



Community Call #1

Francisco Giordano

frangio@openzeppelin.com

🐦 @frangio_

Hadrien Croubois

hadrien@openzeppelin.com

🐦 @Amxx



Our mission is to protect
the open economy

OpenZeppelin is a software company that
provides **security audits** and **products** for
decentralized systems.

Projects from any size — from new startups to
established organizations — trust OpenZeppelin
to build, inspect and connect to the open
economy.



Security, Reliability and Risk Management

OpenZeppelin provides a complete suite of **security and reliability products** to build, manage, and inspect all aspects of software development and operations for Ethereum projects.



Why do a community call

Give visibility to new features & improvements

Involve you in the process

Provide feedback

Request features

Engage discussion

Review the code



OpenZeppelin Contracts Security Process

Internal code reviews

99% test coverage

External audit and formal verification

Community review

→ Release candidates

→ Open Review Period

More TBA 🤖





master ▾

openzeppelin-contracts / CHANGELOG.md

Go to file



397 lines (298 sloc) | 38.4 KB



Raw

Blame



Changelog

Unreleased

- `Ownable` : add an internal `_transferOwnership(address)` . (#2568)
- `AccessControl` : add internal `_grantRole(bytes32,address)` and `_revokeRole(bytes32,address)` . (#2568)
- `AccessControl` : mark `_setupRole(bytes32,address)` as deprecated in favor of `_grantRole(bytes32,address)` . (#2568)
- `AccessControlEnumerable` : hook into `_grantRole(bytes32,address)` and `_revokeRole(bytes32,address)` . (#2946)
- `EIP712` : cache `address(this)` to immutable storage to avoid potential issues if a vanilla contract is used in a delegatecall context. (#2852)
- Add internal `_setApprovalForAll` to `ERC721` and `ERC1155` . (#2834)
- `Governor` : shift vote start and end by one block to better match Compound's GovernorBravo and prevent voting at the Governor level if the voting snapshot is not ready. (#2892)
- `GovernorSettings` : a new governor module that manages voting settings updatable through governance actions. (#2904)
- `PaymentSplitter` : now supports ERC20 assets in addition to Ether. (#2858)
- `ECDSA` : add a variant of `toEthSignedMessageHash` for arbitrary length message hashing. (#2865)
- `MerkleProof` : add a `processProof` function that returns the rebuilt root hash given a leaf and a proof. (#2841)
- `VestingWallet` : new contract that handles the vesting of Ether and ERC20 tokens following a customizable vesting schedule. (#2748)
- `Governor` : enable receiving Ether when a Timelock contract is not used. (#2748)
- `GovernorTimelockCompound` : fix ability to use Ether stored in the Timelock contract. (#2748)

Add internal functions to Ownable, AccessControl, ERC721 and ERC1155

Goal: Allow the developers to trigger “internal operations”, without access restriction, in certain cases:

- **Ownable:** TransferOwnership “withSignature”.
- **AccessControl:** GrantRole / RevokeRole “withSignature”.
- **ERC721/ERC1155:** SetApprovalForAll “WithSignature”.
- **Other:** SellableOwnable (transfer ownership on payment).

```
abstract contract OwnableWithSig is Ownable, EIP712 {
    using Counters for Counters.Counter;

    mapping(address => Counters.Counter) private _nonces;

    // solhint-disable-next-line var-name-mixedcase
    bytes32 private immutable TRANSFEROWNERSHIP_TYPEHASH =
        keccak256("TransferOwnership(address newOwner,uint256 nonce)");

    function transferOwnershipWithSignature(
        address newOwner,
        uint8 v,
        bytes32 r,
        bytes32 s
    ) public virtual {
        require(
            owner() == ECDSA.recover(
                _hashTypedDataV4(keccak256(abi.encode(
                    TRANSFEROWNERSHIP_TYPEHASH,
                    newOwner,
                    _useNonce(owner())
                ))),
                v,
                r,
                s
            ),
            "Invalid signature"
        );
        _transferOwnership(newOwner);
    }

    /**
     * !!! Copied from token/ERC20/extensions/ERC20Permit.sol !!!
     */
    function nonces(address owner) public view virtual override returns (uint256) {
        return _nonces[owner].current();
    }

    // solhint-disable-next-line func-name-mixedcase
    function DOMAIN_SEPARATOR() external view override returns (bytes32) {
        return _domainSeparatorV4();
    }

    function useNonce(address owner) internal virtual returns (uint256 current) {
        Counters.Counter storage nonce = _nonces[owner];
        current = nonce.current();
        nonce.increment();
    }
}
```

GovernorSettings

Goal: Make governance parameters settable via governance proposals.

```
function setVotingDelay(uint256 newVotingDelay) public onlyGovernance;  
function setVotingPeriod(uint256 newVotingPeriod) public onlyGovernance;  
function setProposalThreshold(uint256 newProposalThreshold) public onlyGovernance;  
  
modifier onlyGovernance() {  
    require(_msgSender() == _executor());  
    _;  
}
```


ETH funds in Governor & Compound Timelock

Goal: Allow a Governor to handle ETH funds when using the Compound Timelock.

Issue identified by [Tally](#).

```
+ /**  
+  * @dev Function to receive ETH that will be handled  
+  */  
+ receive() external payable virtual {  
+     require(_executor() == address(this));  
+ }  
+
```

```
uint256 eta = proposalEta(proposalId);  
require(eta > 0, "GovernorTimelockCompound: proposal not yet qu  
+ Address.sendValue(payable(_timelock), msg.value);  
for (uint256 i = 0; i < targets.length; ++i) {  
-     _timelock.executeTransaction{value: values[i]}(targets[i],  
+     _timelock.executeTransaction(targets[i], values[i], "", ca  
}
```

Governor vote start and end shifted

Goal: Correct small difference with GovernorBravo, and mitigate a risk with bad vote tokens.

Reported by @zgfzgf.

```
-      } else if (proposal.voteStart.isPending()) {  
+      } else if (proposal.voteStart.getDeadline() ≥ block.number) {  
        return ProposalState.Pending;  
-      } else if (proposal.voteEnd.isPending()) {  
+      } else if (proposal.voteEnd.getDeadline() ≥ block.number) {  
        return ProposalState.Active;
```

EIP712: cache address(this)

Goal: Add address check, on top of chain id check before reading from cache to prevent potential issues if contract is used through proxy

Advisory

When using OpenZeppelin Contracts through proxies, use:

@openzeppelin/contracts-upgradeable

PR proposed by [@k06a](#)

```
29 29 // Invalidate the cached domain separator if the chain id changes.
30 30 bytes32 private immutable _CACHED_DOMAIN_SEPARATOR;
31 31 uint256 private immutable _CACHED_CHAIN_ID;
32 32 address private immutable _CACHED_THIS;
33 33 bytes32 private immutable _HASHED_NAME;
34 34 bytes32 private immutable _HASHED_VERSION;
35 35
36 36
37 37
38 38
39 39
40 40
41 41
42 42
43 43
44 44
45 45
46 46
47 47
48 48
49 49
50 50
51 51
52 52
53 53
54 54
55 55
56 56
57 57
58 58
59 59
60 60
61 61
62 62
63 63
64 64
65 65
66 66
67 67
68 68
69 69
70 70
71 71
72 72
73 73
74 74
75 75
76 76
77 77
78 78
79 79
80 80
81 81
82 82
83 83
84 84
85 85
86 86
87 87
88 88
89 89
90 90
91 91
92 92
93 93
94 94
95 95
96 96
97 97
98 98
99 99
100 100
101 101
102 102
103 103
104 104
105 105
106 106
107 107
108 108
109 109
110 110
111 111
112 112
113 113
114 114
115 115
116 116
117 117
118 118
119 119
120 120
121 121
122 122
123 123
124 124
125 125
126 126
127 127
128 128
129 129
130 130
131 131
132 132
133 133
134 134
135 135
136 136
137 137
138 138
139 139
140 140
141 141
142 142
143 143
144 144
145 145
146 146
147 147
148 148
149 149
150 150
151 151
152 152
153 153
154 154
155 155
156 156
157 157
158 158
159 159
160 160
161 161
162 162
163 163
164 164
165 165
166 166
167 167
168 168
169 169
170 170
171 171
172 172
173 173
174 174
175 175
176 176
177 177
178 178
179 179
180 180
181 181
182 182
183 183
184 184
185 185
186 186
187 187
188 188
189 189
190 190
191 191
192 192
193 193
194 194
195 195
196 196
197 197
198 198
199 199
200 200
201 201
202 202
203 203
204 204
205 205
206 206
207 207
208 208
209 209
210 210
211 211
212 212
213 213
214 214
215 215
216 216
217 217
218 218
219 219
220 220
221 221
222 222
223 223
224 224
225 225
226 226
227 227
228 228
229 229
230 230
231 231
232 232
233 233
234 234
235 235
236 236
237 237
238 238
239 239
240 240
241 241
242 242
243 243
244 244
245 245
246 246
247 247
248 248
249 249
250 250
251 251
252 252
253 253
254 254
255 255
256 256
257 257
258 258
259 259
260 260
261 261
262 262
263 263
264 264
265 265
266 266
267 267
268 268
269 269
270 270
271 271
272 272
273 273
274 274
275 275
276 276
277 277
278 278
279 279
280 280
281 281
282 282
283 283
284 284
285 285
286 286
287 287
288 288
289 289
290 290
291 291
292 292
293 293
294 294
295 295
296 296
297 297
298 298
299 299
300 300
301 301
302 302
303 303
304 304
305 305
306 306
307 307
308 308
309 309
310 310
311 311
312 312
313 313
314 314
315 315
316 316
317 317
318 318
319 319
320 320
321 321
322 322
323 323
324 324
325 325
326 326
327 327
328 328
329 329
330 330
331 331
332 332
333 333
334 334
335 335
336 336
337 337
338 338
339 339
340 340
341 341
342 342
343 343
344 344
345 345
346 346
347 347
348 348
349 349
350 350
351 351
352 352
353 353
354 354
355 355
356 356
357 357
358 358
359 359
360 360
361 361
362 362
363 363
364 364
365 365
366 366
367 367
368 368
369 369
370 370
371 371
372 372
373 373
374 374
375 375
376 376
377 377
378 378
379 379
380 380
381 381
382 382
383 383
384 384
385 385
386 386
387 387
388 388
389 389
390 390
391 391
392 392
393 393
394 394
395 395
396 396
397 397
398 398
399 399
400 400
401 401
402 402
403 403
404 404
405 405
406 406
407 407
408 408
409 409
410 410
411 411
412 412
413 413
414 414
415 415
416 416
417 417
418 418
419 419
420 420
421 421
422 422
423 423
424 424
425 425
426 426
427 427
428 428
429 429
430 430
431 431
432 432
433 433
434 434
435 435
436 436
437 437
438 438
439 439
440 440
441 441
442 442
443 443
444 444
445 445
446 446
447 447
448 448
449 449
450 450
451 451
452 452
453 453
454 454
455 455
456 456
457 457
458 458
459 459
460 460
461 461
462 462
463 463
464 464
465 465
466 466
467 467
468 468
469 469
470 470
471 471
472 472
473 473
474 474
475 475
476 476
477 477
478 478
479 479
480 480
481 481
482 482
483 483
484 484
485 485
486 486
487 487
488 488
489 489
490 490
491 491
492 492
493 493
494 494
495 495
496 496
497 497
498 498
499 499
500 500
501 501
502 502
503 503
504 504
505 505
506 506
507 507
508 508
509 509
510 510
511 511
512 512
513 513
514 514
515 515
516 516
517 517
518 518
519 519
520 520
521 521
522 522
523 523
524 524
525 525
526 526
527 527
528 528
529 529
530 530
531 531
532 532
533 533
534 534
535 535
536 536
537 537
538 538
539 539
540 540
541 541
542 542
543 543
544 544
545 545
546 546
547 547
548 548
549 549
550 550
551 551
552 552
553 553
554 554
555 555
556 556
557 557
558 558
559 559
560 560
561 561
562 562
563 563
564 564
565 565
566 566
567 567
568 568
569 569
570 570
571 571
572 572
573 573
574 574
575 575
576 576
577 577
578 578
579 579
580 580
581 581
582 582
583 583
584 584
585 585
586 586
587 587
588 588
589 589
590 590
591 591
592 592
593 593
594 594
595 595
596 596
597 597
598 598
599 599
600 600
601 601
602 602
603 603
604 604
605 605
606 606
607 607
608 608
609 609
610 610
611 611
612 612
613 613
614 614
615 615
616 616
617 617
618 618
619 619
620 620
621 621
622 622
623 623
624 624
625 625
626 626
627 627
628 628
629 629
630 630
631 631
632 632
633 633
634 634
635 635
636 636
637 637
638 638
639 639
640 640
641 641
642 642
643 643
644 644
645 645
646 646
647 647
648 648
649 649
650 650
651 651
652 652
653 653
654 654
655 655
656 656
657 657
658 658
659 659
660 660
661 661
662 662
663 663
664 664
665 665
666 666
667 667
668 668
669 669
670 670
671 671
672 672
673 673
674 674
675 675
676 676
677 677
678 678
679 679
680 680
681 681
682 682
683 683
684 684
685 685
686 686
687 687
688 688
689 689
690 690
691 691
692 692
693 693
694 694
695 695
696 696
697 697
698 698
699 699
700 700
701 701
702 702
703 703
704 704
705 705
706 706
707 707
708 708
709 709
710 710
711 711
712 712
713 713
714 714
715 715
716 716
717 717
718 718
719 719
720 720
721 721
722 722
723 723
724 724
725 725
726 726
727 727
728 728
729 729
730 730
731 731
732 732
733 733
734 734
735 735
736 736
737 737
738 738
739 739
740 740
741 741
742 742
743 743
744 744
745 745
746 746
747 747
748 748
749 749
750 750
751 751
752 752
753 753
754 754
755 755
756 756
757 757
758 758
759 759
760 760
761 761
762 762
763 763
764 764
765 765
766 766
767 767
768 768
769 769
770 770
771 771
772 772
773 773
774 774
775 775
776 776
777 777
778 778
779 779
780 780
781 781
782 782
783 783
784 784
785 785
786 786
787 787
788 788
789 789
790 790
791 791
792 792
793 793
794 794
795 795
796 796
797 797
798 798
799 799
800 800
801 801
802 802
803 803
804 804
805 805
806 806
807 807
808 808
809 809
810 810
811 811
812 812
813 813
814 814
815 815
816 816
817 817
818 818
819 819
820 820
821 821
822 822
823 823
824 824
825 825
826 826
827 827
828 828
829 829
830 830
831 831
832 832
833 833
834 834
835 835
836 836
837 837
838 838
839 839
840 840
841 841
842 842
843 843
844 844
845 845
846 846
847 847
848 848
849 849
850 850
851 851
852 852
853 853
854 854
855 855
856 856
857 857
858 858
859 859
860 860
861 861
862 862
863 863
864 864
865 865
866 866
867 867
868 868
869 869
870 870
871 871
872 872
873 873
874 874
875 875
876 876
877 877
878 878
879 879
880 880
881 881
882 882
883 883
884 884
885 885
886 886
887 887
888 888
889 889
890 890
891 891
892 892
893 893
894 894
895 895
896 896
897 897
898 898
899 899
900 900
901 901
902 902
903 903
904 904
905 905
906 906
907 907
908 908
909 909
910 910
911 911
912 912
913 913
914 914
915 915
916 916
917 917
918 918
919 919
920 920
921 921
922 922
923 923
924 924
925 925
926 926
927 927
928 928
929 929
930 930
931 931
932 932
933 933
934 934
935 935
936 936
937 937
938 938
939 939
940 940
941 941
942 942
943 943
944 944
945 945
946 946
947 947
948 948
949 949
950 950
951 951
952 952
953 953
954 954
955 955
956 956
957 957
958 958
959 959
960 960
961 961
962 962
963 963
964 964
965 965
966 966
967 967
968 968
969 969
970 970
971 971
972 972
973 973
974 974
975 975
976 976
977 977
978 978
979 979
980 980
981 981
982 982
983 983
984 984
985 985
986 986
987 987
988 988
989 989
990 990
991 991
992 992
993 993
994 994
995 995
996 996
997 997
998 998
999 999
1000 1000
```

ECDSA.toEthSignedMessageHash(bytes)

Goal: Expand support of EIP191 signed messages to arbitrary length buffers.

PR proposed by [@td-bn](#)

```
196  /**
197   * @dev Returns an Ethereum Signed Message, created from a `hash`. This
198   * produces hash corresponding to the one signed with the
199   * https://eth.wiki/json-rpc/API#eth_sign[`eth_sign`]
200   * JSON-RPC method as part of EIP-191.
201   *
202   * See {recover}.
203   */
204   function toEthSignedMessageHash(bytes32 hash) internal pure returns (bytes32) {
205       // 32 is the length in bytes of hash,
206       // enforced by the type signature above
207       return keccak256(abi.encodePacked("\x19Ethereum Signed Message:\n32", hash));
208   }
209
210  /**
211   * @dev Returns an Ethereum Signed Message, created from `s`. This
212   * produces hash corresponding to the one signed with the
213   * https://eth.wiki/json-rpc/API#eth_sign[`eth_sign`]
214   * JSON-RPC method as part of EIP-191.
215   *
216   * See {recover}.
217   */
218   function toEthSignedMessageHash(bytes memory s) internal pure returns (bytes32) {
219       return keccak256(abi.encodePacked("\x19Ethereum Signed Message:\n", Strings.toString(s.length), s));
220   }
```

MerkleProof.processProof(bytes32[], bytes32)

Goal: Improve support for Merkle trees, particularly when multiple trees are valid

```
15 library MerkleProof {
16     /**
17      * @dev Returns true if a `leaf` can be proved to be a part of a Merkle tree
18      * defined by `root`. For this, a `proof` must be provided, containing
19      * sibling hashes on the branch from the leaf to the root of the tree. Each
20      * pair of leaves and each pair of pre-images are assumed to be sorted.
21      */
22     function verify(
23         bytes32[] memory proof,
24         bytes32 root,
25         bytes32 leaf
26     ) internal pure returns (bool) {
27         return processProof(proof, leaf) == root;
28     }
29
30     /**
31      * @dev Returns the rebuilt hash obtained by traversing a Merkle tree up
32      * from `leaf` using `proof`. A `proof` is valid if and only if the rebuilt
33      * hash matches the root of the tree. When processing the proof, the pairs
34      * of leaves & pre-images are assumed to be sorted.
35      *
36      * _Available since v4.4._
37      */
38     function processProof(bytes32[] memory proof, bytes32 leaf) internal pure returns (bytes32) {
39         bytes32 computedHash = leaf;
40         for (uint256 i = 0; i < proof.length; i++) {
41             bytes32 proofElement = proof[i];
42             if (computedHash <= proofElement) {
43                 // Hash(current computed hash + current element of the proof)
44                 computedHash = keccak256(abi.encodePacked(computedHash, proofElement));
45             } else {
46                 // Hash(current element of the proof + current computed hash)
47                 computedHash = keccak256(abi.encodePacked(proofElement, computedHash));
48             }
49         }
50         return computedHash;
51     }
52 }
```

MerkleProof.processProof(bytes32[], bytes32)

Goal: Improve support for Merkle trees, particularly when multiple trees are valid

function **verify**(bytes32[] memory **proof**, bytes32 **root**, bytes32 **leaf**) internal pure returns (**bool**);

function **processProof**(bytes32[] memory **proof**, bytes32 **leaf**) internal pure returns (**bytes32**);

```
44 function release(Schedule memory schedule, bytes32[] memory proof) public {
45     // check input validity
46     bytes32 leaf = keccak256(abi.encode(schedule));
47     bytes32 drop = MerkleProof.processProof(proof, leaf);
48     require(_airdrops[drop]);
49
50     // compute vesting remains
51     uint256 releasable = vestedAmount(schedule, uint64(block.timestamp)) - _released[leaf];
52     _released[leaf] += releasable;
53
54     // emit notification
55     emit TokensReleased(drop, schedule.token, schedule.recipient, schedule.amount);
56
57     // do release (might have reentrancy)
58     SafeERC20.safeTransfer(schedule.token, schedule.recipient, releasable);
59 }
60
61 function vestedAmount(Schedule memory schedule, uint64 timestamp) public pure returns (uint256) {
62     return timestamp < schedule.start + schedule.cliff
63         ? 0
64         : Math.min(
65             schedule.amount,
66             schedule.amount * (timestamp - schedule.start) / schedule.duration
67         );
68 }
```

Workshop

5/6 - 1PM PST / 8PM UTC

Building an NFT Merkle-Drop

by Hadrien Croubois
Smart Contracts Engineer at OpenZeppelin

Registration Required Limited to 50 participants



<https://www.youtube.com/watch?v=SF-XOwWlwRo>

Payment Splitter support for ERC20 tokens

Goal: Add support for ERC20 tokens in the payment splitter.

- Storage layout is compatible, making upgrades possible.
- Payee management is unmodified.
- Follow the “pull payment” model.

Note: This contract assumes that ERC20 tokens will behave similarly to native tokens (Ether). Rebasing tokens, and tokens that apply fees during transfers, are likely to not be supported as expected. If in doubt, we encourage you to run tests before sending real value to this contract.

```
23  /**
24   * @dev Triggers a transfer to 'account' of the amount of Ether they are owed, according to their percentage of the
25   * total shares and their previous withdrawals.
26   */
27  function release(address payable account) public virtual {
28      require(_shares[account] > 0, "PaymentSplitter: account has no shares");
29
30      uint256 totalReceived = address(this).balance + totalReleased();
31      uint256 payment = _pendingPayment(account, totalReceived, released(account));
32
33      require(payment != 0, "PaymentSplitter: account is not due payment");
34
35      _released[account] += payment;
36      _totalReleased += payment;
37
38      Address.sendValue(account, payment);
39      emit PaymentReleased(account, payment);
40  }
41
42  /**
43   * @dev Triggers a transfer to 'account' of the amount of 'token' tokens they are owed, according to their
44   * percentage of the total shares and their previous withdrawals. 'token' must be the address of an ERC20
45   * contract.
46   */
47  function release(ERC20 token, address account) public virtual {
48      require(_shares[account] > 0, "PaymentSplitter: account has no shares");
49
50      uint256 totalReceived = token.balanceOf(address(this)) + totalReleased(token);
51      uint256 payment = _pendingPayment(account, totalReceived, released(token, account));
52
53      require(payment != 0, "PaymentSplitter: account is not due payment");
54
55      _erc20Released[token][account] += payment;
56      _erc20TotalReleased[token] += payment;
57
58      SafeERC20.safeTransfer(token, account, payment);
59      emit ERC20PaymentReleased(token, account, payment);
60  }
61
62  /**
63   * @dev Internal logic for computing the pending payment of an 'account' given the token historical balances and
64   * already released amounts.
65   */
66  function _pendingPayment(
67      address account,
68      uint256 totalReceived,
69      uint256 alreadyReleased
70  ) private view returns (uint256) {
71      return (totalReceived * _shares[account]) / _totalShares - alreadyReleased;
72  }
```

Vesting Wallet

Standalone contract.

Supported assets (Ether/ERC20) are released following a customizable vesting schedule.

```
constructor(address beneficiary, uint64 startTimestamp, uint64 durationSeconds)
```

```
release() public;
```

```
release(address token) public;
```

```
vestedAmount(uint64 timestamp) public view returns (uint256);
```

```
vestedAmount(address token, uint64 timestamp) public view returns (uint256);
```

```
_vestingSchedule(uint256 totalAllocation, uint64 timestamp) internal view virtual returns  
(uint256);
```

Contribute

Formal bug bounty program

More details to come very soon

Open Review Period

4.4 Release Candidate - Available Now!

<https://zpl.in/contracts/4.4>



docs.openzeppelin.com

blog.openzeppelin.com

forum.openzeppelin.com

defender.openzeppelin.com



We're hiring!

zpl.in/join

Blockchain Security Engineer
Full Stack Ethereum Developer
Site Reliability Engineer
Open Source Developer
Application UX Designer
Technical Project Manager



Thank you!

Learn more

openzeppelin.com/contracts
forum.openzeppelin.com
docs.openzeppelin.com



Contact

 @frangio_
frangio@openzeppelin.com
 @Amxx
hadrien@openzeppelin.com

