# BitCoin és kriptográfia

E-Group ICT Software Zrt.
SZABÓ Áron

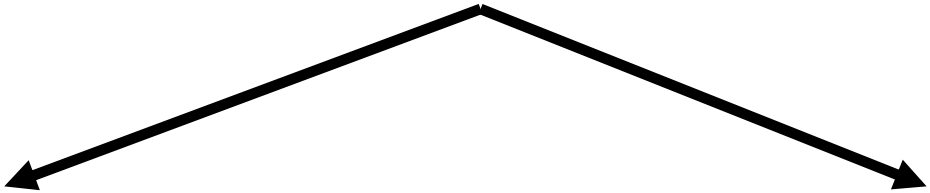
2014. május 22.

# Tartalomjegyzék

E-GROUP
SOFTWARE & BEYOND

# Alkalmazott kriptográfiai algoritmusok

E-GROUP
SOFTWARE & BEYOND



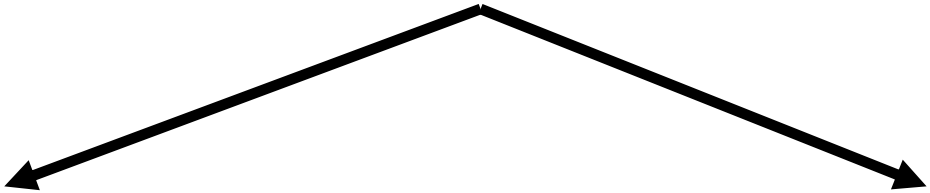
| SHA-256 | scrypt |
|---|---|
| BitCoin (BTC) | LiteCoin (LTC) |
| PeerCoin (PPC) | DogeCoin (DOGE) |
| NameCoin (NMC) | MasterCoin (MSC) |
| TerraCoin (TRC) | CraftCoin (CRC) |
| … | … |

**A lenyomatok ECDSA algoritmus révén kerülnek aláírásra (scriptSig).**

**forrás:** http://coinwik.org/List_of_all_DCs

# Alkalmazott kriptográfiai algoritmusok

E-GROUP
SOFTWARE & BEYOND



| SHA-256 | scrypt |
|---|---|
| NSA (design) | Tarsnap (design) |
| NIST (publish) | IETF RFC draft (publish) |
| 2001 (date) | 2012 (date) |
| 256 bits (output) | 256 bits (output) |
| CPU, GPU, FPGA, ASIC (mining) | CPU, GPU, memory (mining) |
| Merkle-Damgård (structure) | Merkle-Damgård, HMAC (structure) |
| 2*SHA-256 | salt: 80 bytes<br>CPU_memory_cost: n = 1024<br>block_size: r = 1<br>parallelization: p = 1 |

**forrás**: https://en.bitcoin.it/wiki/Mining_hardware_comparison
https://litecoin.info/Mining_hardware_comparison
http://tools.ietf.org/html/draft-josefsson-scrypt-kdf-01

# Tranzakciók, blokkok anatómiája

E-GROUP
SOFTWARE & BEYOND

blockexplorer.com/rawblock/000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f


```
{
  "hash":"000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f",
  "ver":1,
  "prev_block":"0000000000000000000000000000000000000000000000000000000000000000",
  "mrkl_root":"4a5e1e4baab89f3a32518a88c31bc87f618f76673e2cc77ab2127b7afdeda33b",
  "time":1231006505,
  "bits":486604799,
  "nonce":2083236893,
  "n_tx":1,
  "size":285,
  "tx":[
    {
      "hash":"4a5e1e4baab89f3a32518a88c31bc87f618f76673e2cc77ab2127b7afdeda33b",
      "ver":1,
      "vin_sz":1,
      "vout_sz":1,
      "lock_time":0,
      "size":204,
      "in":[
        {
          "prev_out":{
            "hash":"0000000000000000000000000000000000000000000000000000000000000000",
            "n":4294967295
          },
          "coinbase":"04ffff001d0104455468652054696d65732030332f4a616e2f3230303920436816e63656c6c6f72206f6e206272696e6b206f66207365636f6e64206261696c6f757420666f72206261
        }
      ],
      "out":[
        {
          "value":"50.00000000",
          "scriptPubKey":"04678afdb0fe5548271967f1a67130b7105cd6a828e03909a67962e0ea1f61deb649f6bc3f4cef38c4f35504e51ec112de5c384df7ba0b8d578a4c702b6bf11d5f OP_CHECKSIG"
        }
      ]
    }
  ],
  "mrkl_tree":[
    "4a5e1e4baab89f3a32518a88c31bc87f618f76673e2cc77ab2127b7afdeda33b"
  ]
}
```


## Genesis block

**2009. január 3-án került kibocsátásra, 50 BTC értékben, a 1A1zP1eP5QGefi2DMPTfTL5SLmv7DivfNa címre szólóan, az alábbi coinbase értéket tartalmazó első BitCoin blokk:**


```
"coinbase":"04ffff001d0104455468652054696d65732030332f4a616e2f3230303920436816e63656c6c6f72206f6e206272696e6b206f66207365636f6e64206261696c6f757420666f722062616e6b73"
                    T h e   T i m e s   0 3 / J a n / 2 0 0 9   C h a n c e l l o r   o n   b r i n k   o f   s e c o n d   b a i l o u t   f o r   b a n k s
```

# Tranzakciók, blokkok anatómiája

E-GROUP
SOFTWARE & BEYOND

blockexplorer.com/rawblock/000000000a40772eeba407f4fbc20c0ddfaeac29e574133cf5d217790f1c4ad3


```
{
  "hash":"000000000a40772eeba407f4fbc20c0ddfaeac29e574133cf5d217790f1c4ad3",
  "ver":1,
  "prev_block":"0000000000c7074a170fcfdf650f9688f8ee7adacae0ee4652386ba873640a39",
  "mrkl_root":"a3d97089ee541b46816ff1a2dba06651b148ff670b0829724ee4d8873e92e2fd",
  "time":1277142863,
  "bits":470727268,
  "nonce":47901640,
  "n_tx":2,
  "size":415,
  "tx":[
    {
      "hash":"3d5918c58d0a1aa61cec13246f7ed96dc78556264f0677c409f13903b6c86a16",
      "ver":1,
      "vin_sz":1,
      "vout_sz":1,
      "lock_time":0,
      "size":134,
      "in":[
        {
          "prev_out":{
            "hash":"0000000000000000000000000000000000000000000000000000000000000000",
            "n":4294967295
          },
          "coinbase":"0464ba0e1c0164"
        }
      ],
      "out":[
        {
          "value":"50.00000000",
          "scriptPubKey":"0454ea792e9307e6ba0d5e860931ea8ccd113fd2be9abf3ce2e281cdfc4c977c85b77a0983b0fa31d07b1bd998e607b0df22905bcc75d491eb815f0c78688ef386 OP_CHECKSIG"
        }
      ]
    },
    {
      "hash":"9f33a682ba8c433d49abd38aed47e19d6922c49d04767582b4301a2dc8a98663",
      "ver":1,
      "vin_sz":1,
      "vout_sz":1,
      "lock_time":0,
      "size":200,
      "in":[
        {
          "prev_out":{
            "hash":"852d1cca91abf8e50cbff749f854913dcf681d64107d2bce9b4caf8c8d1d4369",
            "n":0
          },
          "scriptSig":"30450221008b6c29c8075286d74b881683ee0f2c0d5ed570c4767f774cbcbe4844f9682e30022037b20f4f01b70cd3b47e1940c191c1bbe5782ea3b8569512c0282ba81d39662f01"
        }
      ],
      "out":[
        {
          "value":"50.00000000",
          "scriptPubKey":"04351f16d2269e28e7f701d3c7c206d78efa64117f2aee046f239ebf744b78ea77d135d49f424b80b339821d34c88c2ac5e4640b2efa419132a0e576713c27cced OP_CHECKSIG"
        }
      ]
    }
  ],
  "mrkl_tree":[
    "3d5918c58d0a1aa61cec13246f7ed96dc78556264f0677c409f13903b6c86a16",
    "9f33a682ba8c433d49abd38aed47e19d6922c49d04767582b4301a2dc8a98663",
    "a3d97089ee541b46816ff1a2dba06651b148ff670b0829724ee4d8873e92e2fd"
  ]
}
```

# Tranzakciók, blokkok anatómiája

E-GROUP
SOFTWARE & BEYOND

blockexplorer.com/rawblock/000000000a40772eeba407f4fbc20c0ddfaeac29e574133cf5d217790f1c4ad3


```
{
  "hash":"000000000a40772eeba407f4fbc20c0ddfaeac29e574133cf5d217790f1c4ad3",
  "ver":1,
  "prev_block":"0000000000c7074a170fcfdf650f9688f8ee7adacae0ee4652386ba873640a39",
  "mrkl_root":"a3d97089ee541b46816ff1a2dba06651b148ff670b0829724ee4d8873e92e2fd",
  "time":1277142863,
  "bits":470727268,
  "nonce":47901640,
  "n_tx":2,
  "size":415,
  "tx":[
    {
      "hash":"3d5918c58d0a1aa61cec13246f7ed96dc78556264f0677c409f13903b6c86a16",
      "ver":1,
      "vin_sz":1,
      "vout_sz":1,
      "lock_time":0,
      "size":134,
      "in":[
        {
          "prev_out":{
            "hash":"0000000000000000000000000000000000000000000000000000000000000000",
            "n":4294967295
          },
          "coinbase":"0464ba0e1c0164"
        }
      ],
      "out":[
        {
          "value":"50.00000000",
          "scriptPubKey":"0454ea792e9307e6ba0d5e860931ea8ccd113fd2be9abf3ce2e281cdfc4c977c85b77a0983b0fa31d07b1bd998e607b0df22905bcc75d491eb815f0c78688ef386 OP_CHECKSIG"
        }
      ]
    },
    {
      "hash":"9f33a682ba8c433d49abd38aed47e19d6922c49d04767582b4301a2dc8a98663",
      "ver":1,
      "vin_sz":1,
      "vout_sz":1,
      "lock_time":0,
      "size":200,
      "in":[
        {
          "prev_out":{
            "hash":"852d1cca91abf8e50cbff749f854913dcf681d64107d2bce9b4caf8c8d1d4369",
            "n":0
          },
          "scriptSig":"30450221008b6c29c8075286d74b881683ee0f2c0d5ed570c4767f774cbcbe4844f9682e30022037b20f4f01b70cd3b47e1940c191c1bbe5782ea3b8569512c0282ba81d39662f01"
        }
      ],
      "out":[
        {
          "value":"50.00000000",
          "scriptPubKey":"04351f16d2269e28e7f701d3c7c206d78efa64117f2aee046f239ebf744b78ea77d135d49f424b80b339821d34c88c2ac5e4640b2efa419132a0e576713c27cced OP_CHECKSIG"
        }
      ]
    }
  ],
  "mrkl_tree":[
    "3d5918c58d0a1aa61cec13246f7ed96dc78556264f0677c409f13903b6c86a16",
    "9f33a682ba8c433d49abd38aed47e19d6922c49d04767582b4301a2dc8a98663",
    "a3d97089ee541b46816ff1a2dba06651b148ff670b0829724ee4d8873e92e2fd"
  ]
}
```

# Tranzakciók, blokkok anatómiája

E-GROUP
SOFTWARE & BEYOND

blockexplorer.com/rawblock/000000000a40772eeba407f4fbc20c0ddfaeac29e574133cf5d217790f1c4ad3


```
{
  "hash":"000000000a40772eeba407f4fbc20c0ddfaeac29e574133cf5d217790f1c4ad3",
  "ver":1,
  "prev_block":"0000000000c7074a170fcfdf650f9688f8ee7adacae0ee4652386ba873640a39",
  "mrkl_root":"a3d97089ee541b46816ff1a2dba06651b148ff670b0829724ee4d8873e92e2fd",
  "time":1277142863,
  "bits":470727268,
  "nonce":47901640,
  "n_tx":2,
  "size":415,
  "tx":[
    {
    "hash":"3d5918c58d0a1aa61cec13246f7ed96dc78556264f0677c409f13903b6c86a16",
    "ver":1,
    "vin_sz":1,
    "vout_sz":1,
    "lock_time":0,
    "size":134,
    "in":[
      {
        "prev_out":{
          "hash":"0000000000000000000000000000000000000000000000000000000000000000",
          "n":4294967295
        },
        "coinbase":"0464ba0e1c0164"
      }
    ],
    "out":[
      {
        "value":"50.00000000",
        "scriptPubKey":"0454ea792e9307e6ba0d5e860931ea8ccd113fd2be9abf3ce2e281cdfc4c977c85b77a0983b0fa31d07b1bd998e607b0df22905bcc75d491eb815f0c78688ef386 OP_CHECKSIG"
      }
    ]
  },
  {
    "hash":"9f33a682ba8c433d49abd38aed47e19d6922c49d04767582b4301a2dc8a98663",
    "ver":1,
    "vin_sz":1,
    "vout_sz":1,
    "lock_time":0,
    "size":200,
    "in":[
      {
        "prev_out":{
          "hash":"852d1cca91abf8e50cbff749f854913dcf681d64107d2bce9b4caf8c8d1d4369",
          "n":0
        },
        "scriptSig":"30450221008b6c29c8075286d74b881683ee0f2c0d5ed570c4767f774cbcbe4844f9682e30022037b20f4f01b70cd3b47e1940c191c1bbe5782ea3b8569512c0282ba81d39662f01"
      }
    ],
    "out":[
      {
        "value":"50.00000000",
        "scriptPubKey":"04351f16d2269e28e7f701d3c7c206d78efa64117f2aee046f239ebf744b78ea77d135d49f424b80b339821d34c88c2ac5e4640b2efa419132a0e576713c27cced OP_CHECKSIG"
      }
    ]
  }
  ],
  "mrkl_tree":[
    "3d5918c58d0a1aa61cec13246f7ed96dc78556264f0677c409f13903b6c86a16",
    "9f33a682ba8c433d49abd38aed47e19d6922c49d04767582b4301a2dc8a98663",
    "a3d97089ee541b46816ff1a2dba06651b148ff670b0829724ee4d8873e92e2fd"
  ]
}
```

# Tranzakciók, blokkok anatómiája

E-GROUP
SOFTWARE & BEYOND

blockexplorer.com/rawblock/000000000a40772eeba407f4fbc20c0ddfaeac29e574133cf5d217790f1c4ad3


```
{
  "hash":"000000000a40772eeba407f4fbc20c0ddfaeac29e574133cf5d217790f1c4ad3",
  "ver":1,
  "prev_block":"0000000000c7074a170fcfdf650f9688f8ee7adacae0ee4652386ba873640a39",
  "mrkl_root":"a3d97089ee541b46816ff1a2dba06651b148ff670b0829724ee4d8873e92e2fd",
  "time":1277142863,
  "bits":470727268,
  "nonce":47901640,
  "n_tx":2,
  "size":415,
  "tx":[
    {
      "hash":"3d5918c58d0a1aa61cec13246f7ed96dc78556264f0677c409f13903b6c86a16",
      "ver":1,
      "vin_sz":1,
      "vout_sz":1,
      "lock_time":0,
      "size":134,
      "in":[
        {
          "prev_out":{
            "hash":"0000000000000000000000000000000000000000000000000000000000000000",
            "n":4294967295
          },
          "coinbase":"0464ba0e1c0164"
        }
      ],
      "out":[
        {
          "value":"50.00000000",
          "scriptPubKey":"0454ea792e9307e6ba0d5e860931ea8ccd113fd2be9abf3ce2e281cdfc4c977c85b77a0983b0fa31d07b1bd998e607b0df22905bcc75d491eb815f0c78688ef386 OP_CHECKSIG"
        }
      ]
    },
    {
      "hash":"9f33a682ba8c433d49abd38aed47e19d6922c49d04767582b4301a2dc8a98663",
      "ver":1,
      "vin_sz":1,
      "vout_sz":1,
      "lock_time":0,
      "size":200,
      "in":[
        {
          "prev_out":{
            "hash":"852d1cca91abf8e50cbff749f854913dcf681d64107d2bce9b4caf8c8d1d4369",
            "n":0
          },
          "scriptSig":"30450221008b6c29c8075286d74b881683ee0f2c0d5ed570c4767f774cbcbe4844f9682e30022037b20f4f01b70cd3b47e1940c191c1bbe5782ea3b8569512c0282ba81d39662f01"
        }
      ],
      "out":[
        {
          "value":"50.00000000",
          "scriptPubKey":"04351f16d2269e28e7f701d3c7c206d78efa64117f2aee046f239ebf744b78ea77d135d49f424b80b339821d34c88c2ac5e4640b2efa419132a0e576713c27cced OP_CHECKSIG"
        }
      ]
    }
  ],
  "mrkl_tree":[
    "3d5918c58d0a1aa61cec13246f7ed96dc78556264f0677c409f13903b6c86a16",
    "9f33a682ba8c433d49abd38aed47e19d6922c49d04767582b4301a2dc8a98663",
    "a3d97089ee541b46816ff1a2dba06651b148ff670b0829724ee4d8873e92e2fd"
  ]
}
```

# Tranzakciók, blokkok anatómiája

E-GROUP
SOFTWARE & BEYOND

blockexplorer.com/rawblock/000000000a40772eeba407f4fbc20c0ddfaeac29e574133cf5d217790f1c4ad3


```
{
  "hash":"000000000a40772eeba407f4fbc20c0ddfaeac29e574133cf5d217790f1c4ad3",
  "ver":1,
  "prev_block":"0000000000c7074a170fcfdf650f9688f8ee7adacae0ee4652386ba873640a39",
  "mrkl_root":"a3d97089ee541b46816ff1a2dba06651b148ff670b0829724ee4d8873e92e2fd",
  "time":1277142863,
  "bits":470727268,
  "nonce":47901640,
  "n_tx":2,
  "size":415,
  "tx":[
    {
      "hash":"3d5918c58d0a1aa61cec13246f7ed96dc78556264f0677c409f13903b6c86a16",
      "ver":1,
      "vin_sz":1,
      "vout_sz":1,
      "lock_time":0,
      "size":134,
      "in":[
        {
          "prev_out":{
            "hash":"0000000000000000000000000000000000000000000000000000000000000000",
            "n":4294967295
          },
          "coinbase":"0464ba0e1c0164"
        }
      ],
      "out":[
        {
          "value":"50.00000000",
          "scriptPubKey":"0454ea792e9307e6ba0d5e860931ea8ccd113fd2be9abf3ce2e281cdfc4c977c85b77a0983b0fa31d07b1bd998e607b0df22905bcc75d491eb815f0c78688ef386 OP_CHECKSIG"
        }
      ]
    },
    {
      "hash":"9f33a682ba8c433d49abd38aed47e19d6922c49d04767582b4301a2dc8a98663",
      "ver":1,
      "vin_sz":1,
      "vout_sz":1,
      "lock_time":0,
      "size":200,
      "in":[
        {
          "prev_out":{
            "hash":"852d1cca91abf8e50cbff749f854913dcf681d64107d2bce9b4caf8c8d1d4369",
            "n":0
          },
          "scriptSig":"30450221008b6c29c8075286d74b881683ee0f2c0d5ed570c4767f774cbcbe4844f9682e30022037b20f4f01b70cd3b47e1940c191c1bbe5782ea3b8569512c0282ba81d39662f01"
        }
      ],
      "out":[
        {
          "value":"50.00000000",
          "scriptPubKey":"04351f16d2269e28e7f701d3c7c206d78efa64117f2aee046f239ebf744b78ea77d135d49f424b80b339821d34c88c2ac5e4640b2efa419132a0e576713c27cced OP_CHECKSIG"
        }
      ]
    }
  ],
  "mrkl_tree":[
    "3d5918c58d0a1aa61cec13246f7ed96dc78556264f0677c409f13903b6c86a16",
    "9f33a682ba8c433d49abd38aed47e19d6922c49d04767582b4301a2dc8a98663",
    "a3d97089ee541b46816ff1a2dba06651b148ff670b0829724ee4d8873e92e2fd"
  ]
}
```

# Tranzakciók, blokkok anatómiája

E-GROUP
SOFTWARE & BEYOND

blockexplorer.com/rawblock/000000000a40772eeba407f4fbc20c0ddfaeac29e574133cf5d217790f1c4ad3


```
{
  "hash":"000000000a40772eeba407f4fbc20c0ddfaeac29e574133cf5d217790f1c4ad3",
  "ver":1,
  "prev_block":"0000000000c7074a170fcfdf650f9688f8ee7adacae0ee4652386ba873640a39",
  "mrkl_root":"a3d97089ee541b46816ff1a2dba06651b148ff670b0829724ee4d8873e92e2fd",
  "time":1277142863,
  "bits":470727268,
  "nonce":47901640,
  "n_tx":2,
  "size":415,
  "tx":[
    {
      "hash":"3d5918c58d0a1aa61cec13246f7ed96dc78556264f0677c409f13903b6c86a16",
      "ver":1,
      "vin_sz":1,
      "vout_sz":1,
      "lock_time":0,
      "size":134,
      "in":[
        {
          "prev_out":{
            "hash":"0000000000000000000000000000000000000000000000000000000000000000",
            "n":4294967295
          },
          "coinbase":"0464ba0e1c0164"
        }
      ],
      "out":[
        {
          "value":"50.00000000",
          "scriptPubKey":"0454ea792e9307e6ba0d5e860931ea8ccd113fd2be9abf3ce2e281cdfc4c977c85b77a0983b0fa31d07b1bd998e607b0df22905bcc75d491eb815f0c78688ef386 OP_CHECKSIG"
        }
      ]
    },
    {
      "hash":"9f33a682ba8c433d49abd38aed47e19d6922c49d04767582b4301a2dc8a98663",
      "ver":1,
      "vin_sz":1,
      "vout_sz":1,
      "lock_time":0,
      "size":200,
      "in":[
        {
          "prev_out":{
            "hash":"852d1cca91abf8e50cbff749f854913dcf681d64107d2bce9b4caf8c8d1d4369",
            "n":0
          },
          "scriptSig":"30450221008b6c29c8075286d74b881683ee0f2c0d5ed570c4767f774cbcbe4844f9682e30022037b20f4f01b70cd3b47e1940c191c1bbe5782ea3b8569512c0282ba81d39662f01"
        }
      ],
      "out":[
        {
          "value":"50.00000000",
          "scriptPubKey":"04351f16d2269e28e7f701d3c7c206d78efa64117f2aee046f239ebf744b78ea77d135d49f424b80b339821d34c88c2ac5e4640b2efa419132a0e576713c27cced OP_CHECKSIG"
        }
      ]
    }
  ],
  "mrkl_tree":[
    "3d5918c58d0a1aa61cec13246f7ed96dc78556264f0677c409f13903b6c86a16",
    "9f33a682ba8c433d49abd38aed47e19d6922c49d04767582b4301a2dc8a98663",
    "a3d97089ee541b46816ff1a2dba06651b148ff670b0829724ee4d8873e92e2fd"
  ]
}
```

# Tranzakciók, blokkok anatómiája

E-GROUP
SOFTWARE & BEYOND

**Calculate addresses based on scriptPubKey**

Genesis Block - address[scriptPubKey]: 04678afdb0fe5548271967f1a67130b7105cd6a828e03909a67962e0ea1f61deb649f6
Genesis Block - address[BASE58]: 1A1zP1eP5QGefi2DMPTfTL5SLmv7DivfNa
Genesis Block - address[OP_HASH160]: 62e907b15cbf27d5425399ebf6f0fb50ebb88f18

Non-Genesis Block - address[scriptPubKey]: 04e9bcda6dc37fc394cfe8e2a2612a098da9ea13fb677694ddd0fe1078fbb1b957
Non-Genesis Block - address[BASE58]: 1FKr1wEARahr8m45fFJjL2HJjfCGkdk6rH
Non-Genesis Block - address[OP_HASH160]: 9d222a35a9dc9dda9afe8f7823b8591b083c2355

Full Block - address[scriptPubKey]: 0454ea792e9307e6ba0d5e860931ea8ccd113fd2be9abf3ce2e281cdfc4c977c85b77a0983
Full Block - address[BASE58]: 1J4r3ik4NnxmwVxzrMcYD8NdgkJ5wjcyce
Full Block - address[OP_HASH160]: bb345418179b278abc456cfbe494d1b542608c4e

# Tranzakciók, blokkok anatómiája

E-GROUP
SOFTWARE & BEYOND

```php
//derive address from public key (scriptPubKey)

$address                = scriptPubKey_to_address($tx_out_scriptPubKey_data, $ver);

function scriptPubKey_to_address($scriptPubKey, $ver)
{
    $address = array();
    $address['scriptPubKey'] = $scriptPubKey;
    $address['BASE58'] = '';
    $address['OP_HASH160'] = '';

    //key_hash: first hash (SHA-256)
    $data = pack('H*', $scriptPubKey);
    $hash = hash('sha256', $data, FALSE);

    //key_hash: second hash (RIPEMD-160)
    $data = pack('H*', $hash);
    $hash = hash('ripemd160', $data, FALSE);
    $address['OP_HASH160'] = $hash;
    $key_hash = $ver . $hash;

    //checksum: first hash (SHA-256)
    $data = pack('H*', $key_hash);
    $hash = hash('sha256', $data, FALSE);

    //checksum: second hash (SHA-256)
    $data = pack('H*', $hash);
    $hash = hash('sha256', $data, FALSE);
    $checksum = substr($hash, 0, 8);

    //address
    $address['BASE58'] = base58_encode($key_hash . $checksum);

    return $address;
}
```

# Tranzakciók, blokkok anatómiája

E-GROUP
SOFTWARE & BEYOND

**Calculate block hash based on block chain data**

Genesis Block - block hash: 000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f
Non-Genesis Block - block hash: 00000000000003455fec9ec2513defdca2dde2c5d3d991c9aa59e622626c8fcc
Full Block - block hash: 000000000a40772eeba407f4fbc20c0ddfaeac29e574133cf5d217790f1c4ad3

**Calculate transaction hash based on transaction data**

Genesis Block - tx_hash (coinbase): 4a5e1e4baab89f3a32518a88c31bc87f618f76673e2cc77ab2127b7afdeda33b
Non-Genesis Block - tx_hash (scriptSig): 08901b81e39bc61d632c93241c44ec3763366bd57444b01494481ed46079c898
Full Block - tx_hash (coinbase): 3d5918c58d0a1aa61cec13246f7ed96dc78556264f0677c409f13903b6c86a16
Full Block - tx_hash (scriptSig): 9f33a682ba8c433d49abd38aed47e19d6922c49d04767582b4301a2dc8a98663

# Tranzakciók, blokkok anatómiája

E-GROUP
SOFTWARE & BEYOND

```php
//block hash

$hash                   = hex_reversed(integer_to_hex($ver, 8)) .
                          hex_reversed($prev_block) .
                          hex_reversed($mrkl_root) .
                          hex_reversed(integer_to_hex($time, 8)) .
                          hex_reversed(integer_to_hex($bits, 8)) .
                          hex_reversed(integer_to_hex($nonce, 8));

calculate_block_tx_hash($hash);

function calculate_block_tx_hash($data)
{
    //block hash: first hash (SHA-256)
    $data = pack('H*', $data);
    $hash = hash('sha256', $data, FALSE);

    //block hash: second hash (SHA-256)
    $data = pack('H*', $hash);
    $hash = hash('sha256', $data, FALSE);

    //reverse byte order
    $block_hash = hex_reversed($hash);

    return $block_hash;
}
```

# Tranzakciók, blokkok anatómiája

E-GROUP
SOFTWARE & BEYOND

```
//tx_hash (coinbase)

$tx_in                  = $tx_in .
                          hex_reversed($tx_in_prev_out_hash[$counter]) .
                          hex_reversed(integer_to_hex($tx_in_prev_out_n[$counter], 8)) .
                          hex_reversed(integer_to_hex(strlen($tx_in_coinbase[$counter])/2, 2)) .
                          $tx_in_coinbase[$counter];
$tx_in_coinbase[0]      = hex_reversed(integer_to_hex(strlen(hex_reversed(integer_to_hex($bits, 8)))/2, 2)) .
                          hex_reversed(integer_to_hex($bits, 8)) .
                          hex_reversed(integer_to_hex(strlen(hex_reversed(integer_to_hex($tx_in_coinbase_extranonce[0], 2)))/2, 2)) .
                          hex_reversed(integer_to_hex($tx_in_coinbase_extranonce[0], 2)) .
                          hex_reversed(integer_to_hex(strlen($tx_in_coinbase_data[0])/2, 2)) .
                          $tx_in_coinbase_data[0];
$tx_out                 = $tx_out .
                          hex_reversed(integer_to_hex($tx_out_value[$counter] * pow(10, 8), 16)) .
                          hex_reversed(integer_to_hex(strlen($tx_out_scriptPubKey)/2, 2)) .
                          $tx_out_scriptPubKey;
$tx_out_scriptPubKey    = hex_reversed(integer_to_hex(strlen($tx_out_scriptPubKey_data[$counter])/2, 2)) .
                          $tx_out_scriptPubKey_data[$counter] .
                          $OP_CHECKSIG;
$tx_hash                = hex_reversed(integer_to_hex($ver, 8)) .
                          hex_reversed(integer_to_hex($tx_vin_sz, 2)) .
                          $tx_in .
                          hex_reversed(integer_to_hex($tx_sequence_number, 8)) .
                          hex_reversed(integer_to_hex($tx_vout_sz, 2)) .
                          $tx_out .
                          hex_reversed(integer_to_hex($tx_lock_time, 8));

calculate_block_tx_hash($tx_hash);
```

# Tranzakciók, blokkok anatómiája

E-GROUP
SOFTWARE & BEYOND

```
//tx_hash (scriptSig)

$tx_in                  = $tx_in .
                          hex_reversed($tx_in_prev_out_hash[$counter]) .
                          hex_reversed(integer_to_hex($tx_in_prev_out_n[$counter], 8)) .
                          hex_reversed(integer_to_hex(strlen($tx_in_scriptSig)/2)) .
                          $tx_in_scriptSig;
$tx_in_scriptSig        = hex_reversed(integer_to_hex(strlen($tx_in_scriptSig_sig_data[$counter])/2)) .
                          $tx_in_scriptSig_sig_data[$counter] .
                          hex_reversed(integer_to_hex(strlen($tx_in_scriptSig_pubKey_data[$counter])/2)) .
                          $tx_in_scriptSig_pubKey_data[$counter];
$tx_out                 = $tx_out .
                          hex_reversed(integer_to_hex($tx_out_value[$counter] * pow(10, 8), 16)) .
                          hex_reversed(integer_to_hex(strlen($tx_out_scriptPubKey)/2, 2)) .
                          $tx_out_scriptPubKey;
$tx_out_scriptPubKey    = hex_reversed(integer_to_hex(strlen($tx_out_scriptPubKey_data[$counter])/2, 2)) .
                          $tx_out_scriptPubKey_data[$counter] .
                          $OP_CHECKSIG;
$tx_hash                = hex_reversed(integer_to_hex($ver, 8)) .
                          hex_reversed(integer_to_hex($tx_vin_sz, 2)) .
                          $tx_in .
                          hex_reversed(integer_to_hex($tx_sequence_number, 8)) .
                          hex_reversed(integer_to_hex($tx_vout_sz, 2)) .
                          $tx_out .
                          hex_reversed(integer_to_hex($tx_lock_time, 8));

calculate_block_tx_hash($tx_hash);
```

# Tranzakciók, blokkok anatómiája

E-GROUP
SOFTWARE & BEYOND

**Calculate Merkle Tree hashes based on transaction hashes**

Merkle-tree Block - 1 coinbase + 5 scriptSig: 000000000000a85d42610b292d2baebe54ff0c854847fe3d2ca37ac7d6e46b99

mrkl_tree[0]: 3a459eab5f0cf8394a21e04d2ed3b2beeaa59795912e20b9c680e9db74dfb18c
mrkl_tree[1]: be38f46f0eccba72416aed715851fd07b881ffb7928b7622847314588e06a6b7
mrkl_tree[2]: d173f2a12b6ff63a77d9fe7bbb590bdb02b826d07739f90ebb016dc9297332be
mrkl_tree[3]: 59d1e83e5268bbb491234ff23cbbf2a7c0aa87df553484afee9e82385fc7052f
mrkl_tree[4]: f1ce77a69d06efb79e3b08a0ff441fa3b1deaf71b358df55244d56dd797ac60c
mrkl_tree[5]: 84053cba91fe659fd3afa1bf2fd0e3746b99215b50cd74e44bda507d8edf52e0
mrkl_tree[6] = mrkl_tree[0] + mrkl_tree[1]: 13a3595f2610c8e4d727130daade66c772fdec4bd2463d773fd0f85c20ced32d
mrkl_tree[7] = mrkl_tree[2] + mrkl_tree[3]: f6ae335dc2d2aecb6a255ebd03caaf6820e6c0534531051066810080e0d822c8
mrkl_tree[8] = mrkl_tree[4] + mrkl_tree[5]: a751efbeabe73bdf9d08df5760104feff915d9d807d4c62178cdeb98d8c25f43
mrkl_tree[9] = mrkl_tree[6] + mrkl_tree[7]: 59545fd8dfdd821ca7accecab0655d77437f5bba5aaa5ea8c042a26bc9ae514b
mrkl_tree[10] = mrkl_tree[8] + mrkl_tree[8]: 15eca0aa3e2cc2b9b4fbe0629f1dda87f329500fcdcd6ef546d163211266b3b3
mrkl_tree[11] = mrkl_tree[9] + mrkl_tree[10]: 9cdf7722eb64015731ba9794e32bdefd9cf69b42456d31f5e59aedb68c57ed52

# Tranzakciók, blokkok anatómiája

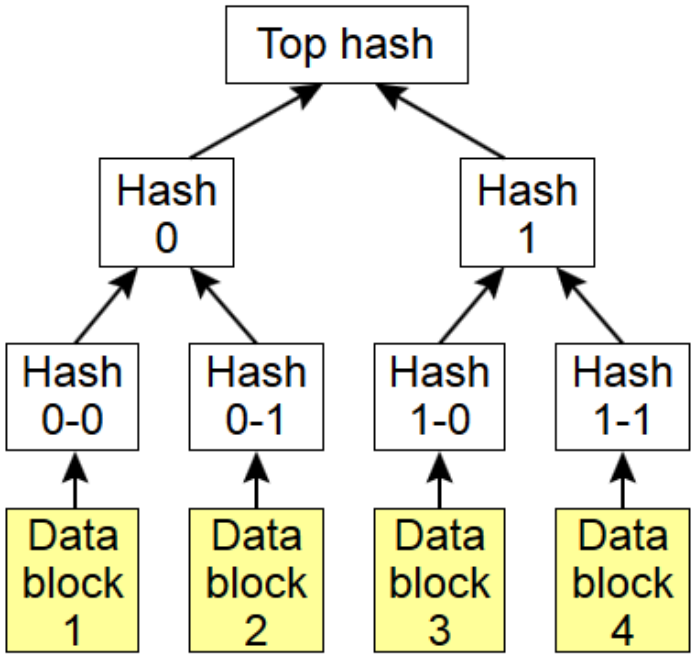
E-GROUP
SOFTWARE & BEYOND

```php
function calculate_merkle_tree_hash($data)
{
    //block hash: first hash (SHA-256)
    $data = pack('H*', $data);
    $hash = hash('sha256', $data, FALSE);

    //block hash: second hash (SHA-256)
    $data = pack('H*', $hash);
    $hash = hash('sha256', $data, FALSE);

    //reverse byte order
    $block_hash = hex_reversed($hash);

    return $block_hash;
}
```



# Tranzakciók, blokkok anatómiája

E-GROUP
SOFTWARE & BEYOND

**scriptSig/sig aláírás:** DSA, ECDSA

Elliptikus görbén alapuló DSA, ahol a nyilvános kulcs egy (x1, y1) pont a kiválasztott görbén (pl. secp256k1).

**m:** üzenet
**k:** véletlenszám [1, n-1]
**x1, y1:** görbe pontja, nyilvános kulcs
**n:** bázispont rendje
**d:** véletlenszám [1, n-1], titkos kulcs
**(r, s):** aláírás

## Elliptic Curve DSA

For Alice to sign a message $m$, she follows these steps:

1. Calculate $e = \mathrm{HASH}(m)$, where HASH is a cryptographic hash function, such as SHA-1.
2. Let $z$ be the $L_n$ leftmost bits of $e$, where $L_n$ is the bit length of the group order $n$.
3. Select a random integer $k$ from $[1, n-1]$.
4. Calculate the curve point $(x_1, y_1) = k \times G$.
5. Calculate $r = x_1 \bmod n$. If $r = 0$, go back to step 3.
6. Calculate $s = k^{-1}(z + rd_A) \bmod n$. If $s = 0$, go back to step 3.
7. The signature is the pair $(r, s)$.

**forrás:** http://en.wikipedia.org/wiki/Elliptic_curve_cryptography

# Tranzakciók, blokkok anatómiája

E-GROUP
SOFTWARE & BEYOND

## ECDSA: secp256k1 vs. secp256r1

### 2.4.1 Recommended Parameters secp256k1

The elliptic curve domain parameters over $\mathbb{F}_p$ associated with a Koblitz curve secp256k1 are specified by the sextuple $T = (p, a, b, G, n, h)$ where the finite field $\mathbb{F}_p$ is defined by:

$p$ = FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFE FFFFFC2F

= $2^{256} - 2^{32} - 2^9 - 2^8 - 2^7 - 2^6 - 2^4 - 1$

The curve $E$: $y^2 = x^3 + ax + b$ over $\mathbb{F}_p$ is defined by:

$a$ = 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000

$b$ = 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000007

The base point $G$ in compressed form is:

$G$ = 02 79BE667E F9DCBBAC 55A06295 CE870B07 029BFCDB 2DCE28D9 59F2815B 16F81798

and in uncompressed form is:

$G$ = 04 79BE667E F9DCBBAC 55A06295 CE870B07 029BFCDB 2DCE28D9 59F2815B 16F81798 483ADA77 26A3C465 5DA4FBFC 0E1108A8 FD17B448 A6855419 9C47D08F FB10D4B8

Finally the order $n$ of $G$ and the cofactor are:

$n$ = FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFE BAAEDCE6 AF48A03B BFD25E8C D0364141

$h$ = 01

### 2.4.2 Recommended Parameters secp256r1

The verifiably random elliptic curve domain parameters over $\mathbb{F}_p$ secp256r1 are specified by the sextuple $T = (p, a, b, G, n, h)$ where the finite field $\mathbb{F}_p$ is defined by:

$p$ = FFFFFFFF 00000001 00000000 00000000 00000000 FFFFFFFF FFFFFFFF FFFFFFFF

= $2^{224}(2^{32} - 1) + 2^{192} + 2^{96} - 1$

The curve $E$: $y^2 = x^3 + ax + b$ over $\mathbb{F}_p$ is defined by:

$a$ = FFFFFFFF 00000001 00000000 00000000 00000000 FFFFFFFF FFFFFFFF FFFFFFFC

$b$ = 5AC635D8 AA3A93E7 B3EBBD55 769886BC 651D06B0 CC53B0F6 3BCE3C3E 27D2604B

$E$ was chosen verifiably at random as specified in ANSI X9.62 [X9.62] from the seed:

$S$ = C49D3608 86E70493 6A6678E1 139D26B7 819F7E90

The base point $G$ in compressed form is:

$G$ = 03 6B17D1F2 E12C4247 F8BCE6E5 63A440F2 77037D81 2DEB33A0 F4A13945 D898C296

and in uncompressed form is:

$G$ = 04 6B17D1F2 E12C4247 F8BCE6E5 63A440F2 77037D81 2DEB33A0 F4A13945 D898C296 4FE342E2 FE1A7F9B 8EE7EB4A 7C0F9E16 2BCE3357 6B315ECE CBB64068 37BF51F5

Finally the order $n$ of $G$ and the cofactor are:

$n$ = FFFFFFFF 00000000 FFFFFFFF FFFFFFFF BCE6FAAD A7179E84 F3B9CAC2 FC632551

$h$ = 01

forrás: http://www.secg.org/download/aid-784/sec2-v2.pdf

# Tranzakciók, blokkok anatómiája

E-GROUP
SOFTWARE & BEYOND

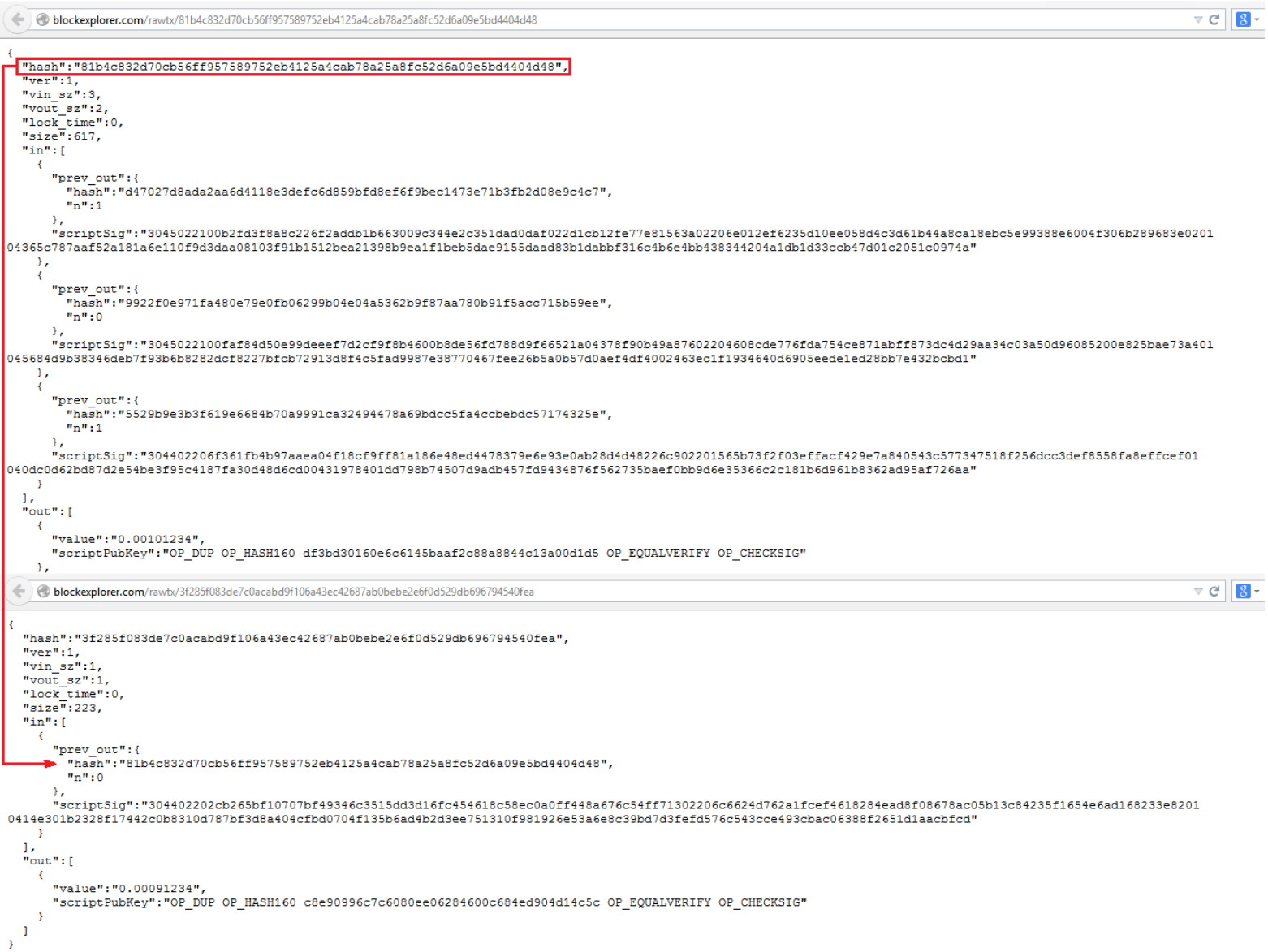
blockexplorer.com/rawtx/81b4c832d70cb56ff957589752eb4125a4cab78a25a8fc52d6a09e5bd4404d48


```
{
  "hash":"81b4c832d70cb56ff957589752eb4125a4cab78a25a8fc52d6a09e5bd4404d48",
  "ver":1,
  "vin_sz":3,
  "vout_sz":2,
  "lock_time":0,
  "size":617,
  "in":[
    {
      "prev_out":{
        "hash":"d47027d8ada2aa6d4118e3defc6d859bfd8ef6f9bec1473e71b3fb2d08e9c4c7",
        "n":1
      },
      "scriptSig":"3045022100b2fd3f8a8c226f2addb1b663009c344e2c351dad0daf022d1cb12fe77e81563a02206e012ef6235d10ee058d4c3d61b44a8ca18ebc5e99388e6004f306b289683e0201
04365c787aaf52a181a6e110f9d3daa08103f91b1512bea21398b9ea1f1beb5dae9155daad83b1dabbf316c4b6e4bb438344204a1db1d33ccb47d01c2051c0974a"
    },
    {
      "prev_out":{
        "hash":"9922f0e971fa480e79e0fb06299b04e04a5362b9f87aa780b91f5acc715b59ee",
        "n":0
      },
      "scriptSig":"3045022100faf84d50e99deeef7d2cf9f8b4600b8de56fd788d9f66521a04378f90b49a87602204608cde776fda754ce871abff873dc4d29aa34c03a50d96085200e825bae73a401
045684d9b38346deb7f93b6b8282dcf8227bfcb72913d8f4c5fad9987e38770467fee26b5a0b57d0aef4df4002463ec1f1934640d6905eede1ed28bb7e432bcbd1"
    },
    {
      "prev_out":{
        "hash":"5529b9e3b3f619e6684b70a9991ca32494478a69bdcc5fa4ccbebdc57174325e",
        "n":1
      },
      "scriptSig":"304402206f361fb4b97aaea04f18cf9ff81a186e48ed4478379e6e93e0ab28d4d48226c902201565b73f2f03effacf429e7a840543c577347518f256dcc3def8558fa8effcef01
040dc0d62bd87d2e54be3f95c4187fa30d48d6cd00431978401dd798b74507d9adb457fd9434876f562735baef0bb9d6e35366c2c181b6d961b8362ad95af726aa"
    }
  ],
  "out":[
    {
      "value":"0.00101234",
      "scriptPubKey":"OP_DUP OP_HASH160 df3bd30160e6c6145baaf2c88a8844c13a00d1d5 OP_EQUALVERIFY OP_CHECKSIG"
    },
```


blockexplorer.com/rawtx/3f285f083de7c0acabd9f106a43ec42687ab0bebe2e6f0d529db696794540fea


```
{
  "hash":"3f285f083de7c0acabd9f106a43ec42687ab0bebe2e6f0d529db696794540fea",
  "ver":1,
  "vin_sz":1,
  "vout_sz":1,
  "lock_time":0,
  "size":223,
  "in":[
    {
      "prev_out":{
        "hash":"81b4c832d70cb56ff957589752eb4125a4cab78a25a8fc52d6a09e5bd4404d48",
        "n":0
      },
      "scriptSig":"304402202cb265bf10707bf49346c3515dd3d16fc454618c58ec0a0ff448a676c54ff71302206c6624d762a1fcef4618284ead8f08678ac05b13c84235f1654e6ad168233e8201
0414e301b2328f17442c0b8310d787bf3d8a404cfbd0704f135b6ad4b2d3ee751310f981926e53a6e8c39bd7d3fefd576c543cce493cbac06388f2651d1aacbfcd"
    }
  ],
  "out":[
    {
      "value":"0.00091234",
      "scriptPubKey":"OP_DUP OP_HASH160 c8e90996c7c6080ee06284600c684ed904d14c5c OP_EQUALVERIFY OP_CHECKSIG"
    }
  ]
}
```

# Tranzakciók, blokkok anatómiája



# Tranzakciók, blokkok anatómiája

E-GROUP
SOFTWARE & BEYOND

blockexplorer.com/rawtx/81b4c832d70cb56ff957589752eb4125a4cab78a25a8fc52d6a09e5bd4404d48

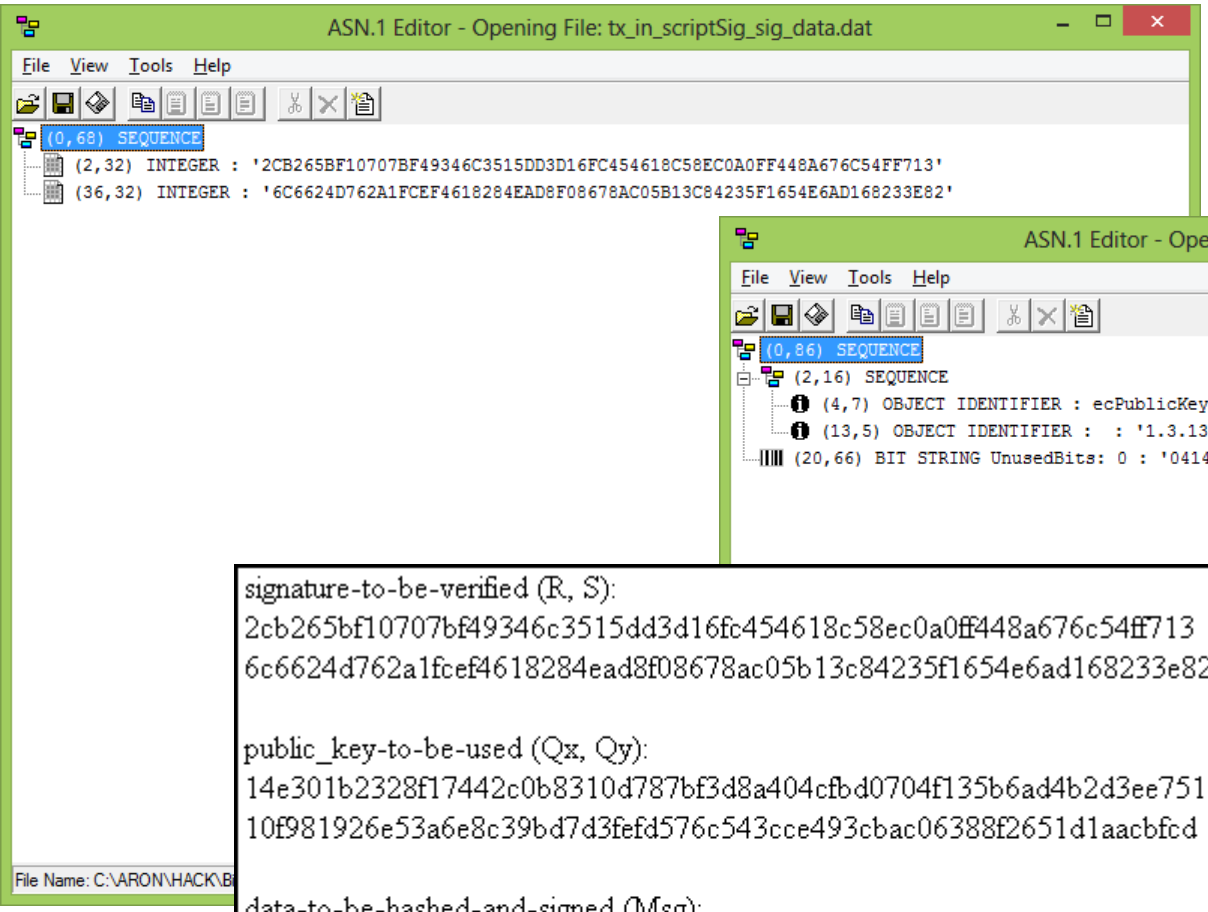

```
{
  "hash":"81b4c832d70cb56ff957589752eb4125a4cab78a25a8fc52d6a09e5bd4404d48",
  "ver":1,
  "vin_sz":3,
  "vout_sz":2,
  "lock_time":0,
  "size":617,
  "in":[
    {
      "prev_out":{
        "hash":"d47027d8ada2aa6d4118e3defc6d859bfd8ef6f9bec1473e71b3fb2d08e9c4c7",
        "n":1
      },
      "scriptSig":"3045022100b2fd3f8a8c226f2addb1b663009c344e2c351dad0daf022d1cb12fe77e81563a02206e012ef6235d10ee058d4c3d61b44a8ca18ebc5e99388e6004f306b289683e0201
04365c787aaf52a181a6e110f9d3daa08103f91b1512bea21398b9ea1f1beb5dae9155daad83b1dabbf316c4b6e4bb438344204a1db1d33ccb47d01c2051c0974a"
    },
    {
      "prev_out":{
        "hash":"9922f0e971fa480e79e0fb06299b04e04a5362b9f87aa780b91f5acc715b59ee",
        "n":0
      },
      "scriptSig":"3045022100faf84d50e99deeef7d2cf9f8b4600b8de56fd788d9f66521a04378f90b49a87602204608cde776fda754ce871abff873dc4d29aa34c03a50d96085200e825bae73a401
045684d9b38346deb7f93b6b8282dcf8227bfcb72913d8f4c5fad9987e38770467fee26b5a0b57d0aef4df4002463ec1f1934640d6905eede1ed28bb7e432bcbd1"
    },
    {
      "prev_out":{
        "hash":"5529b9e3b3f619e6684b70a9991ca32494478a69bdcc5fa4ccbebdc57174325e",
        "n":1
      },
      "scriptSig":"304402206f361fb4b97aaea04f18cf9ff81a186e48ed4478379e6e93e0ab28d4d48226c902201565b73f2f03effacf429e7a840543c577347518f256dcc3def8558fa8effcef01
040dc0d62bd87d2e54be3f95c4187fa30d48d6cd00431978401dd798b74507d9adb457fd9434876f562735baef0bb9d6e35366c2c181b6d961b8362ad95af726aa"
    }
  ],
  "out":[
    {
      "value":"0.00101234",
      "scriptPubKey":"OP_DUP OP_HASH160 df3bd30160e6c6145baaf2c88a8844c13a00d1d5 OP_EQUALVERIFY OP_CHECKSIG"
    },
```

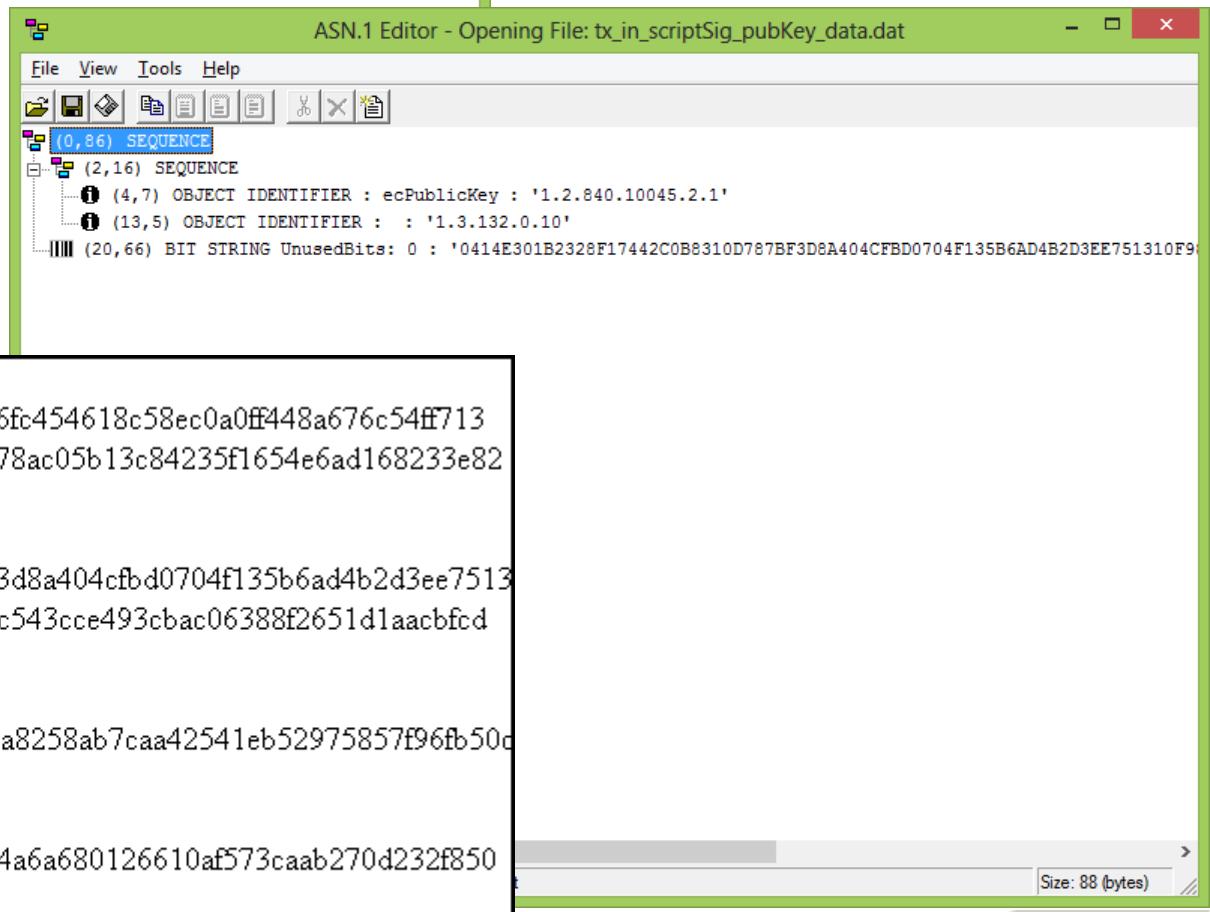

blockexplorer.com/rawtx/3f285f083de7c0acabd9f106a43ec42687ab0bebe2e6f0d529db696794540fea


```
{
  "hash":"3f285f083de7c0acabd9f106a43ec42687ab0bebe2e6f0d529db696794540fea",
  "ver":1,
  "vin_sz":1,
  "vout_sz":1,
  "lock_time":0,
  "size":223,
  "in":[
    {
      "prev_out":{
        "hash":"81b4c832d70cb56ff957589752eb4125a4cab78a25a8fc52d6a09e5bd4404d48",
        "n":0
      },
      "scriptSig":"304402202cb265bf10707bf49346c3515dd3d16fc454618c58ec0a0ff448a676c54ff71302206c6624d762a1fcef4618284ead8f08678ac05b13c84235f1654e6ad168233e8201
0414e301b2328f17442c0b8310d787bf3d8a404cfbd0704f135b6ad4b2d3ee751310f981926e53a6e8c39bd7d3fefd576c543cce493cbac06388f2651d1aacbfcd"
    }
  ],
  "out":[
    {
      "value":"0.00091234",
      "scriptPubKey":"OP_DUP OP_HASH160 c8e90996c7c6080ee06284600c684ed904d14c5c OP_EQUALVERIFY OP_CHECKSIG"
    }
  ]
}
```

# Tranzakciók, blokkok anatómiája

E-GROUP
SOFTWARE & BEYOND




signature-to-be-verified (R, S):
2cb265bf10707bf49346c3515dd3d16fc454618c58ec0a0ff448a676c54ff713
6c6624d762a1fcef4618284ead8f08678ac05b13c84235f1654e6ad168233e82

public_key-to-be-used (Qx, Qy):
14e301b2328f17442c0b8310d787bf3d8a404cfbd0704f135b6ad4b2d3ee7513
10f981926e53a6e8c39bd7d3fefd576c543cce493cbac06388f2651d1aacbfcd

data-to-be-hashed-and-signed (Msg):
0100000001484d40d45b9ea0d652fca8258ab7caa42541eb52975857f96fb50c

data-to-be-signed (hash(Msg)):
5fda68729a6312e17e641e9a49fac2a4a6a680126610af573caab270d232f850

Signature tested as expected: received true, expected true.

# Hibák, ötletek

E-GROUP
SOFTWARE & BEYOND

ECDSA és secp256k1 (Koblitz-görbe)

a) nincs elterjedt HW támogatás kulcstároláshoz
pl. Thales nCipher HSM-ek csak secp256r1 görbét támogatnak,
ezért sem lehetett HW-alapú kulcstárolás a hack-elt, online BitCoin pénztárca-szolgáltatóknál (ld. bitcash.cz, inputs.io, bitcoinica.com)

egyedi HW megoldások léteznek (pl. SatoshiLabs Trezor, Hardbit)

forrás: http://bitcoin.hu/napokon-belul-uj-hardware-alapu-bitcoin-penztarcak-jelennek-meg-a-piacon/

# Hibák, ötletek

E-GROUP
SOFTWARE & BEYOND

## ECDSA és secp256k1 (Koblitz-görbe)

**b) D. J. Bernstein szerint bizonyos támadások ellen nem védett (Safe? False):**

| | | Parameters: | | | ECDLP security: | | | | ECC security: | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Curve | Safe? | field | equation | base | rho | transfer | disc | rigid | ladder | twist | complete | ind |
| Anomalous | False | True✓ | True✓ | True✓ | True✓ | False | False | True✓ | False | False | False | False |
| M-221 | True✓ | True✓ | True✓ | True✓ | True✓ | True✓ | True✓ | True✓ | True✓ | True✓ | True✓ | True✓ |
| E-222 | True✓ | True✓ | True✓ | True✓ | True✓ | True✓ | True✓ | True✓ | True✓ | True✓ | True✓ | True✓ |
| NIST P-224 | False | True✓ | True✓ | True✓ | True✓ | True✓ | True✓ | False | False | False | False | False |
| Curve1174 | True✓ | True✓ | True✓ | True✓ | True✓ | True✓ | True✓ | True✓ | True✓ | True✓ | True✓ | True✓ |
| Curve25519 | True✓ | True✓ | True✓ | True✓ | True✓ | True✓ | True✓ | True✓ | True✓ | True✓ | True✓ | True✓ |
| BN(2,254) | False | True✓ | True✓ | True✓ | True✓ | False | False | True✓ | False | False | False | False |
| brainpoolP256t1 | False | True✓ | True✓ | True✓ | True✓ | True✓ | True✓ | True✓ | False | False | False | False |
| ANSSI FRP256v1 | False | True✓ | True✓ | True✓ | True✓ | True✓ | True✓ | False | False | False | False | False |
| NIST P-256 | False | True✓ | True✓ | True✓ | True✓ | True✓ | True✓ | False | False | True✓ | False | False |
| secp256k1 | False | True✓ | True✓ | True✓ | True✓ | True✓ | False | True✓ | False | True✓ | False | False |
| E-382 | True✓ | True✓ | True✓ | True✓ | True✓ | True✓ | True✓ | True✓ | True✓ | True✓ | True✓ | True✓ |
| M-383 | True✓ | True✓ | True✓ | True✓ | True✓ | True✓ | True✓ | True✓ | True✓ | True✓ | True✓ | True✓ |
| Curve383187 | True✓ | True✓ | True✓ | True✓ | True✓ | True✓ | True✓ | True✓ | True✓ | True✓ | True✓ | True✓ |
| brainpoolP384t1 | False | True✓ | True✓ | True✓ | True✓ | True✓ | True✓ | True✓ | False | True✓ | False | False |
| NIST P-384 | False | True✓ | True✓ | True✓ | True✓ | True✓ | True✓ | False | False | True✓ | False | False |
| Curve41417 | True✓ | True✓ | True✓ | True✓ | True✓ | True✓ | True✓ | True✓ | True✓ | True✓ | True✓ | True✓ |
| Ed448-Goldilocks | True✓ | True✓ | True✓ | True✓ | True✓ | True✓ | True✓ | True✓ | True✓ | True✓ | True✓ | True✓ |
| M-511 | True✓ | True✓ | True✓ | True✓ | True✓ | True✓ | True✓ | True✓ | True✓ | True✓ | True✓ | True✓ |
| E-521 | True✓ | True✓ | True✓ | True✓ | True✓ | True✓ | True✓ | True✓ | True✓ | True✓ | True✓ | True✓ |

disc: CM field discriminants
"SafeCurves requires the absolute value of this complex-multiplication field discriminant D to be larger than 2^100."

ladder: Ladders
"SafeCurves requires curves to support simple, fast, constant-time single-coordinate single-scalar multiplication [...]."

complete: Completeness
"SafeCurves requires curves to support [...] complete multiplication."

ind: Indistinguishability from uniform random strings
"Standard representations of elliptic-curve points are easily distinguishable from uniform random strings. This poses a problem for many cryptographic protocols using elliptic curves: censorship-circumvention protocols, for example, and password-authenticated key-exchange protocols."

**forrás:** http://safecurves.cr.yp.to/

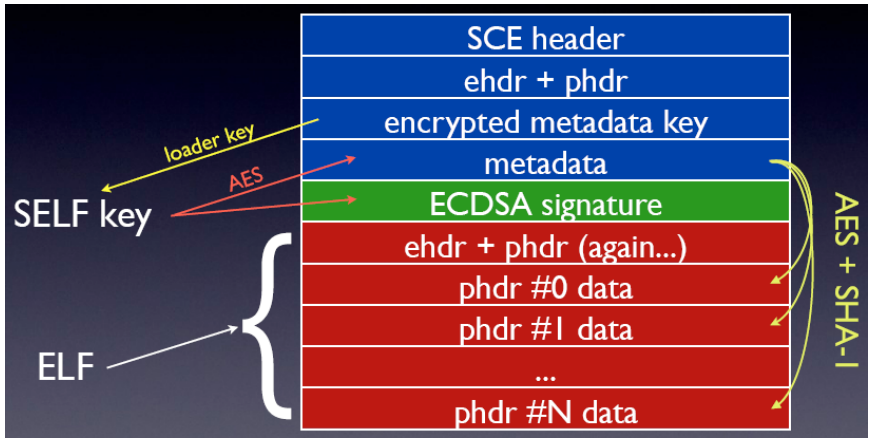
# Hibák, ötletek

E-GROUP
SOFTWARE & BEYOND

## ECDSA és PRNG

Az ECDSA algoritmus esetében nem csak a kulcspár létrehozásához van szükség PRNG adatra (mint pl. RSA algoritmusnál), hanem az aláírások létrehozásához is. Kérdéses azonban, hogy a klienseknél, a tranzakciók aláírásához milyen minőségű PRNG áll rendelkezésre? (ld. Android JCA PRNG hibája, amit pont a BitCoin csapata fedezett fel, 2013. augusztus 15.)

A rossz minőségű PRNG és ECDSA aláírások kihasználására jó példa volt a Sony PlayStation3 esete (ld. fail0verflow előadása, 2010. december 29.).




forrás: http://www.youtube.com/watch?v=4loZGYqaZ7I

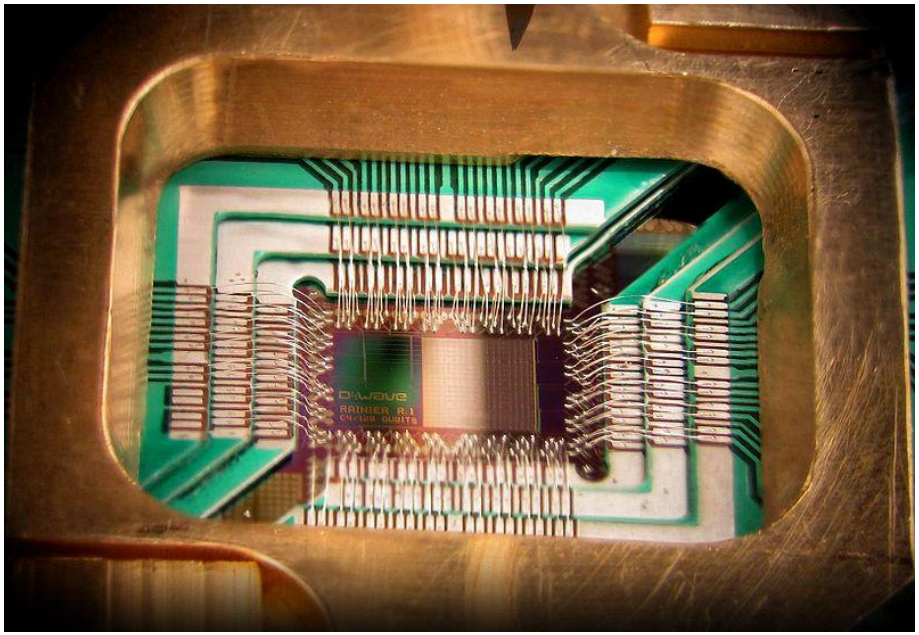
# Hibák, ötletek

E-GROUP
SOFTWARE & BEYOND

**ECDSA és kvantumszámítógép**

A kvantumszámítógépen futtatott Shor és módosított Shor algoritmus érinteni fogja mind az RSA, mind az ECDSA algoritmus alapjait (prímfaktorizáció, diszkrét logaritmus probléma).

Hosszabb távon (10+ év) szükség lesz pqcrypto algoritmusok alkalmazására a crypto currency megoldásoknál.



# Hibák, ötletek

E-GROUP
SOFTWARE & BEYOND

SHA-256 vagy scrypt

Az SHA-256 algoritmus esetében elméletileg könnyebben fordulhat elő az „>50% attack” - vagyis amikor a támadó birtokolja a számítási kapacitások több, mint felét, és ezáltal tudja manipulálni a rendszert (pl. más láncok propagálása, „double spending”) -, mint scrypt esetében (ld. ASIC vs. memóriaigényes műveletek). Ennek a lehetősége azonban csak kisebb közösségeknél lehet valós veszély, másrészt a scrypt esetében is találtak már egyszerűsítési lehetőségeket, amelyek csökkentik a két modell közötti különbséget.

forrás: http://blog.ircmaxell.com/2014/03/why-i-dont-recommend-scrypt.html

# Hibák, ötletek

E-GROUP
SOFTWARE & BEYOND

**döntési logika**

**A „selfish mining strategy” támadásról szóló tanulmányt 2013. november 1-én tették közzé, amely a BitCoin protokolljában levő, tranzakciókat, blokkokat érintő döntési logika hibáját használja ki. A nem nyilvánosságra hozott tranzakciók, blokkok továbbnövelésével és alternatív blokkok kialakításával lehetőség van „double spending” támadás végrehajtására. A jelenlegi – csak a tranzakciók száma, blokkok hossza – alapján történő döntés helyett más logikára lesz szükség (pl. kriptográfiai időbélyeg, megbízható harmadik felektől, jogi értelemben vett időbélyeg szolgáltatóktól).**

**forrás: http://arxiv.org/pdf/1311.0243v5.pdf**

# Köszönöm a figyelmet!

eDOX™ for Office System

iDServer

transform

DocMark

Secure and Authentic Paper Documents

mailto: aron.szabo@egroup.hu

web: http://www.egroup.hu