

Reveal

**An interesting solution to
a boring problem**

Mike MacCana 20240201

(3) TREATMENT AS CASH FOR PURPOSES OF SECTION 6050I.—Section 6050I(d) of such Code is amended by striking “and” at the end of paragraph (1), by striking the period at the end of paragraph (2) and inserting “, and”, and by inserting after paragraph (2) the following new paragraph:

“(3) any digital asset (as defined in section 6045(g)(3)(D)).”.

(c) EFFECTIVE DATE.—The amendments made by this section shall apply to returns required to be filed, and statements required to be furnished, after December 31, 2023.

(d) RULE OF CONSTRUCTION.—Nothing in this section or the amendments made by this section shall be construed to create any inference, for any period prior to the effective date of such amendments, with respect to—

(1) whether any person is a broker under section 6045(c)(1) of the Internal Revenue Code of 1986, or

(2) whether any digital asset is property which is a specified security under section 6045(g)(3)(B) of such Code.

26 USC 6050I.

26 USC 6045 note.

26 USC 6045 note.

IRS Form 8300

Requirement for
crypto transactions
larger than 10K USD
from 1 Jan 2024

IRS Form 8300
(Rev. December 2023)

Department of the Treasury
Internal Revenue Service

Report of Cash Payments Over \$10,000
Received in a Trade or Business

See instructions for definition of cash.

Use this form for transactions occurring after December 31, 2023. Do not use prior versions after this date.

For Privacy Act and Paperwork Reduction Act Notice, see the instructions.

FinCEN Form 8300
(Rev. August 2014)
OMB No. 1506-0018
Department of the Treasury
Financial Crimes
Enforcement Network

1

Check appropriate box(es) if:

a

☐ Amends prior report;

b

☐ Suspicious transaction.

Part I

Identity of Individual From Whom the Cash Was Received

2

If more than one individual is involved, check here and see instructions

☐

3

Last name

4

First name

5

M.I.

6

Taxpayer identification number

7

Address (number, street, and apt. or suite no.)

8

Date of birth
(see instructions)

M

M

D

D

Y

Y

Y

Y

9

City

10

State

11

ZIP code

12

Country (if not U.S.)

13

Occupation, profession, or business

14

Identifying document (ID)

a

Describe ID

c

Number

b

Issued by

Part II

Person on Whose Behalf This Transaction Was Conducted

15

If this transaction was conducted on behalf of more than one person, check here and see instructions

☐

16

Individual's last name or organization's name

17

First name

18

M.I.

19

Taxpayer identification number

20

Doing business as (DBA) name (see instructions)

Employer identification number

21

Address (number, street, and apt. or suite no.)

22

Occupation, profession, or business

23

City

24

State

25

ZIP code

26

Country (if not U.S.)

27

Alien identification (ID)

a

Describe ID

c

Number

b

Issued by

Part III

Description of Transaction and Method of Payment

28

Date cash received

M

M

D

D

Y

Y

Y

Y

29

Total cash received

\$

.00

30

If cash was received in more than one payment, check here

☐

31

Total price if different from item 29

\$

.00

32

Amount of cash received (in U.S. dollar equivalent) (must equal item 29) (see instructions):

a

U.S. currency

\$

.00

(Amount in \$100 bills or higher \$

.00

)

b

Foreign currency

\$

.00

(Country

)

c

Cashier's check(s)

\$

.00

d

Money order(s)

\$

.00

e

Bank draft(s)

\$

.00

f

Traveler's check(s)

\$

.00

Issuer's name(s) and serial number(s) of the monetary instrument(s)

33

Type of transaction

a

☐ Personal property purchased

f

☐ Debt obligations paid

b

☐ Real property purchased

g

☐ Exchange of cash

c

☐ Personal services provided

h

☐ Escrow or trust funds

d

☐ Business services provided

i

☐ Bail received by court clerks

e

☐ Intangible property purchased

j

☐ Other (specify in item 34)

34

Specific description of property or service shown in 33. Give serial or registration number, address, docket number, etc.

Part IV

Business That Received Cash

35

Name of business that received cash

36

Employer identification number

37

Address (number, street, and apt. or suite no.)

Social security number

38

City

39

State

40

ZIP code

41

Nature of your business

42

Under penalties of perjury, I declare that to the best of my knowledge the information I have furnished above is true, correct, and complete.

Signature

Title

Or maybe not quite yet...

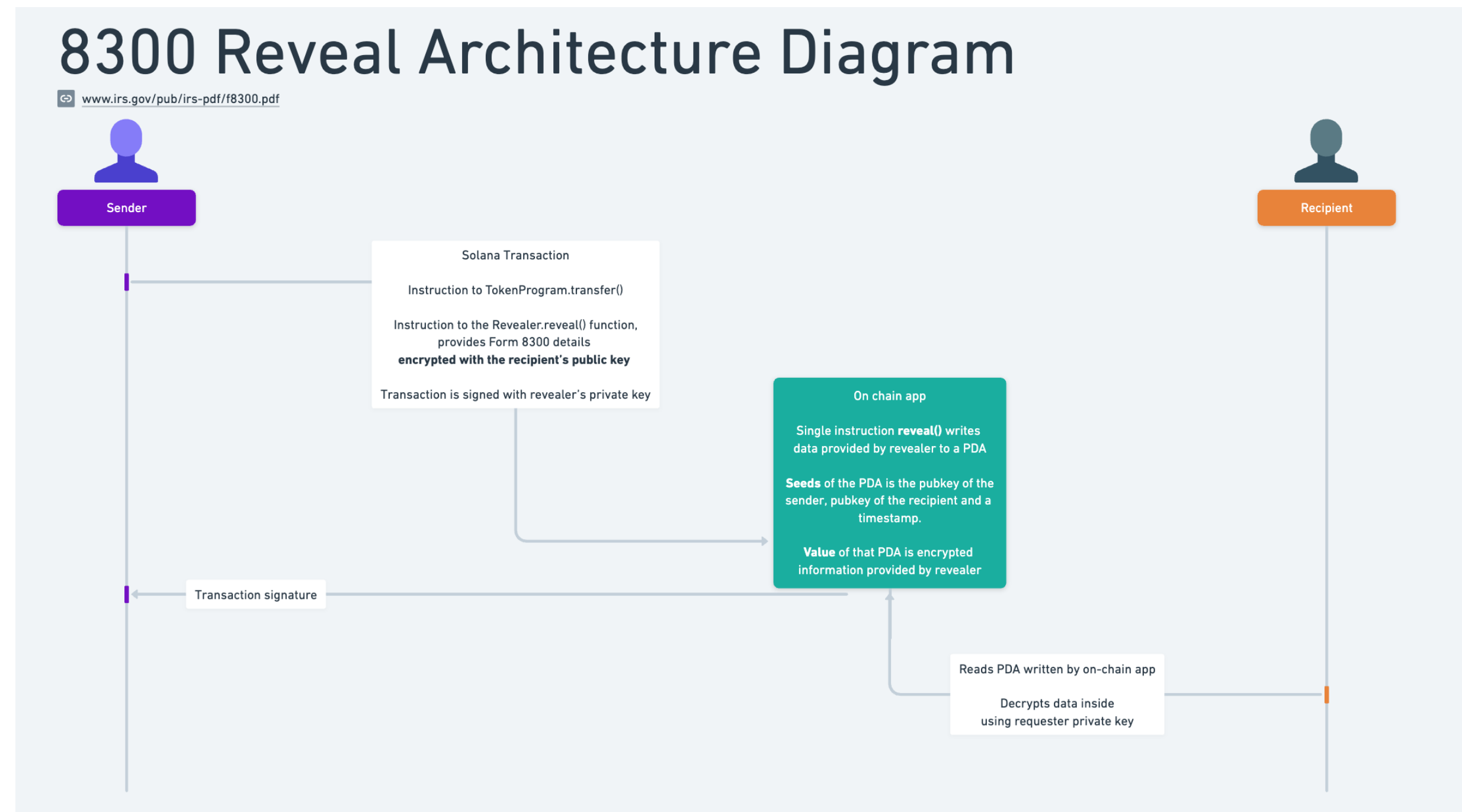
Feb 25: “Cryptocurrency Users Relieved As IRS Delays Form 8300 Reporting”

<https://www.forbes.com/sites/digital-assets/2024/01/25/cryptocurrency-users-relieved-as-irs-delays-form-8300-reporting/>

Reveal stores Form8300 data

Just another instruction to add to your SPL transfers

- A transaction with reveal is just:
 - `ComputeBudgetProgram.setComputeUnitLimit()`
 - `TokenProgram.transfer()`
 - **`RevealProgram.reveal()`**
- Receiver has data they need for IRS
- Sender keeps their data private

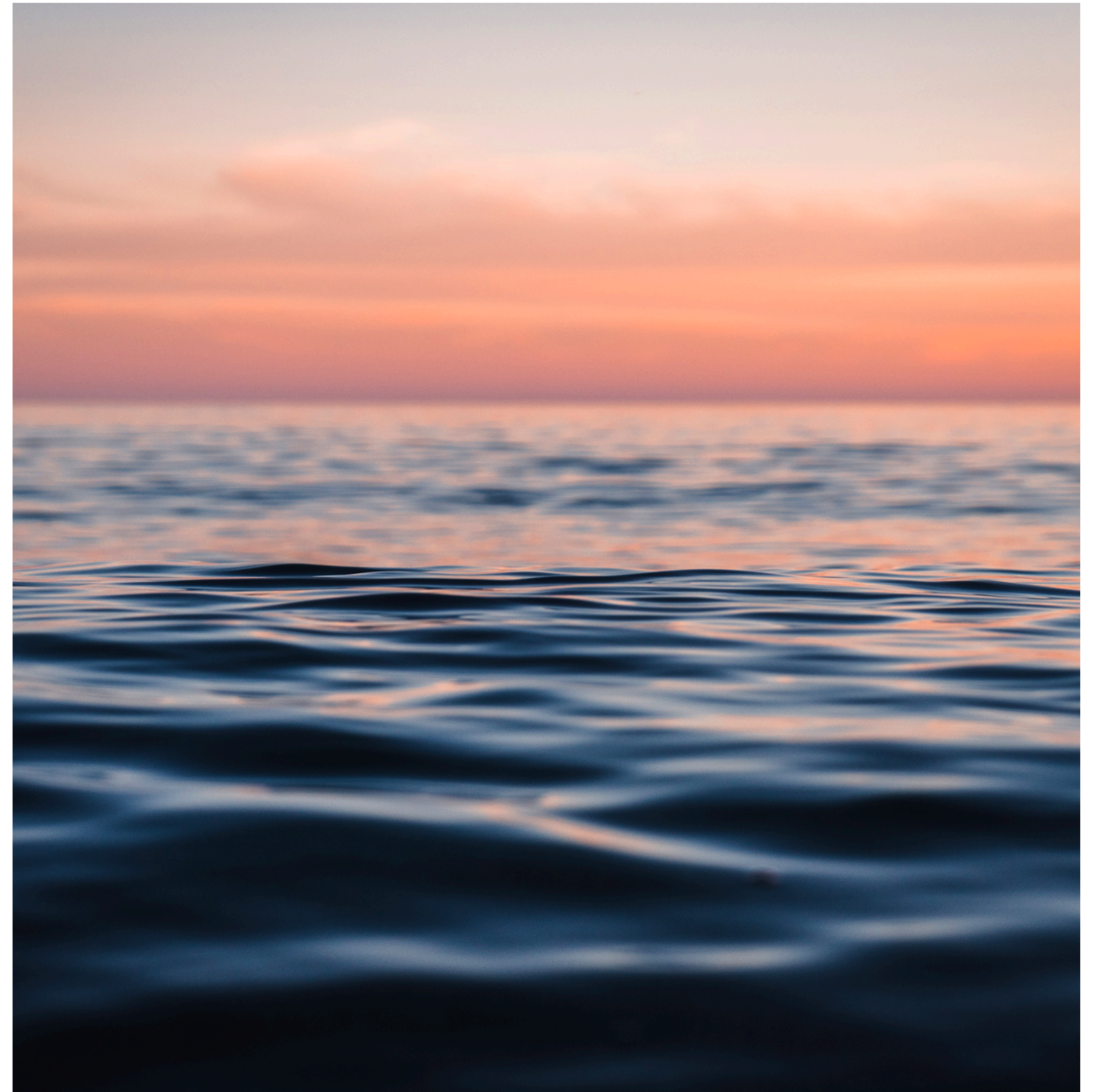


More on reveal()

**Just the sender-specific parts of
8300**

Just under 1K of data

**Format is built / validated entirely
client-side & stored in PDA**



Tech Stack

InitSpace macro because I hate adding numbers!

‘instructions’ dir and functional style with Anchor’s **‘multiple’** template.

Transactions composed of both SPL and Anchor instructions, via Anchor’s **.instruction()** converter to convert to web3.js instructions.

web3js 1.x -> webcrypto bridge for client side encryption (still WIP!)

```
#[derive(Accounts)]
#[instruction(id: u64)]
5 implementations
pub struct RevealAccounts<'info> {
    #[account(mut)]
    pub sender: Signer<'info>,

    #[account(
        init,
        payer = sender,
        space = ANCHOR_DISCRIMINATOR_SIZE +
        Revelation::INIT_SPACE,
        seeds=[b"revelation", sender.key().as_ref(), id.to_le_bytes().as_ref()],
        bump
    )]
    pub revelation: Account<'info, Revelation>,

    pub system_program: Program<'info, System>,
}

pub fn handler(context: Context<RevealAccounts>,
id: u64, data: [u8; DATA_SIZE]) -> Result<()> {
    msg!("ID is: {}", id);
    msg!("Data is: {:?}", data);

    context.accounts.revelation.set_inner
    (Revelation {
        id,
        data,
```

Tech Stack Continued

Tests and Debugging

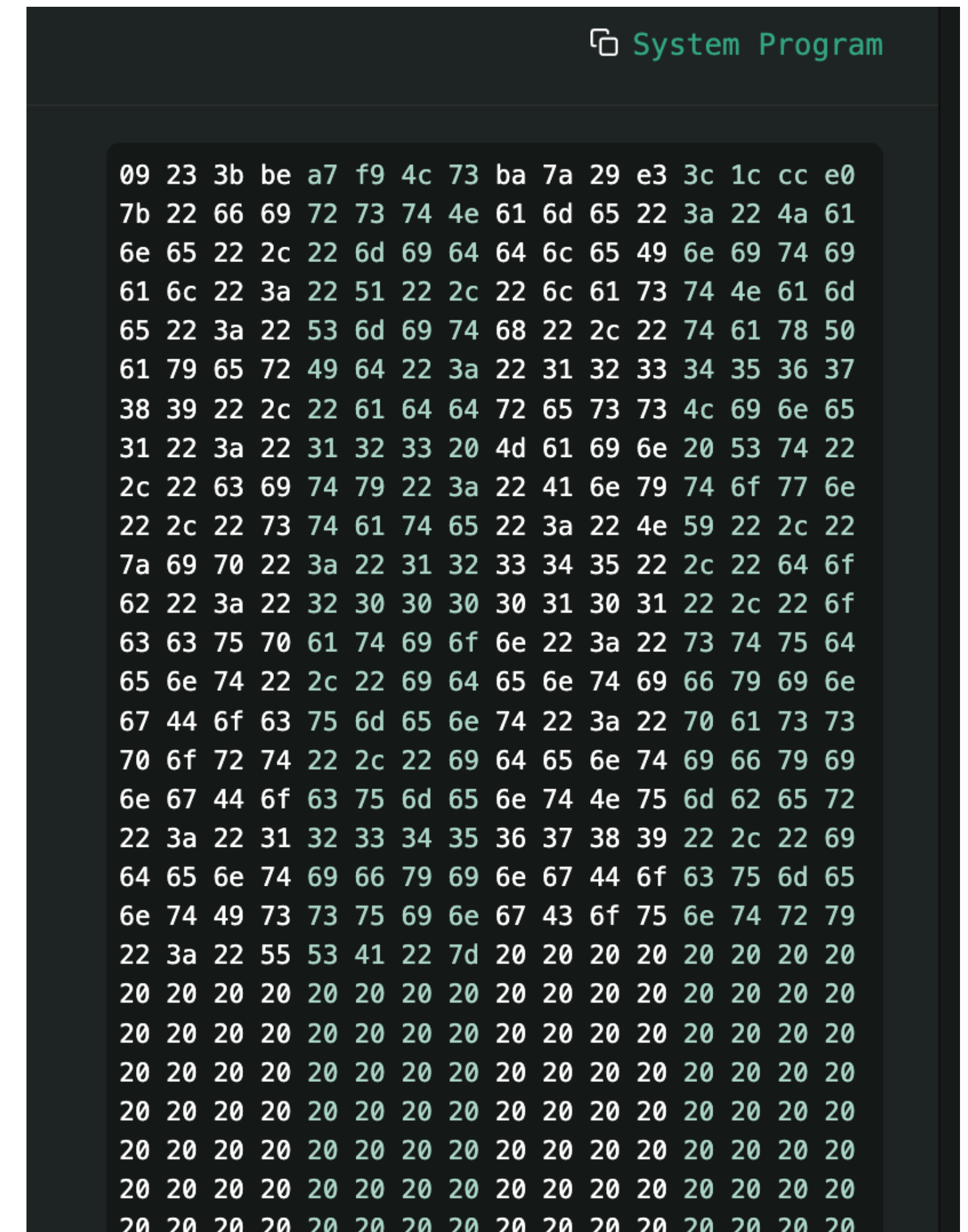
Tests are using **node:test** and **node:assert**, rather than mocha/chai.

Tests put 5800 data in, make sure they can get it back out!

Debug macro was useful for logging structs etc.

Using **Solana Explorer** pointed at **localhost** was helpful - run own validator so it stays up after tests, then anchor test —skip-local-validator.

It took me too long to work out that **I need to provide the PDAs in the accounts list even when creating the PDA**, so Solana can know which transactions overlap!



Thanks WBA!

@mikemaccana