VerifySignature

This smart contract handles the signature of an agreement, confirming that the winner can claim the price.

Functions

canWithdraw

called from GrantEscrow when claiming funds in escrow

Name	Type	Description
_from	address	The address of the Grant Orga
_to	address	The address of the recipient

Returns:

Name	Type	Description
	bool	

getEthSignedMessageHash

Name	Type	Description
_messageHash	bytes32	The hash from getMEssageHash

Returns:

Name	Type	Description
	bytes32	

getMessageHash

Only the account deploying can call this function
require boolean yugoAddrSet to be false
yugoAddrSet is updated to true to avoid any further attempt to change the address

Name	Type	Description
_to	address	Address of the recipient
_amount	uint256	Funds required by the action
_agreement	string	Agreement unsigned
_nonce	uint256	The secret number used for the hash

Returns:

Name	Type	Description
	bytes32	

owner

Returns the address of the current owner.

No parameters

Returns:

Name	Type	Description
	address	

recoverSigner

Name	Type	Description
_ethSignedMessageHash	bytes32	The first part of the signature
_signature	bytes	The hash signed by the Grant Orga

Returns:

Name	Type	Description
	address	

renounceOwnership

Leaves the contract without owner. It will not be possible to call `onlyOwner` functions anymore. Can only be called by the current owner. NOTE: Renouncing ownership will leave the contract without an owner, thereby removing any functionality that is only available to the owner.

No parameters

Returns:

No parameters

setYugoDaoAddress

Only the account deploying can call this function
require boolean yugoAddrSet to be false
yugoAddrSet is updated to true to avoid any further attempt to change the address

Name	Type	Description
_dao	address	YugoDao contract address

Returns:

No parameters

splitSignature

Name	Type	Description
sig	bytes	The hash signed by the Grant Orga

Returns:

Name	Type	Description
r	bytes32	
s	bytes32	
v	uint8	

transferOwnership

Transfers ownership of the contract to a new account (`newOwner`). Can only be called by the current owner.

Name	Type	Description
newOwner	address	

Returns:

No parameters

verify

Name	Type	Description
_to	address	Address of the recipient
_amount	uint256	Funds required by the action
_agreement	string	Agreement unsigned
_nonce	uint256	The secret number used for the hash
signature	bytes	The hash signed fy teh Grant Orga

Returns:

Name	Type	Description
	bool	