cipher //

Understand
IPFS
Technology

Data Storage

IPFS ALLOWS TORRENT-LIKE SHARE OF UNCENSORED, SECURE AND PERMANENT CONTENT ALL OVER THE WORLD.
IT ALSO GIVES EACH USER THE CHOICE TO STORE JUST WHAT IT NEEDS;
ALLOWING REDUNDANCY, OFFLINE USAGE AND THE ABILITY TO ACCESS IT FROM ANY DEVICE.

"WHEN DATA OF ANY SORT ARE PLACED IN STORAGE, THEY ARE FILED ALPHABETICALLY OR NUMERICALLY, AND INFORMATION IS FOUND (WHEN IT IS) BY TRACING IT DOWN FROM SUBCLASS TO SUBCLASS. IT CAN BE IN ONLY ONE PLACE UNLESS DUPLICATES ARE USED." (VANNEVAR BUSH — "AS WE MAY THINK")

"IF YOU ASKED PEOPLE IN 1989 WHAT THEY NEEDED TO MAKE THEIR LIFE BETTER, IT WAS UNLIKELY THAT THEY WOULD HAVE SAID A DECENTRALIZED NETWORK OF INFORMATION NODES THAT ARE LINKED USING HYPERTEXT." (FARMER&FARMER — "THE HEART OF THE BUILDER")

"A CRUSADE AGAINST TECHNOLOGY MISUSAGE WOULD BE THE NOT SO SIMPLE KEY TO RENAISSANCE 2.0" (C2 — "HELLO WORLD!")

#PINGTOOHIGH / BANDWIDTH

A SERVER MANAGES ITS REACHABILITY IN VARIOUS WAYS.
BY CONNECTING TO A WEB PAGE, YOU LEAVE YOUR PC'S FINGERPRINT IN THAT SERVER, BY HANDSHAKING IT. IT IS CONVENTIONAL PRACTICE, COMMON IN STANDARD PROTOCOLS; IT IS SIMPLE, BUT SEVERELY LIMITATED.
MOST OF THE TIME, THE PROVIDER CHUNKS A SINGLE MACHINE FOR EACH WEBSITE IT CAN HOST.
THE LIMITS THAT A SINGLE REMOTELY-ACCESSED SUPERCOMPUTER CAN HAVE ARE THE HARDWARE ITSELF, AND ITS LOCATION IN THE WORLD:
-IF A HUNDRED STUDENTS CONNECT TO THE SAME DOCUMENT ON THE INTERNET, IT WILL LAG A LITTLE FOR EVERYBODY CONNECTED TO THE SERVER.
-IF A EUROPEAN OPERATES WITH AN AUSTRALIAN, IT WILL LAG BY DEFAULT FOR BOTH OF THEM.

SCALING NUMBERS AND SPACE BECOMES QUITE CHALLENGING, BUT WHO NEEDS SUCH A CONNECTION? YOU CAN STILL BUY MORE RELAY SERVERS AROUND THE WORLD FOR SURE, BUT THEY DON'T ONLY COME WITH A PRICE, YOU CAN'T KNOW IN ADVANCE IF THE SERVER YOU'RE ADDING WOULD BE FOR A FEW SPIKES OF ATTENTION OR NOT.

"THE GENERAL RULE IS THAT THE MORE DISTANCE BETWEEN BRIDGED SERVERS, THE MORE PING AND PACKET LOSS GOES UGLY." (C2 — "STOOPEED 3D WORLD")

P
R
O
B
L
E
M

#OOF / SECURITY

"IT USUALLY REQUIRES A BROWSER AND SOME RESEARCH, BUT IF A SERVER GETS SOME NEGATIVE ATTENTION, DDOS ATTACKS ARE ACHIEVABLE BY ANYONE." (C2 — "DDTOYS")

THE SYMPTOMS OF A POORLY HOSTED SERVER GENERALLY ARE: YOU CAN'T ACCESS THE WEBSITE, OR IT REACTS INCREDIBLY SLOWLY. SOMETIMES THE SERVER GOES DOWN, GIVING THE OLD-FASHIONED 404 ERROR.

"THANKS TO THE INTERNET DISTRIBUTION, SOME TEENAGERS GREW UP PLAYING WITH INTERNET APPLIANCES, BECOMING GREAT CYBERSECURITY RESOURCES, BUT NO DRAMATIC SECURITY UPDATES WERE RELEASED." (C2 — "CRITICAL UPDATE REQUIRED")

HTTP AND ITS SPECIAL BROTHER WITH THE VERIFIED MARK, HTTPS, ARE ALREADY EXHAUSTED PROTOCOLS COMPARED TO TODAY'S PATTERNS. TOOLS THAT TRY ALL SORTS OF THINGS TO WEBSITES PROVE FLAWS IN THE SYSTEM AND TRY TO PRE-EMPT THEM. IT MEANS THAT THE SYSTEM HAS FLAWS, BUT YOU CAN PLAY AT BEING THE PLUMBER. WHEN TRYING TO SELL A DIGITAL PRODUCT, REMEMBER THAT YOU'RE STILL COMPETING WITH THE WORLD'S PEOPLE STRENGTH OF PERSONAL RESEARCH AND 30Y OF PEN-TESTERS ON THIS SAME PROTOCOL.

TRUSTING A THIRD-PARTY SERVICE PROVIDER TO HOST YOUR WEBSITE ON LIMITED HARDWARE DEVICES, WITH ALL THE ESSENTIAL EXTRA PAID PROTECTION FEATURES AND THE RISK OF WORKING ON A MACHINE WITH NEGATIVE ATTENTION, IS UNSUSTAINABLE.

P
R
O
B
L
E
M

"THE WORST PART COMES IN TERMS OF PRIVACY, BUT DON'T WORRY. JUST A BOT WOULD LIKE TO GOOF AROUND ALL YOUR STUFF." (C2 — "WHAT CAN'T AN AI DO?")

#CLUSTERS? / SPACE

ANY SERVER HAS AN OS THAT LINKS SEVERAL RACKS OF HARD DRIVES SO THAT YOU CAN ACCESS IT WITH CALLS THAT CAN BE MEMORIZED FROM ANY DEVICE. CLOUD SERVICE PROVIDING IS A SERIES OF LINKED SERVERS USED TO STORE ENTIRE DATA ON SHARED HARD DRIVES. IT RESULTS IN A LINK WITHIN THE PROVIDER'S DOMAIN, SERVED VIA A GRAPHICAL INTERFACE. THESE MACHINES CAN CLOG UP QUICKLY BECAUSE YOU CAN'T KNOW IF THE USER WANTS TO UPLOAD SMALL OR BIG FILES, SO YOU CHOOSE TINY SPACE AT SIGN UP. ADDITIONAL SPACE CAN BE BOUGHT, AND BASED ON THE USUAL FLOW OF CLIENTS, YOU, AS A PROVIDER, CAN EITHER EXPAND OR CUT EXPENSES.
ON THE CLIENT-SIDE, YOU WILL ALWAYS HAVE TO PAY TO LOCK SOME FUNCTIONAL SPACE FOR USE.

"THERE IS NO CHEAP CLOUDING SOLUTION THAT ALLOWS THE STORAGE OF TERABYTES REMOTELY AND SECURELY, NO METTER THE USAGE. $CENTRALIZED SYSTEMS ARE NOT MEANT TO SCALE WITHOUT TECHNICAL EFFORTS." (C2 — "MEET IPFS $CLUSTER")

P
R
O
B
L
E
M

#HISTORY / BAD-HABITS TAKE EXAMPLES TO CORRECT

BACK IN THE 60S, DARPA USED TO WORK ON MACHINES REMOTELY: SERVERS WERE ROOMS FULL OF ROLLS WITH HOLES AND A HOLE READER. YOU ACCESSED THEM REMOTELY FROM A COMPUTER WITH A CONSOLE-LIKE INTERFACE.

"ROOMS O' ROLLS WERE SPREAD PHYSICALLY IN DIFFERENT PLACES, THOUGH ACCESSED FROM ONE POINT. IT WAS A HUGE LAN, REMOTELY ACCESSIBLE FROM ONE IP." (C2 — "WHERE BUGS WERE STILL BUGS")

WE DECIDE TO STICK WITH THE PATTERN BECAUSE THESE MACHINES ARE INCREDIBLY EXPENSIVE AND CUMBERSOME, BUT LET'S SKIP THROUGH DECADES:
-IN THE EARLY 70S WE INVENT MICROPROCESSORS. TO CATCH UP WITH THE IMMINENT TREND, SERVERS BECOME CLOSER TO HOW VERY CHEAP PORTABLE COMPUTERS PERFORM TODAY.
MORE MACHINES COULD BE STACKED INTO A SINGLE ROOM, CREATING A MARKET. THE ROOM OWNER THEN SOLD THE VIRTUAL COMPUTING SPACE, UNIFORMING THE STANDARD WEB TO A FULLY CENTRALIZED FASHION.

-IN THE 80S, WE CREATED DOMAIN NAMES; YOU CAN ACCESS MACHINES BY MEMORIZING ONE STRING OF CHARACTERS AND SOME CREDENTIALS. PERSONAL COMPUTERS ARE GROWING CHEAPER AND THE CHANCE TO CONNECT FROM ANYWHERE TO THESE ROOMS IS NOW PALPABLE.
-IT'S THE 90S AND SUPER-THICK NOT-SO-PORTABLE COMPUTERS, AKA LAPTOPS, APPEAR IN THE STORES.
-IT'S THE 00S, COMPUTERS ARE BECOMING MORE COMMON AND GET DISTRIBUTED IN HUMAN INFRASTRUCTURES AS A STANDARD IN MOST FIRST GRADE STATES.
-IT'S 2012, AND THE WORLD IS ABOUT TO END, AGAIN.
ENORMOUS RADIO DEVICES, BORN ALMOST 30 YEARS BEFORE, REFLOURISH

AT THE TIME OF WRITING, THE MAJORITY OF PEOPLE HAVE ONE OR MORE PHONES.

"THESE MACHINES ARE NOT EVEN ON A SCALE WITH HOLE READERS, YET WE USE THE SAME PARADIGM: A FEW REMOTE MACHINES HAVE THE FILES, EVERYBODY CONNECTS DIRECTLY TO THEM THROUGH A SINGLE GATEWAY." (C2 — "CENTRALIZED NETWORK PARADIGM")

#P2PFTW / THE INTERPLANETARY FILE SYSTEM

THE SYSTEM IS SIMILAR TO TORRENTS AND HOW COLLABORATION PLATFORM WORKS. IT HAS AN EXTRA FEATURE: ITS FILES BECOME UNIQUE HASHES GENERATED BY THEIR CONTENT, AVOIDING DUPLICATES. DATA CAN EITHER BE ENCRYPTED WITH A CRYPTOGRAPHIC KEY OR NOT, THEY ARE STILL SECURE FOR MOSTLY NOT SENSITIVE DATA USAGES.
THIS IS A CONTENT-ADDRESSABLE SYSTEM. FILES CAN BE SPLIT INTO MANY NODES, AND YET BE CALLED BY THEIR SINGLE IDENTITIES BECAUSE UNIQUE. HASHES ARE PORTIONS OF A URL THAT, IF SEARCHED ON A BROWSER, WILL SERVE THE FILE. THE STANDARD GATEWAYS ARE HTTPS://IPFS.IO/IPFS/" OR "HTTPS://IPFS.IO/IPNS/" FOR PUBLIC PEERS.
YOU CAN CONFIGURE THEM TO WORK WITH COMMON DOMAINS OR $ENS.

"THE INTERNET OF THINGS IS FORMULATED BY THOSE DEVICES THAT COMMUNICATE INDEPENDENTLY WITH OTHER MACHINES THROUGH THE NETWORK, USUALLY MONITORING AND EXECUTING SIMPLE ACTIONS ON TRIGGERS. IOT AND IPFS CAN LEAD TO THE PRACTICAL APPLICATION OF THE $MEMEX REVISITED" (C2 — "MACHINE LEARNING AT ITS FINEST")

1.#SWARM / CONNECTIONS

SWARM IS THE SERVICE THAT ALLOWS PEERS (LIKE LEECH AND SEEDS FROM TORRENT) TO CHECK THEIR KNOWLEDGE ON WHO HAS WHICH FILES REGULARLY. IT CAN BE BANDWIDTH-HEAVY OR VERY LIGHT, DEPENDING ON HOW FAST YOU WANT YOUR NODE TO HAVE ITS FILES DISTRIBUTED VIA THE COMMON URLS. THERE'S A FEATURE THAT ALLOWS SOME "TRUSTABLE WELL KNOWN, VERIFIABLE PEER" AS A BOOTSTRAP TO FASTEN AND LIGHTEN THIS PROCESS.

"WHAT IF I DON'T WANT TO TRUST ANYONE ON THE INTERNET? ICNES WOULD BE A REMEDY." (C2 — "ANYONE HAS TRUST ISSUES SOMETIMES")

#IPFS / STATIC FILES

DATA SPLIT INTO BLOCKS; EACH ONE IS ~256KB. ANYTIME A FILE GETS ADDED AND SPREAD ACROSS NODES, A CLOCK FOR GARBAGE COLLATION SETS. IF YOU NEVER WANT YOUR DOCUMENT TO GO $504, THE DISTRIBUTED VERSION OF ERROR $404, YOU CAN PIN IT ON YOUR MACHINE, SO IT DOESN'T GET OUT OF THE GATEWAY'S REACH. THE SYSTEM ALLOWS FILES THAT ARE REQUESTED THE MOST BY ANYONE TO STICK FURTHER ON NODES ALLOWING LESS BRIDGING AND FULL BANDWIDTH ON CONNECTIONS. PRIVATE NETWORKS ARE A WAY TO AVOID THE CONSTANT SHARE OF THE ENTIRE SYSTEM ACKNOWLEDGMENT, BUT RATHER JUST A USEFUL SHARE.

THIS CAN BE USED AS A LAYER TO HOST STATIC WEBSITES.

UNDERSTAND

2.#IPLD / DATABASE

FILES ABOVE THE LIMIT FOR BLOCK SIZE, RESULT IN A HASH THAT IS A LINK TO A DIRECTORY-LIKE SERIES OF CHUNKS. IT WORKS AS ONE FILE, BUT IT ALSO OPERATES AS A SERIES OF LINKS, AKA DAG. THERE IS NO LIMIT TO SPACE AND NO RESTRICTION IN FILE TYPOLOGY. YOU CAN ONLY DISPLAY NOT-ENCRYPTED COMMON TYPES BY DEFAULT, AS YOU ACCESS IT DIRECTLY THROUGH A WEB BROWSER, IT ONLY KNOWS A FEW FORMATS.

THIS CAN BE USED AS A LAYER TO HOST DATABASE-LIKE DATA.

3.#IPNS / DYNAMIC FILES

PEER HAS UNIQUE GENERATED IDENTITIES, SIMILAR TO FILES. YOU CAN USE A GENERATED HASH TO PUBLISH MUTABLE-CONTENT ON THE SAME LINK, AS IT CONTAINS A REDIRECT TO THE ACTUAL FILE HASH. YOU CAN CONSIDER IT AS THE CONVENTIONAL DOMAIN NAME SYSTEM, AKA DNS. AS IPFS USES HASHES GENERATED BY CONTENT-AWARENESS, EVEN PEERS CAN DISCOVER WITHOUT SHARING AN IP. RATHER THAN CONNECTING TO A SINGLE ENTITY, YOU TORRENT FROM MANY, STILL UTILIZING A DOMAIN MASK.

THIS CAN BE USED AS A LAYER TO HOST DYNAMIC WEBSITES.

UNDERSTAND

4#PUBSUB / STREAMING

STREAMS ON P2P ARE KNOWN TO BE UNSAFE, SLOW, AND HARD TO CODE. THE IPFS STREAMING PROTOCOL HANDLES CONNECTIONS LIKE A FORUM. YOU ACCESS ONE OR MORE TOPICS BY NAME AND START BROADCASTING DATA AS TONS OF POSTS. THESE CAN BE ENCODED OR ENCRYPTED. MEANING YOU CAN TRANSFER ANYTHING LIKE AUDIO, VIDEO, OR MULTIPLAYER COMPONENTS SECURELY AND MODULARLY. THE DATA SENDER USES SMALL PACKETS SENT AT HIGH SPEED THROUGH EACH OTHER PEER LISTENING ON THAT TOPIC. THE LISTENER COLLECTS THE NEEDED PACKAGES FROM ANY PEER THAT HAS IT.

THIS CAN BE USED AS A LAYER FOR REAL-TIME COMMUNICATION.

5.#PRACTICE / EXAMPLES

BOB HAS A 4K VIDEO AND A DOMAIN NAME. HE WANTS TO HOST THE VIDEO ON HIS RASPBERRY PI FOREVER. HE THEN WANTS TO SHARE IT WITH ANYONE HAVING A SIMPLE "DOMAIN/LINK."
BOB INSTALLS AN OS AND IPFS ON THE RASPBERRY, HE UPLOADS THE FILE TO THE IPFS NETWORK AND GETS A HASH IN RESPONSE.
BOB PUBLISHES THE FILE HASH THROUGH IPNS CALLING IT "4KVIDEO," WHICH GIVES HIM A MACHINEHASH AND A REDIRECTHASH THAT LINKS TO THE REDIRECT FILE. THE DOMAIN NAME WILL POINT AT SOMETHING LIKE "HTTPS://IPFS.IO/IPNS/MACHINEHASH/REDIRECTHASH"; THE DATA IS STILL AT "HTTPS://IPFS.IO/IPFS/ORIGINALHASH," BUT ACTUALLY, IT IS TORRENT-ABLE DIRECTLY BY "HTTPS://WWW.BOBWEBSITE.COM/4KVIDEO".

BOB CAN UPLOAD WHATEVER HIS RASPBERRY PI'S HARD DRIVE CAN HOLD.

WHAT HAPPENS IF BOB DOESN'T PIN THE FILE?
THE FILE GETS DESTROYED AFTER A CERTAIN AMOUNT OF TIME, GIVEN BY ITS ACCESSES. THE RESULT ON BOB'S WEBSITE WOULD BE TO LOAD FOREVER. THE BROWSER IS LOOKING INTO EACH IPFS NODE THAT KNEW BOB'S RASP TO FIND THE FILE THAT WAS GARBAGE COLLECTED.

WHAT HAPPENS IF HE DOES PIN THE FILE?
THE FILE WILL BE FOREVER ACCESSIBLE AS LONG AS HE DOESN'T DISCONNECT THE RASP FOR TOO LONG WHILE NO ONE OPENS THE VIDEO LINK. ACCESS IT FROM ANYWHERE IN THE WORLD WITHOUT THE CHANCE OF LAG GIVEN BY THE NUMBER OF CONNECTIONS. INDEED, THE MORE IT'S USED, THE BETTER IT WORKS.

UNDERSTAND

#C2_COMPONENTS / TOOLS TO STORE BIG CUSTOM DATA

EACH TYPE OF FILE YOU CAN THINK OF IS SERIALIZED INTO DESCRIPTORS. THEY CAN BE RECREATED BY ANY DEVICE THAT KNOWS HOW TO DESERIALIZE AND DISPLAY THEM. WITH DESCRIPTORS, A RAW 4K IMAGE OF ~60MB GETS CLOSER TO ~5MB WITHOUT ANY QUALITY LOSS.

WE STORE MANY DAGS AS DESCRIPTORS CONTAINING LINKS TO OTHER DESCRIPTORS.
DAGS MAY CONTAIN TEXTS, 3D MODELS, IMAGES, AUDIO, LOGIC-COMPONENTS WITH PARAMETERS, AND SO ON.

WE PICKED A MODULAR APPROACH TO REDUCE DATA USAGE, BOOST PERFORMANCE, AND ALLOW USERS TO COMBINE THESE MODULES WITHOUT ANY TECHNICAL KNOWLEDGE.

WE USE THE IPFS KEYCHAIN SYSTEM TO ENCRYPT ALL FILES WITH A SHARED KEY. KEYS CAN BE CREATED AND EXPORTED WITH A SIMPLE PASSWORD WITHOUT EXPOSING DATA TO RISK. YOU CAN EITHER HAVE YOUR DATA SET TO PRIVATE OR PUBLIC, MEANING THAT ITS KEY WILL BE THE SHARED ONE.
YOU CAN DECRYPT, EXPORT, AND USE FILES AMONG ANY THIRD-PARTY SOFTWARE IF ITS LICENSE IS SET TO "EDITABLE".

WE ALSO USE IPFS AS A PRIVATE NETWORK SO THAT OUR CLIENTS DON'T GET DRAINED IN THE LONG RUN. WE SET A LITTLE SPACE ON OUR MASTER NODES TO BE KNOWN BY THE WHOLE IPFS ECOSYSTEM, ALLOWING PUBLIC CONTENT TO BE DISPLAYED ON ANY BROWSER.

USECASE

"DON'T UPLOAD STUFF YOU MIGHT REGRET. IT CAN BE BURNED OR HIDDEN, BUT IT CAN'T BE DELETED. ANYONE ABLE TO INSPECT THIS STUFF WILL HAVE A CHANCE TO COMPROMISE YOUR ACCOUNT IN THE LONG RUN." (C2 — MESSING UP YOUR TIME ADVENTURE)

YOU CAN USE THE IPFS STREAMING SYSTEM WITH MANY PURPOSES THROUGH OUR DAPPS:
SHARE REAL-TIME VIDEO CONTENT THAT CAN EITHER BE CAPTURED IN-UNIVERSE OR FROM YOUR DEVICE SCREEN.
SHARE VOICE COMMUNICATION ON CHANNELS WITH A CUSTOMIZABLE PANEL FOR STREAMERS' SAKE.
REMOTE PLAY ON ICNES, CONTROL THE DEVICE FROM A DISTANCE. USE IT FOR TECHNICAL ASSISTANCE, LOW PERFORMING DEVICES, OR DEMONSTRATIONS.
MMODN: MASSIVELY MULTIPLAYER ONLINE DECENTRALIZED NETWORK. WE USE A TORRENT-LIKE STREAMING TECHNIQUE TO OPTIMIZE COMMON USAGES AND AVOID ANY SINGLE POINT OF FAILURE.

#C2_PRIVACY / ANYTHING CAN BE SECRET BUT...

THE ONLY EXTRA DATA WE KEEP TRACK OF ARE: VERSIONING OF THE FILES AND WHO OWNED IT. USERS CAN KNOW WHERE ITEMS COME FROM, ALLOWING THEM TO TRACK, REFUSE, AND EVENTUALLY SPREAD KNOWLEDGE AGAINST FRAUDULENT MATERIAL WITH THE EASE OF A VOTE.

USERS CAN USE THEIR SECRECY AGAINST THE SYSTEM IF THE COMMUNITY HAS THE TOOLS TO ACKNOWLEDGE IT.

"WITH TIME AND EFFORT, WHOEVER MOVES BY THE HAND OF EVIL, WILL HAVE NO UN-EDUCATED NAIVE VICTIMS TO ABUSE." (C2 — "A BIG LAP FOR SMALL MINDS")
