net2o: MINΩΣ2 GUI, $quid "crypto"

($quid = ethical micropayment with efficient BlockChain)

Bernd Paysan

EuroForth 2018, Edinburgh

Motivation

MINΩΣ2 Widgets

Design principle is a Lego-style combination of many extremely simple objects

actor	base class that reacts on all actions (clicks, touchs, keys)
animation	action for animations
widget	base class for all visible objects
glue	base class for flexible objects
tile	colored rectangle
frame	colored rectangle with border
icon	icon from an icon texture
image	larger image
edit	editable text: 中秋节快乐！ Happy autumn festival! 🌙🟡
text	text element/Emoji/中文/... 😀😁😊😂😇😈🙈🙉🙊❤️💔💕💖💗💘🍺👋🎉🎻🎸
part-text	pseudo-element for paragraph breaking
canvas	vector graphics (TBD)
video	video player (TBD)

MINΩΣ2 Displays

Render into different kinds of displays

viewport	Into a texture, used as viewport
display	To the actual display (no class, just the default)

5 Years after Snowden

What changed?

Politics

- EU parliament wants upload filters
- EU parliament taxes the link (instead: "right")
- EU parliament wants filtering "terrorist contents"
- Germany wants a Cyberadministration like CAC (Medienstaatsvertrag)
- Backdoors still wanted ("reasonable encryption")

Competition

- Cambridge Analytica scandal (Facebook)
- Security fuckups: Passwords pawned, chat log saved unprotected in the cloud, etc.

Progress

- The ECHR ruled that GCHQ's dragnet surveillances violates your rights
- net2o becomes more and more usable

Minimize Draw Calls

OpenGL wants as few draw-calls per frame, so different contexts are drawn in stacks with a draw-call each

init	Initialization round
bg	background round
text	text round (same draw call as bg round, just different code)
image	draw images with one draw-call per image

5 Years after Snowden

What changed?

Politics

- Germany wants a Cyberadministration like CAC (Medienstaatsvertrag)
- Backdoors still wanted ("reasonable encryption")
- Legalize it (dragnet surveillance)
- You can't reasonably expect privacy on your own PC
- "Crypto" now means BitCoin

Competition

- Cambridge Analytica scandal (Facebook)
- Security fuckups: Passwords pawned, chat log saved unprotected in the cloud, etc.

Progress

- The ECHR ruled that GCHQ's dragnet surveillances violates your rights
- net2o becomes more and more usable

$quid & SwapDragonChain

Content:

Money	What's that all about?
BitCoin	Shortcomings of a first proof of concept
Wealth	Ethical implication in deflationary systems
Proof of	Trust instead Work
BlockChain	What's the actual point?
Scale	How to scale a BlockChain?
Contracts	Smart oder dumb?
$quid	Ethical ways to create money

MINΩΣ2 Widgets

Design principle is a Lego-style combination of many extremely simple objects

actor	base class that reacts on all actions (clicks, touchs, keys)
animation	action for animations
widget	base class for all visible objects
glue	base class for flexible objects
tile	colored rectangle
frame	colored rectangle with border
icon	icon from an icon texture
image	larger image
edit	editable text: 中秋节快乐！ Happy autumn festival! 🌙🟡
text	text element/Emoji/中文/... 😀😁😊😂😇😈🙈🙉🙊❤️💔💕💖💗💘🍺👋🎉🎻🎸
part-text	pseudo-element for paragraph breaking
canvas	vector graphics (TBD)
video	video player (TBD)

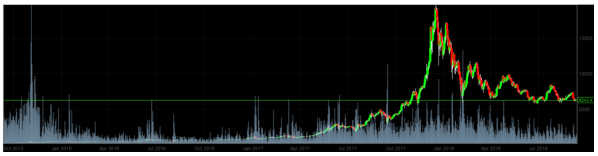
What's Money?

Commodity ~:	Objects with inherent value
Promissory note:	Bank created paper for commodity
Representative ~:	Promise to exchange with "standard object" (e.g. gold)
Fiat ~:	No inherent value; promise, if any, as legal tender
Legal tender:	Medium of payment by law




BitCoins — early “Crypto” shortcomings

- Proof of work: wasteful and yet only marginally secure
- Inflation is money’s cancer, deflation its infarct
- Consequences: unstable exange rate, high transaction fees
- Ponzi scheme–style bubble
- (Instead of getting Viagra spam I now get BitCoin spam)
- Can’t even do the exchange transaction on–chain

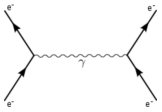


Dumb Contracts

- Smart Contracts: Token–Forth subset (BitCoin), JavaScript (Ethereum)
- For Smart Contracts you need a lawyer, a programmer, *and* a pentester
- Keep it simple: A contract must have a balanced balance
- Select sources (S), select their assets (A), debit them (±)
- select destinations (D), set assets&credit them
- Shortcut: balance an asset (B)
- Obligations for debt and futures (O)
- Sign the target account with new content+hash of the contrat

Examples:

Transfer	SA–SBDD
Cheque	SA–D, cash: SA–DSBD
Exchange/Purchase	SA+A–DSBBD



Wealth & Ethics

- Huge first mover advantage
- Already worse wealth distribution than neoliberal economy
- Huge inequality drives society into servitude, not into freedom
- No concept of a credit
- Lightning network also binds assets (will have fees as consequence)

$quid: Ethical mining

- Concept of mining: Provide difficult and rare work
- Suggesting: Provide vouchers for free software development sponsorships
- These vouchers are tradeable on their own
- Free software is public infrastructure for the information age
- That way, we can encourage people to sponsor out of self–interest
- They get a useful and valueable token back
- Or they develop FOSS themselves to earn (fiat) money

Decentral bank?

- Central bank grants big banks credits, which then are gambled in the stock market
- The decentral bank gives credits to small business
- Credit assessment more like croudfunding

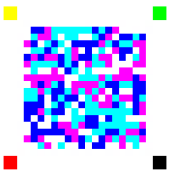
Proof of What?!

Challenge	Avoid double–spending
State of the art:	Proof of work
Problem:	Proof of work burns energy and GPUs
Suggestion 1:	Proof of stake (money buys influence)
Problem:	Money corrupts, and corrupt entities misbehave
Suggestion 2:	Proof of well–behaving (trust, trustworthyness)
How?	Having signed many blocks in the chain gains points
Multiple signers	Not only have one signer, but many
Suspicion	Don't accept transactions in low confidence blocks
Idea	Repeated prisoner’s dilemma rewards cooperation

BTW: The attack for double spending also requires a MITM–attack

Literatur & Links

Bernd Paysan *net2o fossil repository*
https://net2o.de/
Bernd Paysan *$quid cryptocurrency & SwapDragonChain*
https://squid.cash/



SwapDragon BlockChain

- Banks distrust each others, too (i. e. GNU Taler is not a solution)
- Problem size: WeChat Pay peaks at 0.5MTPS (BTC at 5TPS)
- Lightning Network doesn’t stand an overrun–the–arbiter attack
- Therefore, the BlockChain itself needs to scale
- Introduce double entry booking into the distributed ledger
- Partitionate the ledgers by coin pubkey
- Use n–dimensional ledger space to route transactions