

The Σ RG0 Yellowpaper

Alexander Chepurnoy

Dmitry Meshkov

February 22, 2018

Contents

| | | |
|-------|--------------------------------------------------------------------------------------|----|
| 0.1 | Introduction | 1 |
| 0.1.1 | Multiple Modes | 1 |
| 0.1.2 | Full-Node Mode | 2 |
| 0.1.3 | Pruned Full-Node Mode | 3 |
| 0.1.4 | Light Full-Node Mode | 4 |
| 0.1.5 | Light-SPV Mode | 5 |
| 0.1.6 | Mode-Related Settings | 5 |
| 0.2 | Ergo Block Structure | 5 |
| 0.2.1 | ErgoMinimalHeader is a minimal data amount, required to calculate blockId: | 5 |
| 0.2.2 | ErgoHeader is a header to keep in History and transfer: | 6 |
| 0.3 | Ergo Modifiers Processing | 6 |
| 0.3.1 | Modifiers processing | 7 |
| 0.3.2 | bootstrap | 7 |
| 0.3.3 | Regular | 9 |
| 0.4 | Multiple Modes | 9 |
| 0.4.1 | Full-Node Mode | 9 |
| 0.4.2 | Pruned Full-Node Mode | 10 |
| 0.4.3 | Light Full-Node Mode | 10 |
| 0.4.4 | Light-SPV Mode | 10 |
| 0.4.5 | Mode-Related Settings | 10 |
| 0.5 | Ergo Block Structure | 11 |
| 0.6 | Ergo Modifiers Processing | 11 |
| 0.6.1 | Modifiers processing | 11 |
| 0.6.2 | Bootstrap | 11 |
| 0.6.3 | regular | 11 |
| 0.7 | Components | 12 |
| 0.7.1 | History | 12 |
| 0.7.2 | State | 12 |
| 0.7.3 | Memory Pool | 12 |
| 0.8 | Transactional Language | 12 |
| 0.9 | Protocol Updates | 12 |
| 0.10 | Peer-to-Peer Network | 12 |
| | References | 12 |

Introduction

Multiple Modes

Ergo (since the very first testing network Testnet0) is supporting multiple security models. In addition to full node mode, which is similar to Bitcoin fullnode, Ergo reference implementation will support Light-SPV, Light-Fullnode, Pruned-Fullnode modes.

Full-Node Mode

Like in Bitcoin, a full node is storing all the full blocks since genesis block. Full node checks proofs of work, linking structure correctness (parent block id, interlink elements), and all the transactions in all the blocks. A fullnode is storing all the full blocks forever. It is also holding full UTXO set to be able to validate an arbitrary transaction. The only optimization a fullnode is doing is that is is skipping downloading and checking AD-transformation block part (see below in the "Light-Fullnode" section). For full node regime, modifiers precessing workflow is as follows:

1. Send ErgoSyncInfo message to connected peers.
2. Get response with INV message, containing ids of blocks, better than our best block.
3. Request headers for all ids from 2.
4. On receiving header:

```
if(History.apply(header).isSuccess) {  
    if(!isInitialBootstrapping) Broadcast INV for this header  
    Request transaction ids from this block  
} else {  
    blacklist peer  
}
```

5. On receiving transaction ids from header:

```
Mempool.apply(transactionIdsForHeader)  
transactionIdsForHeader.filter(txId => !MemPool.contains(txId)).foreach { txId =>  
    request transaction with txId  
}
```

6. On receiving a transaction:

```
if(Mempool.apply(transaction).isSuccess) {  
    if(!isInitialBootstrapping) Broadcast INV for this transaction  
    Mempool.getHeadersWithAllTransactions { BlockTransactions =>  
        GOTO 7  
    }  
}
```

7. Now we have BlockTransactions: all transactions corresponding to some Header

```
if(History.apply(BlockTransactions) == Success(ProgressInfo)) {  
    if(!isInitialBootstrapping) Broadcast INV for BlockTransactions  
    /*We should notify our neighbours, that now we have all the transactions  
    State apply modifiers (may be empty for block in a fork chain)  
    and generate ADProofs for them.  
    TODO requires different interface from scorex-core,  
    because it should return ADProofs  
    TODO when mininal state apply Progress info,  
    it may also create UTXOSnapshot  
    (e.g. every 30000 blocks like in Ethereum).  
    This UTXOSnapshot should be required for mining by Rollerchain*/  
    if(State().apply(ProgressInfo) == Success((newState, ADProofs))) {  
        if("mode"=="full" || "mode"=="pruned-full") ADProofs.foreach ( ADProof => History.apply(ADProof)  
        if("mode"=="pruned-full" || "mode"=="light-full") drop BlockTransactions and ADProofs older  
    } else {
```

```

        //Drop Header from history, because it's transaction sequence is not valid
        History.drop(BlockTransactions.headerId)
    }
} else {
    blacklist peer who sent header
}

```

Pruned Full-Node Mode

This mode is similar to fast-sync in Geth or Grothendieck, warp-mode in Parity (all the three are Ethereum protocol clients), but makes more aggressive optimizations. In particular, a pruned-fullnode is not downloading and storing full blocks not residing in a target blockchain suffix, and also removing full blocks going out of the suffix. In detail, a pruned client is downloading all the headers, then, by using them, it checks proofs-of-work and linking structure(or parent id only?). Then it downloads a UTXO snapshot for some height from its peers. Finally, full blocks after the snapshot are to be downloaded and applied to get a current UTXO set. A pruned fullnode is also skipping AD-transformation block part, like a fullnode. Additional setting: "suffix" - how much full blocks to store(w. some minimum set?). Its regular modifiers processing is the same as for fullnode regime, while its bootstrap process is different:

1. Send ErgoSyncInfo message to connected peers.
2. Get response with INV message, containing ids of blocks, better than our best block.
3. Request headers for all ids from 2.
4. On receiving header:

```

if(History.apply(header).isSuccess) {
    if(!(localScore == networkScore)) GOTO 1
    else GOTO 5
} else {
    blacklist peer
}

```

5. Request historical UTXOManifest for at least BlocksToKeep back.
6. On receiving UTXOSnapshotManifest:

```

UTXOSnapshotManifest.chunks.foreach { chunk =>
    request chunk from sender() //Or from random fullnode
}

```

7. On receiving UTXOSnapshotChunk:

```

State.applyChunk(UTXOSnapshotChunk) match {
    case Success(Some(newMinimalState)) => GOTO 8
    case Success(None) => stay at 7
    /*we need more chunks to construct state.
    TODO periodically request missed chunks*/
    case Failure(e) => ???
    //UTXOSnapshotChunk or constcuted state roothash is invalid
}

```

8. Request BlockTransactions starting from State we have

```

History.headersStartingFromId(State.headerId).foreach { header =>
    send message(GetBlockTransactionsForHeader(header)) to Random fullnode
}

```

9. On receiving BlockTransactions: same as in Fullnode.7 .
10. Operate as Fullnode.

Light Full-Node Mode

This mode is based on an idea to use a 2-party authenticated dynamic dictionary built on top of UTXO set. A light-fullnode holds only a root digest of a dictionary. It check all the full blocks, or some suffix of the full blockchain, depending on setting, thus starting from a trusted pre-genesis digest or some digest in the blockchain. A light-fullnode is using AD-transformations (authenticated dictionary transformations) block section containing batch-proof for UTXO transformations to get a new digest from an old one. It also checks all the transactions, but doesn't store anything but a single digest for that. Details can be found in the paper <https://eprint.iacr.org/2016/994>.

Additional settings : "depth" - from which block in the past to check transactions (if 0, then go from genesis).

"additional-checks" - light-fullnode trusts previous digest and checks current digest validity by using the previous one as well as AD-transformations.

"additional-depth" - depth to start additional checks from.

1. Send ErgoSyncInfo message to connected peers.
2. Get response with INV message, containing ids of blocks, better than our best block.
3. Request headers for all ids from 2.
4. On receiving header:

```
if(History.apply(header).isSuccess) {
    if(!(localScore == networkScore)) GOTO 1
    else GOTO 5
} else {
    blacklist peer
}
```

5. Request BlockTransactions and ADProofs starting from BlocksToKeep back in History (just 1 last header after node bootstrapping):

```
History.lastBestHeaders(BlocksToKeep).foreach { header =>
    send message(GetBlockTransactionsForHeader(header)) to Random fullnode
    send message(GetAdProofsHeader(header)) to Random fullnode
}
```

6. On receiving modifier BlockTransactions or ADProofs:

```
if(History.apply(modifier) == Success(ProgressInfo)) {
    /* TODO if history now contains both ADProofs and BlockTransactions,
    it should return ProgressInfo with both of them, otherwise
    it should return empty ProgressInfo */
    if(State().apply(ProgressInfo) == Success((newState, ADProofs)))
    {
        if("mode"=="pruned-full") drop BlockTransactions and ADProofs older than BlocksToKeep
    }
    else {
        /*Drop Header from history, because it's transaction sequence is not valid*/
        History.drop(BlockTransactions.headerId)
    }
}
```

Light-SPV Mode

This mode is not about checking any full blocks. Like in Bitcoin, an SPV node is downloading block headers only, and so checks only proofs of work and links. Unlike Bitcoin's SPV, the Light-SPV is downloading and checking not all the headers but a sublinear(in blockchain length) number of them(in benchmarks, this is about just tens of kilobytes instead of tens or hundreds of megabytes for Bitcoin/Ethereum). Light-SPV mode is intended to be useful for mobile phones and low-end hardware.

Bootstrap

1. Send GetPoPoWProof for all connections.
2. On receive PoPoWProof apply it to History (History should be able to determine, whether this PoPoWProof is better, than it's current best header chain).
3. GOTO regular regime.

Regular

1. Send ErgoSyncInfo message to connected peers
2. Get response with INV message, containing ids of blocks, better than our best block.
3. Request headers for all ids from 2.
4. On receiving header:

```
if(History.apply(header).isSuccess) {  
    State.apply(header) // just change state roothash  
    if(!isInitialBootstrapping) Broadcast INV for this header  
} else {  
    blacklist peer  
}
```

Mode-Related Settings

Ergo has the following settings determines a mode:

- ADState: Boolean - keeps state roothash only.
- VerifyTransactions: Boolean - download block transactions and verify them (requires BlocksToKeep == 0 if disabled).
- PoPoWBootstrap: Boolean - download PoPoW proof only
- BlocksToKeep: Int - number of last blocks to keep with transactions, for all other blocks it keep header only. Keep all blocks from genesis if negative
- MinimalSuffix: Int - minimal suffix size for PoPoW proof (may be pre-defined constant).

‘if(VerifyTransactions == false) require(BlocksToKeep == 0)‘ Mode from `***multimode.md***` can be determined as follows:

Ergo Block Structure

ErgoMinimalHeader is a minimal data amount, required to calculate blockId:

payloadRootHash: Array[Byte] - root hash (or simple hash of all payload data) of block payload. nonce: Int - field to iterate and generate valid PoW.

ErgoHeader is a header to keep in History and transfer:

| Field | Size | Description |
|------------------|------|-----------------------------------------------------------------|
| version | 1 | block version, to be increased on every soft- and hardfork |
| parentId | 32 | id of parent block |
| interlinksRoot | 32 | root hash of interlinks structure |
| ADProofsRoot | 32 | hash of ADProofs for transactions in a block |
| stateRoot | 32 | root hash (for an AVL+ tree) of a state after block application |
| transactionsRoot | 32 | root hash (for a Merkle tree) of transactions in a block |
| timestamp | 8 | block timestamp(in milliseconds since beginning of Unix Epoch) |
| nonce | 8 | Proof-of-Work nonce |

Some of this fields may be calculated by node by itself:

- parentId: if(status==bootstrap AND PoPoWBootstrap == false).
- interlinksRoot: if(PoPoWBootstrap == false).
- ADProofsRoot: if(status==regular AND ADState==false AND BlocksToKeep>0).
- stateRoot: if(status==regular AND ADState==false AND BlocksToKeep>0).

Ergo Modifiers Processing

This section describes processing algorithm for Ergo modifiers in all security modes. Unlike most of blockchain systems, Ergo have the following types of **modifiers**: In-memory:

1. In-memory:

- Transaction - in-memory modifier.
- TransactionIdsForHeader - ids of transactions in concrete block.
- UTXOSnapshotManifest - ids of UTXO chunks and

2. Persistent:

- BlockTransactions - Sequence of transactions, corresponding to 1 block.
- ADProofs - proof of transaction correctness relative to corresponding UTXO.
- Header, that contains data required to verify PoW, link to previous block, state root hash and root hash to it's payload (BlockTransactions, ADProofs, Interlinks ...).
- UTXOSnapshotChunk - part of UTXO.
- PoPoWProof

Ergo will have the following parameters, that will determine concrete security regime:

- ADState: Boolean - keep state roothash only.
- VerifyTransactions: Boolean - download block transactions and verify them (requires BlocksToKeep == 0 if disabled).
- PoPoWBootstrap: Boolean - download PoPoW proof only.
- BlocksToKeep: Int - number of last blocks to keep with transactions, for all other blocks it keep header only. Keep all blocks from genesis if negative.

- MinimalSuffix: Int - minimal suffix size for PoPoW proof (may be pre-defined constant).

```
if(VerifyTransactions == false) require(BlocksToKeep == 0)
```

Mode from "multimode.md" can be determined as follows:

```
mode = if(ADState == false && VerifyTransactions == true
&& PoPoWBootstrap == false && BlocksToKeep < 0) "full"
else if(ADState == false && VerifyTransactions == true
&& PoPoWBootstrap == false && BlocksToKeep >= 0) "pruned-full"
else if(ADState == true && VerifyTransactions == true
&& PoPoWBootstrap == false) "light-full"
else if(ADState == true && VerifyTransactions == false
&& PoPoWBootstrap == true && BlocksToKeep == 0) "light-spv"
else if(ADState == true && VerifyTransactions == true
&& PoPoWBootstrap == true && BlocksToKeep == 0) "light-full-PoPoW"
else //Other combinations are possible
```

Modifiers processing

```
def updateHeadersChainToBestInNetwork() = {
  1.2.1. Send ErgoSyncInfo message to connected peers
  1.2.2. Get response with INV message,
  containing ids of blocks, better than our best block
  1.2.3. Request headers for all ids from 1.2.2.
  1.2.4. On receiving header
    if(History.apply(header).isSuccess) {
      if(!(localScore == networkScore)) GOTO 1.2.1
    } else {
      blacklist peer
      GOTO 1.2.1
    }
}
```

bootstrap

Download headers:

```
if(PoPoW) {
  1.1.1. Send GetPoPoWProof(suffix = Max(MinimalSuffix ,BlocksToKeep)) for all connections
  1.1.2. On receive PoPoWProof apply it to History
  /*
  History should be able to determine,
  whether this PoPoWProof is better, than it's current best header chain */
} else {
  updateHeadersChainToBestInNetwork()
}
```

Download initial State to start process transactions:

```
if(ADState == true) {
  Initialize state with state roothash from block header BlocksToKeep ago
} else if(BlocksToKeep < 0 || BlocksToKeep > History.headersHeight) {
  Initialize state with genesis State
} else {
  /*
```



```

We need to download full state BlocksToKeep back in history
TODO what if we can download state only "BlocksToKeep - N"
or "BlocksToKeep + N" blocks back?
*/
2.1. Request historical UTXOSnapshotManifest for at least BlocksToKeep back
2.2. On receiving UTXOSnapshotManifest:
    UTXOSnapshotManifest.chunks.foreach ( chunk => request chunk from sender()
/*Or from random fullnode*/
2.3. On receiving UTXOSnapshotChunk
State.applyChunk(UTXOSnapshotChunk) match {
    case Success(Some(newMinimalState)) => GOTO 3
    case Success(None) => stay at 2.3
    /*we need more chunks to construct state. TODO periodically request missed chunks*/
    case Failure(e) => ???
    /*UTXOSnapshotChunk or constucted state roothash is invalid*/
}
}

```

Update State to best headers height:

```

if(State.bestHeader == History.bestHeader) {
    //Do nothing, State is already updated
} else if(VerifyTransactions == false) {
    /*Just update State rootshash to best header in history*/
    State.setBestHeader(History.bestHeader)
} else {
    /*we have headers chain better then full block */
    3.1.
        assert(history contains header chain from State.bestHeader to History.bestHeaders)
        History.continuation(from = State.bestHeader, size = ???).get.foreach { header =>
            sendToRandomFullNode(GetBlockTransactionsForHeader(header))
            if(ADState == true) sendToRandomFullNode(GetADProofsForHeader(header))
        }
    3.2. On receiving modifiers ADProofs or BlockTransactions
        /*TODO History should return non-empty ProgressInfo
        only if it contains both ADProofs and BlockTransactions,
        or it contains BlockTransactions and ADState==false*/
        if(History.apply(modifier) == Success(ProgressInfo)) {
            if(State().apply(ProgressInfo) == Success((newState, ADProofs))) {
                if(ADState==false) ADProofs.foreach ( ADProof => History.apply(ADProof))
                if(BlocksToKeep>=0)
                    /*remove BlockTransactions and ADProofs older than BlocksToKeep from history*/
            } else {
                /*Drop Header from history,
                because it's transaction sequence is not valid*/
                History.drop(modifier.headerId)
            }
        } else {
            blacklistPeer
        }
        GOTO 3
    }
}

```

GOTO regular mode.

Regular

Two infinite loops in different threads with the following functions inside:

1. UpdateHeadersChainToBestInNetwork()
2. Download and update full blocks when needed

```
if(State.bestHeader == History.bestHeader) {  
    //Do nothing, State is already updated  
} else if(VerifyTransactions == false) {  
    //Just update State rootshash to best header in history  
    State.setBestHeader(History.bestHeader)  
} else {  
    //we have headers chain better then full block  
    3.1. Request transaction ids from all headers without transactions  
    assert(history contains header chain from State.bestHeader to History.bestHeaders)  
    History.continuation(from = State.bestHeader, size = ???).get.foreach { header =>  
        sendToRandomFullNode(GetTransactionIdsForHeader(header))  
        if(ADState == true) sendToRandomFullNode(GetADProofsForHeader(header))  
    }  
    3.2. On receiving TransactionIdsForHeader:  
    Mempool.apply(TransactionIdsForHeader)  
    TransactionIdsForHeader.filter(txId => !Mempool.contains(txId)).foreach { txId =>  
        request transaction with txId  
    }  
    3.3. On receiving a transaction:  
    if(Mempool.apply(transaction).isSuccess) {  
        Broadcast INV for this transaction  
        Mempool.getHeadersWithAllTransactions { BlockTransactions =>  
            GOTO 3.4 //now we have BlockTransactions  
        }  
    }  
    3.4. (same as 3.2. from bootstrap)  
}
```

Multiple Modes

Ergo (since the very first testing network Testnet0) is supporting multiple security models. In addition to fullnode mode, which is similar to Bitcoin fullnode, Ergo reference implementation will support Light-SPV, Light-Fullnode, Pruned-Fullnode modes.

Full-Node Mode

Like in Bitcoin, a full node is storing all the full blocks since genesis block. Full node checks proofs of work, linking structure correctness (parent block id, interlink elements), and all the transactions in all the blocks. A fullnode is storing all the full blocks forever. It is also holding full UTXO set to be able to validate an arbitrary transaction.

The only optimization a fullnode is doing is that is is skipping downloading and checking AD-transformation block part (see below in the "Light-Fullnode" section).

Pruned Full-Node Mode

This mode is similar to fast-sync in Geth or Grothendieck, warp-mode in Parity (all the three are Ethereum protocol clients), but makes more aggressive optimizations. In particular, a pruned-fullnode is not downloading and storing full blocks not residing in a target blockchain suffix, and also removing full blocks going out of the suffix.

In detail, a pruned client is downloading all the headers, then, by using them, it checks proofs-of-work and linking structure(or parent id only?). Then it downloads a UTXO snapshot for some height from its peers. Finally, full blocks after the snapshot are to be downloaded and applied to get a current UTXO set.

A pruned fullnode is also skipping AD-transformation block part, like a fullnode.

Additional setting: "suffix" - how much full blocks to store(w. some minimum set?)

Light Full-Node Mode

This mode is based on an idea to use a 2-party authenticated dynamic dictionary built on top of UTXO set. A light-fullnode holds only a root digest of a dictionary. It check all the full blocks, or some suffix of the full blockchain, depending on setting, thus starting from a trusted pre-genesis digest or some digest in the blockchain. A light-fullnode is using AD-transformations (authenticated dictionary transformations) block section containing batch-proof for UTXO transformations to get a new digest from an old one. It also checks all the transactions, but doesn't store anything but a single digest for that. Details can be found in the paper <https://eprint.iacr.org/2016/994>.

Additional settings : "depth" - from which block in the past to check transactions (if 0, then go from genesis)

"additional-checks" - light-fullnode trusts previous digest and checks current digest validity by using the previous one as well as AD-transformations.

"additional-depth" - depth to start additional checks from.

Light-SPV Mode

This mode is not about checking any full blocks. Like in Bitcoin, an SPV node is downloading block headers only, and so checks only proofs of work and links. Unlike Bitcoin's SPV, the Light-SPV is downloading and checking not all the headers but a sublinear(in blockchain length) number of them(in benchmarks, this is about just tens of kilobytes instead of tens or hundreds of megabytes for Bitcoin/Ethereum).

Light-SPV mode is intended to be useful for mobile phones and low-end hardware.

Mode-Related Settings

Ergo has the following settings determines a mode:

- ADState: Boolean - keeps state roothash only
- VerifyTransactions: Boolean - download block transactions and verify them (requires BlocksToKeep == 0 if disabled)
- PoPoWBootstrap: Boolean - download PoPoW proof only
- BlocksToKeep: Int - number of last blocks to keep with transactions, for all other blocks it keep header only. Keep all blocks from genesis if negative
- MinimalSuffix: Int - minimal suffix size for PoPoW proof (may be pre-defined constant)

‘if(VerifyTransactions == false) require(BlocksToKeep == 0)’

Mode from `**"multimode.md"` can be determined as follows:

Ergo Block Structure

ErgoMinimalHeader is a minimal data amount, required to calculate blockId:

payloadRootHash: Array[Byte] - root hash (or simple hash of all payload data) of block payload nonce:
Int - field to iterate and generate valid PoW

ErgoHeader is a header to keep in History and transfer:

| Field | Size | Description |
|------------------|------|-----------------------------------------------------------------|
| version | 1 | block version, to be increased on every soft- and hardfork |
| parentId | 32 | id of parent block |
| interlinksRoot | 32 | root hash of interlinks structure |
| ADProofsRoot | 32 | hash of ADProofs for transactions in a block |
| stateRoot | 32 | root hash (for an AVL+ tree) of a state after block application |
| transactionsRoot | 32 | root hash (for a Merkle tree) of transactions in a block |
| timestamp | 8 | block timestamp(in milliseconds since beginning of Unix Epoch) |
| nonce | 8 | Proof-of-Work nonce |

Some of this fields may be calculated by node by itself: - parentId: $if(status == bootstrap \wedge PoPoWBootstrap == false)$ (kushti: ???) - interlinksRoot: $if(PoPoWBootstrap == false)$ - ADProofsRoot: $if(status == regular \wedge ADState == false \wedge BlocksToKeep > 0)$ - stateRoot: $if(status == regular \wedge ADState == false \wedge BlocksToKeep > 0)$

Ergo Modifiers Processing

This section describes processing algorithm for Ergo modifiers in all security modes.

Unlike most of blockchain systems, Ergo have the following types of **modifiers**:

In-memory:

- *Transaction* - in-memory modifier
- *TransactionIdsForHeader* - ids of transactions of a block
- *UTXOSnapshotManifest* - ids of UTXO chunks and

Persistent:

- *BlockTransactions* - Sequence of transactions, corresponding to 1 block.
- *ADProofs* - proof of transaction correctness relative to corresponding UTXO
- *Header* , that contains data required to verify PoW, link to previous block, state root hash and root hash to it's payload (BlockTransactions, ADProofs, Interlinks ...)
- *UTXOSnapshotChunk* - part of UTXO
- *PoPoWProof*

Modifiers processing

Bootstrap

2.Download initial State to start process transactions:

- 3.Update State to best headers height
4. GOTO regular mode

regular

Two infinite loops in different threads with the following functions inside:

1. *updateHeadersChainToBestInNetwork()*
- 2.Download and update full blocks when needed

Components

History

State

Memory Pool

Transactional Language

Protocol Updates

Peer-to-Peer Network