

# PEPITAS CRYPTOCURRENCY

Generated by Doxygen 1.8.17



<b>1 PEPITAS</b>	<b>1</b>
1.1 CODING STYLE	1
1.1.1 Coding case	1
1.1.2 Tests	1
<b>2 Data Structure Index</b>	<b>3</b>
2.1 Data Structures	3
<b>3 File Index</b>	<b>5</b>
3.1 File List	5
<b>4 Data Structure Documentation</b>	<b>7</b>
4.1 Block Struct Reference	7
4.1.1 Detailed Description	7
4.1.2 Field Documentation	7
4.1.2.1 block_data	7
4.1.2.2 block_signature	8
4.1.2.3 chunk_id	8
4.1.2.4 signature_len	8
4.2 BlockData Struct Reference	8
4.2.1 Detailed Description	8
4.2.2 Field Documentation	9
4.2.2.1 block_timestamp	9
4.2.2.2 height	9
4.2.2.3 magic	9
4.2.2.4 nb_transactions	9
4.2.2.5 previous_block_hash	9
4.2.2.6 transactions	10
4.2.2.7 validator_public_key	10
4.3 ChunkBlockchain Struct Reference	10
4.3.1 Detailed Description	10
4.3.2 Field Documentation	10
4.3.2.1 chunk	10
4.3.2.2 chunk_nb	11
4.4 client_connection Struct Reference	11
4.4.1 Detailed Description	11
4.4.2 Field Documentation	11
4.4.2.1 info	11
4.4.2.2 socket	11
4.5 Neighbour Struct Reference	12
4.5.1 Detailed Description	12
4.5.2 Field Documentation	12
4.5.2.1 client_sockfd	12

4.5.2.2 family	12
4.5.2.3 hostname	12
4.5.2.4 server_sockfd	13
4.6 Node Struct Reference	13
4.6.1 Detailed Description	13
4.6.2 Field Documentation	13
4.6.2.1 neighbours	13
4.7 Transaction Struct Reference	13
4.7.1 Detailed Description	14
4.7.2 Field Documentation	14
4.7.2.1 signature_len	14
4.7.2.2 transaction_data	14
4.7.2.3 transaction_signature	14
4.8 TransactionData Struct Reference	14
4.8.1 Detailed Description	15
4.8.2 Field Documentation	15
4.8.2.1 amount	15
4.8.2.2 asset	15
4.8.2.3 cause	15
4.8.2.4 organisation_public_key	16
4.8.2.5 receiver_public_key	16
4.8.2.6 receiver_remaining_money	16
4.8.2.7 sender_public_key	16
4.8.2.8 sender_remaining_money	16
4.8.2.9 transaction_timestamp	16
4.9 Wallet Struct Reference	17
4.9.1 Detailed Description	17
4.9.2 Field Documentation	17
4.9.2.1 amount	17
4.9.2.2 is_validator	17
4.9.2.3 priv_key	17
4.9.2.4 pub_key	17
<b>5 File Documentation</b>	<b>19</b>
5.1 /home/runner/work/PEPITAS-Cryptocurrency/PEPITAS-Cryptocurrency/headers/core/blockchain/block.h	
File Reference	19
5.2 /home/runner/work/PEPITAS-Cryptocurrency/PEPITAS-Cryptocurrency/headers/core/blockchain/transaction.h	
File Reference	19
5.2.1 Macro Definition Documentation	20
5.2.1.1 TRANSACTION_DATA_SIZE	20
5.2.1.2 TRANSACTION_SIZE	20
5.2.2 Typedef Documentation	20
5.2.2.1 Transaction	20

5.2.2.2 TransactionData . . . . .	20
5.2.3 Function Documentation . . . . .	20
5.2.3.1 send_money() . . . . .	20
5.3 /home/runner/work/PEPITAS-Cryptocurrency/PEPITAS-Cryptocurrency/headers/core/blockchain/wallet.h File Reference . . . . .	21
5.3.1 Typedef Documentation . . . . .	21
5.3.1.1 Wallet . . . . .	21
5.3.2 Function Documentation . . . . .	22
5.3.2.1 create_account() . . . . .	22
5.3.2.2 get_my_wallet() . . . . .	22
5.4 /home/runner/work/PEPITAS-Cryptocurrency/PEPITAS-Cryptocurrency/headers/core/validation/stake.h File Reference . . . . .	22
5.4.1 Function Documentation . . . . .	23
5.4.1.1 pop_stake() . . . . .	23
5.4.1.2 push_stake() . . . . .	23
5.5 /home/runner/work/PEPITAS-Cryptocurrency/PEPITAS-Cryptocurrency/headers/core/validation/validations.h File Reference . . . . .	24
5.5.1 Function Documentation . . . . .	24
5.5.1.1 get_amount() . . . . .	24
5.5.1.2 get_next_committee() . . . . .	24
5.6 /home/runner/work/PEPITAS-Cryptocurrency/PEPITAS-Cryptocurrency/headers/cryptosystem/hash.h File Reference . . . . .	25
5.6.1 Function Documentation . . . . .	25
5.6.1.1 hash_block_transactions() . . . . .	25
5.6.1.2 sha384_data() . . . . .	26
5.7 /home/runner/work/PEPITAS-Cryptocurrency/PEPITAS-Cryptocurrency/headers/cryptosystem/rsa.h File Reference . . . . .	26
5.7.1 Macro Definition Documentation . . . . .	26
5.7.1.1 RSA_BEGIN_SIZE . . . . .	27
5.7.1.2 RSA_END_SIZE . . . . .	27
5.7.1.3 RSA_FILE_TOTAL_SIZE . . . . .	27
5.7.1.4 RSA_KEY_SIZE . . . . .	27
5.7.2 Function Documentation . . . . .	27
5.7.2.1 get_keys() . . . . .	27
5.8 /home/runner/work/PEPITAS-Cryptocurrency/PEPITAS-Cryptocurrency/headers/cryptosystem/signature.h File Reference . . . . .	28
5.8.1 Function Documentation . . . . .	28
5.8.1.1 get_blockdata_data() . . . . .	28
5.8.1.2 get_transaction_data() . . . . .	29
5.8.1.3 sign_block() . . . . .	29
5.8.1.4 sign_block_transactions() . . . . .	30
5.8.1.5 sign_message() . . . . .	30
5.8.1.6 sign_transaction() . . . . .	30
5.8.1.7 verify_block_signature() . . . . .	31

5.8.1.8	verify_signature()	31
5.8.1.9	verify_transaction_signature()	32
5.8.1.10	write_block()	32
5.8.1.11	write_blockdata()	32
5.9	/home/runner/work/PEPITAS-Cryptocurrency/PEPITAS-Cryptocurrency/headers/misc/files.h File Reference	34
5.9.1	Function Documentation	34
5.9.1.1	last_file_in_folder()	34
5.10	/home/runner/work/PEPITAS-Cryptocurrency/PEPITAS-Cryptocurrency/headers/misc/math.h File Reference	35
5.10.1	Macro Definition Documentation	35
5.10.1.1	MAX	35
5.10.1.2	MIN	35
5.11	/home/runner/work/PEPITAS-Cryptocurrency/PEPITAS-Cryptocurrency/headers/misc/safe.h File Reference	35
5.11.1	Function Documentation	36
5.11.1.1	safe_fread()	36
5.11.1.2	safe_read()	36
5.11.1.3	safe_write()	37
5.12	/home/runner/work/PEPITAS-Cryptocurrency/PEPITAS-Cryptocurrency/headers/network/client.h File Reference	37
5.12.1	Macro Definition Documentation	38
5.12.1.1	MAX_NEIGHBOURS	38
5.12.2	Typedef Documentation	38
5.12.2.1	Neighbour	38
5.12.2.2	Node	38
5.12.3	Function Documentation	39
5.12.3.1	get_my_node()	39
5.12.3.2	listen_to()	39
5.12.3.3	ping_client()	39
5.12.3.4	set_neighbour()	40
5.13	/home/runner/work/PEPITAS-Cryptocurrency/PEPITAS-Cryptocurrency/headers/network/get_data.h File Reference	40
5.13.1	Function Documentation	40
5.13.1.1	fetch_client_list()	40
5.13.1.2	read_header()	41
5.14	/home/runner/work/PEPITAS-Cryptocurrency/PEPITAS-Cryptocurrency/headers/network/network.h File Reference	41
5.14.1	Macro Definition Documentation	42
5.14.1.1	HD_GET_BLOCKCHAIN	42
5.14.1.2	HD_GET_CLIENT_LIST	42
5.14.1.3	HD_SEND_BLOCKCHAIN	42
5.14.1.4	HD_SEND_CLIENT_LIST	42
5.14.1.5	NB_HARD_CODED_ADDR	43

5.14.1.6 STATIC_PORT . . . . .	43
5.14.2 Variable Documentation . . . . .	43
5.14.2.1 HARD_CODED_ADDR . . . . .	43
5.15 /home/runner/work/PEPITAS-Cryptocurrency/PEPITAS-Cryptocurrency/headers/network/send_↵ data.h File Reference . . . . .	43
5.15.1 Function Documentation . . . . .	43
5.15.1.1 send_client_list() . . . . .	43
5.16 /home/runner/work/PEPITAS-Cryptocurrency/PEPITAS-Cryptocurrency/headers/network/server.h File Reference . . . . .	44
5.16.1 Typedef Documentation . . . . .	44
5.16.1.1 client_connection . . . . .	44
5.16.2 Function Documentation . . . . .	45
5.16.2.1 init_server() . . . . .	45
5.16.2.2 send_block() . . . . .	45
5.17 /home/runner/work/PEPITAS-Cryptocurrency/PEPITAS-Cryptocurrency/headers/ui/ui.h File Reference	45
5.17.1 Function Documentation . . . . .	46
5.17.1.1 add_contact() . . . . .	46
5.17.1.2 on_add_contact_button1_press() . . . . .	47
5.17.1.3 on_connect_but_press() . . . . .	47
5.17.1.4 on_create_key_but1_press() . . . . .	47
5.17.1.5 on_create_key_but2_press() . . . . .	47
5.17.1.6 on_invest_button1_press() . . . . .	48
5.17.1.7 on_invest_button2_press() . . . . .	48
5.17.1.8 on_main_window_delete() . . . . .	48
5.17.1.9 on_main_window_destroy() . . . . .	49
5.17.1.10 on_pkey_button_press() . . . . .	49
5.17.1.11 on_recover_button1_press() . . . . .	49
5.17.1.12 on_recover_button2_press() . . . . .	50
5.17.1.13 on_transaction_button_press() . . . . .	50
5.17.1.14 setup() . . . . .	51
5.17.1.15 update_labels() . . . . .	51
5.18 /home/runner/work/PEPITAS-Cryptocurrency/PEPITAS-Cryptocurrency/README.md File Reference	51
5.19 /home/runner/work/PEPITAS-Cryptocurrency/PEPITAS-Cryptocurrency/src/client.c File Reference .	51
5.19.1 Function Documentation . . . . .	52
5.19.1.1 main() . . . . .	52
5.20 /home/runner/work/PEPITAS-Cryptocurrency/PEPITAS-Cryptocurrency/src/network/client.c File Reference . . . . .	52
5.20.1 Function Documentation . . . . .	52
5.20.1.1 get_my_node() . . . . .	52
5.20.1.2 listen_to() . . . . .	52
5.20.1.3 set_neighbour() . . . . .	53
5.21 /home/runner/work/PEPITAS-Cryptocurrency/PEPITAS-Cryptocurrency/src/core/blockchain/block.c File Reference . . . . .	53

5.21.1 Function Documentation . . . . .	54
5.21.1.1 convert_data_to_block() . . . . .	54
5.21.1.2 convert_data_to_blockdata() . . . . .	54
5.21.1.3 convert_data_to_transaction() . . . . .	54
5.21.1.4 convert_data_to_transactiondata() . . . . .	55
5.21.1.5 free_block() . . . . .	55
5.21.1.6 get_block() . . . . .	55
5.21.1.7 get_blockchain() . . . . .	55
5.21.1.8 get_next_block() . . . . .	56
5.21.1.9 get_prev_block() . . . . .	56
5.21.1.10 write_block_file() . . . . .	56
5.22 /home/runner/work/PEPITAS-Cryptocurrency/PEPITAS-Cryptocurrency/src/core/blockchain/wallet.c File Reference . . . . .	57
5.22.1 Function Documentation . . . . .	57
5.22.1.1 create_account() . . . . .	57
5.22.1.2 get_my_wallet() . . . . .	58
5.23 /home/runner/work/PEPITAS-Cryptocurrency/PEPITAS-Cryptocurrency/src/core/validation/validations.c File Reference . . . . .	58
5.23.1 Macro Definition Documentation . . . . .	58
5.23.1.1 MAX_VALIDATORS_PER_BLOCK . . . . .	59
5.23.1.2 NB_RSA_CHUNK . . . . .	59
5.23.2 Function Documentation . . . . .	59
5.23.2.1 define_nb_validators() . . . . .	59
5.23.2.2 get_next_committee() . . . . .	59
5.24 /home/runner/work/PEPITAS-Cryptocurrency/PEPITAS-Cryptocurrency/src/cryptosystem/hash.c File Reference . . . . .	60
5.24.1 Function Documentation . . . . .	60
5.24.1.1 hash_block_transactions() . . . . .	60
5.24.1.2 sha384_data() . . . . .	60
5.25 /home/runner/work/PEPITAS-Cryptocurrency/PEPITAS-Cryptocurrency/src/cryptosystem/rsa.c File Reference . . . . .	61
5.25.1 Macro Definition Documentation . . . . .	61
5.25.1.1 RSA_NUM_E . . . . .	62
5.25.2 Function Documentation . . . . .	62
5.25.2.1 get_keys() . . . . .	62
5.26 /home/runner/work/PEPITAS-Cryptocurrency/PEPITAS-Cryptocurrency/src/cryptosystem/signature.c File Reference . . . . .	62
5.26.1 Function Documentation . . . . .	63
5.26.1.1 get_blockdata_data() . . . . .	63
5.26.1.2 get_transaction_data() . . . . .	63
5.26.1.3 sign_block() . . . . .	64
5.26.1.4 sign_block_transactions() . . . . .	64
5.26.1.5 sign_message() . . . . .	64



5.26.1.6 sign_transaction()	65
5.26.1.7 verify_block_signature()	65
5.26.1.8 verify_signature()	66
5.26.1.9 verify_transaction_signature()	66
5.26.1.10 write_block()	67
5.26.1.11 write_blockdata()	67
5.26.1.12 write_transaction()	67
5.26.1.13 write_transactiondata()	67
5.27 /home/runner/work/PEPITAS-Cryptocurrency/PEPITAS-Cryptocurrency/src/gui.c File Reference	68
5.27.1 Function Documentation	68
5.27.1.1 main()	68
5.28 /home/runner/work/PEPITAS-Cryptocurrency/PEPITAS-Cryptocurrency/src/misc/files.c File Reference	68
5.28.1 Macro Definition Documentation	69
5.28.1.1 _GNU_SOURCE	69
5.28.2 Function Documentation	69
5.28.2.1 last_file_in_folder()	69
5.29 /home/runner/work/PEPITAS-Cryptocurrency/PEPITAS-Cryptocurrency/src/misc/safe.c File Reference	69
5.29.1 Function Documentation	70
5.29.1.1 safe_fread()	70
5.29.1.2 safe_read()	70
5.29.1.3 safe_write()	71
5.30 /home/runner/work/PEPITAS-Cryptocurrency/PEPITAS-Cryptocurrency/src/network/get_data.c File Reference	71
5.30.1 Function Documentation	71
5.30.1.1 fetch_client_list()	71
5.30.1.2 process_header()	72
5.30.1.3 read_header()	72
5.31 /home/runner/work/PEPITAS-Cryptocurrency/PEPITAS-Cryptocurrency/src/network/network.c File Reference	72
5.31.1 Variable Documentation	73
5.31.1.1 HARD_CODED_ADDR	73
5.32 /home/runner/work/PEPITAS-Cryptocurrency/PEPITAS-Cryptocurrency/src/network/send_data.c File Reference	73
5.32.1 Function Documentation	73
5.32.1.1 send_client_list()	73
5.33 /home/runner/work/PEPITAS-Cryptocurrency/PEPITAS-Cryptocurrency/src/network/server.c File Reference	74
5.33.1 Function Documentation	74
5.33.1.1 accept_connection()	74
5.33.1.2 init_server()	74
5.34 /home/runner/work/PEPITAS-Cryptocurrency/PEPITAS-Cryptocurrency/src/server.c File Reference	75
5.34.1 Function Documentation	75
5.34.1.1 main()	75

5.35 /home/runner/work/PEPITAS-Cryptocurrency/PEPITAS-Cryptocurrency/src/sign.c File Reference	75
5.35.1 Function Documentation	76
5.35.1.1 main()	76
5.36 /home/runner/work/PEPITAS-Cryptocurrency/PEPITAS-Cryptocurrency/src/ui/ui.c File Reference	76
5.36.1 Function Documentation	77
5.36.1.1 add_contact()	77
5.36.1.2 on_add_contact_button1_press()	78
5.36.1.3 on_connect_but_press()	78
5.36.1.4 on_create_key_but1_press()	78
5.36.1.5 on_create_key_but2_press()	78
5.36.1.6 on_invest_button1_press()	78
5.36.1.7 on_invest_button2_press()	79
5.36.1.8 on_main_window_delete()	79
5.36.1.9 on_main_window_destroy()	79
5.36.1.10 on_pkey_button_press()	79
5.36.1.11 on_recover_button1_press()	80
5.36.1.12 on_recover_button2_press()	80
5.36.1.13 on_transaction_button_press()	80
5.36.1.14 setup()	80
5.36.1.15 update_labels()	81
5.36.2 Variable Documentation	81
5.36.2.1 balance_1	81
5.36.2.2 balance_2	81
5.36.2.3 cr1_con	81
5.36.2.4 cr1_th	81
5.36.2.5 cr2_con	82
5.36.2.6 cr2_th	82
5.36.2.7 cr3_th	82
5.36.2.8 cr4_th	82
5.36.2.9 cx1_con	82
5.36.2.10 cx1_th	82
5.36.2.11 cx2_con	83
5.36.2.12 cx2_th	83
5.36.2.13 cx3_th	83
5.36.2.14 cx4_th	83
5.36.2.15 invest_entry	83
5.36.2.16 name_entry_con	83
5.36.2.17 password_entry1	84
5.36.2.18 password_entry2	84
5.36.2.19 private_key_label	84
5.36.2.20 public_key_entry_con	84
5.36.2.21 recipient_key	84

5.36.2.22 recover_entry . . . . .	84
5.36.2.23 stake_label1 . . . . .	85
5.36.2.24 stake_label2 . . . . .	85
5.36.2.25 stake_label3 . . . . .	85
5.36.2.26 transa_amount . . . . .	85
5.36.2.27 ts_con . . . . .	85
5.36.2.28 ts_th . . . . .	85
5.36.2.29 tv_con . . . . .	86
5.36.2.30 tv_th . . . . .	86
5.37 /home/runner/work/PEPITAS-Cryptocurrency/PEPITAS-Cryptocurrency/tests/gen/GEN_blockchain↔ _files.c File Reference . . . . .	86
5.37.1 Function Documentation . . . . .	86
5.37.1.1 gen_blockchain() . . . . .	86
5.37.1.2 rand_data() . . . . .	87
5.38 /home/runner/work/PEPITAS-Cryptocurrency/PEPITAS-Cryptocurrency/tests/gen/GEN_validators↔ _file.c File Reference . . . . .	87
5.38.1 Macro Definition Documentation . . . . .	87
5.38.1.1 NB_FAKE_VALIDATORS . . . . .	87
5.38.1.2 str . . . . .	88
5.38.2 Function Documentation . . . . .	88
5.38.2.1 gen_validators_file() . . . . .	88
5.39 /home/runner/work/PEPITAS-Cryptocurrency/PEPITAS-Cryptocurrency/tests/main_test.c File Refer- ence . . . . .	88
5.39.1 Function Documentation . . . . .	89
5.39.1.1 main() . . . . .	89
5.40 /home/runner/work/PEPITAS-Cryptocurrency/PEPITAS-Cryptocurrency/tests/src/core/blockchain/block↔ _test.c File Reference . . . . .	89
5.40.1 Macro Definition Documentation . . . . .	89
5.40.1.1 NB_BLOCK_PER_CHUNK . . . . .	89
5.40.1.2 NB MOCK_BLOCKS . . . . .	90
5.40.2 Function Documentation . . . . .	90
5.40.2.1 block_test() . . . . .	90
5.41 /home/runner/work/PEPITAS-Cryptocurrency/PEPITAS-Cryptocurrency/tests/src/core/blockchain/block↔ _test.h File Reference . . . . .	90
5.41.1 Function Documentation . . . . .	90
5.41.1.1 block_test() . . . . .	90
5.42 /home/runner/work/PEPITAS-Cryptocurrency/PEPITAS-Cryptocurrency/tests/src/core/validation/validations↔ _test.c File Reference . . . . .	91
5.42.1 Function Documentation . . . . .	91
5.42.1.1 validations_test() . . . . .	91
5.43 /home/runner/work/PEPITAS-Cryptocurrency/PEPITAS-Cryptocurrency/tests/src/cryptosystem/rsa↔ _test.c File Reference . . . . .	91
5.43.1 Macro Definition Documentation . . . . .	92
5.43.1.1 MAX . . . . .	92

5.43.2 Function Documentation . . . . .	92
5.43.2.1 get_keys_equality_test() . . . . .	92
5.43.2.2 get_keys_test() . . . . .	92
5.44 /home/runner/work/PEPITAS-Cryptocurrency/PEPITAS-Cryptocurrency/tests/src/cryptosystem/rsa↔ _test.h File Reference . . . . .	92
5.44.1 Function Documentation . . . . .	93
5.44.1.1 get_keys_equality_test() . . . . .	93
5.44.1.2 get_keys_test() . . . . .	93
5.45 /home/runner/work/PEPITAS-Cryptocurrency/PEPITAS-Cryptocurrency/tests/src/cryptosystem/signature↔ _test.c File Reference . . . . .	93
5.45.1 Function Documentation . . . . .	93
5.45.1.1 verify_sign_test() . . . . .	94
5.46 /home/runner/work/PEPITAS-Cryptocurrency/PEPITAS-Cryptocurrency/tests/src/cryptosystem/signature↔ _test.h File Reference . . . . .	94
5.46.1 Function Documentation . . . . .	94
5.46.1.1 verify_sign_test() . . . . .	94
5.47 /home/runner/work/PEPITAS-Cryptocurrency/PEPITAS-Cryptocurrency/tests/src/network/client_↔ test.c File Reference . . . . .	94
5.47.1 Function Documentation . . . . .	95
5.47.1.1 network_test() . . . . .	95
5.48 /home/runner/work/PEPITAS-Cryptocurrency/PEPITAS-Cryptocurrency/tests/src/network/server_↔ test.c File Reference . . . . .	95
5.48.1 Function Documentation . . . . .	95
5.48.1.1 main() . . . . .	95
5.49 /home/runner/work/PEPITAS-Cryptocurrency/PEPITAS-Cryptocurrency/tests/tests_macros.h File Reference . . . . .	95
5.49.1 Macro Definition Documentation . . . . .	96
5.49.1.1 DEBUG . . . . .	96
5.49.1.2 LOG . . . . .	96
5.49.1.3 TEST_FAILED . . . . .	96
5.49.1.4 TEST_PASSED . . . . .	97
5.49.1.5 TEST_WARNING . . . . .	97
5.50 /home/runner/work/PEPITAS-Cryptocurrency/PEPITAS-Cryptocurrency/tests/unit_testing.c File Ref- erence . . . . .	97
5.50.1 Function Documentation . . . . .	97
5.50.1.1 main() . . . . .	97

# Chapter 1

## PEPITAS

C cryptocurrency.

### 1.1 CODING STYLE

#### 1.1.1 Coding case

- *Functions, variables and filenames* must be written in `snake_case`.
- *Structures* must be written in `PascalCase`.
- *Constants or MACRO* must be written in `UPPER_SNAKE_CASE`.

#### 1.1.2 Tests

Each function must be tested before **marked as done**. To create a test function, you must write it in the `test/` directory and call the file `filename_test.c` and its functions `functionname_test`. Note that the test file must be at the same relative place than his real function

exemple : if you want to test `init_server()` in the file `network/client.c`, you must write the test in `test/network/client_test.c` and call the test function `init_server_test()`



## Chapter 2

# Data Structure Index

### 2.1 Data Structures

Here are the data structures with brief descriptions:

Block	7
BlockData	8
ChunkBlockchain	10
client_connection	11
Neighbour	12
Node	13
Transaction	13
TransactionData	14
Wallet	17





## Chapter 3

# File Index

### 3.1 File List

Here is a list of all files with brief descriptions:

/home/runner/work/PEPITAS-Cryptocurrency/PEPITAS-Cryptocurrency/headers/core/blockchain/block.h	19
/home/runner/work/PEPITAS-Cryptocurrency/PEPITAS-Cryptocurrency/headers/core/blockchain/transaction.h	19
/home/runner/work/PEPITAS-Cryptocurrency/PEPITAS-Cryptocurrency/headers/core/blockchain/wallet.h	21
/home/runner/work/PEPITAS-Cryptocurrency/PEPITAS-Cryptocurrency/headers/core/validation/stake.h	22
/home/runner/work/PEPITAS-Cryptocurrency/PEPITAS-Cryptocurrency/headers/core/validation/validations.h	24
/home/runner/work/PEPITAS-Cryptocurrency/PEPITAS-Cryptocurrency/headers/cryptosystem/hash.h	25
/home/runner/work/PEPITAS-Cryptocurrency/PEPITAS-Cryptocurrency/headers/cryptosystem/rsa.h	26
/home/runner/work/PEPITAS-Cryptocurrency/PEPITAS-Cryptocurrency/headers/cryptosystem/signature.h	28
/home/runner/work/PEPITAS-Cryptocurrency/PEPITAS-Cryptocurrency/headers/misc/files.h	34
/home/runner/work/PEPITAS-Cryptocurrency/PEPITAS-Cryptocurrency/headers/misc/math.h	35
/home/runner/work/PEPITAS-Cryptocurrency/PEPITAS-Cryptocurrency/headers/misc/safe.h	35
/home/runner/work/PEPITAS-Cryptocurrency/PEPITAS-Cryptocurrency/headers/network/client.h	37
/home/runner/work/PEPITAS-Cryptocurrency/PEPITAS-Cryptocurrency/headers/network/get_data.h	40
/home/runner/work/PEPITAS-Cryptocurrency/PEPITAS-Cryptocurrency/headers/network/network.h	41
/home/runner/work/PEPITAS-Cryptocurrency/PEPITAS-Cryptocurrency/headers/network/send_data.h	43
/home/runner/work/PEPITAS-Cryptocurrency/PEPITAS-Cryptocurrency/headers/network/server.h	44
/home/runner/work/PEPITAS-Cryptocurrency/PEPITAS-Cryptocurrency/headers/ui/ui.h	45
/home/runner/work/PEPITAS-Cryptocurrency/PEPITAS-Cryptocurrency/src/client.c	51
/home/runner/work/PEPITAS-Cryptocurrency/PEPITAS-Cryptocurrency/src/gui.c	68
/home/runner/work/PEPITAS-Cryptocurrency/PEPITAS-Cryptocurrency/src/server.c	75
/home/runner/work/PEPITAS-Cryptocurrency/PEPITAS-Cryptocurrency/src/sign.c	75
/home/runner/work/PEPITAS-Cryptocurrency/PEPITAS-Cryptocurrency/src/core/blockchain/block.c	53
/home/runner/work/PEPITAS-Cryptocurrency/PEPITAS-Cryptocurrency/src/core/blockchain/wallet.c	57
/home/runner/work/PEPITAS-Cryptocurrency/PEPITAS-Cryptocurrency/src/core/validation/validations.c	58
/home/runner/work/PEPITAS-Cryptocurrency/PEPITAS-Cryptocurrency/src/cryptosystem/hash.c	60
/home/runner/work/PEPITAS-Cryptocurrency/PEPITAS-Cryptocurrency/src/cryptosystem/rsa.c	61
/home/runner/work/PEPITAS-Cryptocurrency/PEPITAS-Cryptocurrency/src/cryptosystem/signature.c	62
/home/runner/work/PEPITAS-Cryptocurrency/PEPITAS-Cryptocurrency/src/misc/files.c	68
/home/runner/work/PEPITAS-Cryptocurrency/PEPITAS-Cryptocurrency/src/misc/safe.c	69
/home/runner/work/PEPITAS-Cryptocurrency/PEPITAS-Cryptocurrency/src/network/client.c	52
/home/runner/work/PEPITAS-Cryptocurrency/PEPITAS-Cryptocurrency/src/network/get_data.c	71
/home/runner/work/PEPITAS-Cryptocurrency/PEPITAS-Cryptocurrency/src/network/network.c	72

/home/runner/work/PEPITAS-Cryptocurrency/PEPITAS-Cryptocurrency/src/network/ <a href="#">send_data.c</a> . . . . .	73
/home/runner/work/PEPITAS-Cryptocurrency/PEPITAS-Cryptocurrency/src/network/ <a href="#">server.c</a> . . . . .	74
/home/runner/work/PEPITAS-Cryptocurrency/PEPITAS-Cryptocurrency/src/ui/ <a href="#">ui.c</a> . . . . .	76
/home/runner/work/PEPITAS-Cryptocurrency/PEPITAS-Cryptocurrency/tests/ <a href="#">main_test.c</a> . . . . .	88
/home/runner/work/PEPITAS-Cryptocurrency/PEPITAS-Cryptocurrency/tests/ <a href="#">tests_macros.h</a> . . . . .	95
/home/runner/work/PEPITAS-Cryptocurrency/PEPITAS-Cryptocurrency/tests/ <a href="#">unit_testing.c</a> . . . . .	97
/home/runner/work/PEPITAS-Cryptocurrency/PEPITAS-Cryptocurrency/tests/gen/ <a href="#">GEN_blockchain_files.c</a> 86	
/home/runner/work/PEPITAS-Cryptocurrency/PEPITAS-Cryptocurrency/tests/gen/ <a href="#">GEN_validators_file.c</a> 87	87
/home/runner/work/PEPITAS-Cryptocurrency/PEPITAS-Cryptocurrency/tests/src/core/blockchain/ <a href="#">block_test.c</a> 89	
/home/runner/work/PEPITAS-Cryptocurrency/PEPITAS-Cryptocurrency/tests/src/core/blockchain/ <a href="#">block_test.h</a> 90	
/home/runner/work/PEPITAS-Cryptocurrency/PEPITAS-Cryptocurrency/tests/src/core/validation/ <a href="#">validations_test.c</a> 91	
/home/runner/work/PEPITAS-Cryptocurrency/PEPITAS-Cryptocurrency/tests/src/cryptosystem/ <a href="#">rsa_test.c</a> 91	
/home/runner/work/PEPITAS-Cryptocurrency/PEPITAS-Cryptocurrency/tests/src/cryptosystem/ <a href="#">rsa_test.h</a> 92	
/home/runner/work/PEPITAS-Cryptocurrency/PEPITAS-Cryptocurrency/tests/src/cryptosystem/ <a href="#">signature_test.c</a> 93	
/home/runner/work/PEPITAS-Cryptocurrency/PEPITAS-Cryptocurrency/tests/src/cryptosystem/ <a href="#">signature_test.h</a> 94	
/home/runner/work/PEPITAS-Cryptocurrency/PEPITAS-Cryptocurrency/tests/src/network/ <a href="#">client_test.c</a> .	94
/home/runner/work/PEPITAS-Cryptocurrency/PEPITAS-Cryptocurrency/tests/src/network/ <a href="#">server_test.c</a> .	95

## Chapter 4

# Data Structure Documentation

### 4.1 Block Struct Reference

```
#include <block.h>
```

Collaboration diagram for Block:

#### Data Fields

- uint16\_t [chunk\\_id](#)
- [BlockData](#) [block\\_data](#)
- size\_t [signature\\_len](#)
- char \* [block\\_signature](#)

#### 4.1.1 Detailed Description

Definition at line 31 of file block.h.

#### 4.1.2 Field Documentation

##### 4.1.2.1 [block\\_data](#)

[BlockData](#) [block\\_data](#)

Definition at line 34 of file block.h.

#### 4.1.2.2 block\_signature

```
char* block_signature
```

Definition at line 37 of file block.h.

#### 4.1.2.3 chunk\_id

```
uint16_t chunk_id
```

Definition at line 33 of file block.h.

#### 4.1.2.4 signature\_len

```
size_t signature_len
```

Definition at line 36 of file block.h.

The documentation for this struct was generated from the following file:

- </home/runner/work/PEPITAS-Cryptocurrency/PEPITAS-Cryptocurrency/headers/core/blockchain/block.h>

## 4.2 BlockData Struct Reference

```
#include <block.h>
```

Collaboration diagram for BlockData:

### Data Fields

- char [magic](#)
- char [previous\\_block\\_hash](#) [SHA384\_DIGEST\_LENGTH \*2+1]
- size\_t [height](#)
- uint16\_t [nb\\_transactions](#)
- [Transaction](#) \*\* [transactions](#)
- RSA \* [validator\\_public\\_key](#)
- time\_t [block\\_timestamp](#)

#### 4.2.1 Detailed Description

Definition at line 17 of file block.h.

## 4.2.2 Field Documentation

### 4.2.2.1 block\_timestamp

```
time_t block_timestamp
```

Definition at line 28 of file block.h.

### 4.2.2.2 height

```
size_t height
```

Definition at line 21 of file block.h.

### 4.2.2.3 magic

```
char magic
```

Definition at line 19 of file block.h.

### 4.2.2.4 nb\_transactions

```
uint16_t nb_transactions
```

Definition at line 23 of file block.h.

### 4.2.2.5 previous\_block\_hash

```
char previous_block_hash[SHA384_DIGEST_LENGTH *2+1]
```

Definition at line 20 of file block.h.

#### 4.2.2.6 transactions

```
Transaction** transactions
```

Definition at line 24 of file block.h.

#### 4.2.2.7 validator\_public\_key

```
RSA* validator_public_key
```

Definition at line 27 of file block.h.

The documentation for this struct was generated from the following file:

- /home/runner/work/PEPITAS-Cryptocurrency/PEPITAS-Cryptocurrency/headers/core/blockchain/[block.h](#)

### 4.3 ChunkBlockchain Struct Reference

```
#include <block.h>
```

Collaboration diagram for ChunkBlockchain:

#### Data Fields

- size\_t [chunk\\_nb](#)
- [Block](#)\*\* [chunk](#)

#### 4.3.1 Detailed Description

Definition at line 41 of file block.h.

#### 4.3.2 Field Documentation

##### 4.3.2.1 chunk

```
Block** chunk
```

Definition at line 44 of file block.h.

#### 4.3.2.2 chunk\_nb

```
size_t chunk_nb
```

Definition at line 43 of file block.h.

The documentation for this struct was generated from the following file:

- /home/runner/work/PEPITAS-Cryptocurrency/PEPITAS-Cryptocurrency/headers/core/blockchain/[block.h](#)

## 4.4 client\_connection Struct Reference

```
#include <server.h>
```

### Data Fields

- struct addrinfo [info](#)
- int [socket](#)

#### 4.4.1 Detailed Description

Definition at line 8 of file server.h.

#### 4.4.2 Field Documentation

##### 4.4.2.1 info

```
struct addrinfo info
```

Definition at line 10 of file server.h.

##### 4.4.2.2 socket

```
int socket
```

Definition at line 11 of file server.h.

The documentation for this struct was generated from the following file:

- /home/runner/work/PEPITAS-Cryptocurrency/PEPITAS-Cryptocurrency/headers/network/[server.h](#)

## 4.5 Neighbour Struct Reference

```
#include <client.h>
```

### Data Fields

- int [family](#)
- char \* [hostname](#)
- int [server\\_sockfd](#)
- int [client\\_sockfd](#)

### 4.5.1 Detailed Description

Definition at line 8 of file client.h.

### 4.5.2 Field Documentation

#### 4.5.2.1 [client\\_sockfd](#)

```
int client_sockfd
```

Definition at line 13 of file client.h.

#### 4.5.2.2 [family](#)

```
int family
```

Definition at line 10 of file client.h.

#### 4.5.2.3 [hostname](#)

```
char* hostname
```

Definition at line 11 of file client.h.



#### 4.5.2.4 server\_sockfd

```
int server_sockfd
```

Definition at line 12 of file client.h.

The documentation for this struct was generated from the following file:

- /home/runner/work/PEPITAS-Cryptocurrency/PEPITAS-Cryptocurrency/headers/network/[client.h](#)

## 4.6 Node Struct Reference

```
#include <client.h>
```

Collaboration diagram for Node:

### Data Fields

- [Neighbour](#) \* [neighbours](#)

#### 4.6.1 Detailed Description

Definition at line 16 of file client.h.

#### 4.6.2 Field Documentation

##### 4.6.2.1 neighbours

```
Neighbour* neighbours
```

Definition at line 18 of file client.h.

The documentation for this struct was generated from the following file:

- /home/runner/work/PEPITAS-Cryptocurrency/PEPITAS-Cryptocurrency/headers/network/[client.h](#)

## 4.7 Transaction Struct Reference

```
#include <transaction.h>
```

Collaboration diagram for Transaction:

## Data Fields

- [TransactionData](#) \* [transaction\\_data](#)
- `size_t` [signature\\_len](#)
- `char *` [transaction\\_signature](#)

### 4.7.1 Detailed Description

Definition at line 28 of file `transaction.h`.

### 4.7.2 Field Documentation

#### 4.7.2.1 `signature_len`

```
size_t signature_len
```

Definition at line 32 of file `transaction.h`.

#### 4.7.2.2 `transaction_data`

```
TransactionData* transaction_data
```

Definition at line 30 of file `transaction.h`.

#### 4.7.2.3 `transaction_signature`

```
char* transaction_signature
```

Definition at line 33 of file `transaction.h`.

The documentation for this struct was generated from the following file:

- `/home/runner/work/PEPITAS-Cryptocurrency/PEPITAS-Cryptocurrency/headers/core/blockchain/transaction.h`

## 4.8 TransactionData Struct Reference

```
#include <transaction.h>
```

## Data Fields

- RSA \* [sender\\_public\\_key](#)
- RSA \* [receiver\\_public\\_key](#)
- RSA \* [organisation\\_public\\_key](#)
- size\_t [amount](#)
- size\_t [sender\\_remaining\\_money](#)
- size\_t [receiver\\_remaining\\_money](#)
- time\_t [transaction\\_timestamp](#)
- char [cause](#) [512]
- char [asset](#) [512]

### 4.8.1 Detailed Description

Definition at line 11 of file transaction.h.

### 4.8.2 Field Documentation

#### 4.8.2.1 amount

```
size_t amount
```

Definition at line 17 of file transaction.h.

#### 4.8.2.2 asset

```
char asset[512]
```

Definition at line 25 of file transaction.h.

#### 4.8.2.3 cause

```
char cause[512]
```

Definition at line 24 of file transaction.h.

#### 4.8.2.4 organisation\_public\_key

```
RSA* organisation_public_key
```

Definition at line 16 of file transaction.h.

#### 4.8.2.5 receiver\_public\_key

```
RSA* receiver_public_key
```

Definition at line 15 of file transaction.h.

#### 4.8.2.6 receiver\_remaining\_money

```
size_t receiver_remaining_money
```

Definition at line 19 of file transaction.h.

#### 4.8.2.7 sender\_public\_key

```
RSA* sender_public_key
```

Definition at line 14 of file transaction.h.

#### 4.8.2.8 sender\_remaining\_money

```
size_t sender_remaining_money
```

Definition at line 18 of file transaction.h.

#### 4.8.2.9 transaction\_timestamp

```
time_t transaction_timestamp
```

Definition at line 20 of file transaction.h.

The documentation for this struct was generated from the following file:

- /home/runner/work/PEPITAS-Cryptocurrency/PEPITAS-Cryptocurrency/headers/core/blockchain/[transaction.h](#)

## 4.9 Wallet Struct Reference

```
#include <wallet.h>
```

### Data Fields

- RSA \* [priv\\_key](#)
- RSA \* [pub\\_key](#)
- size\_t [amount](#)
- char [is\\_validator](#)

### 4.9.1 Detailed Description

Definition at line 10 of file wallet.h.

### 4.9.2 Field Documentation

#### 4.9.2.1 amount

```
size_t amount
```

Definition at line 15 of file wallet.h.

#### 4.9.2.2 is\_validator

```
char is_validator
```

Definition at line 16 of file wallet.h.

#### 4.9.2.3 priv\_key

```
RSA* priv_key
```

Definition at line 12 of file wallet.h.

#### 4.9.2.4 pub\_key

```
RSA* pub_key
```

Definition at line 13 of file wallet.h.

The documentation for this struct was generated from the following file:

- /home/runner/work/PEPITAS-Cryptocurrency/PEPITAS-Cryptocurrency/headers/core/blockchain/[wallet.h](#)



## Chapter 5

# File Documentation

### 5.1 [/home/runner/work/PEPITAS-Cryptocurrency/PEPITAS-Cryptocurrency/headers/core/blockchain/block.h](#) File Reference

```
#include <stdlib.h>
#include <openssl/sha.h>
#include "transaction.h"
Include dependency graph for block.h:
```

### 5.2 [/home/runner/work/PEPITAS-Cryptocurrency/PEPITAS-Cryptocurrency/headers/core/blockchain/transaction.h](#) File Reference

```
#include <stdlib.h>
#include <openssl/rsa.h>
#include <openssl/sha.h>
#include <time.h>
Include dependency graph for transaction.h: This graph shows which files directly or indirectly include this file:
```

#### Data Structures

- struct [TransactionData](#)
- struct [Transaction](#)

#### Macros

- #define [TRANSACTION\\_DATA\\_SIZE](#) sizeof(size\_t) \* 3 + sizeof(time\_t) + (512 \* 2)
- #define [TRANSACTION\\_SIZE](#) sizeof(size\_t) + 2048 + [TRANSACTION\\_DATA\\_SIZE](#)

## Typedefs

- typedef struct [TransactionData](#) [TransactionData](#)
- typedef struct [Transaction](#) [Transaction](#)

## Functions

- int [send\\_money](#) (size\_t amount, u\_int64\_t receiver\_public\_key)  
*Send 'amount' money to 'receiver\_public\_key'. This will broadcast a transaction to the network.*

### 5.2.1 Macro Definition Documentation

#### 5.2.1.1 TRANSACTION\_DATA\_SIZE

```
#define TRANSACTION_DATA_SIZE sizeof(size_t) * 3 + sizeof(time_t) + (512 * 2)
```

Definition at line 9 of file transaction.h.

#### 5.2.1.2 TRANSACTION\_SIZE

```
#define TRANSACTION_SIZE sizeof(size_t) + 2048 + TRANSACTION\_DATA\_SIZE
```

Definition at line 10 of file transaction.h.

### 5.2.2 Typedef Documentation

#### 5.2.2.1 Transaction

```
typedef struct Transaction Transaction
```

#### 5.2.2.2 TransactionData

```
typedef struct TransactionData TransactionData
```

### 5.2.3 Function Documentation

#### 5.2.3.1 send\_money()

```
int send_money (  
    size_t amount,  
    u_int64_t receiver_public_key )
```

Send 'amount' money to 'receiver\_public\_key'. This will broadcast a transaction to the network.



### 5.3

/home/runner/work/PEPITAS-Cryptocurrency/PEPITAS-Cryptocurrency/headers/core/blockchain/wallet.h

#### File Reference

21

##### Parameters

<i>amount</i>	The amount to send
<i>receiver_public_key</i>	The receiver public key

##### Returns

returns 0 if the broadcast succeeds, -1 otherwise

### 5.3 /home/runner/work/PEPITAS-Cryptocurrency/PEPITAS-Cryptocurrency/headers/core/blockchain/wallet.h File Reference

```
#include <openssl/rsa.h>
#include <stdlib.h>
#include <stdbool.h>
#include <time.h>
```

Include dependency graph for wallet.h: This graph shows which files directly or indirectly include this file:

#### Data Structures

- struct [Wallet](#)

#### Typedefs

- typedef struct [Wallet](#) [Wallet](#)

#### Functions

- [Wallet](#) \* [get\\_my\\_wallet](#) ()  
*Get my wallet object.*
- int [create\\_account](#) ()  
*Creates an account in local and broadcasts the creation to the network.*

#### 5.3.1 Typedef Documentation

##### 5.3.1.1 Wallet

```
typedef struct Wallet Wallet
```

### 5.3.2 Function Documentation

#### 5.3.2.1 create\_account()

```
int create_account ( )
```

Creates an account in local and broadcasts the creation to the network.

##### Returns

0 if the broadcast succeeds, otherwise 1

Definition at line 19 of file wallet.c.

Here is the call graph for this function:

#### 5.3.2.2 get\_my\_wallet()

```
Wallet* get_my_wallet ( )
```

Get my wallet object.

##### Returns

Wallet

Definition at line 7 of file wallet.c.

Here is the caller graph for this function:

## 5.4 /home/runner/work/PEPITAS-Cryptocurrency/PEPITAS-Cryptocurrency/headers/core/validation/stake.h File Reference

```
#include <stdlib.h>
```

Include dependency graph for stake.h:

### Functions

- int [push\\_stake](#) (size\_t amount)  
*Push an amount on the stake.*
- int [pop\\_stake](#) (size\_t amount)  
*Pops an amount on the stake.*

## 5.4.1 Function Documentation

### 5.4.1.1 pop\_stake()

```
int pop_stake (
    size_t amount )
```

Pops an amount on the stake.

This will broadcast a stake pop on the network.

#### See also

The stake account public key is '1'

#### Parameters

<i>amount</i>	The amount to pop
---------------	-------------------

#### Returns

0 if the broadcast succeeds, else returns -1

### 5.4.1.2 push\_stake()

```
int push_stake (
    size_t amount )
```

Push an amount on the stake.

This will broadcast a stake push on the network.

#### See also

The stake account public key is '1'

#### Parameters

<i>amount</i>	The amount to push
---------------	--------------------

#### Returns

0 if the broadcast succeeds, else returns -1

## 5.5 /home/runner/work/PEPITAS-Cryptocurrency/PEPITAS-Cryptocurrency/headers/core/validation/validations.h File Reference

```
#include <stdlib.h>
#include <openssl/rsa.h>
```

Include dependency graph for validations.h: This graph shows which files directly or indirectly include this file:

### Functions

- RSA \*\* [get\\_next\\_committee](#) (size\_t \*nb\_validators)  
*Get the 'next block' validators RSA public keys.*
- ssize\_t [get\\_amount](#) (RSA \*public\_key)  
*Searches how much money 'public\_key' has.*

### 5.5.1 Function Documentation

#### 5.5.1.1 [get\\_amount\(\)](#)

```
ssize_t get_amount (
    RSA * public_key )
```

Searches how much money 'public\_key' has.

##### Parameters

<i>public_key</i>	The RSA public key
-------------------	--------------------

##### Returns

The amount, or -1 in case of an error

#### 5.5.1.2 [get\\_next\\_committee\(\)](#)

```
RSA** get_next_committee (
    size_t * nb_validators )
```

Get the 'next block' validators RSA public keys.

##### Parameters

<i>nb_validators</i>	return value, the number of selected validators
----------------------	---

#### See also

The 'next block' is referring to block after the last block available OFFLINE

#### Returns

[\*RSA]

Definition at line 31 of file validations.c.

Here is the call graph for this function: Here is the caller graph for this function:

## 5.6 /home/runner/work/PEPITAS-Cryptocurrency/PEPITAS-Cryptocurrency/headers/cryptosystem/hash.h File Reference

```
#include <stdlib.h>
```

```
#include "core/blockchain/block.h"
```

Include dependency graph for hash.h: This graph shows which files directly or indirectly include this file:

### Functions

- char \* [sha384\\_data](#) (void \*data, size\_t len\_data)  
*Apply the SHA384 algorithm on a 'data' of size 'len\_data'.*
- char \* [hash\\_block\\_transactions](#) ([Block](#) \*block)  
*Apply the SHA384 to all block transactions.*

### 5.6.1 Function Documentation

#### 5.6.1.1 hash\_block\_transactions()

```
char* hash_block_transactions (  
    Block * block )
```

Apply the SHA384 to all block transactions.

#### Parameters

<i>block</i>	The block to deal with
--------------	------------------------

#### Returns

sha384[SHA384\_DIGEST\_LENGTH]

Definition at line 24 of file hash.c.

Here is the call graph for this function: Here is the caller graph for this function:

### 5.6.1.2 sha384\_data()

```
char* sha384_data (
    void * data,
    size_t len_data )
```

Apply the SHA384 algorithm on a 'data' of size 'len\_data'.

#### Parameters

<i>data</i>	The buffer to hash
<i>len_data</i>	The length of the buffer

#### Returns

char[97] (on heap)

Definition at line 6 of file hash.c.

Here is the caller graph for this function:

## 5.7 /home/runner/work/PEPITAS-Cryptocurrency/PEPITAS-Cryptocurrency/headers/cryptosystem/rsa.h File Reference

This graph shows which files directly or indirectly include this file:

### Macros

- #define [RSA\\_KEY\\_SIZE](#) 366
- #define [RSA\\_FILE\\_TOTAL\\_SIZE](#) 426
- #define [RSA\\_BEGIN\\_SIZE](#) 31
- #define [RSA\\_END\\_SIZE](#) 29

### Functions

- void [get\\_keys](#) ()  
*Get the keys object.*

### 5.7.1 Macro Definition Documentation

### 5.7.1.1 RSA\_BEGIN\_SIZE

```
#define RSA_BEGIN_SIZE 31
```

Definition at line 6 of file rsa.h.

### 5.7.1.2 RSA\_END\_SIZE

```
#define RSA_END_SIZE 29
```

Definition at line 7 of file rsa.h.

### 5.7.1.3 RSA\_FILE\_TOTAL\_SIZE

```
#define RSA_FILE_TOTAL_SIZE 426
```

Definition at line 5 of file rsa.h.

### 5.7.1.4 RSA\_KEY\_SIZE

```
#define RSA_KEY_SIZE 366
```

Definition at line 4 of file rsa.h.

## 5.7.2 Function Documentation

### 5.7.2.1 get\_keys()

```
void get_keys ( )
```

Get the keys object.

Definition at line 21 of file rsa.c.

Here is the call graph for this function: Here is the caller graph for this function:

## 5.8 /home/runner/work/PEPITAS-Cryptocurrency/PEPITAS-Cryptocurrency/headers/cryptosystem/signature.h File Reference

```
#include <stdlib.h>
#include <err.h>
#include <string.h>
#include <openssl/crypto.h>
#include <openssl/ssl3.h>
#include <openssl/rsa.h>
#include <openssl/err.h>
#include "core/blockchain/wallet.h"
#include "core/blockchain/block.h"
```

Include dependency graph for signature.h: This graph shows which files directly or indirectly include this file:

### Functions

- char \* [sign\\_message](#) (char \*data, size\_t len\_data, size\_t \*signature\_len)  
*encrypt(SHA284(msg,len\_data),priv\_key)*
- int [verify\\_signature](#) (void \*data, size\_t data\_len, char \*signature, size\_t signature\_len, RSA \*pub\_key)  
*Apply the SHA384 algorithm on a 'data' of size 'len\_data' and verifies if SHA384(data, len\_data) == 'signature'.*
- int [verify\\_block\\_signature](#) (Block block)  
*Verifies if a block signature is valid.*
- int [verify\\_transaction\\_signature](#) (Transaction transaction)  
*Verifies if a transaction signature is valid.*
- void [get\\_transaction\\_data](#) (Transaction \*trans, char \*\*buff, size\_t \*size)  
*Convert transactions to char \* buffer.*
- char \* [get\\_blockdata\\_data](#) (Block \*block, size\_t \*size)  
*Get the blockdata data object.*
- void [write\\_blockdata](#) (BlockData blockdata, int fd)  
*Writes blockdata in a file.*
- void [write\\_block](#) (Block block, int fd)  
*Writes a block in a file.*
- void [sign\\_block](#) (Block \*block)  
*Signs a block.*
- void [sign\\_transaction](#) (Transaction \*transaction)  
*Sign a transaction.*
- void [sign\\_block\\_transactions](#) (Block \*block)  
*Signs transactions of a block.*

### 5.8.1 Function Documentation

#### 5.8.1.1 [get\\_blockdata\\_data\(\)](#)

```
char* get_blockdata_data (
    Block * block,
    size_t * size )
```

Get the blockdata data object.



## Parameters

<i>block</i>	The block
<i>size</i>	The size of the block

## Returns

char\*

Definition at line 144 of file signature.c.

Here is the call graph for this function: Here is the caller graph for this function:

**5.8.1.2 get\_transaction\_data()**

```
void get_transaction_data (
    Transaction * trans,
    char ** buff,
    size_t * size )
```

Convert transactions to char \* buffer.

## Parameters

<i>transactions</i>	The transaction array
<i>buff</i>	The buffer that receives the transactions
<i>size</i>	The number of transactions in the array

## Returns

The buffer allocated (Must be freed)

Definition at line 93 of file signature.c.

Here is the caller graph for this function:

**5.8.1.3 sign\_block()**

```
void sign_block (
    Block * block )
```

Signs a block.

## Parameters

<i>block</i>	The block to sign
--------------	-------------------

Definition at line 233 of file signature.c.

Here is the call graph for this function:

#### 5.8.1.4 sign\_block\_transactions()

```
void sign_block_transactions (
    Block * block )
```

Signs transactions of a block.

##### Parameters

<i>block</i>	The block to sign
--------------	-------------------

Definition at line 258 of file signature.c.

Here is the call graph for this function:

#### 5.8.1.5 sign\_message()

```
char* sign_message (
    char * data,
    size_t len_data,
    size_t * signature_len )
```

encrypt(SHA284(msg,len\_data),priv\_key)

##### Parameters

<i>data</i>	The data to sign
<i>len_data</i>	The length of the data
<i>signature_len</i>	The length of the data signature

##### Returns

char\*

Definition at line 10 of file signature.c.

Here is the call graph for this function: Here is the caller graph for this function:

#### 5.8.1.6 sign\_transaction()

```
void sign_transaction (
    Transaction * transaction )
```

Sign a transaction.

## Parameters

<i>transaction</i>	The transaction to sign
--------------------	-------------------------

Definition at line 245 of file signature.c.

Here is the call graph for this function: Here is the caller graph for this function:

**5.8.1.7 verify\_block\_signature()**

```
int verify_block_signature (
    Block block )
```

Verifies if a block signature is valid.

## Parameters

<i>block</i>	The block to verify
--------------	---------------------

## Returns

1 if valid, 0 otherwise

Definition at line 206 of file signature.c.

Here is the call graph for this function:

**5.8.1.8 verify\_signature()**

```
int verify_signature (
    void * data,
    size_t data_len,
    char * signature,
    size_t signature_len,
    RSA * pub_key )
```

Apply the SHA384 algorithm on a 'data' of size 'len\_data' and verifies if SHA384(data, len\_data) == 'signature'.

## Parameters

<i>data</i>	The buffer to verify
<i>data_len</i>	The length of the buffer
<i>signature</i>	The signature to compare with SHA384(data, len_data)
<i>signature_len</i>	The length of the signature
<i>pub_key</i>	The RSA public key used for the decryption

**Returns**

int

Definition at line 31 of file signature.c.

Here is the call graph for this function: Here is the caller graph for this function:

**5.8.1.9 verify\_transaction\_signature()**

```
int verify_transaction_signature (  
    Transaction transaction )
```

Verifies if a transaction signature is valid.

**Parameters**

<i>transaction</i>	The transaction to verify
--------------------	---------------------------

**Returns**

1 if valid, 0 otherwise

Definition at line 219 of file signature.c.

Here is the call graph for this function:

**5.8.1.10 write\_block()**

```
void write_block (  
    Block block,  
    int fd )
```

Writes a block in a file.

**Parameters**

<i>block</i>	The block to write
<i>fd</i>	the file descriptor of the file in which the block is written

Definition at line 199 of file signature.c.

Here is the call graph for this function: Here is the caller graph for this function:

**5.8.1.11 write\_blockdata()**

```
void write_blockdata (  
    BlockData blockdata,  
    int fd )
```

Writes blockdata in a file.

## Parameters

<i>blockdata</i>	The blockdata to write
<i>fd</i>	The file descriptor of the file in which the blockdata is written

Definition at line 174 of file signature.c.

Here is the call graph for this function: Here is the caller graph for this function:

## 5.9 /home/runner/work/PEPITAS-Cryptocurrency/PEPITAS-Cryptocurrency/headers/misc/files.h File Reference

This graph shows which files directly or indirectly include this file:

### Functions

- char \* [last\\_file\\_in\\_folder](#) (char folder\_path[])  
Return the last file (reverse alphabetical order) of a folder path.

### 5.9.1 Function Documentation

#### 5.9.1.1 last\_file\_in\_folder()

```
char* last_file_in_folder (
    char folder_path[] )
```

Return the last file (reverse alphabetical order) of a folder path.

## Parameters

<i>folder_path</i>	The path of the folder
--------------------	------------------------

## Returns

char\*, return NULL if any error, must be freed !

Definition at line 7 of file files.c.

Here is the caller graph for this function:

## 5.10 /home/runner/work/PEPITAS-Cryptocurrency/PEPITAS-Cryptocurrency/headers/misc/math.h File Reference

This graph shows which files directly or indirectly include this file:

### Macros

- `#define MIN(a, b) ((a) < (b)) ? (a) : (b)`
- `#define MAX(a, b) ((a) > (b)) ? (a) : (b)`

### 5.10.1 Macro Definition Documentation

#### 5.10.1.1 MAX

```
#define MAX(  
    a,  
    b ) ((a) > (b)) ? (a) : (b)
```

Definition at line 2 of file math.h.

#### 5.10.1.2 MIN

```
#define MIN(  
    a,  
    b ) ((a) < (b)) ? (a) : (b)
```

Definition at line 1 of file math.h.

## 5.11 /home/runner/work/PEPITAS-Cryptocurrency/PEPITAS-Cryptocurrency/headers/misc/safe.h File Reference

```
#include <stdlib.h>  
#include <err.h>  
#include <unistd.h>  
#include <string.h>  
#include <errno.h>
```

Include dependency graph for safe.h: This graph shows which files directly or indirectly include this file:

## Functions

- int [safe\\_write](#) (int fd, const void \*buf, ssize\_t count)  
*Writes safely to a file descriptor.*
- ssize\_t [safe\\_read](#) (int fd, const void \*\*buf, size\_t \*bufsize)  
*Reads safely in a file descriptor until '\r\n\r\n'.*
- ssize\_t [safe\\_fread](#) (void \*buffer, const size\_t size, const size\_t n, FILE \*file)  
*Calls 'fread' but safely !*

### 5.11.1 Function Documentation

#### 5.11.1.1 [safe\\_fread\(\)](#)

```

ssize_t safe_fread (
    void * buffer,
    const size_t size,
    const size_t n,
    FILE * file )

```

Calls 'fread' but safely !

##### Parameters

<i>buffer</i>	The buffer to write on
<i>size</i>	The size of 1 read element
<i>n</i>	The number of elements to read
<i>file</i>	The IO FILE

##### Returns

ssize\_t, -1 if error or the number of read items

Definition at line 40 of file safe.c.

Here is the caller graph for this function:

#### 5.11.1.2 [safe\\_read\(\)](#)

```

ssize_t safe_read (
    int fd,
    const void ** buf,
    size_t * bufsize )

```

Reads safely in a file descriptor until '\r\n\r\n'.



#### Parameters

<i>fd</i>	The file descriptor
<i>buf</i>	The buffer which contains the message

#### Returns

The number of byte the file 'fd', if -1 error

Definition at line 18 of file safe.c.

Here is the caller graph for this function:

#### 5.11.1.3 safe\_write()

```
int safe_write (
    int fd,
    const void * buf,
    ssize_t count )
```

Writes safely to a file descriptor.

#### Parameters

<i>fd</i>	The file descriptor
<i>buf</i>	The buffer to write
<i>count</i>	The number of byte to write in fd

#### Returns

Error code

Definition at line 4 of file safe.c.

Here is the caller graph for this function:

## 5.12 /home/runner/work/PEPITAS-Cryptocurrency/PEPITAS-Cryptocurrency/headers/network/client.h File Reference

```
#include <stddef.h>
```

Include dependency graph for client.h: This graph shows which files directly or indirectly include this file:

#### Data Structures

- struct [Neighbour](#)
- struct [Node](#)

## Macros

- `#define MAX_NEIGHBOURS 64`

## Typedefs

- `typedef struct Neighbour Neighbour`
- `typedef struct Node Node`

## Functions

- `Node * get_my_node ()`  
*Get the my node object.*
- `int set_neighbour (char *hostname, int family)`  
*Sets a neighbour in the client.neighbours section.*
- `int listen_to (size_t neighbour_id)`  
*Tries to connect to the peer-to-peer network via a node in the Node structure.*
- `int ping_client (size_t neighbour_id)`  
*Pings the client side of 'neighbour\_id' and deletes it from struct Node if there is no response.*

### 5.12.1 Macro Definition Documentation

#### 5.12.1.1 MAX\_NEIGHBOURS

```
#define MAX_NEIGHBOURS 64
```

Definition at line 6 of file client.h.

### 5.12.2 Typedef Documentation

#### 5.12.2.1 Neighbour

```
typedef struct Neighbour Neighbour
```

#### 5.12.2.2 Node

```
typedef struct Node Node
```

### 5.12.3 Function Documentation

#### 5.12.3.1 `get_my_node()`

```
Node* get_my_node ( )
```

Get the my node object.

##### Returns

Node\*

Definition at line 5 of file client.c.

Here is the caller graph for this function:

#### 5.12.3.2 `listen_to()`

```
int listen_to (
    size_t neighbour_id )
```

Tries to connect to the peer-to-peer network via a node in the [Node](#) structure.

##### Parameters

<i>neighbour_id</i>	The neighbour's index (in struct <a href="#">Node</a> ) to connect with
---------------------	---

##### Returns

socket FD or -1 if an error occurs

Definition at line 57 of file client.c.

Here is the call graph for this function: Here is the caller graph for this function:

#### 5.12.3.3 `ping_client()`

```
int ping_client (
    size_t neighbour_id )
```

Pings the client side of 'neighbour\_id' and deletes it from struct [Node](#) if there is no response.

##### Parameters

<i>neighbour_id</i>	
---------------------	--

**Returns**

0 if success, -1 otherwise

**5.12.3.4 set\_neighbour()**

```
int set_neighbour (
    char * hostname,
    int family )
```

Sets a neighbour in the client.neighbours section.

**Returns**

0 if success, -1 otherwise

Definition at line 14 of file client.c.

Here is the call graph for this function: Here is the caller graph for this function:

## 5.13 /home/runner/work/PEPITAS-Cryptocurrency/PEPITAS-Cryptocurrency/headers/network/get\_data.h File Reference

This graph shows which files directly or indirectly include this file:

**Functions**

- int [read\\_header](#) (int sockfd)  
*Waits a header in 'sockfd', reads it and processes it.*
- int [fetch\\_client\\_list](#) (int neighbour\_id)  
*Merges my neighbours list with the one sent by 'neighbour\_id'.*

**5.13.1 Function Documentation****5.13.1.1 fetch\_client\_list()**

```
int fetch_client_list (
    int neighbour_id )
```

Merges my neighbours list with the one sent by 'neighbour\_id'.

## Parameters

<code>neighbour↵ _id</code>	The id of the neighbour list to merge
---------------------------------	---------------------------------------

## Returns

0 if sucess, -1 otherwise

Definition at line 32 of file `get_data.c`.

Here is the call graph for this function: Here is the caller graph for this function:

### 5.13.1.2 read\_header()

```
int read_header (  
    int sockfd )
```

Waits a header in 'sockfd', reads it and processes it.

## Parameters

<code>sockfd</code>	The sock FD
---------------------	-------------

## Returns

0 if sucess, -1 otherwise

Definition at line 86 of file `get_data.c`.

Here is the call graph for this function: Here is the caller graph for this function:

## 5.14 /home/runner/work/PEPITAS-Cryptocurrency/PEPITAS-↵ Cryptocurrency/headers/network/network.h File Reference

```
#include <stdio.h>  
#include <stdlib.h>  
#include <unistd.h>  
#include <sys/un.h>  
#include <sys/types.h>  
#include <sys/socket.h>  
#include <netdb.h>  
#include <err.h>  
#include <string.h>  
#include <pthread.h>  
#include <arpa/inet.h>  
#include "misc/safe.h"  
#include "client.h"
```

Include dependency graph for `network.h`: This graph shows which files directly or indirectly include this file:

## Macros

- `#define NB_HARD_CODED_ADDR 2`
- `#define STATIC_PORT "4242"`
- `#define HD_GET_CLIENT_LIST "GET CLIENT LIST\r\n\r\n"`
- `#define HD_SEND_CLIENT_LIST "SEND CLIENT LIST\n"`
- `#define HD_GET_BLOCKCHAIN "GET BLOCKCHAIN\r\n\r\n"`
- `#define HD_SEND_BLOCKCHAIN "SEND BLOCKCHAIN\n"`

## Variables

- `const Neighbour HARD_CODED_ADDR []`

### 5.14.1 Macro Definition Documentation

#### 5.14.1.1 HD\_GET\_BLOCKCHAIN

```
#define HD_GET_BLOCKCHAIN "GET BLOCKCHAIN\r\n\r\n"
```

Definition at line 25 of file network.h.

#### 5.14.1.2 HD\_GET\_CLIENT\_LIST

```
#define HD_GET_CLIENT_LIST "GET CLIENT LIST\r\n\r\n"
```

Definition at line 23 of file network.h.

#### 5.14.1.3 HD\_SEND\_BLOCKCHAIN

```
#define HD_SEND_BLOCKCHAIN "SEND BLOCKCHAIN\n"
```

Definition at line 26 of file network.h.

#### 5.14.1.4 HD\_SEND\_CLIENT\_LIST

```
#define HD_SEND_CLIENT_LIST "SEND CLIENT LIST\n"
```

Definition at line 24 of file network.h.

#### 5.14.1.5 NB\_HARD\_CODED\_ADDR

```
#define NB_HARD_CODED_ADDR 2
```

Definition at line 17 of file network.h.

#### 5.14.1.6 STATIC\_PORT

```
#define STATIC_PORT "4242"
```

Definition at line 20 of file network.h.

### 5.14.2 Variable Documentation

#### 5.14.2.1 HARD\_CODED\_ADDR

```
const Neighbour HARD_CODED_ADDR[ ]
```

Definition at line 4 of file network.c.

## 5.15 /home/runner/work/PEPITAS-Cryptocurrency/PEPITAS-Cryptocurrency/headers/network/send\_data.h File Reference

This graph shows which files directly or indirectly include this file:

### Functions

- int [send\\_client\\_list](#) (int sockfd)  
*Sends my client list to a node via 'sockfd'.*

### 5.15.1 Function Documentation

#### 5.15.1.1 send\_client\_list()

```
int send_client_list (  
    int sockfd )
```

Sends my client list to a node via 'sockfd'.

**Parameters**

<code>sockfd</code>	The sock FD
---------------------	-------------

**Returns**

0 if success, -1 otherwise

Definition at line 3 of file `send_data.c`.

Here is the call graph for this function: Here is the caller graph for this function:

## 5.16 /home/runner/work/PEPITAS-Cryptocurrency/PEPITAS-Cryptocurrency/headers/network/server.h File Reference

```
#include <sys/socket.h>
#include "network.h"
#include "core/blockchain/block.h"
```

Include dependency graph for `server.h`: This graph shows which files directly or indirectly include this file:

**Data Structures**

- struct [client\\_connection](#)

**Typedefs**

- typedef struct [client\\_connection](#) [client\\_connection](#)

**Functions**

- int [init\\_server](#) ()  
*Launches a server instance, connected to the peer-to-peer network 'hostname'.*
- int [send\\_block](#) ([Block](#) block, int sockfd)  
*Sends a block to a user via a socket FD.*

**5.16.1 Typedef Documentation****5.16.1.1 client\_connection**

```
typedef struct client\_connection client\_connection
```



## 5.16.2 Function Documentation

### 5.16.2.1 `init_server()`

```
int init_server ( )
```

Launches a server instance, connected to the peer-to-peer network 'hostname'.

#### Returns

0 if success, -1 otherwise

Definition at line 30 of file server.c.

Here is the call graph for this function: Here is the caller graph for this function:

### 5.16.2.2 `send_block()`

```
int send_block (
    Block block,
    int sockfd )
```

Sends a block to a user via a socket FD.

#### Parameters

<i>sockfd</i>	The socket FD
<i>block</i>	The block to send

#### Returns

int

## 5.17 /home/runner/work/PEPITAS-Cryptocurrency/PEPITAS-Cryptocurrency/headers/ui/ui.h File Reference

```
#include <gtk/gtk.h>
#include <stdio.h>
#include <string.h>
```

Include dependency graph for ui.h: This graph shows which files directly or indirectly include this file:

## Functions

- int `setup()`

*Setups the gtk widgets for the GUI.*

- gboolean [on\\_main\\_window\\_delete](#) (GtkWidget \*widget, \_\_attribute\_\_((unused)) gpointer data)

*Destroys the window when it is closed.*

- void [on\\_main\\_window\\_destroy](#) (\_\_attribute\_\_((unused)) GtkWidget \*widget, \_\_attribute\_\_((unused)) gpointer data)

*Quits GTK when the program ends.*

- gboolean [on\\_transaction\\_button\\_press](#) (GtkWidget \*widget, GdkEventKey \*event, gpointer user\_data)

*Will be used when the transaction function is ready.*

- gboolean [on\\_pkey\\_button\\_press](#) (GtkWidget \*widget, GdkEventKey \*event, gpointer user\_data)

*Hides the private key of the user, or shows it if it was already hidden.*

- gboolean [on\\_invest\\_button1\\_press](#) (GtkWidget \*widget, GdkEventKey \*event, gpointer user\_data)

*Opens the invest window.*

- gboolean [on\\_invest\\_button2\\_press](#) (GtkWidget \*widget, GdkEventKey \*event, gpointer user\_data)

*Resets the entry in the invest window and closes it, will later be used for the invest function.*

- gboolean [on\\_recover\\_button1\\_press](#) (GtkWidget \*widget, GdkEventKey \*event, gpointer user\_data)

*Opens the recover window.*

- gboolean [on\\_recover\\_button2\\_press](#) (GtkWidget \*widget, GdkEventKey \*event, gpointer user\_data)

*Resets the entry in the recover window and closes it, will later be used for the recover function.*

- gboolean [on\\_add\\_contact\\_button1\\_press](#) (GtkWidget \*widget, GdkEventKey \*event, gpointer user\_data)

*Opens the contact window.*

- gboolean [add\\_contact](#) (GtkWidget \*widget, GdkEventKey \*event, gpointer user\_data)

*Adds a contact to the treeview if the entrys weren't empty, and closes the contact window.*

- gboolean [on\\_create\\_key\\_but1\\_press](#) (GtkWidget \*widget, GdkEventKey \*event, gpointer user\_data)

- gboolean [on\\_create\\_key\\_but2\\_press](#) (GtkWidget \*widget, GdkEventKey \*event, gpointer user\_data)

- gboolean [on\\_connect\\_but\\_press](#) (GtkWidget \*widget, GdkEventKey \*event, gpointer user\_data)

- gboolean [update\\_labels](#) (GtkWidget \*widget, GdkEventKey \*event, gpointer user\_data)

## 5.17.1 Function Documentation

### 5.17.1.1 [add\\_contact\(\)](#)

```
gboolean add_contact (
    GtkWidget * widget,
    GdkEventKey * event,
    gpointer user_data )
```

Adds a contact to the treeview if the entrys weren't empty, and closes the contact window.

#### Parameters

<i>widget</i>	unused
<i>event</i>	unused
<i>user_data</i>	unused

#### Returns

gboolean Error code

#### 5.17.1.2 on\_add\_contact\_button1\_press()

```
gboolean on_add_contact_button1_press (
    GtkWidget * widget,
    GdkEventKey * event,
    gpointer user_data )
```

Opens the contact window.

##### Parameters

<i>widget</i>	unused
<i>event</i>	unused
<i>user_data</i>	unused

##### Returns

gboolean Error code

#### 5.17.1.3 on\_connect\_but\_press()

```
gboolean on_connect_but_press (
    GtkWidget * widget,
    GdkEventKey * event,
    gpointer user_data )
```

#### 5.17.1.4 on\_create\_key\_but1\_press()

```
gboolean on_create_key_but1_press (
    GtkWidget * widget,
    GdkEventKey * event,
    gpointer user_data )
```

#### 5.17.1.5 on\_create\_key\_but2\_press()

```
gboolean on_create_key_but2_press (
    GtkWidget * widget,
    GdkEventKey * event,
    gpointer user_data )
```

#### 5.17.1.6 on\_invest\_button1\_press()

```
gboolean on_invest_button1_press (  
    GtkWidget * widget,  
    GdkEventKey * event,  
    gpointer user_data )
```

Opens the invest window.

##### Parameters

<i>widget</i>	unused
<i>event</i>	unused
<i>user_data</i>	unused

##### Returns

gboolean

#### 5.17.1.7 on\_invest\_button2\_press()

```
gboolean on_invest_button2_press (  
    GtkWidget * widget,  
    GdkEventKey * event,  
    gpointer user_data )
```

Resets the entry in the invest window and closes it, will later be used for the invest function.

##### Parameters

<i>widget</i>	unused
<i>event</i>	unused
<i>user_data</i>	unused

##### Returns

gboolean Error Code

#### 5.17.1.8 on\_main\_window\_delete()

```
gboolean on_main_window_delete (  
    GtkWidget * widget,  
    __attribute__((unused)) gpointer data )
```

Destroys the window when it is closed.

**Parameters**

<i>widget</i>	The main window of the GUI
---------------	----------------------------

**Returns**

gboolean Error code

Definition at line 157 of file ui.c.

**5.17.1.9 on\_main\_window\_destroy()**

```
void on_main_window_destroy (
    __attribute__((unused)) GtkWidget * widget,
    __attribute__((unused)) gpointer data )
```

Quits GTK when the program ends.

**5.17.1.10 on\_pkey\_button\_press()**

```
gboolean on_pkey_button_press (
    GtkWidget * widget,
    GdkEventKey * event,
    gpointer user_data )
```

Hides the private key of the user, or shows it if it was already hidden.

**Parameters**

<i>widget</i>	unused
<i>event</i>	unused
<i>user_data</i>	unused

**Returns**

gboolean Error code

**5.17.1.11 on\_recover\_button1\_press()**

```
gboolean on_recover_button1_press (
    GtkWidget * widget,
    GdkEventKey * event,
    gpointer user_data )
```

Opens the recover window.

**Parameters**

<i>widget</i>	unused
<i>event</i>	unused
<i>user_data</i>	unused

**Returns**

gboolean Error code

**5.17.1.12 on\_recover\_button2\_press()**

```
gboolean on_recover_button2_press (  
    GtkWidget * widget,  
    GdkEventKey * event,  
    gpointer user_data )
```

Resets the entry in the recover window and closes it, will later be used for the recover function.

**Parameters**

<i>widget</i>	unused
<i>event</i>	unused
<i>user_data</i>	unused

**Returns**

gboolean Error code

**5.17.1.13 on\_transaction\_button\_press()**

```
gboolean on_transaction_button_press (  
    GtkWidget * widget,  
    GdkEventKey * event,  
    gpointer user_data )
```

Will be used when the transaction function is ready.

**Parameters**

<i>widget</i>	unused
<i>event</i>	unused
<i>user_data</i>	unused

#### Returns

gboolean Error code

#### 5.17.1.14 setup()

```
int setup ( )
```

Setups the gtk widgets for the GUI.

#### Returns

int Returns 1 if there is an error, 0 otherwise

Definition at line 55 of file ui.c.

Here is the caller graph for this function:

#### 5.17.1.15 update\_labels()

```
gboolean update_labels (
    GtkWidget * widget,
    GdkEventKey * event,
    gpointer user_data )
```

## 5.18 /home/runner/work/PEPITAS-Cryptocurrency/PEPITAS-Cryptocurrency/README.md File Reference

## 5.19 /home/runner/work/PEPITAS-Cryptocurrency/PEPITAS-Cryptocurrency/src/client.c File Reference

```
#include <signal.h>
#include <stdlib.h>
#include "network/network.h"
#include "network/client.h"
#include "network/server.h"
#include "network/send_data.h"
#include "network/get_data.h"
```

Include dependency graph for client.c:

#### Functions

- int [main](#) ()

## 5.19.1 Function Documentation

### 5.19.1.1 main()

```
int main ( )
```

Definition at line 10 of file client.c.

Here is the call graph for this function:

## 5.20 /home/runner/work/PEPITAS-Cryptocurrency/PEPITAS-Cryptocurrency/src/network/client.c File Reference

```
#include "network/client.h"
#include "network/server.h"
#include "network/network.h"
```

Include dependency graph for client.c:

## Functions

- [Node](#) \* [get\\_my\\_node](#) ()  
*Get the my node object.*
- int [set\\_neighbour](#) (char \*hostname, int family)  
*Sets a neighbour in the client.neighbours section.*
- int [listen\\_to](#) (size\_t neighbour\_id)  
*Tries to connect to the peer-to-peer network via a node in the [Node](#) structure.*

## 5.20.1 Function Documentation

### 5.20.1.1 get\_my\_node()

```
Node* get_my_node ( )
```

Get the my node object.

#### Returns

[Node](#)\*

Definition at line 5 of file client.c.

Here is the caller graph for this function:

### 5.20.1.2 listen\_to()

```
int listen_to (
    size_t neighbour_id )
```

Tries to connect to the peer-to-peer network via a node in the [Node](#) structure.



## Parameters

<code>neighbour↔ _id</code>	The neighbour's index (in struct <a href="#">Node</a> ) to connect with
---------------------------------	---

## Returns

socket FD or -1 if an error occurs

Definition at line 57 of file client.c.

Here is the call graph for this function: Here is the caller graph for this function:

### 5.20.1.3 set\_neighbour()

```
int set_neighbour (
    char * hostname,
    int family )
```

Sets a neighbour in the client.neighbours section.

## Returns

0 if success, -1 otherwise

Definition at line 14 of file client.c.

Here is the call graph for this function: Here is the caller graph for this function:

## 5.21 /home/runner/work/PEPITAS-Cryptocurrency/PEPITAS- Cryptocurrency/src/core/blockchain/block.c File Reference

```
#include "core/blockchain/block.h"
#include "cryptosystem/signature.h"
#include <sys/stat.h>
#include <unistd.h>
#include <err.h>
#include <errno.h>
#include <openssl/rsa.h>
#include <openssl/crypto.h>
#include <fcntl.h>
#include <sys/types.h>
Include dependency graph for block.c:
```

## Functions

- `ChunkBlockchain * get_blockchain` (size\_t nb\_chunk)  
*Loads a blockchain object with a padding of 'nb\_chunk'.*
- void `write_block_file` (Block block)  
*Writes a block struct in a file.*
- void `convert_data_to_transactiondata` (TransactionData \*transactiondata, FILE \*blockfile)
- void `convert_data_to_transaction` (Transaction \*transaction, FILE \*blockfile)
- void `convert_data_to_blockdata` (BlockData \*blockdata, FILE \*blockfile)
- void `convert_data_to_block` (Block \*block, FILE \*blockfile)
- Block \* `get_block` (size\_t block\_height)
- void `free_block` (Block \*block)  
*Free a block struct.*
- Block \* `get_next_block` (Block \*block)  
*For a block of height  $h$ , returns the block of height  $h+1$*
- Block \* `get_prev_block` (Block \*block)  
*For a block of height  $h$ , return the block of height  $h-1$*

### 5.21.1 Function Documentation

#### 5.21.1.1 convert\_data\_to\_block()

```
void convert_data_to_block (
    Block * block,
    FILE * blockfile )
```

Definition at line 142 of file block.c.

Here is the call graph for this function: Here is the caller graph for this function:

#### 5.21.1.2 convert\_data\_to\_blockdata()

```
void convert_data_to_blockdata (
    BlockData * blockdata,
    FILE * blockfile )
```

Definition at line 116 of file block.c.

Here is the call graph for this function: Here is the caller graph for this function:

#### 5.21.1.3 convert\_data\_to\_transaction()

```
void convert_data_to_transaction (
    Transaction * transaction,
    FILE * blockfile )
```

Definition at line 106 of file block.c.

Here is the call graph for this function: Here is the caller graph for this function:

#### 5.21.1.4 convert\_data\_to\_transactiondata()

```
void convert_data_to_transactiondata (
    TransactionData * transactiondata,
    FILE * blockfile )
```

Definition at line 69 of file block.c.

Here is the caller graph for this function:

#### 5.21.1.5 free\_block()

```
void free_block (
    Block * block )
```

Free a block struct.

##### Parameters

<i>block</i>	The block to free
--------------	-------------------

Definition at line 168 of file block.c.

Here is the caller graph for this function:

#### 5.21.1.6 get\_block()

```
Block* get_block (
    size_t block_height )
```

Definition at line 150 of file block.c.

Here is the call graph for this function: Here is the caller graph for this function:

#### 5.21.1.7 get\_blockchain()

```
ChunkBlockchain* get_blockchain (
    size_t nb_chunk )
```

Loads a blockchain object with a padding of 'nb\_chunk'.

##### Parameters

<i>nb_chunk</i>	The chunk nb, if 0 : return the current blockchain object without modification
-----------------	--

##### Returns

ChunkBlockchain\*, NULL if the [ChunkBlockchain](#) is empty after switching

Definition at line 12 of file block.c.

Here is the call graph for this function: Here is the caller graph for this function:

#### 5.21.1.8 `get_next_block()`

```
Block* get_next_block (  
    Block * block )
```

For a block of height  $h$ , returns the block of height  $h+1$

##### Parameters

<i>block</i>	The base block
--------------	----------------

##### Returns

The next Block\*

Definition at line 184 of file block.c.

Here is the call graph for this function: Here is the caller graph for this function:

#### 5.21.1.9 `get_prev_block()`

```
Block* get_prev_block (  
    Block * block )
```

For a block of height  $h$ , return the block of height  $h-1$

##### Parameters

<i>block</i>	The base block
--------------	----------------

##### Returns

The next Block\*

Definition at line 194 of file block.c.

Here is the call graph for this function: Here is the caller graph for this function:

#### 5.21.1.10 `write_block_file()`

```
void write_block_file (  
    Block block )
```

Writes a block struct in a file.

## Parameters

<i>block</i>	The block to write
--------------	--------------------

Definition at line 51 of file block.c.

Here is the call graph for this function: Here is the caller graph for this function:

## 5.22 /home/runner/work/PEPITAS-Cryptocurrency/PEPITAS-Cryptocurrency/src/core/blockchain/wallet.c File Reference

```
#include <time.h>
#include "core/blockchain/wallet.h"
#include "cryptosystem/rsa.h"
#include "core/blockchain/transaction.h"
Include dependency graph for wallet.c:
```

### Functions

- [Wallet \\*](#) [get\\_my\\_wallet](#) ()  
*Get my wallet object.*
- int [create\\_account](#) ()  
*Creates an account in local and broadcasts the creation to the network.*

### 5.22.1 Function Documentation

#### 5.22.1.1 [create\\_account](#)()

```
int create_account ( )
```

Creates an account in local and broadcasts the creation to the network.

#### Returns

0 if the broadcast succeeds, otherwise 1

Definition at line 19 of file wallet.c.

Here is the call graph for this function:

### 5.22.1.2 `get_my_wallet()`

```
Wallet* get_my_wallet ( )
```

Get my wallet object.

#### Returns

[Wallet](#)

Definition at line 7 of file wallet.c.

Here is the caller graph for this function:

## 5.23 [/home/runner/work/PEPITAS-Cryptocurrency/PEPITAS-Cryptocurrency/src/core/validation/validations.c](#) File Reference

```
#include "core/validation/validations.h"
#include "core/blockchain/block.h"
#include "cryptosystem/signature.h"
#include "cryptosystem/rsa.h"
#include "cryptosystem/hash.h"
#include "misc/math.h"
#include "misc/files.h"
#include "misc/safe.h"
#include <string.h>
#include <openssl/bio.h>
```

Include dependency graph for validations.c:

### Macros

- `#define NB_RSA_CHUNK 2048 / 64`
- `#define MAX_VALIDATORS_PER_BLOCK 10000`

### Functions

- `uint16_t define_nb_validators (size_t n)`
- `RSA ** get_next_committee (size_t *nb_validators)`

*Get the 'next block' validators RSA public keys.*

### 5.23.1 Macro Definition Documentation

### 5.23.1.1 MAX\_VALIDATORS\_PER\_BLOCK

```
#define MAX_VALIDATORS_PER_BLOCK 10000
```

Definition at line 14 of file validations.c.

### 5.23.1.2 NB\_RSA\_CHUNK

```
#define NB_RSA_CHUNK 2048 / 64
```

Definition at line 13 of file validations.c.

## 5.23.2 Function Documentation

### 5.23.2.1 define\_nb\_validators()

```
uint16_t define_nb_validators (
    size_t n )
```

Definition at line 16 of file validations.c.

Here is the caller graph for this function:

### 5.23.2.2 get\_next\_committee()

```
RSA** get_next_committee (
    size_t * nb_validators )
```

Get the 'next block' validators RSA public keys.

#### Parameters

<i>nb_validators</i>	return value, the number of selected validators
----------------------	---

#### See also

The 'next block' is referring to block after the last block available OFFLINE

#### Returns

[\*RSA]

Definition at line 31 of file validations.c.

Here is the call graph for this function: Here is the caller graph for this function:

## 5.24 /home/runner/work/PEPITAS-Cryptocurrency/PEPITAS-Cryptocurrency/src/cryptosystem/hash.c File Reference

```
#include <openssl/sha.h>
#include "cryptosystem/hash.h"
#include "core/blockchain/block.h"
#include "cryptosystem/signature.h"
Include dependency graph for hash.c:
```

### Functions

- char \* [sha384\\_data](#) (void \*data, size\_t len\_data)  
*Apply the SHA384 algorithm on a 'data' of size 'len\_data'.*
- char \* [hash\\_block\\_transactions](#) ([Block](#) \*block)  
*Apply the SHA384 to all block transactions.*

### 5.24.1 Function Documentation

#### 5.24.1.1 hash\_block\_transactions()

```
char* hash_block_transactions (
    Block * block )
```

Apply the SHA384 to all block transactions.

#### Parameters

<i>block</i>	The block to deal with
--------------	------------------------

#### Returns

sha384[SHA384\_DIGEST\_LENGTH]

Definition at line 24 of file hash.c.

Here is the call graph for this function: Here is the caller graph for this function:

#### 5.24.1.2 sha384\_data()

```
char* sha384_data (
    void * data,
    size_t len_data )
```

Apply the SHA384 algorithm on a 'data' of size 'len\_data'.



## Parameters

<i>data</i>	The buffer to hash
<i>len_data</i>	The length of the buffer

## Returns

char[97] (on heap)

Definition at line 6 of file hash.c.

Here is the caller graph for this function:

## 5.25 /home/runner/work/PEPITAS-Cryptocurrency/PEPITAS-Cryptocurrency/src/cryptosystem/rsa.c File Reference

```
#include "cryptosystem/rsa.h"
#include "core/blockchain/wallet.h"
#include <stdio.h>
#include <stdlib.h>
#include <openssl/rsa.h>
#include <openssl/pem.h>
#include <time.h>
#include <sys/types.h>
#include <sys/stat.h>
#include <unistd.h>
#include <err.h>
#include <errno.h>
#include <openssl/bn.h>
#include <openssl/crypto.h>
#include <string.h>
```

Include dependency graph for rsa.c:

## Macros

- `#define RSA_NUM_E 3`

## Functions

- void `get_keys` ()  
*Get the keys object.*

### 5.25.1 Macro Definition Documentation

### 5.25.1.1 RSA\_NUM\_E

```
#define RSA_NUM_E 3
```

Definition at line 16 of file rsa.c.

## 5.25.2 Function Documentation

### 5.25.2.1 get\_keys()

```
void get_keys ( )
```

Get the keys object.

Definition at line 21 of file rsa.c.

Here is the call graph for this function: Here is the caller graph for this function:

## 5.26 /home/runner/work/PEPITAS-Cryptocurrency/PEPITAS-Cryptocurrency/src/cryptosystem/signature.c File Reference

```
#include "core/blockchain/block.h"
#include "cryptosystem/signature.h"
#include "cryptosystem/hash.h"
#include <openssl/bio.h>
#include <openssl/rsa.h>
#include <string.h>
#include <stdio.h>
#include <unistd.h>
```

Include dependency graph for signature.c:

## Functions

- char \* [sign\\_message](#) (char \*data, size\_t len\_data, size\_t \*signature\_len)  
*encrypt(SHA284(msg,len\_data),priv\_key)*
- int [verify\\_signature](#) (void \*data, size\_t data\_len, char \*signature, size\_t signature\_len, RSA \*pub\_key)  
*Apply the SHA384 algorithm on a 'data' of size 'len\_data' and verifies if SHA384(data, len\_data) == 'signature'.*
- void [write\\_transactiondata](#) (TransactionData \*transaction, int fd)
- void [write\\_transaction](#) (Transaction \*transaction, int fd)
- void [get\\_transaction\\_data](#) (Transaction \*trans, char \*\*buff, size\_t \*index)  
*Convert transactions to char \* buffer.*
- char \* [get\\_blockdata\\_data](#) (Block \*block, size\_t \*size)  
*Get the blockdata data object.*
- void [write\\_blockdata](#) (BlockData blockdata, int fd)  
*Writes blockdata in a file.*

- void `write_block` (`Block` block, int fd)  
*Writes a block in a file.*
- int `verify_block_signature` (`Block` block)  
*Verifies if a block signature is valid.*
- int `verify_transaction_signature` (`Transaction` transaction)  
*Verifies if a transaction signature is valid.*
- void `sign_block` (`Block` \*block)  
*Signs a block.*
- void `sign_transaction` (`Transaction` \*transaction)  
*Sign a transaction.*
- void `sign_block_transactions` (`Block` \*block)  
*Signs transactions of a block.*

## 5.26.1 Function Documentation

### 5.26.1.1 `get_blockdata_data()`

```
char* get_blockdata_data (
    Block * block,
    size_t * size )
```

Get the blockdata data object.

#### Parameters

<i>block</i>	The block
<i>size</i>	The size of the block

#### Returns

char\*

Definition at line 144 of file signature.c.

Here is the call graph for this function: Here is the caller graph for this function:

### 5.26.1.2 `get_transaction_data()`

```
void get_transaction_data (
    Transaction * trans,
    char ** buff,
    size_t * size )
```

Convert transactions to char \* buffer.

**Parameters**

<i>transactions</i>	The transaction array
<i>buff</i>	The buffer that receives the transactions
<i>size</i>	The number of transactions in the array

**Returns**

The buffer allocated (Must be freed)

Definition at line 93 of file signature.c.

Here is the caller graph for this function:

**5.26.1.3 sign\_block()**

```
void sign_block (  
    Block * block )
```

Signs a block.

**Parameters**

<i>block</i>	The block to sign
--------------	-------------------

Definition at line 233 of file signature.c.

Here is the call graph for this function:

**5.26.1.4 sign\_block\_transactions()**

```
void sign_block_transactions (  
    Block * block )
```

Signs transactions of a block.

**Parameters**

<i>block</i>	The block to sign
--------------	-------------------

Definition at line 258 of file signature.c.

Here is the call graph for this function:

**5.26.1.5 sign\_message()**

```
char* sign_message (  
    char * data,
```

```
size_t len_data,  
size_t * signature_len )
```

encrypt(SHA284(msg,len\_data),priv\_key)

#### Parameters

<i>data</i>	The data to sign
<i>len_data</i>	The length of the data
<i>signature_len</i>	The length of the data signature

#### Returns

char\*

Definition at line 10 of file signature.c.

Here is the call graph for this function: Here is the caller graph for this function:

#### 5.26.1.6 sign\_transaction()

```
void sign_transaction (  
    Transaction * transaction )
```

Sign a transaction.

#### Parameters

<i>transaction</i>	The transaction to sign
--------------------	-------------------------

Definition at line 245 of file signature.c.

Here is the call graph for this function: Here is the caller graph for this function:

#### 5.26.1.7 verify\_block\_signature()

```
int verify_block_signature (  
    Block block )
```

Verifies if a block signature is valid.

#### Parameters

<i>block</i>	The block to verify
--------------	---------------------

#### Returns

1 if valid, 0 otherwise

Definition at line 206 of file signature.c.

Here is the call graph for this function:

#### 5.26.1.8 verify\_signature()

```
int verify_signature (
    void * data,
    size_t data_len,
    char * signature,
    size_t signature_len,
    RSA * pub_key )
```

Apply the SHA384 algorithm on a 'data' of size 'len\_data' and verifies if SHA384(data, len\_data) == 'signature'.

##### Parameters

<i>data</i>	The buffer to verify
<i>data_len</i>	The length of the buffer
<i>signature</i>	The signature to compare with SHA384(data, len_data)
<i>signature_len</i>	The length of the signature
<i>pub_key</i>	The RSA public key used for the decryption

##### Returns

int

Definition at line 31 of file signature.c.

Here is the call graph for this function: Here is the caller graph for this function:

#### 5.26.1.9 verify\_transaction\_signature()

```
int verify_transaction_signature (
    Transaction transaction )
```

Verifies if a transaction signature is valid.

##### Parameters

<i>transaction</i>	The transaction to verify
--------------------	---------------------------

##### Returns

1 if valid, 0 otherwise

Definition at line 219 of file signature.c.

Here is the call graph for this function:

#### 5.26.1.10 write\_block()

```
void write_block (
    Block block,
    int fd )
```

Writes a block in a file.

##### Parameters

<i>block</i>	The block to write
<i>fd</i>	the file descriptor of the file in which the block is written

Definition at line 199 of file signature.c.

Here is the call graph for this function: Here is the caller graph for this function:

#### 5.26.1.11 write\_blockdata()

```
void write_blockdata (
    BlockData blockdata,
    int fd )
```

Writes blockdata in a file.

##### Parameters

<i>blockdata</i>	The blockdata to write
<i>fd</i>	The file descriptor of the file in which the blockdata is written

Definition at line 174 of file signature.c.

Here is the call graph for this function: Here is the caller graph for this function:

#### 5.26.1.12 write\_transaction()

```
void write_transaction (
    Transaction * transaction,
    int fd )
```

Definition at line 86 of file signature.c.

Here is the call graph for this function: Here is the caller graph for this function:

#### 5.26.1.13 write\_transactiondata()

```
void write_transactiondata (
    TransactionData * transaction,
    int fd )
```

Definition at line 50 of file signature.c.

Here is the caller graph for this function:

## 5.27 /home/runner/work/PEPITAS-Cryptocurrency/PEPITAS-Cryptocurrency/src/gui.c File Reference

```
#include "ui/ui.h"
Include dependency graph for gui.c:
```

### Functions

- int [main](#) (int argc, char \*\*argv)

### 5.27.1 Function Documentation

#### 5.27.1.1 main()

```
int main (
    int argc,
    char ** argv )
```

Definition at line 3 of file gui.c.

Here is the call graph for this function:

## 5.28 /home/runner/work/PEPITAS-Cryptocurrency/PEPITAS-Cryptocurrency/src/misc/files.c File Reference

```
#include "misc/files.h"
#include <dirent.h>
#include <string.h>
#include <stdlib.h>
Include dependency graph for files.c:
```

### Macros

- #define [\\_GNU\\_SOURCE](#)

### Functions

- char \* [last\\_file\\_in\\_folder](#) (char folder\_path[])  
*Return the last file (reverse alphabetical order) of a folder path.*



## 5.28.1 Macro Definition Documentation

### 5.28.1.1 `_GNU_SOURCE`

```
#define _GNU_SOURCE
```

Definition at line 1 of file files.c.

## 5.28.2 Function Documentation

### 5.28.2.1 `last_file_in_folder()`

```
char* last_file_in_folder (
    char folder_path[] )
```

Return the last file (reverse alphabetical order) of a folder path.

#### Parameters

<i>folder_path</i>	The path of the folder
--------------------	------------------------

#### Returns

char\*, return NULL if any error, must be freed !

Definition at line 7 of file files.c.

Here is the caller graph for this function:

## 5.29 /home/runner/work/PEPITAS-Cryptocurrency/PEPITAS-Cryptocurrency/src/misc/safe.c File Reference

```
#include <stdio.h>
#include "misc/safe.h"
Include dependency graph for safe.c:
```

## Functions

- int [safe\\_write](#) (int fd, const void \*buf, ssize\_t count)  
*Writes safely to a file descriptor.*
- ssize\_t [safe\\_read](#) (int fd, const void \*\*buf, size\_t \*bufsize)  
*Reads safely in a file descriptor until '\r\n\r\n'.*
- ssize\_t [safe\\_fread](#) (void \*buffer, const size\_t size, const size\_t n, FILE \*file)  
*Calls 'fread' but safely !*

## 5.29.1 Function Documentation

### 5.29.1.1 `safe_fread()`

```
ssize_t safe_fread (
    void * buffer,
    const size_t size,
    const size_t n,
    FILE * file )
```

Calls 'fread' but safely !

#### Parameters

<i>buffer</i>	The buffer to write on
<i>size</i>	The size of 1 read element
<i>n</i>	The number of elements to read
<i>file</i>	The IO FILE

#### Returns

ssize\_t, -1 if error or the number of read items

Definition at line 40 of file safe.c.

Here is the caller graph for this function:

### 5.29.1.2 `safe_read()`

```
ssize_t safe_read (
    int fd,
    const void ** buf,
    size_t * bufsize )
```

Reads safely in a file descriptor until '\r\n\r\n'.

#### Parameters

<i>fd</i>	The file descriptor
<i>buf</i>	The buffer which contains the message

#### Returns

The number of byte the file 'fd', if -1 error

Definition at line 18 of file safe.c.

Here is the caller graph for this function:

### 5.29.1.3 safe\_write()

```
int safe_write (
    int fd,
    const void * buf,
    ssize_t count )
```

Writes safely to a file descriptor.

#### Parameters

<i>fd</i>	The file descriptor
<i>buf</i>	The buffer to write
<i>count</i>	The number of byte to write in fd

#### Returns

Error code

Definition at line 4 of file safe.c.

Here is the caller graph for this function:

## 5.30 /home/runner/work/PEPITAS-Cryptocurrency/PEPITAS-Cryptocurrency/src/network/get\_data.c File Reference

```
#include "network/client.h"
#include "network/server.h"
#include "network/network.h"
#include "network/send_data.h"
#include "network/get_data.h"
```

Include dependency graph for get\_data.c:

### Functions

- int [process\\_header](#) (char \*header, int sockfd)
- int [fetch\\_client\\_list](#) (int neighbour\_id)  
*Merges my neighbours list with the one sent by 'neighbour\_id'.*
- int [read\\_header](#) (int sockfd)  
*Waits a header in 'sockfd', reads it and processes it.*

### 5.30.1 Function Documentation

#### 5.30.1.1 fetch\_client\_list()

```
int fetch_client_list (
    int neighbour_id )
```

Merges my neighbours list with the one sent by 'neighbour\_id'.

**Parameters**

<i>neighbour</i> ↔ _id	The id of the neighbour list to merge
---------------------------	---------------------------------------

**Returns**

0 if success, -1 otherwise

Definition at line 32 of file `get_data.c`.

Here is the call graph for this function: Here is the caller graph for this function:

**5.30.1.2 process\_header()**

```
int process_header (
    char * header,
    int sockfd )
```

Definition at line 7 of file `get_data.c`.

Here is the call graph for this function: Here is the caller graph for this function:

**5.30.1.3 read\_header()**

```
int read_header (
    int sockfd )
```

Waits a header in 'sockfd', reads it and processes it.

**Parameters**

<i>sockfd</i>	The sock FD
---------------	-------------

**Returns**

0 if success, -1 otherwise

Definition at line 86 of file `get_data.c`.

Here is the call graph for this function: Here is the caller graph for this function:

## 5.31 /home/runner/work/PEPITAS-Cryptocurrency/PEPITAS-↔ Cryptocurrency/src/network/network.c File Reference

```
#include "network/client.h"
#include <arpa/inet.h>
Include dependency graph for network.c:
```

## Variables

- const [Neighbour](#) `HARD_CODED_ADDR` [ ]

### 5.31.1 Variable Documentation

#### 5.31.1.1 `HARD_CODED_ADDR`

```
const Neighbour HARD_CODED_ADDR[ ]
```

##### Initial value:

```
=  
{  
    {AF_INET, "34.72.117.116", 0, 0},  
    {AF_INET, "127.0.0.1", 0, 0}  
}
```

Definition at line 4 of file network.c.

## 5.32 /home/runner/work/PEPITAS-Cryptocurrency/PEPITAS-Cryptocurrency/src/network/send\_data.c File Reference

```
#include "network/network.h"  
Include dependency graph for send_data.c:
```

## Functions

- int [send\\_client\\_list](#) (int sockfd)  
*Sends my client list to a node via 'sockfd'.*

### 5.32.1 Function Documentation

#### 5.32.1.1 `send_client_list()`

```
int send_client_list (  
    int sockfd )
```

Sends my client list to a node via 'sockfd'.

##### Parameters

<code>sockfd</code>	The sock FD
---------------------	-------------

#### Returns

0 if success, -1 otherwise

Definition at line 3 of file send\_data.c.

Here is the call graph for this function: Here is the caller graph for this function:

## 5.33 /home/runner/work/PEPITAS-Cryptocurrency/PEPITAS-Cryptocurrency/src/network/server.c File Reference

```
#include "network/server.h"
#include "network/client.h"
#include "network/get_data.h"
#include "network/network.h"
#include "misc/safe.h"
Include dependency graph for server.c:
```

### Functions

- void \* [accept\\_connection](#) (void \*arg)
- int [init\\_server](#) ()

*Launches a server instance, connected to the peer-to-peer network 'hostname'.*

### 5.33.1 Function Documentation

#### 5.33.1.1 [accept\\_connection\(\)](#)

```
void* accept_connection (
    void * arg )
```

Definition at line 7 of file server.c.

Here is the call graph for this function: Here is the caller graph for this function:

#### 5.33.1.2 [init\\_server\(\)](#)

```
int init_server ( )
```

Launches a server instance, connected to the peer-to-peer network 'hostname'.

#### Returns

0 if success, -1 otherwise

Definition at line 30 of file server.c.

Here is the call graph for this function: Here is the caller graph for this function:

## 5.34 /home/runner/work/PEPITAS-Cryptocurrency/PEPITAS-Cryptocurrency/src/server.c File Reference

```
#include "network/server.h"
#include "network/client.h"
#include "cryptosystem/signature.h"
#include "core/blockchain/block.h"
#include <time.h>
Include dependency graph for server.c:
```

### Functions

- int [main](#) ()

#### 5.34.1 Function Documentation

##### 5.34.1.1 main()

```
int main ( )
```

Definition at line 7 of file server.c.

Here is the call graph for this function:

## 5.35 /home/runner/work/PEPITAS-Cryptocurrency/PEPITAS-Cryptocurrency/src/sign.c File Reference

```
#include "network/network.h"
#include "network/client.h"
#include "network/server.h"
#include "network/send_data.h"
#include "network/get_data.h"
#include "cryptosystem/signature.h"
#include "cryptosystem/rsa.h"
#include "cryptosystem/hash.h"
Include dependency graph for sign.c:
```

### Functions

- int [main](#) ()

## 5.35.1 Function Documentation

### 5.35.1.1 main()

```
int main ( )
```

Definition at line 10 of file sign.c.

Here is the call graph for this function:

## 5.36 /home/runner/work/PEPITAS-Cryptocurrency/PEPITAS-Cryptocurrency/src/ui/ui.c File Reference

```
#include "ui/ui.h"
```

Include dependency graph for ui.c:

## Functions

- int [setup](#) ()  
*Setups the gtk widgets for the GUI.*
- gboolean [on\\_main\\_window\\_delete](#) (GtkWidget \*widget, \_\_attribute\_\_((unused)) gpointer data)  
*Destroys the window when it is closed.*
- void [on\\_main\\_window\\_destroy](#) (\_\_attribute\_\_((unused)) GtkWidget \*widget, \_\_attribute\_\_((unused)) gpointer data)
- gboolean [on\\_transaction\\_button\\_press](#) (\_\_attribute\_\_((unused)) GtkWidget \*widget, \_\_attribute\_\_((unused)) GdkEventKey \*event, \_\_attribute\_\_((unused)) gpointer user\_data)
- gboolean [on\\_pkey\\_button\\_press](#) (\_\_attribute\_\_((unused)) GtkWidget \*widget, \_\_attribute\_\_((unused)) GdkEventKey \*event, \_\_attribute\_\_((unused)) gpointer user\_data)
- gboolean [on\\_invest\\_button1\\_press](#) (\_\_attribute\_\_((unused)) GtkWidget \*widget, \_\_attribute\_\_((unused)) GdkEventKey \*event, \_\_attribute\_\_((unused)) gpointer user\_data)
- gboolean [on\\_invest\\_button2\\_press](#) (\_\_attribute\_\_((unused)) GtkWidget \*widget, \_\_attribute\_\_((unused)) GdkEventKey \*event, \_\_attribute\_\_((unused)) gpointer user\_data)
- gboolean [on\\_recover\\_button1\\_press](#) (\_\_attribute\_\_((unused)) GtkWidget \*widget, \_\_attribute\_\_((unused)) GdkEventKey \*event, \_\_attribute\_\_((unused)) gpointer user\_data)
- gboolean [on\\_recover\\_button2\\_press](#) (\_\_attribute\_\_((unused)) GtkWidget \*widget, \_\_attribute\_\_((unused)) GdkEventKey \*event, \_\_attribute\_\_((unused)) gpointer user\_data)
- gboolean [on\\_add\\_contact\\_button1\\_press](#) (\_\_attribute\_\_((unused)) GtkWidget \*widget, \_\_attribute\_\_((unused)) GdkEventKey \*event, \_\_attribute\_\_((unused)) gpointer user\_data)
- gboolean [add\\_contact](#) (\_\_attribute\_\_((unused)) GtkWidget \*widget, \_\_attribute\_\_((unused)) GdkEventKey \*event, \_\_attribute\_\_((unused)) gpointer user\_data)
- gboolean [on\\_create\\_key\\_but1\\_press](#) (\_\_attribute\_\_((unused)) GtkWidget \*widget, \_\_attribute\_\_((unused)) GdkEventKey \*event, \_\_attribute\_\_((unused)) gpointer user\_data)
- gboolean [on\\_create\\_key\\_but2\\_press](#) (\_\_attribute\_\_((unused)) GtkWidget \*widget, \_\_attribute\_\_((unused)) GdkEventKey \*event, \_\_attribute\_\_((unused)) gpointer user\_data)
- gboolean [on\\_connect\\_but\\_press](#) (\_\_attribute\_\_((unused)) GtkWidget \*widget, \_\_attribute\_\_((unused)) GdkEventKey \*event, \_\_attribute\_\_((unused)) gpointer user\_data)
- gboolean [update\\_labels](#) (\_\_attribute\_\_((unused)) GtkWidget \*widget, \_\_attribute\_\_((unused)) GdkEventKey \*event, \_\_attribute\_\_((unused)) gpointer user\_data)



## Variables

- GtkLabel \* [balance\\_1](#)
- GtkLabel \* [balance\\_2](#)
- GtkLabel \* [private\\_key\\_label](#)
- GtkLabel \* [stake\\_label1](#)
- GtkLabel \* [stake\\_label2](#)
- GtkLabel \* [stake\\_label3](#)
- GtkEntry \* [transa\\_amount](#)
- GtkEntry \* [recipient\\_key](#)
- GtkEntry \* [invest\\_entry](#)
- GtkEntry \* [recover\\_entry](#)
- GtkEntry \* [name\\_entry\\_con](#)
- GtkEntry \* [public\\_key\\_entry\\_con](#)
- GtkEntry \* [password\\_entry1](#)
- GtkEntry \* [password\\_entry2](#)
- GtkTreeView \* [tv\\_con](#)
- GtkTreeStore \* [ts\\_con](#)
- GtkTreeViewColumn \* [cx1\\_con](#)
- GtkTreeViewColumn \* [cx2\\_con](#)
- GtkCellRenderer \* [cr1\\_con](#)
- GtkCellRenderer \* [cr2\\_con](#)
- GtkTreeView \* [tv\\_th](#)
- GtkTreeStore \* [ts\\_th](#)
- GtkTreeViewColumn \* [cx1\\_th](#)
- GtkTreeViewColumn \* [cx2\\_th](#)
- GtkTreeViewColumn \* [cx3\\_th](#)
- GtkTreeViewColumn \* [cx4\\_th](#)
- GtkCellRenderer \* [cr1\\_th](#)
- GtkCellRenderer \* [cr2\\_th](#)
- GtkCellRenderer \* [cr3\\_th](#)
- GtkCellRenderer \* [cr4\\_th](#)

### 5.36.1 Function Documentation

#### 5.36.1.1 `add_contact()`

```
gboolean add_contact (
    __attribute__((unused)) GtkWidget * widget,
    __attribute__((unused)) GdkEventKey * event,
    __attribute__((unused)) gpointer user_data )
```

Definition at line 247 of file ui.c.

#### 5.36.1.2 on\_add\_contact\_button1\_press()

```
gboolean on_add_contact_button1_press (
    __attribute__((unused)) GtkWidget * widget,
    __attribute__((unused)) GdkEventKey * event,
    __attribute__((unused)) gpointer user_data )
```

Definition at line 238 of file ui.c.

#### 5.36.1.3 on\_connect\_but\_press()

```
gboolean on_connect_but_press (
    __attribute__((unused)) GtkWidget * widget,
    __attribute__((unused)) GdkEventKey * event,
    __attribute__((unused)) gpointer user_data )
```

Definition at line 287 of file ui.c.

#### 5.36.1.4 on\_create\_key\_but1\_press()

```
gboolean on_create_key_but1_press (
    __attribute__((unused)) GtkWidget * widget,
    __attribute__((unused)) GdkEventKey * event,
    __attribute__((unused)) gpointer user_data )
```

Definition at line 268 of file ui.c.

#### 5.36.1.5 on\_create\_key\_but2\_press()

```
gboolean on_create_key_but2_press (
    __attribute__((unused)) GtkWidget * widget,
    __attribute__((unused)) GdkEventKey * event,
    __attribute__((unused)) gpointer user_data )
```

Definition at line 277 of file ui.c.

#### 5.36.1.6 on\_invest\_button1\_press()

```
gboolean on_invest_button1_press (
    __attribute__((unused)) GtkWidget * widget,
    __attribute__((unused)) GdkEventKey * event,
    __attribute__((unused)) gpointer user_data )
```

Definition at line 199 of file ui.c.

### 5.36.1.7 on\_invest\_button2\_press()

```
gboolean on_invest_button2_press (
    __attribute__((unused)) GtkWidget * widget,
    __attribute__((unused)) GdkEventKey * event,
    __attribute__((unused)) gpointer user_data )
```

Definition at line 208 of file ui.c.

### 5.36.1.8 on\_main\_window\_delete()

```
gboolean on_main_window_delete (
    GtkWidget * widget,
    __attribute__((unused)) gpointer data )
```

Destroys the window when it is closed.

#### Parameters

<i>widget</i>	The main window of the GUI
---------------	----------------------------

#### Returns

gboolean Error code

Definition at line 157 of file ui.c.

### 5.36.1.9 on\_main\_window\_destroy()

```
void on_main_window_destroy (
    __attribute__((unused)) GtkWidget * widget,
    __attribute__((unused)) gpointer data )
```

Definition at line 166 of file ui.c.

### 5.36.1.10 on\_pkey\_button\_press()

```
gboolean on_pkey_button_press (
    __attribute__((unused)) GtkWidget * widget,
    __attribute__((unused)) GdkEventKey * event,
    __attribute__((unused)) gpointer user_data )
```

Definition at line 181 of file ui.c.

#### 5.36.1.11 on\_recover\_button1\_press()

```
gboolean on_recover_button1_press (
    __attribute__((unused)) GtkWidget * widget,
    __attribute__((unused)) GdkEventKey * event,
    __attribute__((unused)) gpointer user_data )
```

Definition at line 218 of file ui.c.

#### 5.36.1.12 on\_recover\_button2\_press()

```
gboolean on_recover_button2_press (
    __attribute__((unused)) GtkWidget * widget,
    __attribute__((unused)) GdkEventKey * event,
    __attribute__((unused)) gpointer user_data )
```

Definition at line 227 of file ui.c.

#### 5.36.1.13 on\_transaction\_button\_press()

```
gboolean on_transaction_button_press (
    __attribute__((unused)) GtkWidget * widget,
    __attribute__((unused)) GdkEventKey * event,
    __attribute__((unused)) gpointer user_data )
```

Definition at line 173 of file ui.c.

#### 5.36.1.14 setup()

```
int setup ( )
```

Setups the gtk widgets for the GUI.

##### Returns

int Returns 1 if there is an error, 0 otherwise

Definition at line 55 of file ui.c.

Here is the caller graph for this function:

#### 5.36.1.15 update\_labels()

```
gboolean update_labels (
    __attribute__((unused)) GtkWidget * widget,
    __attribute__((unused)) GdkEventKey * event,
    __attribute__((unused)) gpointer user_data )
```

Definition at line 300 of file ui.c.

### 5.36.2 Variable Documentation

#### 5.36.2.1 balance\_1

```
GtkLabel* balance_1
```

Definition at line 23 of file ui.c.

#### 5.36.2.2 balance\_2

```
GtkLabel* balance_2
```

Definition at line 24 of file ui.c.

#### 5.36.2.3 cr1\_con

```
GtkCellRenderer* cr1_con
```

Definition at line 41 of file ui.c.

#### 5.36.2.4 cr1\_th

```
GtkCellRenderer* cr1_th
```

Definition at line 49 of file ui.c.

#### 5.36.2.5 cr2\_con

`GtkCellRenderer* cr2_con`

Definition at line 42 of file ui.c.

#### 5.36.2.6 cr2\_th

`GtkCellRenderer* cr2_th`

Definition at line 50 of file ui.c.

#### 5.36.2.7 cr3\_th

`GtkCellRenderer* cr3_th`

Definition at line 51 of file ui.c.

#### 5.36.2.8 cr4\_th

`GtkCellRenderer* cr4_th`

Definition at line 52 of file ui.c.

#### 5.36.2.9 cx1\_con

`GtkTreeViewColumn* cx1_con`

Definition at line 39 of file ui.c.

#### 5.36.2.10 cx1\_th

`GtkTreeViewColumn* cx1_th`

Definition at line 45 of file ui.c.

#### 5.36.2.11 cx2\_con

GtkTreeViewColumn\* cx2\_con

Definition at line 40 of file ui.c.

#### 5.36.2.12 cx2\_th

GtkTreeViewColumn\* cx2\_th

Definition at line 46 of file ui.c.

#### 5.36.2.13 cx3\_th

GtkTreeViewColumn\* cx3\_th

Definition at line 47 of file ui.c.

#### 5.36.2.14 cx4\_th

GtkTreeViewColumn\* cx4\_th

Definition at line 48 of file ui.c.

#### 5.36.2.15 invest\_entry

GtkEntry\* invest\_entry

Definition at line 31 of file ui.c.

#### 5.36.2.16 name\_entry\_con

GtkEntry\* name\_entry\_con

Definition at line 33 of file ui.c.

**5.36.2.17 password\_entry1**

`GtkEntry* password_entry1`

Definition at line 35 of file ui.c.

**5.36.2.18 password\_entry2**

`GtkEntry* password_entry2`

Definition at line 36 of file ui.c.

**5.36.2.19 private\_key\_label**

`GtkLabel* private_key_label`

Definition at line 25 of file ui.c.

**5.36.2.20 public\_key\_entry\_con**

`GtkEntry* public_key_entry_con`

Definition at line 34 of file ui.c.

**5.36.2.21 recipient\_key**

`GtkEntry* recipient_key`

Definition at line 30 of file ui.c.

**5.36.2.22 recover\_entry**

`GtkEntry* recover_entry`

Definition at line 32 of file ui.c.



#### 5.36.2.23 stake\_label1

```
GtkLabel* stake_label1
```

Definition at line 26 of file ui.c.

#### 5.36.2.24 stake\_label2

```
GtkLabel* stake_label2
```

Definition at line 27 of file ui.c.

#### 5.36.2.25 stake\_label3

```
GtkLabel* stake_label3
```

Definition at line 28 of file ui.c.

#### 5.36.2.26 transa\_amount

```
GtkEntry* transa_amount
```

Definition at line 29 of file ui.c.

#### 5.36.2.27 ts\_con

```
GtkTreeStore* ts_con
```

Definition at line 38 of file ui.c.

#### 5.36.2.28 ts\_th

```
GtkTreeStore* ts_th
```

Definition at line 44 of file ui.c.

**5.36.2.29 tv\_con**

```
GtkTreeView* tv_con
```

Definition at line 37 of file ui.c.

**5.36.2.30 tv\_th**

```
GtkTreeView* tv_th
```

Definition at line 43 of file ui.c.

## **5.37 /home/runner/work/PEPITAS-Cryptocurrency/PEPITAS-Cryptocurrency/tests/gen/GEN\_blockchain\_files.c File Reference**

```
#include "tests_macros.h"
#include "core/blockchain/block.h"
#include "core/blockchain/transaction.h"
```

Include dependency graph for GEN\_blockchain\_files.c: This graph shows which files directly or indirectly include this file:

**Functions**

- void \* [rand\\_data](#) (size\_t size)
- void [gen\\_blockchain](#) (size\_t nb\_blocks)

**5.37.1 Function Documentation****5.37.1.1 gen\_blockchain()**

```
void gen_blockchain (
    size_t nb_blocks )
```

Definition at line 20 of file GEN\_blockchain\_files.c.

Here is the call graph for this function: Here is the caller graph for this function:

### 5.37.1.2 rand\_data()

```
void* rand_data (
    size_t size )
```

Definition at line 5 of file GEN\_blockchain\_files.c.

Here is the caller graph for this function:

## 5.38 /home/runner/work/PEPITAS-Cryptocurrency/PEPITAS-Cryptocurrency/tests/gen/GEN\_validators\_file.c File Reference

```
#include <stdio.h>
#include <openssl/rsa.h>
#include <openssl/pem.h>
#include <string.h>
#include <time.h>
#include <stdlib.h>
#include <math.h>
#include "cryptosystem/rsa.h"
```

Include dependency graph for GEN\_validators\_file.c: This graph shows which files directly or indirectly include this file:

### Macros

- #define NB\_FAKE\_VALIDATORS 10
- #define str(x) #x

### Functions

- void gen\_validators\_file (char path[])  
*Generate a mock validators states file.*

## 5.38.1 Macro Definition Documentation

### 5.38.1.1 NB\_FAKE\_VALIDATORS

```
#define NB_FAKE_VALIDATORS 10
```

Definition at line 11 of file GEN\_validators\_file.c.

### 5.38.1.2 str

```
#define str(
    x ) #x
```

Definition at line 12 of file GEN\_validators\_file.c.

## 5.38.2 Function Documentation

### 5.38.2.1 gen\_validators\_file()

```
void gen_validators_file (
    char path[] )
```

Generate a mock validators states file.

#### Parameters

<i>path</i>	The path of the output file
-------------	-----------------------------

#### See also

For one stake transaction, power += amount / block\_height + amount  
Foreach stake withdraw, power -= power \* withdraw\_stake / user\_total\_stake

validators states file description Header : nb\_validators[sizeof(size\_t)], total\_stake[sizeof(size\_t)], block\_height\_↵  
validity[sizeof(size\_t)] '  
[sizeof(char)] For each 'nb\_validators' : validator\_pkey[RSA\_KEY\_SIZE], user\_stake[sizeof(size\_t)] ,validator\_↵  
power[sizeof(size\_t)], '  
[sizeof(char)]

Definition at line 28 of file GEN\_validators\_file.c.

Here is the caller graph for this function:

## 5.39 /home/runner/work/PEPITAS-Cryptocurrency/PEPITAS-↵ Cryptocurrency/tests/main\_test.c File Reference

```
#include "gen/GEN_validators_file.c"
Include dependency graph for main_test.c:
```

### Functions

- int [main](#) ()

## 5.39.1 Function Documentation

### 5.39.1.1 main()

```
int main ( )
```

Definition at line 3 of file main\_test.c.

Here is the call graph for this function:

## 5.40 /home/runner/work/PEPITAS-Cryptocurrency/PEPITAS- Cryptocurrency/tests/src/core/blockchain/block\_test.c File Reference

```
#include "tests_macros.h"  
#include "core/blockchain/block.h"  
#include "core/blockchain/transaction.h"  
#include "gen/GEN_blockchain_files.c"  
Include dependency graph for block_test.c:
```

### Macros

- #define `NB_BLOCK_PER_CHUNK` 10
- #define `NB MOCK_BLOCKS` 13

### Functions

- void `block_test` (void)

## 5.40.1 Macro Definition Documentation

### 5.40.1.1 NB\_BLOCK\_PER\_CHUNK

```
#define NB_BLOCK_PER_CHUNK 10
```

Definition at line 7 of file block\_test.c.

### 5.40.1.2 NB MOCK BLOCKS

```
#define NB MOCK_BLOCKS 13
```

Definition at line 9 of file block\_test.c.

## 5.40.2 Function Documentation

### 5.40.2.1 block\_test()

```
void block_test (
    void )
```

Definition at line 11 of file block\_test.c.

Here is the call graph for this function: Here is the caller graph for this function:

## 5.41 /home/runner/work/PEPITAS-Cryptocurrency/PEPITAS-Cryptocurrency/tests/src/core/blockchain/block\_test.h File Reference

This graph shows which files directly or indirectly include this file:

### Functions

- void [block\\_test](#) (void)

### 5.41.1 Function Documentation

#### 5.41.1.1 block\_test()

```
void block_test (
    void )
```

Definition at line 11 of file block\_test.c.

Here is the call graph for this function: Here is the caller graph for this function:

## 5.42 /home/runner/work/PEPITAS-Cryptocurrency/PEPITAS- Cryptocurrency/tests/src/core/validation/validations\_test.c File Reference

```
#include "gen/GEN_validators_file.c"
#include "core/validation/validations.h"
#include "tests_macros.h"
```

Include dependency graph for validations\_test.c: This graph shows which files directly or indirectly include this file:

### Functions

- void [validations\\_test](#) ()

#### 5.42.1 Function Documentation

##### 5.42.1.1 validations\_test()

```
void validations_test ( )
```

Definition at line 5 of file validations\_test.c.

Here is the call graph for this function: Here is the caller graph for this function:

## 5.43 /home/runner/work/PEPITAS-Cryptocurrency/PEPITAS- Cryptocurrency/tests/src/cryptosystem/rsa\_test.c File Reference

```
#include "tests_macros.h"
#include "cryptosystem/signature.h"
#include "cryptosystem/rsa.h"
#include "core/blockchain/wallet.h"
#include <stdio.h>
#include <unistd.h>
#include <openssl/sha.h>
#include "misc/safe.h"
#include <fcntl.h>
#include <math.h>
#include <sys/stat.h>
```

Include dependency graph for rsa\_test.c:

### Macros

- #define [MAX](#)(a, b)

## Functions

- void [get\\_keys\\_test](#) ()
- void [get\\_keys\\_equality\\_test](#) ()

### 5.43.1 Macro Definition Documentation

#### 5.43.1.1 MAX

```
#define MAX(
    a,
    b )
```

##### Value:

```
(( __typeof__ (a) _a = (a); \
  __typeof__ (b) _b = (b); \
  _a > _b ? _a : _b; ))
```

### 5.43.2 Function Documentation

#### 5.43.2.1 [get\\_keys\\_equality\\_test\(\)](#)

```
void get_keys_equality_test ( )
```

Definition at line 28 of file `rsa_test.c`.

Here is the call graph for this function: Here is the caller graph for this function:

#### 5.43.2.2 [get\\_keys\\_test\(\)](#)

```
void get_keys_test ( )
```

Definition at line 14 of file `rsa_test.c`.

Here is the call graph for this function: Here is the caller graph for this function:

## 5.44 [/home/runner/work/PEPITAS-Cryptocurrency/PEPITAS-Cryptocurrency/tests/src/cryptosystem/rsa\\_test.h](#) File Reference

This graph shows which files directly or indirectly include this file:



## Functions

- void [get\\_keys\\_test](#) ()
- void [get\\_keys\\_equality\\_test](#) ()

### 5.44.1 Function Documentation

#### 5.44.1.1 [get\\_keys\\_equality\\_test](#)()

```
void get_keys_equality_test ( )
```

Definition at line 28 of file `rsa_test.c`.

Here is the call graph for this function: Here is the caller graph for this function:

#### 5.44.1.2 [get\\_keys\\_test](#)()

```
void get_keys_test ( )
```

Definition at line 14 of file `rsa_test.c`.

Here is the call graph for this function: Here is the caller graph for this function:

## 5.45 /home/runner/work/PEPITAS-Cryptocurrency/PEPITAS- Cryptocurrency/tests/src/cryptosystem/signature\_test.c File Reference

```
#include "tests_macros.h"  
#include "cryptosystem/signature.h"  
Include dependency graph for signature_test.c:
```

## Functions

- void [verify\\_sign\\_test](#) ()

### 5.45.1 Function Documentation

#### 5.45.1.1 `verify_sign_test()`

```
void verify_sign_test ( )
```

Definition at line 4 of file `signature_test.c`.

Here is the call graph for this function: Here is the caller graph for this function:

### 5.46 [/home/runner/work/PEPITAS-Cryptocurrency/PEPITAS-Cryptocurrency/tests/src/cryptosystem/signature\\_test.h](#) File Reference

This graph shows which files directly or indirectly include this file:

#### Functions

- void [verify\\_sign\\_test](#) ()

#### 5.46.1 Function Documentation

##### 5.46.1.1 `verify_sign_test()`

```
void verify_sign_test ( )
```

Definition at line 4 of file `signature_test.c`.

Here is the call graph for this function: Here is the caller graph for this function:

### 5.47 [/home/runner/work/PEPITAS-Cryptocurrency/PEPITAS-Cryptocurrency/tests/src/network/client\\_test.c](#) File Reference

```
#include <signal.h>
#include "tests_macros.h"
#include "network/network.h"
#include "network/client.h"
#include "network/server.h"
#include "network/send_data.h"
#include "network/get_data.h"
```

Include dependency graph for `client_test.c`: This graph shows which files directly or indirectly include this file:

## Functions

- void [network\\_test](#) ()

### 5.47.1 Function Documentation

#### 5.47.1.1 network\_test()

```
void network_test ( )
```

Definition at line 10 of file `client_test.c`.

Here is the call graph for this function: Here is the caller graph for this function:

## 5.48 /home/runner/work/PEPITAS-Cryptocurrency/PEPITAS-Cryptocurrency/tests/src/network/server\_test.c File Reference

```
#include "network/server.h"
```

Include dependency graph for `server_test.c`:

## Functions

- int [main](#) ()

### 5.48.1 Function Documentation

#### 5.48.1.1 main()

```
int main ( )
```

Definition at line 4 of file `server_test.c`.

Here is the call graph for this function:

## 5.49 /home/runner/work/PEPITAS-Cryptocurrency/PEPITAS-Cryptocurrency/tests/tests\_macros.h File Reference

```
#include <stdio.h>
```

Include dependency graph for `tests_macros.h`: This graph shows which files directly or indirectly include this file:

## Macros

- #define `DEBUG`(function)
- #define `LOG`(str...)
- #define `TEST_PASSED`(name...)
- #define `TEST_FAILED`(name, reason...)
- #define `TEST_WARNING`(name, reason...)

### 5.49.1 Macro Definition Documentation

#### 5.49.1.1 DEBUG

```
#define DEBUG(  
    function )
```

**Value:**

```
printf("Testing '%s'...\n", #function); \  
function()
```

Definition at line 5 of file tests\_macros.h.

#### 5.49.1.2 LOG

```
#define LOG(  
    str... )
```

**Value:**

```
printf("\033[0;34m[-]  "); \  
printf(str); \  
printf("\033[0m\n")
```

Definition at line 9 of file tests\_macros.h.

#### 5.49.1.3 TEST\_FAILED

```
#define TEST_FAILED(  
    name,  
    reason... )
```

**Value:**

```
printf("\033[0;31m[X] TEST '%s' failed\n\t-> REASON : ", name); \  
printf(reason); \  
printf("\033[0m\n"); \  
exit(1)
```

Definition at line 19 of file tests\_macros.h.

#### 5.49.1.4 TEST\_PASSED

```
#define TEST_PASSED(  
    name... )
```

**Value:**

```
printf("\033[0;32m[OK] TEST -> "); \br/>printf(name); \br/>printf(" success\033[0m\n")
```

Definition at line 14 of file tests\_macros.h.

#### 5.49.1.5 TEST\_WARNING

```
#define TEST_WARNING(  
    name,  
    reason... )
```

**Value:**

```
printf("\033[0;33m[!] WARNING '%s'\n\t-> BECAUSE : ", name); \br/>printf(reason); \br/>printf("\033[0m\n")
```

Definition at line 25 of file tests\_macros.h.

## 5.50 /home/runner/work/PEPITAS-Cryptocurrency/PEPITAS-Cryptocurrency/tests/unit\_testing.c File Reference

```
#include "tests_macros.h"  
#include "cryptosystem/signature_test.h"  
#include "cryptosystem/rsa_test.h"  
#include "network/client_test.c"  
#include "core/blockchain/block_test.h"  
#include "core/validation/validations_test.c"  
Include dependency graph for unit_testing.c:
```

### Functions

- int [main](#) ()

#### 5.50.1 Function Documentation

##### 5.50.1.1 main()

```
int main ( )
```

Definition at line 8 of file unit\_testing.c.

Here is the call graph for this function:



# Index

/home/runner/work/PEPITAS-Cryptocurrency/PEPITAS-Cryptocurrency/README.md, <a href="#">51</a>	/home/runner/work/PEPITAS-Cryptocurrency/PEPITAS-Cryptocurrency/src/core/blockchain/block.c, <a href="#">53</a>
/home/runner/work/PEPITAS-Cryptocurrency/PEPITAS-Cryptocurrency/headers/core/blockchain/block.h, <a href="#">19</a>	/home/runner/work/PEPITAS-Cryptocurrency/PEPITAS-Cryptocurrency/src/core/blockchain/wallet.c, <a href="#">57</a>
/home/runner/work/PEPITAS-Cryptocurrency/PEPITAS-Cryptocurrency/headers/core/blockchain/transaction.h, <a href="#">19</a>	/home/runner/work/PEPITAS-Cryptocurrency/PEPITAS-Cryptocurrency/src/core/validation/validations.c, <a href="#">58</a>
/home/runner/work/PEPITAS-Cryptocurrency/PEPITAS-Cryptocurrency/headers/core/blockchain/wallet.h, <a href="#">21</a>	/home/runner/work/PEPITAS-Cryptocurrency/PEPITAS-Cryptocurrency/src/cryptosystem/hash.c, <a href="#">60</a>
/home/runner/work/PEPITAS-Cryptocurrency/PEPITAS-Cryptocurrency/headers/core/validation/stake.h, <a href="#">22</a>	/home/runner/work/PEPITAS-Cryptocurrency/PEPITAS-Cryptocurrency/src/cryptosystem/rsa.c, <a href="#">61</a>
/home/runner/work/PEPITAS-Cryptocurrency/PEPITAS-Cryptocurrency/headers/core/validation/validations.h, <a href="#">24</a>	/home/runner/work/PEPITAS-Cryptocurrency/PEPITAS-Cryptocurrency/src/cryptosystem/signature.c, <a href="#">62</a>
/home/runner/work/PEPITAS-Cryptocurrency/PEPITAS-Cryptocurrency/headers/cryptosystem/hash.h, <a href="#">25</a>	/home/runner/work/PEPITAS-Cryptocurrency/PEPITAS-Cryptocurrency/src/gui.c, <a href="#">68</a>
/home/runner/work/PEPITAS-Cryptocurrency/PEPITAS-Cryptocurrency/headers/cryptosystem/rsa.h, <a href="#">26</a>	/home/runner/work/PEPITAS-Cryptocurrency/PEPITAS-Cryptocurrency/src/misc/files.c, <a href="#">68</a>
/home/runner/work/PEPITAS-Cryptocurrency/PEPITAS-Cryptocurrency/headers/cryptosystem/signature.h, <a href="#">28</a>	/home/runner/work/PEPITAS-Cryptocurrency/PEPITAS-Cryptocurrency/src/misc/safe.c, <a href="#">69</a>
/home/runner/work/PEPITAS-Cryptocurrency/PEPITAS-Cryptocurrency/headers/misc/files.h, <a href="#">34</a>	/home/runner/work/PEPITAS-Cryptocurrency/PEPITAS-Cryptocurrency/src/network/client.c, <a href="#">52</a>
/home/runner/work/PEPITAS-Cryptocurrency/PEPITAS-Cryptocurrency/headers/misc/math.h, <a href="#">35</a>	/home/runner/work/PEPITAS-Cryptocurrency/PEPITAS-Cryptocurrency/src/network/get_data.c, <a href="#">71</a>
/home/runner/work/PEPITAS-Cryptocurrency/PEPITAS-Cryptocurrency/headers/misc/safe.h, <a href="#">35</a>	/home/runner/work/PEPITAS-Cryptocurrency/PEPITAS-Cryptocurrency/src/network/network.c, <a href="#">72</a>
/home/runner/work/PEPITAS-Cryptocurrency/PEPITAS-Cryptocurrency/headers/network/client.h, <a href="#">37</a>	/home/runner/work/PEPITAS-Cryptocurrency/PEPITAS-Cryptocurrency/src/network/send_data.c, <a href="#">73</a>
/home/runner/work/PEPITAS-Cryptocurrency/PEPITAS-Cryptocurrency/headers/network/get_data.h, <a href="#">40</a>	/home/runner/work/PEPITAS-Cryptocurrency/PEPITAS-Cryptocurrency/src/network/server.c, <a href="#">74</a>
/home/runner/work/PEPITAS-Cryptocurrency/PEPITAS-Cryptocurrency/headers/network/network.h, <a href="#">41</a>	/home/runner/work/PEPITAS-Cryptocurrency/PEPITAS-Cryptocurrency/src/server.c, <a href="#">75</a>
/home/runner/work/PEPITAS-Cryptocurrency/PEPITAS-Cryptocurrency/headers/network/send_data.h, <a href="#">43</a>	/home/runner/work/PEPITAS-Cryptocurrency/PEPITAS-Cryptocurrency/src/sign.c, <a href="#">75</a>
/home/runner/work/PEPITAS-Cryptocurrency/PEPITAS-Cryptocurrency/headers/network/server.h, <a href="#">44</a>	/home/runner/work/PEPITAS-Cryptocurrency/PEPITAS-Cryptocurrency/src/ui/ui.c, <a href="#">76</a>
/home/runner/work/PEPITAS-Cryptocurrency/PEPITAS-Cryptocurrency/headers/ui/ui.h, <a href="#">45</a>	/home/runner/work/PEPITAS-Cryptocurrency/PEPITAS-Cryptocurrency/tests/gen/GEN_blockchain_files.c, <a href="#">86</a>
/home/runner/work/PEPITAS-Cryptocurrency/PEPITAS-Cryptocurrency/src/client.c, <a href="#">51</a>	/home/runner/work/PEPITAS-Cryptocurrency/PEPITAS-Cryptocurrency/tests/gen/GEN_validators_file.c, <a href="#">87</a>
	/home/runner/work/PEPITAS-Cryptocurrency/PEPITAS-Cryptocurrency/tests/main_test.c, <a href="#">88</a>
	/home/runner/work/PEPITAS-Cryptocurrency/PEPITAS-Cryptocurrency/tests/src/core/blockchain/block_test.c, <a href="#">89</a>

- /home/runner/work/PEPITAS-Cryptocurrency/PEPITAS-
  - Cryptocurrency/tests/src/core/blockchain/block\_test.h
    - get\_next\_block, 56
    - get\_prev\_block, 56
    - write\_block\_file, 56
- /home/runner/work/PEPITAS-Cryptocurrency/PEPITAS-
  - Cryptocurrency/tests/src/core/validation/validations\_test.h
    - block\_data
    - block, 7
    - block\_signature
- /home/runner/work/PEPITAS-Cryptocurrency/PEPITAS-
  - Cryptocurrency/tests/src/cryptosystem/rsa\_test.c
    - Block, 7
    - block\_test
    - block\_test.c, 90
- /home/runner/work/PEPITAS-Cryptocurrency/PEPITAS-
  - Cryptocurrency/tests/src/cryptosystem/rsa\_test.h
    - block\_test.h, 90
    - block\_test.c
    - block\_test, 90
- /home/runner/work/PEPITAS-Cryptocurrency/PEPITAS-
  - Cryptocurrency/tests/src/cryptosystem/signature\_test.c
    - NB\_BLOCK\_PER\_CHUNK, 89
    - NB MOCK\_BLOCKS, 89
    - block\_test.h
- /home/runner/work/PEPITAS-Cryptocurrency/PEPITAS-
  - Cryptocurrency/tests/src/cryptosystem/signature\_test.h
    - block\_test, 90
    - block\_timestamp
    - BlockData, 9
- /home/runner/work/PEPITAS-Cryptocurrency/PEPITAS-
  - Cryptocurrency/tests/src/network/client\_test.c,
    - BlockData, 8
    - block\_timestamp, 9
    - height, 9
- /home/runner/work/PEPITAS-Cryptocurrency/PEPITAS-
  - Cryptocurrency/tests/src/network/server\_test.c,
    - magic, 9
    - nb\_transactions, 9
    - previous\_block\_hash, 9
    - transactions, 9
    - validator\_public\_key, 10
- /home/runner/work/PEPITAS-Cryptocurrency/PEPITAS-
  - Cryptocurrency/tests/tests\_macros.h, 95
- /home/runner/work/PEPITAS-Cryptocurrency/PEPITAS-
  - Cryptocurrency/tests/unit\_testing.c, 97
- \_GNU\_SOURCE
  - files.c, 69
- accept\_connection
  - server.c, 74
- add\_contact
  - ui.c, 77
  - ui.h, 46
- amount
  - TransactionData, 15
  - Wallet, 17
- asset
  - TransactionData, 15
- balance\_1
  - ui.c, 81
- balance\_2
  - ui.c, 81
- Block, 7
  - block\_data, 7
  - block\_signature, 7
  - chunk\_id, 8
  - signature\_len, 8
- block.c
  - convert\_data\_to\_block, 54
  - convert\_data\_to\_blockdata, 54
  - convert\_data\_to\_transaction, 54
  - convert\_data\_to\_transactiondata, 54
  - free\_block, 55
  - get\_block, 55
  - get\_blockchain, 55
- cause
  - TransactionData, 15
- chunk
  - ChunkBlockchain, 10
- chunk\_id
  - Block, 8
- chunk\_nb
  - ChunkBlockchain, 10
- ChunkBlockchain, 10
  - chunk, 10
  - chunk\_nb, 10
- client.c
  - get\_my\_node, 52
  - listen\_to, 52
  - main, 52
  - set\_neighbour, 53
- client.h
  - get\_my\_node, 39
  - listen\_to, 39
  - MAX\_NEIGHBOURS, 38
  - Neighbour, 38
  - Node, 38
  - ping\_client, 39
  - set\_neighbour, 40
- client\_connection, 11
  - info, 11
  - server.h, 44
  - socket, 11
- client\_sockfd
  - Neighbour, 12
- client\_test.c
  - network\_test, 95



- convert\_data\_to\_block
  - block.c, [54](#)
- convert\_data\_to\_blockdata
  - block.c, [54](#)
- convert\_data\_to\_transaction
  - block.c, [54](#)
- convert\_data\_to\_transactiondata
  - block.c, [54](#)
- cr1\_con
  - ui.c, [81](#)
- cr1\_th
  - ui.c, [81](#)
- cr2\_con
  - ui.c, [81](#)
- cr2\_th
  - ui.c, [82](#)
- cr3\_th
  - ui.c, [82](#)
- cr4\_th
  - ui.c, [82](#)
- create\_account
  - wallet.c, [57](#)
  - wallet.h, [22](#)
- cx1\_con
  - ui.c, [82](#)
- cx1\_th
  - ui.c, [82](#)
- cx2\_con
  - ui.c, [82](#)
- cx2\_th
  - ui.c, [83](#)
- cx3\_th
  - ui.c, [83](#)
- cx4\_th
  - ui.c, [83](#)
- DEBUG
  - tests\_macros.h, [96](#)
- define\_nb\_validators
  - validations.c, [59](#)
- family
  - Neighbour, [12](#)
- fetch\_client\_list
  - get\_data.c, [71](#)
  - get\_data.h, [40](#)
- files.c
  - \_GNU\_SOURCE, [69](#)
  - last\_file\_in\_folder, [69](#)
- files.h
  - last\_file\_in\_folder, [34](#)
- free\_block
  - block.c, [55](#)
- GEN\_blockchain\_files.c
  - gen\_blockchain, [86](#)
  - rand\_data, [86](#)
- gen\_blockchain
  - GEN\_blockchain\_files.c, [86](#)
- gen\_validators\_file
  - GEN\_validators\_file.c, [88](#)
- GEN\_validators\_file.c
  - gen\_validators\_file, [88](#)
  - NB\_FAKE\_VALIDATORS, [87](#)
  - str, [87](#)
- get\_amount
  - validations.h, [24](#)
- get\_block
  - block.c, [55](#)
- get\_blockchain
  - block.c, [55](#)
- get\_blockdata\_data
  - signature.c, [63](#)
  - signature.h, [28](#)
- get\_data.c
  - fetch\_client\_list, [71](#)
  - process\_header, [72](#)
  - read\_header, [72](#)
- get\_data.h
  - fetch\_client\_list, [40](#)
  - read\_header, [41](#)
- get\_keys
  - rsa.c, [62](#)
  - rsa.h, [27](#)
- get\_keys\_equality\_test
  - rsa\_test.c, [92](#)
  - rsa\_test.h, [93](#)
- get\_keys\_test
  - rsa\_test.c, [92](#)
  - rsa\_test.h, [93](#)
- get\_my\_node
  - client.c, [52](#)
  - client.h, [39](#)
- get\_my\_wallet
  - wallet.c, [57](#)
  - wallet.h, [22](#)
- get\_next\_block
  - block.c, [56](#)
- get\_next\_committee
  - validations.c, [59](#)
  - validations.h, [24](#)
- get\_prev\_block
  - block.c, [56](#)
- get\_transaction\_data
  - signature.c, [63](#)
  - signature.h, [29](#)
- gui.c
  - main, [68](#)
- HARD\_CODED\_ADDR
  - network.c, [73](#)
  - network.h, [43](#)
- hash.c
  - hash\_block\_transactions, [60](#)
  - sha384\_data, [60](#)
- hash.h
  - hash\_block\_transactions, [25](#)
  - sha384\_data, [26](#)

- hash\_block\_transactions
  - hash.c, [60](#)
  - hash.h, [25](#)
- HD\_GET\_BLOCKCHAIN
  - network.h, [42](#)
- HD\_GET\_CLIENT\_LIST
  - network.h, [42](#)
- HD\_SEND\_BLOCKCHAIN
  - network.h, [42](#)
- HD\_SEND\_CLIENT\_LIST
  - network.h, [42](#)
- height
  - BlockData, [9](#)
- hostname
  - Neighbour, [12](#)
- info
  - client\_connection, [11](#)
- init\_server
  - server.c, [74](#)
  - server.h, [45](#)
- invest\_entry
  - ui.c, [83](#)
- is\_validator
  - Wallet, [17](#)
- last\_file\_in\_folder
  - files.c, [69](#)
  - files.h, [34](#)
- listen\_to
  - client.c, [52](#)
  - client.h, [39](#)
- LOG
  - tests\_macros.h, [96](#)
- magic
  - BlockData, [9](#)
- main
  - client.c, [52](#)
  - gui.c, [68](#)
  - main\_test.c, [89](#)
  - server.c, [75](#)
  - server\_test.c, [95](#)
  - sign.c, [76](#)
  - unit\_testing.c, [97](#)
- main\_test.c
  - main, [89](#)
- math.h
  - MAX, [35](#)
  - MIN, [35](#)
- MAX
  - math.h, [35](#)
  - rsa\_test.c, [92](#)
- MAX\_NEIGHBOURS
  - client.h, [38](#)
- MAX\_VALIDATORS\_PER\_BLOCK
  - validations.c, [58](#)
- MIN
  - math.h, [35](#)
- name\_entry\_con
  - ui.c, [83](#)
- NB\_BLOCK\_PER\_CHUNK
  - block\_test.c, [89](#)
- NB\_FAKE\_VALIDATORS
  - GEN\_validators\_file.c, [87](#)
- NB\_HARD\_CODED\_ADDR
  - network.h, [42](#)
- NB MOCK\_BLOCKS
  - block\_test.c, [89](#)
- NB\_RSA\_CHUNK
  - validations.c, [59](#)
- nb\_transactions
  - BlockData, [9](#)
- Neighbour, [12](#)
  - client.h, [38](#)
  - client\_sockfd, [12](#)
  - family, [12](#)
  - hostname, [12](#)
  - server\_sockfd, [12](#)
- neighbours
  - Node, [13](#)
- network.c
  - HARD\_CODED\_ADDR, [73](#)
- network.h
  - HARD\_CODED\_ADDR, [43](#)
  - HD\_GET\_BLOCKCHAIN, [42](#)
  - HD\_GET\_CLIENT\_LIST, [42](#)
  - HD\_SEND\_BLOCKCHAIN, [42](#)
  - HD\_SEND\_CLIENT\_LIST, [42](#)
  - NB\_HARD\_CODED\_ADDR, [42](#)
  - STATIC\_PORT, [43](#)
- network\_test
  - client\_test.c, [95](#)
- Node, [13](#)
  - client.h, [38](#)
  - neighbours, [13](#)
- on\_add\_contact\_button1\_press
  - ui.c, [77](#)
  - ui.h, [47](#)
- on\_connect\_but\_press
  - ui.c, [78](#)
  - ui.h, [47](#)
- on\_create\_key\_but1\_press
  - ui.c, [78](#)
  - ui.h, [47](#)
- on\_create\_key\_but2\_press
  - ui.c, [78](#)
  - ui.h, [47](#)
- on\_invest\_button1\_press
  - ui.c, [78](#)
  - ui.h, [47](#)
- on\_invest\_button2\_press
  - ui.c, [78](#)
  - ui.h, [48](#)
- on\_main\_window\_delete
  - ui.c, [79](#)
  - ui.h, [48](#)

- on\_main\_window\_destroy
  - ui.c, [79](#)
  - ui.h, [49](#)
- on\_pkey\_button\_press
  - ui.c, [79](#)
  - ui.h, [49](#)
- on\_recover\_button1\_press
  - ui.c, [79](#)
  - ui.h, [49](#)
- on\_recover\_button2\_press
  - ui.c, [80](#)
  - ui.h, [50](#)
- on\_transaction\_button\_press
  - ui.c, [80](#)
  - ui.h, [50](#)
- organisation\_public\_key
  - TransactionData, [15](#)
- password\_entry1
  - ui.c, [83](#)
- password\_entry2
  - ui.c, [84](#)
- ping\_client
  - client.h, [39](#)
- pop\_stake
  - stake.h, [23](#)
- previous\_block\_hash
  - BlockData, [9](#)
- priv\_key
  - Wallet, [17](#)
- private\_key\_label
  - ui.c, [84](#)
- process\_header
  - get\_data.c, [72](#)
- pub\_key
  - Wallet, [17](#)
- public\_key\_entry\_con
  - ui.c, [84](#)
- push\_stake
  - stake.h, [23](#)
- rand\_data
  - GEN\_blockchain\_files.c, [86](#)
- read\_header
  - get\_data.c, [72](#)
  - get\_data.h, [41](#)
- receiver\_public\_key
  - TransactionData, [16](#)
- receiver\_remaining\_money
  - TransactionData, [16](#)
- recipient\_key
  - ui.c, [84](#)
- recover\_entry
  - ui.c, [84](#)
- rsa.c
  - get\_keys, [62](#)
  - RSA\_NUM\_E, [61](#)
- rsa.h
  - get\_keys, [27](#)
  - RSA\_BEGIN\_SIZE, [26](#)
  - RSA\_END\_SIZE, [27](#)
  - RSA\_FILE\_TOTAL\_SIZE, [27](#)
  - RSA\_KEY\_SIZE, [27](#)
- RSA\_BEGIN\_SIZE
  - rsa.h, [26](#)
- RSA\_END\_SIZE
  - rsa.h, [27](#)
- RSA\_FILE\_TOTAL\_SIZE
  - rsa.h, [27](#)
- RSA\_KEY\_SIZE
  - rsa.h, [27](#)
- RSA\_NUM\_E
  - rsa.c, [61](#)
- rsa\_test.c
  - get\_keys\_equality\_test, [92](#)
  - get\_keys\_test, [92](#)
  - MAX, [92](#)
- rsa\_test.h
  - get\_keys\_equality\_test, [93](#)
  - get\_keys\_test, [93](#)
- safe.c
  - safe\_fread, [70](#)
  - safe\_read, [70](#)
  - safe\_write, [70](#)
- safe.h
  - safe\_fread, [36](#)
  - safe\_read, [36](#)
  - safe\_write, [37](#)
- safe\_fread
  - safe.c, [70](#)
  - safe.h, [36](#)
- safe\_read
  - safe.c, [70](#)
  - safe.h, [36](#)
- safe\_write
  - safe.c, [70](#)
  - safe.h, [37](#)
- send\_block
  - server.h, [45](#)
- send\_client\_list
  - send\_data.c, [73](#)
  - send\_data.h, [43](#)
- send\_data.c
  - send\_client\_list, [73](#)
- send\_data.h
  - send\_client\_list, [43](#)
- send\_money
  - transaction.h, [20](#)
- sender\_public\_key
  - TransactionData, [16](#)
- sender\_remaining\_money
  - TransactionData, [16](#)
- server.c
  - accept\_connection, [74](#)
  - init\_server, [74](#)
  - main, [75](#)
- server.h

- client\_connection, 44
  - init\_server, 45
  - send\_block, 45
- server\_sockfd
  - Neighbour, 12
- server\_test.c
  - main, 95
- set\_neighbour
  - client.c, 53
  - client.h, 40
- setup
  - ui.c, 80
  - ui.h, 51
- sha384\_data
  - hash.c, 60
  - hash.h, 26
- sign.c
  - main, 76
- sign\_block
  - signature.c, 64
  - signature.h, 29
- sign\_block\_transactions
  - signature.c, 64
  - signature.h, 30
- sign\_message
  - signature.c, 64
  - signature.h, 30
- sign\_transaction
  - signature.c, 65
  - signature.h, 30
- signature.c
  - get\_blockdata\_data, 63
  - get\_transaction\_data, 63
  - sign\_block, 64
  - sign\_block\_transactions, 64
  - sign\_message, 64
  - sign\_transaction, 65
  - verify\_block\_signature, 65
  - verify\_signature, 66
  - verify\_transaction\_signature, 66
  - write\_block, 66
  - write\_blockdata, 67
  - write\_transaction, 67
  - write\_transactiondata, 67
- signature.h
  - get\_blockdata\_data, 28
  - get\_transaction\_data, 29
  - sign\_block, 29
  - sign\_block\_transactions, 30
  - sign\_message, 30
  - sign\_transaction, 30
  - verify\_block\_signature, 31
  - verify\_signature, 31
  - verify\_transaction\_signature, 32
  - write\_block, 32
  - write\_blockdata, 32
- signature\_len
  - Block, 8
- Transaction, 14
- signature\_test.c
  - verify\_sign\_test, 93
- signature\_test.h
  - verify\_sign\_test, 94
- socket
  - client\_connection, 11
- stake.h
  - pop\_stake, 23
  - push\_stake, 23
- stake\_label1
  - ui.c, 84
- stake\_label2
  - ui.c, 85
- stake\_label3
  - ui.c, 85
- STATIC\_PORT
  - network.h, 43
- str
  - GEN\_validators\_file.c, 87
- TEST\_FAILED
  - tests\_macros.h, 96
- TEST\_PASSED
  - tests\_macros.h, 96
- TEST\_WARNING
  - tests\_macros.h, 97
- tests\_macros.h
  - DEBUG, 96
  - LOG, 96
  - TEST\_FAILED, 96
  - TEST\_PASSED, 96
  - TEST\_WARNING, 97
- transa\_amount
  - ui.c, 85
- Transaction, 13
  - signature\_len, 14
  - transaction.h, 20
  - transaction\_data, 14
  - transaction\_signature, 14
- transaction.h
  - send\_money, 20
  - Transaction, 20
  - TRANSACTION\_DATA\_SIZE, 20
  - TRANSACTION\_SIZE, 20
  - TransactionData, 20
- transaction\_data
  - Transaction, 14
- TRANSACTION\_DATA\_SIZE
  - transaction.h, 20
- transaction\_signature
  - Transaction, 14
- TRANSACTION\_SIZE
  - transaction.h, 20
- transaction\_timestamp
  - TransactionData, 16
- TransactionData, 14
  - amount, 15
  - asset, 15

- cause, 15
- organisation\_public\_key, 15
- receiver\_public\_key, 16
- receiver\_remaining\_money, 16
- sender\_public\_key, 16
- sender\_remaining\_money, 16
- transaction.h, 20
- transaction\_timestamp, 16
- transactions
  - BlockData, 9
- ts\_con
  - ui.c, 85
- ts\_th
  - ui.c, 85
- tv\_con
  - ui.c, 85
- tv\_th
  - ui.c, 86
- ui.c
  - add\_contact, 77
  - balance\_1, 81
  - balance\_2, 81
  - cr1\_con, 81
  - cr1\_th, 81
  - cr2\_con, 81
  - cr2\_th, 82
  - cr3\_th, 82
  - cr4\_th, 82
  - cx1\_con, 82
  - cx1\_th, 82
  - cx2\_con, 82
  - cx2\_th, 83
  - cx3\_th, 83
  - cx4\_th, 83
  - invest\_entry, 83
  - name\_entry\_con, 83
  - on\_add\_contact\_button1\_press, 77
  - on\_connect\_but\_press, 78
  - on\_create\_key\_but1\_press, 78
  - on\_create\_key\_but2\_press, 78
  - on\_invest\_button1\_press, 78
  - on\_invest\_button2\_press, 78
  - on\_main\_window\_delete, 79
  - on\_main\_window\_destroy, 79
  - on\_pkey\_button\_press, 79
  - on\_recover\_button1\_press, 79
  - on\_recover\_button2\_press, 80
  - on\_transaction\_button\_press, 80
  - password\_entry1, 83
  - password\_entry2, 84
  - private\_key\_label, 84
  - public\_key\_entry\_con, 84
  - recipient\_key, 84
  - recover\_entry, 84
  - setup, 80
  - stake\_label1, 84
  - stake\_label2, 85
  - stake\_label3, 85
  - transa\_amount, 85
  - ts\_con, 85
  - ts\_th, 85
  - tv\_con, 85
  - tv\_th, 86
  - update\_labels, 80
- ui.h
  - add\_contact, 46
  - on\_add\_contact\_button1\_press, 47
  - on\_connect\_but\_press, 47
  - on\_create\_key\_but1\_press, 47
  - on\_create\_key\_but2\_press, 47
  - on\_invest\_button1\_press, 47
  - on\_invest\_button2\_press, 48
  - on\_main\_window\_delete, 48
  - on\_main\_window\_destroy, 49
  - on\_pkey\_button\_press, 49
  - on\_recover\_button1\_press, 49
  - on\_recover\_button2\_press, 50
  - on\_transaction\_button\_press, 50
  - setup, 51
  - update\_labels, 51
- unit\_testing.c
  - main, 97
- update\_labels
  - ui.c, 80
  - ui.h, 51
- validations.c
  - define\_nb\_validators, 59
  - get\_next\_committee, 59
  - MAX\_VALIDATORS\_PER\_BLOCK, 58
  - NB\_RSA\_CHUNK, 59
- validations.h
  - get\_amount, 24
  - get\_next\_committee, 24
- validations\_test
  - validations\_test.c, 91
- validations\_test.c
  - validations\_test, 91
- validator\_public\_key
  - BlockData, 10
- verify\_block\_signature
  - signature.c, 65
  - signature.h, 31
- verify\_sign\_test
  - signature\_test.c, 93
  - signature\_test.h, 94
- verify\_signature
  - signature.c, 66
  - signature.h, 31
- verify\_transaction\_signature
  - signature.c, 66
  - signature.h, 32
- Wallet, 17
  - amount, 17
  - is\_validator, 17
  - priv\_key, 17

- pub\_key, [17](#)
- wallet.h, [21](#)
- wallet.c
  - create\_account, [57](#)
  - get\_my\_wallet, [57](#)
- wallet.h
  - create\_account, [22](#)
  - get\_my\_wallet, [22](#)
  - Wallet, [21](#)
- write\_block
  - signature.c, [66](#)
  - signature.h, [32](#)
- write\_block\_file
  - block.c, [56](#)
- write\_blockdata
  - signature.c, [67](#)
  - signature.h, [32](#)
- write\_transaction
  - signature.c, [67](#)
- write\_transactiondata
  - signature.c, [67](#)