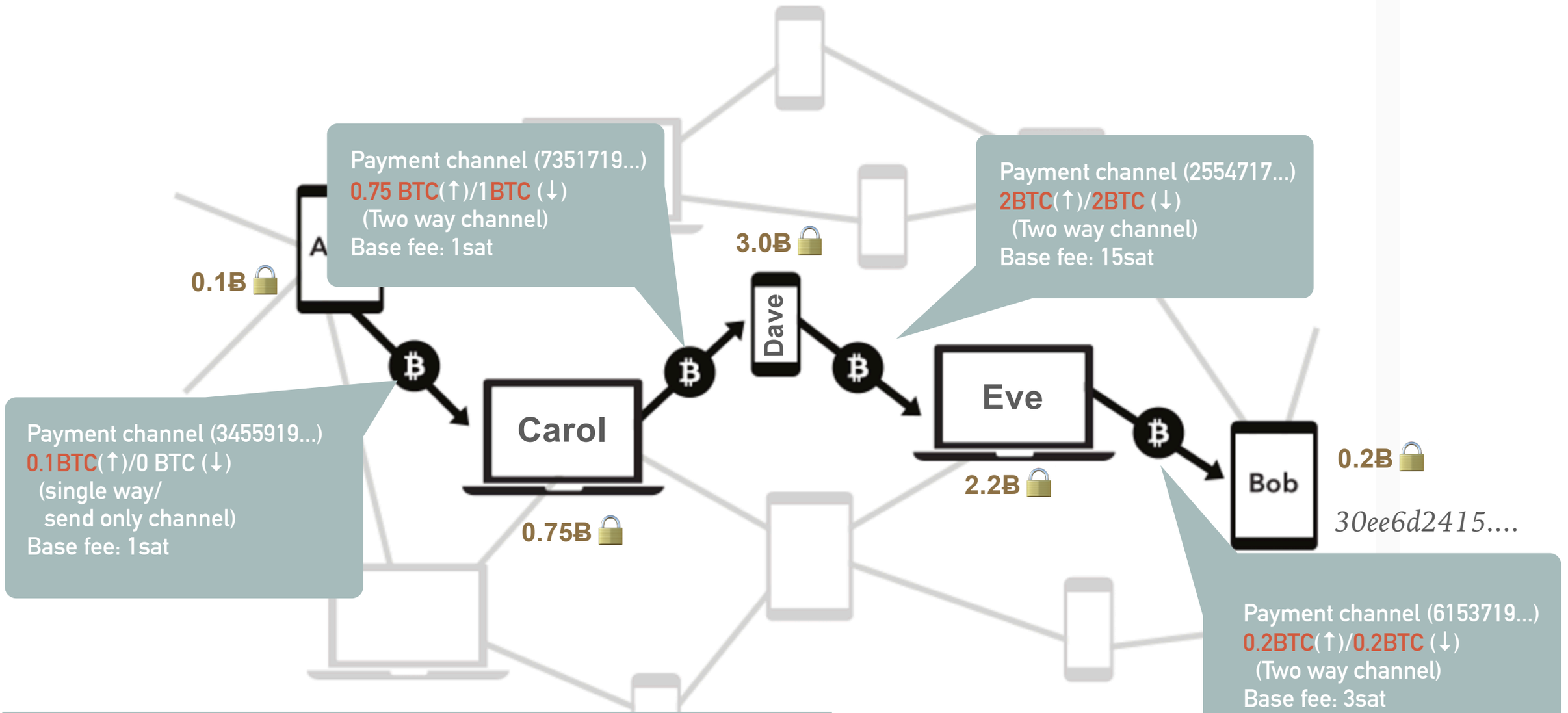
TRUSTLESS LAYER-2 PAYMENT ROUTING ÉS ATOMIC-SWAP



On-chain: Alice (1c3e6ad7455...) send 0.003Ƀ to Bob (30ee6d2415...) - txfee: 0.001Ƀ, delay: ~1 hour

Off-chain: Alice send 0.003Ƀ to Bob over existing routed payment channels - txfee: 1-100sat, delay: Ø

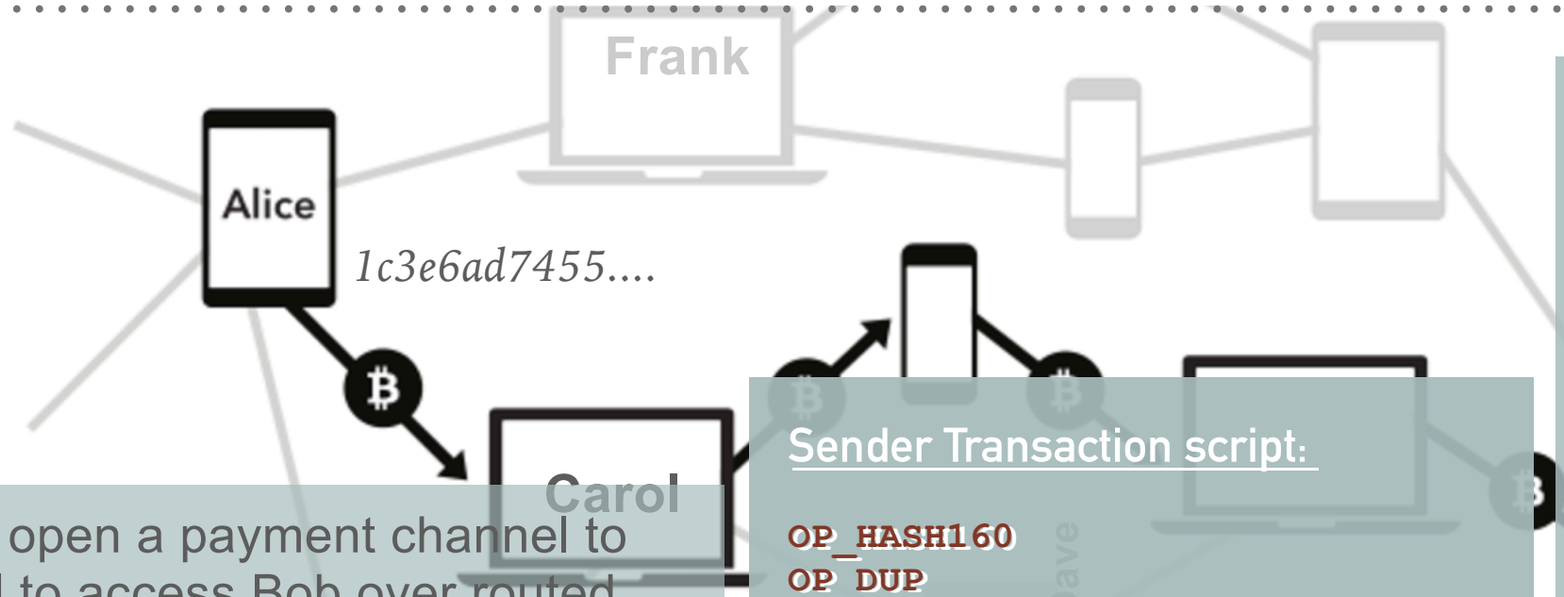
TRUSTLESS LAYER-2 PAYMENT ROUTING ÉS ATOMIC-SWAP



Payments channels:

- *(3455919...) Alice (0,1BTC) to Carol (0 BTC), base fee: 1sat*
- *(7351719...) Carol (0.75 BTC) to Dave (1BTC), base fee: 1 sat*
- *(2554717...) Dave (2 BTC) to Eve (2 BTC), base fee: 15 sat*
- *(6153719...) Eve (0.2 BTC) to Bab (0.2 BTC), base fee: 3sat*

HTLC (HASHED TIME-LOCK CONTRACTS) SCRIPTS



- Alice open a payment channel to Carol to access Bob over routed network
- Alice want to buy something for 1000 satoshis
- Bob: secretHash = SHA256(rand())
- Bob send secretHash to Alice
- Alice uses her payment channel to Charlie to pay him 1000 satoshis with secretHash and time-lock (24h)
- Charlie route payment to next peer
- Alice every time attach "revokeHash" to invalidate previously signed commitment transaction

Sender Transaction script:

```
OP_HASH160
OP_DUP
<secretHash>
OP_EQUAL
OP_SWAP
<revokeHash>
OP_EQUAL
OP_ADD

IF

    <pubKeyAlice>

ELSE

    <Date>
    OP_CHECKLOCKTIMEVERIFY
    <+24Hours>
    OP_CHECKSEQUENCEVERIFY
    OP_2DROP
    <pubKeyBob>

ENDIF
OP_CHECKSIG
```

Recipient Transaction script:

```
OP_HASH160
OP_DUP
<secretHash>
OP_EQUAL

IF

    <+24Hours>
    OP_CHECKSEQUENCEVERIFY
    OP_2DROP
    <pubKeyAlice>

ELSE

    <revokeHash>
    OP_EQUAL

    OP_NOTIF

        <Date>
        OP_CHECKLOCKTIMEVERIFY
        OP_DROP

    ENDIF

    <pubKeyBob>

ENDIF

OP_CHECKSIG
```