WEB3 AND COMMUNITIES AT RISK:

MYTHS AND PROBLEMS WITH CURRENT EXPERIMENTS

Dr Margie Cheesman
November 2022

CONTENTS

FOREWORD

Why are the most at-risk people around the world at the forefront of experiments with untried technologies like cryptocurrencies?

Refugees, low-income populations, and other communities with restricted socio-economic access, rights, and protections are now absorbing the risks and costs of Web3 technological development. Is this how we build a just society?

This report from Dr Margie Cheesman, an affiliate at the Minderoo Centre for Technology and Democracy at the University of Cambridge, makes a pressing and timely intervention by critically analysing the current state of evidence on Web3. The report is informed by her extensive ethnographic research on changes in money and identity infrastructures, especially in global migration governance. This includes the impacts of novel payment systems, demonetisation, biometrics, and decentralised ID on issues of socio-economic inequality.

Thanks to Margie's extensive fieldwork with refugee groups in Jordan and international organisations such as InfoMigrants, GSMA Mobile for Development, and United Nations agencies, this report maps how to advance public conversations about the values that we as a society seek to protect.

At the Minderoo Centre for Technology and Democracy, at the University of Cambridge, we study how digital technology is transforming society to ensure democratic accountability over the increasing power of tech across the globe.

Our research is anchored in creating ways to build capacity in how we as a society can hold tech power systems to account, to create a just future.

We hope that this report will be useful to a wide range of different stakeholders in scrutinising Web3 developments, especially for those who are most at risk in our societies.
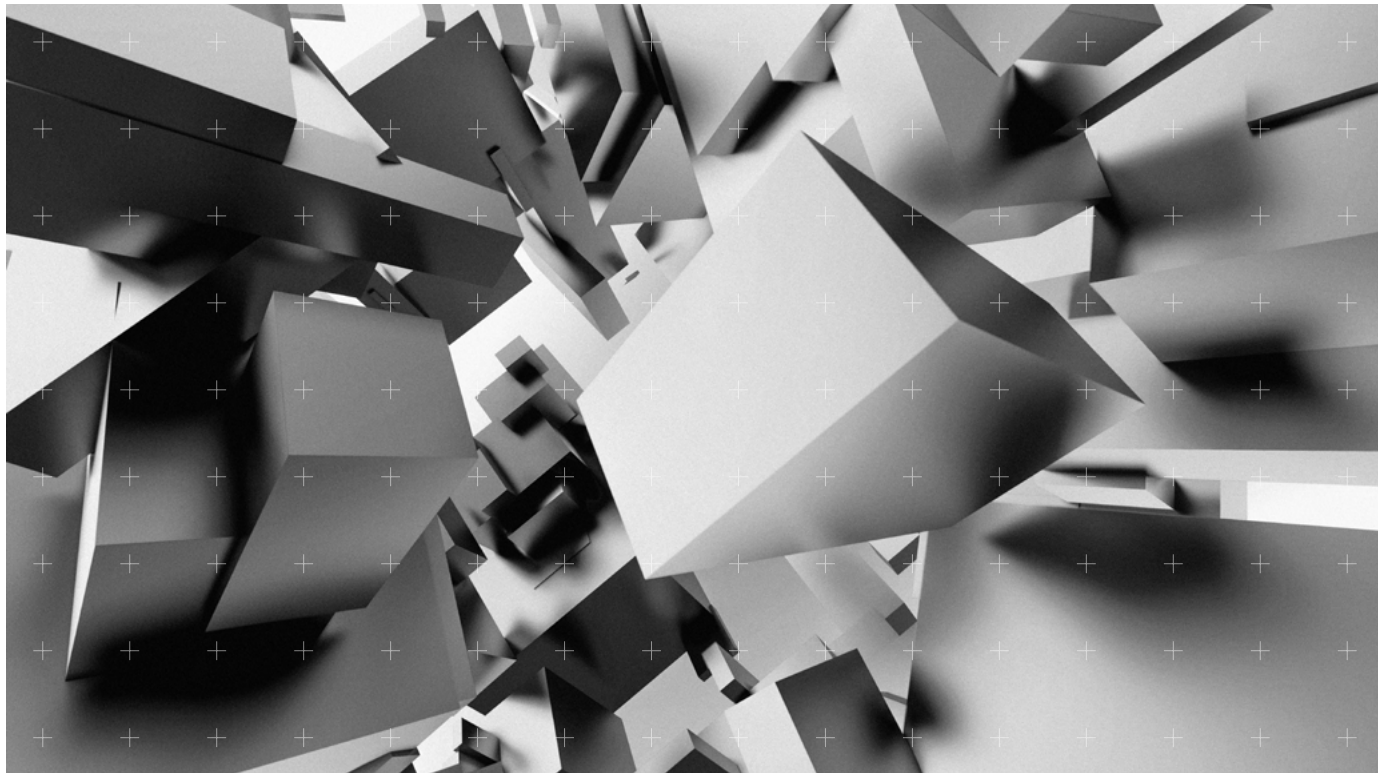
Prof. Gina Neff

Executive Director,
Minderoo Centre for Technology
and Democracy

EXECUTIVE SUMMARY

Web3 technologies and applications have gained traction as solutions to the most intractable problems like humanitarian disaster, forced migration, socio-economic exclusion, and financial crises.

Communities at risk, including refugees and low-income populations are therefore now at the frontline in absorbing the risks and failures of Web3 technological development. Poverty and disaster are major frontiers of capital accumulation by technology companies and infrastructure providers striving for dominance in 'emerging markets'.

Web3/blockchain companies and start-ups are developing models and patents in settings like refugee camps where tax, data protection and other regulation, accountability, and the rights, liberties, and choices of users are diminished.

Web3 refers to a collection of ideas about the future of digital society and blockchain is the enabling technology. The key ideas associated with Web3 are decentralisation, trust, truth, security, and privacy. But in practice, Web3 involves many potential concepts and technologies, all surrounded by misleading PR, myth, and misunderstanding. Marginalised groups — refugees, low-income populations, and other communities with restricted socio-economic access, rights, and protections — are key test subjects of Web3 experiments. But Web3 technologies do not address the root social and economic problems these groups are facing, and they introduce a range of new risks to people who are already in disadvantaged positions.

The report demonstrates 3 key areas where Web3 experimentation from start-ups, humanitarian and development aid organisations, and other non-traditional commercial partners is targeting marginalised groups: Payment, Currency, and Identification.

Payment

Proponents suggest blockchain will democratise payment, facilitating direct, cheap, and borderless digital transactions. Yet, there are significant concerns around the for-profit motives and surveillance issues when blockchain infrastructure replaces established payment systems.

Humanitarian payment projects such as WFP's Building Blocks and Oxfam's Unblocked replace established payment providers with non-traditional commercial partners in tech and other industries like IrisGuard, ConSensys, and supermarket companies. Blockchain-based payment rails can disrupt users' trusted interactions with aid industry providers and provide inadequate recourse mechanisms.

Currency

Proponents of crypto and other alternative currencies suggest they provide a lifeline to people without reliable access to stable currency or liquidity. But they lack stability, usefulness, and accessibility.

Alternative currencies do not resolve the main issues in mainstream financial systems, especially exclusion due to the identity documentation or credit score requirements of banks. Most schemes reinforce inequalities by exposing those with the most to lose to new risks such as scamming and financial volatility.

Cryptocurrencies and alternative currencies may also enhance surveillance and profiling of marginalised groups. For example, Worldcoin has collected 450,000 high resolution images of bodies, faces and eyes from people in countries across the Global South.
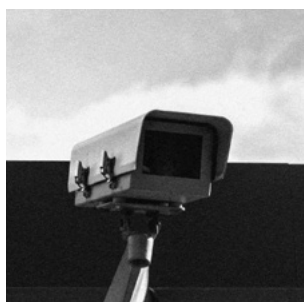
Identification

Decentralised identity schemes seek to facilitate forms of power and agency for technology users, especially people whose protection under national law is in question. Web3 identity schemes claim to allow users to selectively disclose and minimise sensitive data sharing. However, not all do, and this puts the onus on users to manage personal data.

Many blockchain-based systems are tracking and surveillance tools rather than reducing the collection of personal data. Decentralised ID schemes do not mitigate the political structures that hamper certain communities' access to financial, health, and social services and mobility.
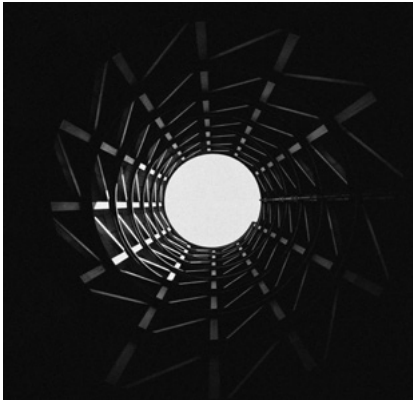
RECOMMENDATIONS

Based on the findings of the report, we recommend:
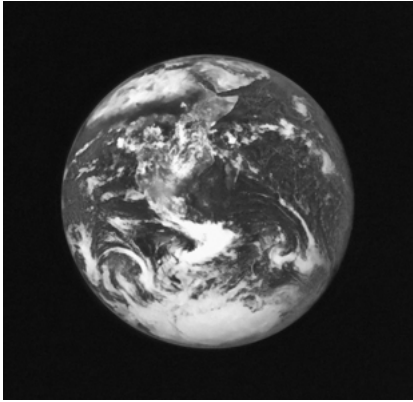
Web3 technologies, especially untested cryptocurrencies, should not be imposed experimentally on marginalised communities.

Public institutions must coordinate around vetting private Web3 companies.

We need qualitative evidence-based research on the design, maintenance, and use of Web3 technologies.

INTRODUCTION

This future is already happening in humanitarian crisis zones and other sensitive settings. What does it look like?

Web3, also known as the Third Web, refers to a collection of ideas about how the future of digital society should look. Around the world, we now see experimental block-chain projects. This growing number of projects target refugees, aid beneficiaries, and other low-income communities. Web3 projects propose to address some of the most challenging social, economic, and political issues affecting these marginalised groups. For example, Web3 is touted as a solution to the problem that many groups are excluded from or have unstable access to mainstream social and financial services.

Web3 is widely seen as the ideal evolution of the World Wide Web that will be realised using the decentralised digital infrastruc-ture, blockchain. Big tech companies like Facebook/Meta and Amazon currently dominate online ecosystems and extract profit from personal data.

Governments wield authority over citizens and non-citizens through digital surveillance systems. Proponents suggest Web3 will combat the concentration of information and power. This egalitarian future may sound promising, especially for commu-nities most disadvantaged by global capitalism and political crisis. But these claims tend to be overblown and specula-tive[1]. Too often they go unchallenged and without rigorous research.

What Web3 is/are — and when, where, and how Web3 is being made and used — is not widely understood. Mystification and confusion surround the term Web3.

To make matters worse, it is conflated with 'Web 3.0', which has nothing to do with blockchain and refers to the 'semantic web', concepts about machine readability proposed by Tim Berners Lee, the World Wide Web's inventor.

This on-rushing tide of new terms, solutions, and catchphrases linked with blockchain is overtaking our ability to understand, research, and evaluate Web3. For example, Twitter CEO Jack Dorsey announced the advent of Web5.

He and a retinue of critics have already dismissed Web3 as empty hype and argue that Web5, based on Bitcoin, will skip ahead to a more genuinely decentralised Internet ecosystem[2]. (When) will Web5 happen? What's the difference between this and Web3? What happened to Web4? There is much scepticism surrounding Web3, not just in circles selling something even more futuristic. At the same time, hype and fascination continue to pervade Web3 debates. Commentary tends to focus on developments in the Global North and the evangelical white male 'tech bro' figures promoting them.

But previously untested Web3 technologies are being trialled to deliver key services to marginalised groups in precarious socio-economic positions.

The implications for real communities and institutions are only just emerging.

This report:

> Provides a critical background to Web3, locating it in the history of digital innovation.

> Introduces Web3 in terms of what kind of thing(s) it is, what key concepts surround it, and who is driving its implementation.

> Evaluates the promises and pitfalls of blockchain experiments targeting marginalised groups from the perspective of real-life case studies.

> Concludes by setting out recommendations for research and policy on Web3.

THE WEB: A BACKGROUND

Web3 is promoted as the latest phase in a series of technical developments that have changed how people use the internet.

The World Wide Web (WWW) is an application running across the Internet. Before WWW went public in 1991, the Internet was a kind of information cooperative designed for military use. No entity owned or made money from the network, but admission requirements—technical literacy, gear, and its costs — were high. WWW provided a more accessible route for navigating the mass of information flowing through the Internet.

With WWW came, for example, a user interface, browsers, the code languages for web pages, and the protocol for inter-machine information exchange (HTTP). What we might call Web1 started off as a decentralised, open information project. But it could only be interacted with in 'read only' form. In the 1990s, WWW users would access static web pages.

By the 2000s, we had a version of WWW — now referred to as Web2 or Web 2.0 — that enabled users to read, write, and interact. However, it introduced gatekeepers in the form of platforms like Google, Amazon, Apple, and Facebook/Meta.

Now, users upload their own content. But the current state of the web tends to be characterised as 'surveillance capitalism' or 'platform capitalism'[3]: platform companies, data brokers, and other players have created a market that capitalises on that content and monopolises profits. Most Web3 proponents suggest it provides a new alternative to the current situation.

3. See Neil Srnicek, *Platform Capitalism*, Theory Redux (Cambridge: Polity, 2016) and Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (London: Profile, 2018).

WEB3: WHAT, WHY, AND WHO?
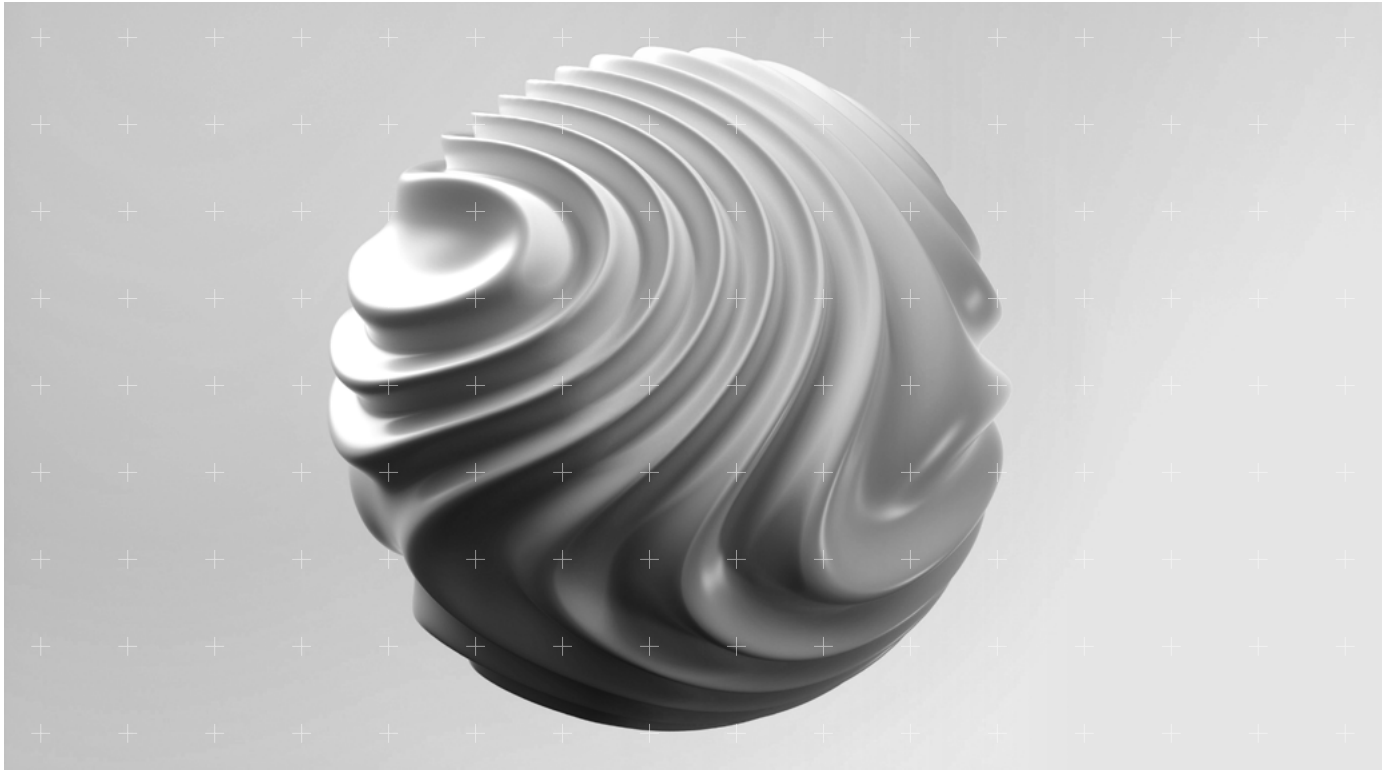
Web3 is a slippery term

This historical background to WWW may give the impression of coherence and linear evolution. However, like Web1 and Web2, Web3 is a slippery term which draws a line around a diversity of technologies, systems, and ideas which have overlapped and competed. Many Web2-era projects have sought to circumvent or dismantle surveillance capitalism, and by the same token, as I will show, many Web3 initiatives extend the agendas of big tech companies.

Web3 as a term is grandiose and misleading: it is often used to refer to a revolutionary new phase of Internet innovation. But Web3 comprises applications that run on top of the Internet. The systems labelled Web3 are ideologically and technically diverse. They are not fundamentally changing how the Web works. It is useful to define what kind of thing(s) Web3 is/are, or tend to be, and the key logics behind it, and agendas associated with it. If Web3 proposes an alternative to big tech platforms, we need to know what that could look like.

The key point to understand is that Web3 is not a singular, bounded entity, but a collection of technologies, techniques, and possibilities. Web3 initiatives deploy blockchain, and they may include other components of the following glossary.

What kind of thing(s) is/are Web3?
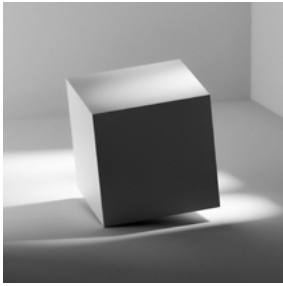
Blockchain

Blockchains are a family of decentralised database systems. They are the emblem of Web3 and the enabling infrastructure behind it.[4]
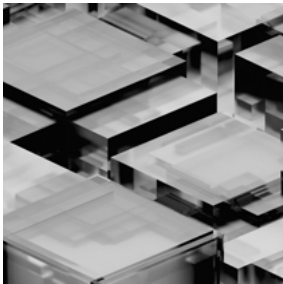
Consensus protocols

Computer protocols that prevent malicious entities from commandeering the validation of data on blockchains. Different consensus algorithms (e.g., based on proof of computational work, authority, or stake) achieve this in different ways. They are all designed to allow transactions to be completed and information to be synced, even if the actors in a network do not trust each other.


Cryptocurrency

Alternative, electronic forms of currency where transactions are made and recorded using blockchain rather than centralised authorities. The most famous example is Bitcoin, invented in the wake of the 2007–8 financial crisis to undercut the hegemony of central banks and states in the global financial system.

Cryptography

Techniques used to authenticate and secure information in a way that maximises its confidentiality, anonymity, and integrity.
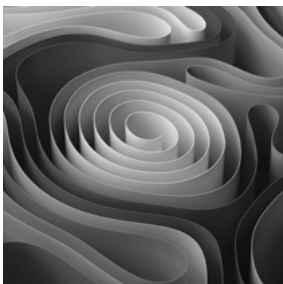
Decentralised Autonomous Organisations (DAOs):

The reimagining of organisations as collections of automated decisions which can be executed using smart contracts and without powerful or unnecessary intermediaries.

---

4. I often use the singular 'blockchain' even though the family of technologies would more accurately be described as 'blockchains', 'blockchain technologies', 'shared ledger technologies' or 'distributed ledger technologies'. I use the singular when I want to emphasise the popular, imaginative dimensions of blockchain.
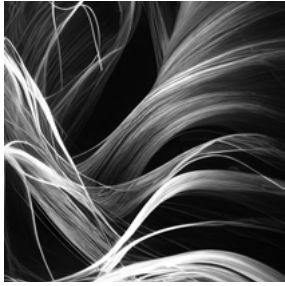
Decentralised Finance (DeFi)

Financial instruments that avoid or reduce reliance on centralised intermediaries such as banks, brokerages, and exchanges. This term encapsulates a variety of projects and systems, especially those based on blockchain and smart contracts.
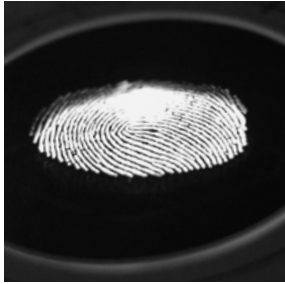
Digital identity

This refers to how people are represented and represent themselves in the digital age. Blockchain-based, decentralised digital identity schemes, like 'Self-Sovereign Identity' (SSI), claim to give individuals control and ownership of their identity information.

Digital wallets

Technological systems that store information and value, enabling users to track and execute transactions. They are used to hold and exchange currency, tokens, and coupons, but also passwords, identity information, and credentials.
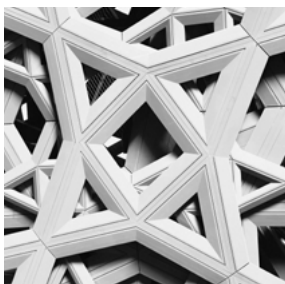
Smart contracts

These are algorithmically enforced decisions. They are programs stored on blockchain that will self-execute when predetermined conditions are met.
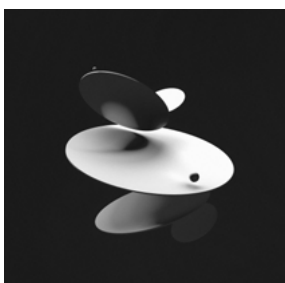
Tokens

Web3 projects often deploy token-based economics. Tokenisation makes a representation of physical or digital assets which have a unique code and can be stored and exchanged with blockchain. Examples include non-fungible tokens (NFTs), which are like placeholders for real-life assets such as artwork.

What are the key concepts surrounding Web3?

Surveying these technologies prompts us to ask what overall difference Web3 proposes to make to the web, its everyday use, and its political economy. Web3 makes some conceptual propositions that contrast with Web2.

Vendors, advocates, and other optimistic commentators tend to associate it with specific benefits and inherent characteristics. The Web3 rhetoric emphasises:

➤ Decentralisation and trustless trust

Uncritical accounts of Web3 proclaim that, in order for systems to work, we no longer need centralised authority nor trust in persons and organisations.

The suggestion is that decentralised, blockchain-based systems do not rely on a central point of authority. Instead, they distribute control across a whole network of nodes. The nodes all maintain a ledger (a set of records) which is constantly updated and transparently details every transaction that takes place. The records are not just financial: they can include cryptocurrency transactions but also votes or medical or identity information. All distributed nodes within a network share the same consensus algorithm. These allow transactions to be completed and information to be synced by instituting algorithm-based, 'trustless' trust.[5] Blockchains are associated with peer production projects.

They are widely presumed to replace the need for trusted human intermediaries, organisations, and social processes with algorithmic governance, technocratic consensus, and trust in supposedly incorruptible code.

➤ Immutability and truth

Blockchains have come to be understood as a tamper-proof way of making immutable, permanent records. Cryptographic techniques and the decentralised format mean that once data are written on a blockchain, they are shared by all computers on the network and nearly impossible to change. Blockchain is associated with objectivity, accuracy, and truth.

Even though blockchains may share the same garbage-in-garbage-out issues as any database system, they are commonly seen as achieving greater accuracy, authenticity, and veracity in record-keeping.

This is linked to the supposed accountability benefits of using blockchains, since they allow records to be transparently copied and synced among the network.

The immutability characteristic has shaped the new ideals of digital ownership associated with blockchain and Web3, especially the idea of unique, un-replicable digital assets like non-fungible tokens (NFTs).

---

5. 'Trustless' in the sense that trust is distributed across network rather than attributed to social entities, and 'trust' in the sense that the infrastructure is seen as trustworthy.

➤ Privacy and security

At the same time as promoting the transparency of information, Web3 rhetoric also tends to promote anti-surveillance ideals.

For example, blockchain-based projects involve cryptographic techniques such as public and private keys, pairs of long numbers associated with the identity of each user which are deployed to authorise transactions, and hashes, mathematical ways of creating and uniquely identifying blocks of transaction data, which are then chained together to create the records.

Overall, blockchains are characterised as a means of tracking information transparently while preserving privacy and mitigating surveillance.

CENTRALISED (A)	DECENTRALISED (B)	DISTRIBUTED (C)

● Station — Link
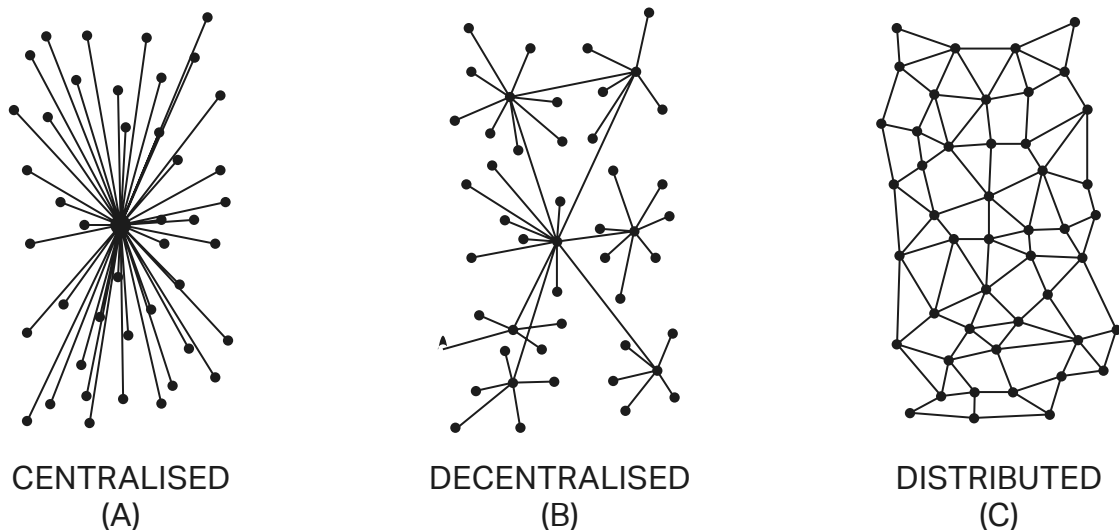
High resolution designer rendition of a figure depicting the structure of centralised, decentralised, and distributed networks. It originates from research prepared in 1962 for the US Air Force in relation to distributed governmental and military telecommunications.[6] The visualisation has become a popular explanatory resource in discussions about blockchains and distributed ledger technologies.

Concepts undermined

However, the concepts surrounding Web3 are in fact emergent, competing, and contested.[7] We cannot fix Web3 to set characteristics, and it would be a mistake to reduce, oversimplify, or smooth out the tensions and contradictions to a single unitary position (Web3: good or bad, mere hype or true revolution?). Ambiguity is an essential dynamic in this space which strategically benefits Web3 vendors and proponents. The core concepts of Web3 rhetoric — decentralisation, trustless trust, and privacy — have been challenged and undermined in notable ways:

6. Paul Baran, *On Distributed Communications: I. Introduction to Distributed Communications Networks. Prepared for: United States Air Force Project RAND, Memorandum* 1, RM-3420-PR (Santa Monica, CA: RAND Corporation, 1964), FIG. 1 Centralized, Decentralized and Distributed Networks

Decentralisation

What decentralisation means and looks like is both unclear and contested in Web3 debates. Socio-technical systems can be decentralised in different respects, to different degrees. Many projects bearing the label of Web3 and the rhetoric of decentralisation do not follow a political commitment to decentralising authority.

Different blockchains, for example, have very different properties, call upon different algorithms and protocols, and include not only public, open access, peer-to-peer networks (as with Bitcoin, where anyone can view and edit code without the permission of an authority) but also private and permissioned systems. Permissioned blockchains involve a predefined set of known entities which can process transactions. While they offer cryptographic auditability, some would argue they resemble traditional proprietary databases.

Studies reveal that even in radically decentralised projects such as Bitcoin or Ethereum we find concentrated centralisations of power, for example, in how governance decisions are made.[8] Block-chain systems are also introducing new intermediaries (e.g., technology vendors and cryptocurrency exchanges), which tend to be unregulated.

Ruptures in trust and volatility

Ruptures in trust and volatility characterise Web3 projects, especially regarding cryptocurrency markets. Web3 advocates are adamant that financial hype cycles are to be expected, just like the dotcom boom and bust. But crypto prices collapsed this year by about 2 trillion dollars as rising interest rates led to a retreat from risky and untested financial assets.[9]

That blockchain will be a reliable foundation for the next iteration of the web is unproven; privacy, security, legal and regulatory concerns persist. The Web3 fantasy of replacing traditional forms of social and institutional trust with algorithm-based trust has come into doubt.

Privacy and safety implications

Web3 has uncertain implications for the privacy and safety of user communities. Blockchains have facilitated criminal and opaque flows of value and information, especially via cryptocurrency.

Critics have raised concerns about the pseudonym-based model of online interactions and its implications for the social and financial security of users and the regulation of the Internet. At the same time, blockchains enhance traceability and tracking.

There is a popular myth that blockchain-based systems are all privacy preserving and anonymous. But surveillance and hacking still happens in Web3 initiatives, especially in permissioned and private blockchain networks.[10]

Who and what are driving Web3?

The Web3 political economy

Web3 supposedly circumvents and undermines the power of the big technology companies and governments. Some states have banned digital financial assets like crypto outright, including the Russian government, based on the idea that Web3 undermines national sovereignty and citizens' economic security.[11]

At the same time, Web3 is being propagated by players like Facebook/Meta (with their payment platform Diem), PayPal (who are funding a project which allows financial institutions to share customer identity checks), and various governments around the globe (UK ministries are exploring how blockchains can be used to deliver benefits payments and secure digital evidence in the justice system; the Chinese state has declared blockchain a national priority for industrial development). Some, including the Web5 proponents I mentioned above, argue that Web3 is merely snake oil. They suggest the emancipatory rhetoric disguises how Web3 innovations channel capital to elites and erode democracy.

The myths and mystification around Web3 are at least partially explained by the vested interests driving it. Celebrity endorsements are misleading people into viewing cryptocurrency and other Web3 projects as wealth-building rather than acknowledging how they are fostering unregulated havens for the rich.[12]

Web3 is being pushed by venture capitalists. For example, Andreessen Horowitz, otherwise known as a16z, launched a $4.5bn Web3 fund in 2022. The company is fuelling investments and profits from Web3 start-ups, while ironically maintaining a strong stake in Web2 — its CEO Horowitz sits on Meta/Facebook's board.[13]

What's more, new commercial players like Coinbase — the cryptocurrency exchange platform which allows people to buy, sell, transfer, and store crypto, and convert it into local and fiat currency — are positioning themselves as the go-to gatekeepers of Web3.

Web3 human experiments

While some people are choosing to adopt new technologies like cryptocurrency themselves as a means of addressing their socio-economic challenges,[14] many Web3 solutions are being imposed on communities such as refugees without the offer of choice or alternatives. Poverty and disaster are major frontiers of capital accumulation by technology companies and infrastructure providers striving for dominance in 'emerging markets'.

Web3/blockchain companies and start-ups are developing models and patents in settings like refugee camps where tax, data protection and other regulation, accountability, and the rights, liberties, and choices of users are diminished.

Humanitarian and development aid organisations are attracted to non-traditional commercial partnerships with Web3 companies. The rhetoric of Web3 fits the sector's goals such as transparency and targeting, efficiency and effectiveness.

Well-meaning innovation experiments seeking to empower marginalised groups are also strategically useful to aid organisations as a means of attracting funding from donors.

Web3 projects must be contextualised within existing patterns of experimental innovation in the Global South in which digital identity and fintech solutions promoting the recognition and empowerment of disadvantaged communities are also used to surveil, control, police, and discriminate against them.[15]

Web3 is being appropriated and adapted to serve a variety of interests, including as a slogan in business-as-usual projects that do not address people's most pressing needs or shift patterns of authority and profit in surveillance capitalism. We need to guard against techno-utopianism and pay attention to the politics of technology design, governance, maintenance, and use.[16]

Photo by Margie Cheesman from a district of Azraq refugee camp, Jordan, October 2018.

CASE STUDIES: TARGETING MARGINALISED GROUPS

Investigating three key areas of socio-economic life where Web3 experiments are reaching and influencing as solutions in humanitarian and development aid.

The term marginalised groups refers to low-income communities disadvantaged by and/or excluded from mainstream financial, welfare, and social services.

I use this term to encapsulate the populations affected by the case studies discussed on the following pages: refugees such as persecuted Rohingya people, or Syrians escaping civil war, who do not have citizenship rights or bank accounts; cyclone survivors in Vanuatu whose income sources and livelihoods have been destroyed; entrepreneurs, cross border traders, and poor communities struggling to sustain income who are targeted for development aid initiatives in Kenya, Rwanda, Chile, Indonesia, and elsewhere.

Technology use never transcends context. Socio-technical systems are always embedded in everyday life. People make the Web, and it looks different depending on where and who you are. This section investigates three key areas of socio-economic life Web3 experiments are reaching and influencing as solutions in humanitarian and development aid.

These are:

➤ **Payment**

➤ **Currency**

➤ **Identification**

> Payment

Digital payments are more popular than ever in the context of the COVID-19 pandemic as they are widely seen as enhancing the effectiveness and safety of financial exchange. Some of the most notable and large-scale experiments in this domain have been in international aid.

These experiments do not necessarily involve cryptocurrency, but they all make use of the digital infrastructure underlying cryptocurrency, blockchain. In the aid industry, blockchain is often seen as a revolutionary, borderless infrastructure that could transform payments by circum-venting fragile local financial systems in the Global South.

Web3 experiments have reduced the costs and transaction times of humanitarian

payments. The Leaf system is promising, for example, (discussed in a case study on the following pages) because it equips technologically skilled and poor migrant populations with fee-saving, independent-ly managed financial tools.

However, a number of issues complicate the benefits of these systems:

Extractive business

New blockchain platforms do not neces-sarily challenge the extractive business logics that financial inclusion initiatives in the aid industry have long exhibited.

Web3 initiatives rely on non-traditional public-private partnerships. Through digital payment systems, companies funnel trans-action and location data into profit.

For example, critics suggest Oxfam's Unblocked Cash has beckoned block-chain companies like Consensys into an influential position from which they can develop their products in circumstances of limited accountability and tax.[17]

The involvement of the biometric technol-ogy company IrisGuard in providing the digital identity component of WFP's Building Blocks project has been criticised.

IrisGuard holds iris scans of 2.7 million Syrian refugees across five countries and works with the Jordanian state. The company's involvement in humanitarian payments threatens to extend both national security and corporate interests in refugee camps.

20

Case Study 1.
The United Nations World Food Programme's Building Blocks project

This project launched in Jordan in 2017 in two camps hosting Syrian refugees. It is now expanding to reach conflict and disaster-affected communities in Bangladesh and Lebanon. Building Blocks delivers aid payments to over a million people; $325m have been transferred using this system.[18]

Photo by Margie Cheesman, Margie's eye through the biometric camera, Za'atari refugee camp, Jordan, March 2019.

Photo by Margie Cheesman, near a Za'atari refugee camp food market, Jordan, January 2020.

The project institutes blockchain as the mutually owned infrastructure for aid organisations to coordinate their payments to refugees. Instead of using competing, proprietary payment systems, Building Blocks encourages the collaboration of United Nations agencies around a shared ('neutral', 'trustless') system. Building Blocks addresses the problem that humanitarian payments depend on financial intermediaries (principally banks, who charge fees), and involve significant risks (funds and beneficiary information are advanced to banks upfront, which involves the potential for bankruptcy, fraud, and data security issues) and inefficiencies (the bank has to verify every transaction, settle with retailers, and produce account summaries).

For its proponents, the project saves aid organisations transaction fees and enhances accountability and data security. Building Blocks provides a real-time record of transactions and allows organisations to make direct settlements, minimising the profits traditional payment intermediaries make in humanitarian contexts.

Regulatory uncertainty

There is persistent uncertainty and concern within aid organisations about the regulation of Web3 payment infrastructure: whether and which laws apply, especially in the absence of blockchain-specific regulation and block-chain's debated compatibility with estab-lished data protection regulations such as the European Union's General Data Protection Regulation (GDPR). Most Web3 payment projects explicitly aim to track data such as transaction patterns, albeit using secure cryptography. Central banks are filing complaints against some Web3 aid initiatives because they threaten to bypass local financial systems, devalue fiat currency, and reduce demand for local banking services.[19]

Case Study 2. Oxfam's Unblocked Cash project

This Vanuatu-based project delivers digital payments to 35,000 'unbanked' people affected by Cyclone Harold and the COVID-19 pandemic.[20] Oxfam deploys digital currencies referred to as borderless 'stablecoins', i.e., currencies that can be held and used across nation state boundaries but at the same time are pegged to a less volatile mainstream currency like the US dollar.

The money comes to people in the form of prepaid cards, which they can use at designated local shops. With blockchain, transactions are verified and recorded across a distributed network of computers. Transacting parties are registered, servers are located, and transaction data is stored in multiple, geographically disparate nodes.

Oxfam suggests the project allows aid organisations and donors to track funds and transactions, and local shops to both exchange their digital tokens into a local currency between themselves, and to make exchanges of goods between themselves without intermediaries. Unblocked Cash is about using Web3 tech to facilitate unmediated, frictionless payments, and create a local community-led monetary ecosystem.

Root issues

Reductions in transaction times and costs may introduce efficiencies for aid recipients when they are accessing aid payments. But these blockchain payment projects do not necessarily address the most pressing issues marginalised and low-income communities such as refugees face, and they also introduce new problems.

For example, my research in Jordan's refugee camps shows that getting paid and managing money in a digital wallet and redeeming digital tokens into local currency involves extra responsibilities, skills, labours, contingencies, and risks compared with the payment systems people were accustomed to.[21]

For example, blockchain experiments can disrupt trusted interactions with established payment providers, jeopardise the material contact people have with their money and with analogue methods of accounting, and provide inadequate recourse mechanisms when payments go wrong.[22]

22. Margie Cheesman, 'Blockchain for Refugees'.

Case Study 3. UNICEF's Leaf wallet

In 2019, UNICEF launched the Leaf project for refugees and cross-border traders in East Africa.

By the end of 2022, the project anticipates reaching 23,847 people. Leaf is a block-chain-based digital wallet through which users can store money in multiple exist-ing currencies (currently RWF, KES, and UGX), pay for goods and services in their selected currency, and make exchanges with other Leaf users within the wallet.

Bypassing traditional money tranfer systems like Western Union or MoneyGram, the Leaf blockchain infrastructure circumvents the fees associated with cross-border finance, which range from twenty to thirty percent.

Settlement costs are almost zero with Leaf, allowing people to reduce spending on their financial transfers. The wallet does not require smartphone or internet connection; it can also be used via feature phone and USSD short codes.

The wallet is integrated with the mobile money ecosystem in East Africa, as users can request funds from mobile money numbers across borders. Twenty percent of Leaf users are under twenty-one: the project targets young, technologically savvy individuals as a way of supporting their financial independence, responsibility, and skills.

> Currency

Just like blockchain payment infrastructures, Web3 currency projects propose to address some of the major problems of 'legacy' banking.

Proponents maintain that new crypto and alternative currencies could transform economies by strengthening grassroots, peer-to-peer economic activity, and deliver financial inclusion and new investment tools to 'unbanked' people.

Proponents of crypto and alternative currencies suggest they provide a lifeline to people without reliable access to

stable currency or liquidity. But at the same time, these currencies pose serious concerns:

Accessibility

Not everyone can or should be self-reliant and entrepreneurial. Not everyone possesses the know-how to safely manage cryptocurrency accounts, exchanges, and investments. Not everyone can afford and maintain access to mobile devices and the Internet.

English is the crypto lingua franca, which excludes people from crypto platforms, news, and information. In Lebanon, with

the collapse of the Lira, people turning to cryptocurrency have had to figure out how to negotiate currency exchanges on the (unregulated, scam-ridden) informal peer-to-peer trading groups that have emerged on WhatsApp and Telegram.[23]

Start-ups like Fluus in Lebanon and Worldcoin in Sudan have taken up the challenge of training people how to download and manage digital wallets on their phones and buy through trustworthy peer-to-peer agents (which the start-ups also need to vet).

These start-ups admit the challenges here, especially training people who have not used email before or cannot afford regular Internet access. The accessibility barriers end-users face are significant in this unregulated space, and there is a concerning lack of evidence that the business service and recourse mechanisms provided by companies and organisations are reliable or sufficient.

23. Csizmazia, 'How Refugees in Lebanon Can Benefit from Cryptocurrencies'.

Case Study 1. Worldcoin

The Worldcoin currency experiment is promoting itself as a wealth distribution project. It has been tested in twenty-four countries, including Indonesia, Chile, Sudan, and Kenya.

In March 2022, 450,000 individuals had been onboarded as users. The Worldcoin company funds local subcontractors to find and enrol low income customers, who receive a 'social assistance giveaway' of WLD (the Worldcoin cryptocurrency) when they register to download the Worldcoin wallet app. WLD is not pegged to a stable currency such as the US dollar.

In fact, in 2022 this cryptocurrency has not yet launched, and the company admitted they cannot confirm what its value would be in established financial markets.[24]

Reinventing the wheel

Some pressure groups focus on advocating for substantive change to mainstream financial systems — for example, by exerting regulatory pressure on local banks to extend loans to low-income communities, or on host governments to give refugees and stateless people forms of ID that allow them to access bank accounts.

By contrast, Web3 currency schemes reinvent the wheel. Indeed, Kenyan banks have contested Sarafu because the scheme does not require users to hold national fiat currency, and so is seen as devaluing the local currency and undermining demand for their services.[25]

Ultimately, people want and need to exchange their crypto, tokens, or vouchers into a useful local currency. This comes at an extra cost in terms of people's time, money, and exposure to risk.

Exploitation

Even the most well-meaning currency initiatives expose people to financial and personal risk. Crypto-related crime is pervasive.[26] New shadow/black market practices inevitably emerge when people need to exchange currency.

Currency brokers' commissions can be extortionate, and fraud and scams are rife. Little is known about the sufficiency of recourse mechanisms, for example, if a scam victim needs to recover funds. The trend for incentive-based, behaviour-shaping models of financial aid is concerning — as in the Sarafu weekly rewards and the free WLD tokens for personal data registration. Other schemes are incentivising communities to adopt crypto trading and investment tools to encourage financial literacy, but they potentially invite great personal and financial risk,[27] since scamming is not an incidental but core feature of crypto and blockchain initiatives.[28] People living in precarious settings and in poverty may see their privacy unravel as they may not be able to turn down the money offered for personal data and signup.

For example, an investigation into a project similar to Worldcoin, called Terra, found that '[t]he platform was riddled with bugs and could crash, leaving people with incomplete tasks for which they were later punished'.[29] These behavioural models reinforce inequalities by exposing those with the most to lose to new demands and risks.

Experimental and volatile

Most experienced humanitarian and development aid organisations have avoided setting up new cryptocurrencies, which may be untested and volatile in value, and instead deploy tokens pegged to established currencies (see World Vision's Sikka project, UNICEF's Leaf project). There is insufficient evidence about the stability, usefulness, and accessibility of alternative currency projects run by reputable organisations such as the Red Cross Sarafu initiative.

But we already know that outfits like Worldcoin offer people meaningless cryptocurrency. In early 2022, investigative journalists at MIT Technology Review revealed that Worldcoin users could not trade WLD from their wallets.

Bugs in its implementation were detrimental. Worldcoin shifted from a web-based to mobile app-based scheme, and in the process many users lost their accounts and coins. There are now many scam-experiments like Worldcoin.

In the case of Terra: '[i]n what some experts suggest may have been a coordinated manoeuvre, a massive push to buy UST caused the stablecoin to lose its peg, resulting in a bank run — and ensuing death spiral — where holders rushed to sell'.[footnote] Users lost everything.'[30] People had to switch between platforms like PayPal and AirTM to move their money, and the infrastructure was not reliable enough to provide regular, timely payments.

Case Study 2. The Red Cross Sarafu project

This 'community inclusive currency' (CIC) scheme for Red Cross beneficiaries involves blockchain-based e-vouchers (Sarafu) being transferred to people's mobile phones. When they participate in Red Cross schemes by providing services or selling goods, users earn Sarafu credit which they hold, share, exchange and spend within the community of users and selected local businesses via a mobile app.

The more someone uses Sarafu, the more 'rewards' they receive on a weekly basis.[31]

Transactions are all recorded on the blockchain, which the Red Cross (the Kenya, Norway, and Denmark branches, in conjunction with the blockchain company Grassroots Economics) suggest enhances the speed, security, and transparency of financial assistance.

The system has been tested in parts of Kenya and Ethiopia among low-income communities. For example, a pilot project in 2020 delivered Sarafu vouchers to 40,000 pandemic-affected people.[32]

Surveillance

Cryptocurrency may be accessible to people who lack legal documents for formal banking such as proof of address — 'anyone can create a digital wallet'.[33]

But cryptocurrencies and alternative currencies may enhance surveillance and profiling of marginalised groups. Under the banner of financial inclusion and wealth distribution, these schemes collect, track, monetise personal data, and use it to train neural networks. The Red Cross currency scheme Sarafu uses the rhetoric of privacy and blockchain, but it also has as its key aim using transaction information to improve the targeting of aid.

Registration for currency schemes like Worldcoin and Terra demand that people share names, phone numbers, email addresses, transaction information, and even biometrics.

Worldcoin has collected 450,000 high resolution images of bodies, faces and eyes from people in countries across the Global South.

Even if the use of blockchain means securing personal data using cryptography, these practices will still open up the likelihood that users can be tracked in future scans.

32. Wamugu, 'The Kenya Red Cross Launches Sarafu'.

33. Csizmazia, 'How Refugees in Lebanon Can Benefit from Cryptocurrencies'.

> Identification

The turn towards *decentralised* digital identity is a popular component of Web3. The decentralised or 'self-sovereign identity' movement proposes to hand over the control and ownership of identity information from institutions to individuals.[34]

How people should be represented and/or represent themselves in digital environments is a core concern in debates about the future of digital governance. Identity documents have long been central to the governance of societies as the basis of political recognition and welfare but also surveillance, policing, and discrimination.[35]

Since COVID-19, vaccination passports and other digital identity tools for accessing public and health services have come to the fore.[36] In many global settings, certain groups face extensive barriers

accessing a safe and persistent form of ID, especially LGBT+ individuals and persecuted ethnic, political, or religious groups.

Decentralised ID projects aim to use blockchain to systematically reduce — or even remove — people's reliance on commercial and state gatekeepers which are potentially hostile or exploitative to groups like refugees. Other decentralised identity projects with noting involve, among others, public authorities, and NGOs in British Columbia,[37] the Netherlands, Belgium, and Germany,[38] Thailand and Indonesia,[39] Lebanon, and Tanzania.[40]

Through blockchain-enabled digital identity, these projects seek to facilitate forms of power and agency for technology users, especially people whose protection under national law is in question. But there are also key risks, myths, and unresolved questions:

---

34. Cheesman, 'Self-Sovereignty for Refugees?'

35. Weitzberg *et al.*, 'Between Surveillance and Recognition'.

36. Aaron Martin, Emrys Schoemaker, Keren Weitzberg, and Margie Cheesman, *Researching Digital Identity in Times of Crisis*, Workshop Report (Alan Turing Institute, August 2021)

Shifting responsibility to users

Not all Web3 identity schemes allow users to selectively disclose and minimize sensitive data sharing. Even when they do, putting the onus on users to manage personal data could be considered an abdication of institutional responsibility— especially given uneven access to Internet, devices, skills training, and technical support.

Decentralised identity initiatives may digitalise bureaucratic processes in a way that enhances efficiency but erodes safeguards, accessibility, and personal contact with institutions.

Case Study 1. The Rohingya project

This project addresses the systematic denial of political recognition to a stateless ethnic group, the Rohingya people, who are denied birth registration and persecuted in Myanmar and beyond.[41]

The project provides Rohingya people with an 'R-ID', which they access through an online platform. The platform allows them to have oversight over personal identity data (e.g., educational certificates or land titles) and make decisions about sharing data with third parties.

The Rohingya Project verifies the identity data and issues users with cryptography-based unique ID numbers and barcodes. With their numbers/codes, users can then attest to their eligibility for certain services — if the service provider accepts the R-ID as valid.

The Rohingya Project aims to provide an alternative route for accessing healthcare, education, microfinances, e-voting, and other services, beyond the mechanisms of any government. The idea is that identity holders manage how they share their information, rather than allowing centralised financial or public institutions to do so.

Case Study 2. Tykn/The International Red Cross

The start-up Tykn aims to set up an alternative identity infrastructure for refugee populations who struggle fulfil the necessary ID checks and credit scores required for banking or employment. The start-up is developing back-end identity solutions using blockchain. In collaboration with the Red Cross initiative '121' they have launched initiatives involving undocumented migrants in the Netherlands,[42] and Syrian refugees in Turkey.[43]

The latter project aims to extend work permits to refugees in collaboration with the Turkish Ministry for Foreign Affairs and United nations agencies such as WFP and UNDP. The emphasis is on enhancing the efficiency of identification processes by cutting out manual bureaucracy: the Tykn co-founder suggests, '[w]ith the use of self-sovereign identity, the processes of issuing and verification of documentation and identity credentials don't need to be slow and costly anymore'.[44]

Data capture

Many blockchain-based systems (like Worldcoin, which also has a digital identity component) are concerning surveillance tools rather than exemplars of data minimisation. Critics have raised concerns around blockchain's compatibility with the right to be forgotten, and the potentially devastating implications of storing personal information about persecuted groups like Rohingya people on an immutable blockchain ledger.[45]

While the EUDI promotes privacy and sensitive disclosure, proponents of an open, blockchain-based digital identity ecosystem stand against the EU's commitment to Know Your Customer (KYC), Anti-Money Laundering (AML), and consumer protection regulations, which would limit possibilities for pseudonymous, self-managed identities. And like all identity schemes before them, Web3 projects cannot escape the fact that enacting identification involves the sensitive and political work of classifying people. Initiatives like the Rohingya Project position themselves as a new intermediary with the authority to determine and gatekeep who counts as a Rohingya person.

Data capture tends to be a basic requirement for participation on new digital identity platforms. Decentralised blockchain initiatives are not exempt from the profit-driven and political motives of the ever-expanding digital identity industry.

---

44. Baker, 'On the Horizon'.

Root issues

Decentralised ID schemes, like other Web3 initiatives, do not address the political structures that hamper certain communities' access to financial, health, and social services and mobility. In most countries, for example, refugees or stateless people have minimal legal and political rights and protections.

Blockchain based IDs like the R-ID are not a substitute for formal recognition by states, such as refugee status or citizenship. Web3 projects like Tykn are working on coordinating recognition processes with government agencies. But these solutions still may not be legally valid, and the services people can access using the decentralised ID may be limited.

Case Study 3. EU Digital Identity wallet

This case study strongly borrows concepts from Web3 identity initiatives, especially decentralisation and privacy. The wallet project does not yet involve marginalised communities, but it is a notable and high stakes example of an experimental identity governance model: it combines finance and identity management and will be consequential in international policy.[46]

The project was launched in 2021 by the European Union and comprises representatives from EU member states. Member states will implement the European Digital Identity (EUDI) wallet, through which citizens will hold identity documents and money in a way that is recognised across EU borders.

The wallet will be accessible to EU citizens via mobile and desktop. Based on shared technical standards and privacy-centred principles, the EUDI wallet allows citizens to selectively disclose information.

The consortium will launch multiple use cases for the EUDI wallet, including educational and professional qualifications, mobile driving license and travel credentials, and payments.

CONCLUSION

Web3 is not a revolutionary or infallible technology, but a family of possible systems that must be designed, governed, and maintained safely, or not at all.

This historical background to WWW may give the impression of coherence and linear evolution.

This report has highlighted the frictions between promise and practice in Web3 experiments involving marginalised groups, countering the big talk about disruption and the revolutionary potential of Web3 technologies. Refugees and low-income populations are at the frontline in absorbing the risks and failures of Web3 technological development.

Web3 rhetoric emphasises an emancipatory, blockchain-based, frictionless, privacy-oriented, peer-to-peer future for digital society in which centralised institutions and technology platforms relinquish authority and profits. But this report has outlined why and how that future is already being undermined.

For start-ups, aid organisations, and other proponents, blockchain payment rails, cryptocurrency savings and investments tools, and decentralised identities offer efficient, cheap, alternative routes to financial inclusion and identity recognition for the most excluded populations. But the barriers, challenges, and costs for user communities are considerable:

> Web3 technological solutions ramp up the responsibilities and demands on marginalised communities to manage and maintain access to digital devices, data, Internet connectivity, English language, digital, and financial skills. They involve ambitious arrangements which most people would struggle with such as managing personal identity data, public and private keys, digital wallets, and new currency conversions.

> Many experiments promote data capture and tracking, e.g., of refugees' financial transactions, despite how central privacy and cryptography are in Web3 PR.

> There is a lack of evidence to suggest Web3 solutions are putting in place adequate safeguards protecting people in unregulated digital ecosystems, especially from cryptocurrency fraud and scams.

> Decentralisation is the cornerstone of Web3 rhetoric, but the case studies do not reveal meaningful shifts in the mainstream distribution of authority and resources in the aid industry or other crisis zones.

> Web3 initiatives tend not to address underlying causes of exclusion from existing finance and identity systems. Web3 projects are not improving structural conditions, for example, through coordination with advocacy groups, government, civic and financial institutions, and the reform of nationality laws to extend loans and meaningful forms of identity recognition to low-income, stateless, and refugee groups.
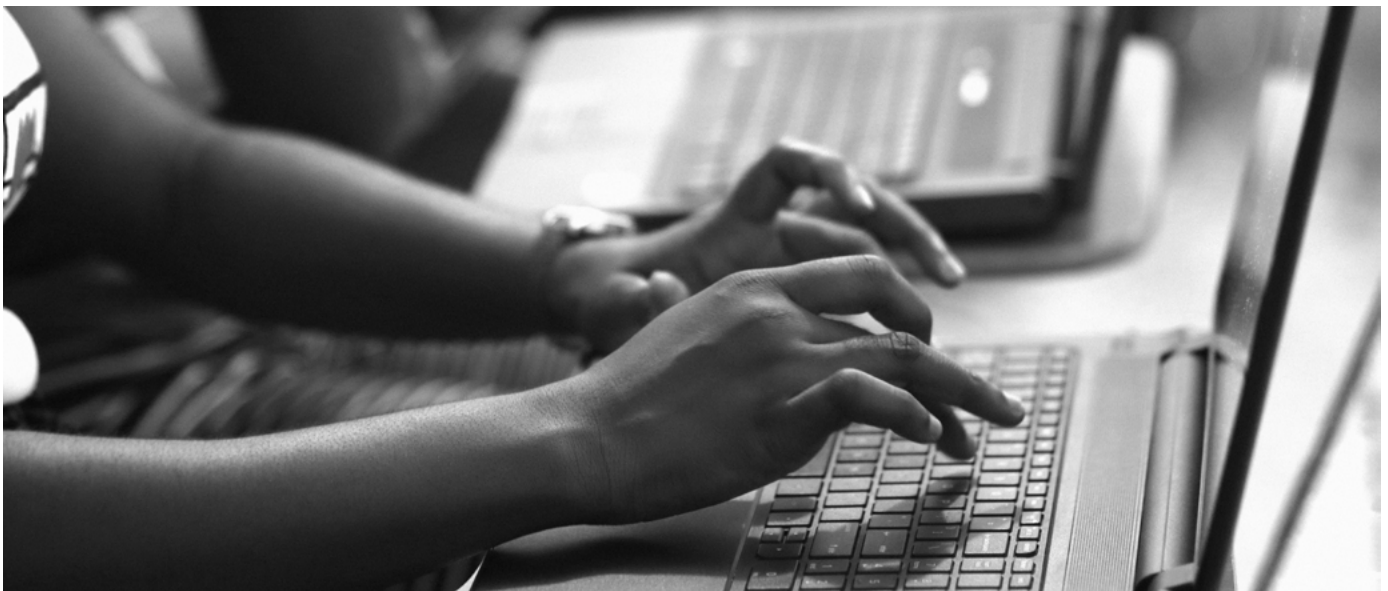
RECOMMENDATIONS

Based on this report we recommend:

> ### 1. Web3 solutions, especially untested cryptocurrencies, should not be imposed experimentally on marginalised communities

Companies and institutions are targeting refugees, aid beneficiaries, low-income groups, and other marginalised communities for Web3 experiments in contexts of limited accountability and regulation. In case studies discussed here, users are missing out on choice or alternatives or are not in position to turn down the incentives start-ups provide. Web3 solutions, especially untested cryptocurrencies, should not be imposed experimentally on marginalised and low-income groups that lack everything from a choice of alternatives to resources, political-economic rights, safety nets, recourse, and protections.

> ### 2. Public institutions need to coordinate around vetting private Web3 companies

Web3 initiatives rely on non-traditional public-private partnerships. Aid organisations are deferring to new private companies as experts and intermediaries in Web3 projects. Organisations could do more to build internal capacities around finance, data, and technology, share learnings from Web3 initiatives, and critically analyse and vet blockchain/crypto vendors and advocates based on a comparative evidence base. If organisations lack the resources to do this, oversight and accountability could be coordinated by an international body, for example in the United Nations system.

> ### 3. We need better research on the design, maintenance, and use of Web3 technologies

Understanding how Web3 innovations are being made, used, and playing out in practice will help policymakers make better choices. Close-up research reveals unintended consequences, frictions and barriers, workarounds, and resistances to new tech. We need to understand how users navigate blockchain and crypto-currency ecosystems and technologies in conjunction with their existing rituals and devices (e.g., with fiat cash, identity systems, payment platforms, currency exchange groups on WhatsApp, or mobile phones). In-depth research on case studies is lacking, especially qualitative studies at the intersection of these technologies and people's values, cultures, and experiences. Such research could illuminate how to develop appropriate recourse and support mechanisms, or indeed when an initiative is inappropriate for use entirely.

BIBLIOGRAPHY

35

Srnicek, Neil, *Platform Capitalism*, Theory Redux (Cambridge: Polity, 2016)

Zuboff, Shoshana, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (London: Profile, 2018)

> Alison Richard Building
7 West Road, Cambridge
CB3 9DT

> www.mctd.ac.uk

> minderoo@crassh.cam.ac.uk

UNIVERSITY OF
CAMBRIDGE